CEMCC Internal Report 2024-01 v1.1

Categorization-Tiering of C2M2 Maturity Model towards AIM Triad

Student in practice: Gemita Escalona Troncoso
Advisor: Julio Fenner Lopez

This publication is available free of charge from:
https://doi.org/10.5281/zenodo.13946146

UNIVERSIDAD DE LA FRONTERA

CEMCC Internal Report 2024-01 v1.1

Categorization-Tiering of C2M2 Maturity Model towards AIM Triad

Student in Practice:
Gemita Escalona Troncoso
Departamento de Ingeniería Civil Matemática
Facultad de Ingeniería y Ciencias
Universidad de La Frontera

Advisor:
Prf. Dr. Julio Fenner Lopez
Cibersecurity WorkGroup
Centro de Modelación y Computación Científica CEMCC
Dertamento Cs. de la Computación e Informática (DCI)
Facultad de Ingeniería y Ciencias
Universidad de La Frontera

This publication is available free of charge from:
https://doi.org/10.5281/zenodo.13946146

October, 2024

Abstract

This report contains a classification for the questions outlined in the C2M2 maturity model, aligning them with the methodology proposed in the AIM triad for future application [1]. In accordance with the sequence of the C2M2 model, it is suggested to categorize each specific objective according to the framework that fits best the AIM triad, accompanied by its respective rationale.

Key words

Maturity Model, Cibersecurity, C2M2, AIM-Triad

Table of Contents

0 AIM Triad **1**
- 0.1 CULTURE AND SOCIETY 1
- 0.2 SITUATIONAL AWARENESS 1
- 0.3 STANDARDS AND TECHNOLOGY 2
- 0.4 ARCHITECTURE 2
- 0.5 THREAT AND VULNERABILITY 2
- 0.6 PROGRAM 3
- 0.7 WORKFORCE 3
- 0.8 ASSET, CHANGE AND CONFIGURATION 3
- 0.9 LEGAL AND REGULATORY FRAMEWORK 4
- 0.10 INCIDENT DETECTION AND RESPONSE 4
- 0.11 POLICY AND STRATEGY 5
- 0.12 KNOWLEDGE AND CAPABILITIES 5
- 0.13 RISK 5

1 Asset, Change, and Configuration Management - 36 questions **6**
- 1.1 IT and OT Asset Inventory 6
- 1.2 Information Asset Inventory 11
- 1.3 IT and OT Asset Configurations 15
- 1.4 Changes to IT and OT Assets 17
- 1.5 Management Activities 20

2 Threat and Vulnerability Management - 30 questions **24**
- 2.1 Reduce Cybersecurity Vulnerabilities 24
- 2.2 Respond to Threats and Share Threat Information 29
- 2.3 Management Activities 32

3 Risk Management - 39 questions **36**
- 3.1 Establish and Maintain Cyber Risk Management Strategy and Program 36
- 3.2 Identify Cyber Risk 39
- 3.3 Analyze Cyber Risk 43
- 3.4 Respond to Cyber Risk 46
- 3.5 Management Activities 48

4 Identity and Access Management - 35 questions **51**
4.1 Establish Identities and Manage Authentication 51
4.2 Control Logical Access 56
4.3 Control Physical Access 62
4.4 Management Activities 66

5 Situational Awareness . 28 questions **70**
5.1 Perform Logging 70
5.2 Perform Monitoring 74
5.3 Establish and Maintain Situational Awareness 78
5.4 Management Activities 82

6 Event and Incident Response, Continuity of Operations - 49 questions **86**
6.1 Detect Cybersecurity Events 86
6.2 Analyze Cybersecurity Events and Declare Incidents 89
6.3 Respond to Cybersecurity Incidents 93
6.4 Address Cybersecurity in Continuity of Operations 99
6.5 Management Activities 107

7 Third-Party Risk Management - 25 questions **112**
7.1 Identify and Prioritize Third Parties 112
7.2 Manage Third-Party Risk 115
7.3 Management Activities 122

8 Workforce Management - 32 questions **126**
8.1 Implement Workforce Controls 126
8.2 Increase Cybersecurity Awareness 130
8.3 Assign Cybersecurity Responsibilities 133
8.4 Develop Cybersecurity Workforce 135
8.5 Management Activities 138

9 Cybersecurity Architecture - 58 questions **142**
9.1 Establish and Maintain Cybersecurity Architecture Strategy and Program 142
9.2 Implement Network Protections as an Element of the Cybersecurity Architecture 147
9.3 Implement IT and OT Asset Security as an Element of the Cybersecurity Architecture 152
9.4 Implement Software Security as an Element of the Cybersecurity Architecture 157
9.5 Implement Data Security as an Element of the Cybersecurity Architecture 160
9.6 Management Activities 164

10 Cybersecurity Program Management - 24 questions **167**
10.1 Establish Cybersecurity Program Strategy 168
10.2 Establish and Maintain Cybersecurity Program 172
10.3 Management Activities 176

References **179**

List of Tables

Table 1 CULTURE AND SOCIETY 1
Table 2 SITUATIONAL AWARENESS 1

Table 3 STANDARDS AND TECHNOLOGY 2
Table 4 ARCHITECTURE 2
Table 5 THREAT AND VULNERABILITY 2
Table 6 PROGRAM 3
Table 7 WORKFORCE 3
Table 8 ASSET, CHANGE AND CONFIGURATION 4
Table 9 LEGAL AND REGULATORY FRAMEWORK 4
Table 10 INCIDENT DETECTION AND RESPONSE 4
Table 11 POLICY AND STRATEGY 5
Table 12 KNOWLEDGE AND CAPABILITIES 5
Table 13 RISK 6

Glossary

AIM-Triad

The AIM Triad, as proposed in [1], is a strategic framework designed to guide public institutions in improving their information security maturity. It encompasses three critical components: Awareness, Infrastructure, and Management. This triad serves as a practical guide for organizations to assess their current security practices and identify areas for improvement. By prioritizing these domains, institutions can create a structured approach to enhance their cybersecurity posture, ensuring that they effectively manage sensitive information and comply with regulatory requirements. The AIM Triad not only facilitates the implementation of best practices but also helps organizations navigate the complexities of adopting multiple information security maturity models, ultimately leading to a more robust and resilient security framework.

C2M2 Maturity Model

The Cybersecurity Capability Maturity Model (C2M2), as proposed in [2], is a free tool to help organizations evaluate their cybersecurity capabilities and optimize security investments. It uses a set of industry-vetted cybersecurity practices focused on both information technology (IT) and operations technology (OT) assets and environments. The model contains more than 350 cybersecurity practices, which are grouped by objective into 10 logical domains. Each practice is assigned a maturity indicator level (MIL) that indicates the progression of practices within a domain, which contains a structured set of cybersecurity practices focused on a specific subject area. For example, the Risk Management domain is a group of practices that an organization can perform to establish and mature its cyber risk management capability.

0. AIM Triad

The AIM Triad is a comprehensive cybersecurity framework designed to enhance an organization's security posture by focusing on three key aspects: Assets, Information, and Management. This triad approach provides a holistic view of cybersecurity, ensuring that all critical elements of an organization's digital infrastructure are adequately protected. The framework is structured around 13 domains, each addressing specific areas of cybersecurity concern. These domains cover a wide range of topics, from asset management and threat detection to risk assessment and incident response. By addressing these 13 domains, organizations can develop a robust and well-rounded cybersecurity strategy that not only protects their assets and information but also ensures effective management of their security processes. The AIM Triad's 13-domain structure allows for a systematic and thorough approach to cybersecurity, enabling organizations to identify vulnerabilities, implement appropriate controls, and continuously improve their security posture in an ever-evolving threat landscape. The 13 domains of the AIM Triad are carefully designed to cover all aspects of cybersecurity, providing a comprehensive framework for organizations to assess and improve their security measures. Each domain focuses on a specific area of cybersecurity, ensuring that organizations address all critical aspects of their security posture. By implementing the AIM Triad and its 13 domains, organizations can create a more resilient and secure environment, better equipped to face the challenges of today's complex cybersecurity landscape.

0.1 CULTURE AND SOCIETY

Refers to the culture and values of an organization and its impact on cyber security. It is about how an organization promotes and fosters cyber security awareness among its employees, suppliers, and customer.
The following practices proposed in the C2M2 maturity model are categorizable within the present category of the AIM Triad:

Table 1. CULTURE AND SOCIETY

ASSET	THREAT	RISK	ACCESS	SITUATION
	1i, 2h	1f, 2c, 3e		2b
RESPONSE	**THIRD-PARTIES**	**WORKFORCE**	**ARCHITECTURE**	**PROGRAM**
3f, 3j, 3k	2d, 3a	1e, 1g, 2a, 2b, 2g	1e	2c

0.2 SITUATIONAL AWARENESS

Ability of an organization to detect, analyze and understand cybersecurity risks and threats in real-time and at different levels of the organization.
The following practices proposed in the C2M2 maturity model are categorizable within the present category of the AIM Triad:

Table 2. SITUATIONAL AWARENESS

ASSET	THREAT	RISK	ACCESS	SITUATION
1a, 2a, 4a	2a, 2b, 2e, 2f	1d, 2g, 2m, 3g	2i	2a to 2i, 3a to 3g 4a to 4f
RESPONSE	**THIRD-PARTIES**	**WORKFORCE**	**ARCHITECTURE**	**PROGRAM**
1d, 1f, 2g, 2i, 3l		2f	1k	

0.3 STANDARDS AND TECHNOLOGY

Use of established cybersecurity standards and technologies to protect an organization's systems and data.
The following practices proposed in the C2M2 maturity model are categorizable within the present category of the AIM Triad:

Table 3. STANDARDS AND TECHNOLOGY

ASSET	THREAT	RISK	ACCESS	SITUATION
1e, 1h, 2e, 2h 3c, 3e, 4e	1h, 1k, 2k	2b, 3b, 4b, 4c	1a, 1b, 1d, 1e 1g to 1j, 2a to 2i	1c, 1d to 1f, 2e 2f, 3b, 3f, 4c
RESPONSE	**THIRD-PARTIES**	**WORKFORCE**	**ARCHITECTURE**	**PROGRAM**
2f, 4b, 4i, 4j	2b, 2c, 2h, 2j		1g, 2a, 2b, 2d, 2e, 2g 2h, 3b, 3m, 4a, 4b, 4e 4g, 4h, 5a, 5d, 5e	1f, 2j

0.4 ARCHITECTURE

Refers to designing and implementing a secure and robust technology infrastructure to protect an organization's assets and data. Security architecture ranges from network and system protection to data and application security.
The following practices proposed in the C2M2 maturity model are categorizable within the present category of the AIM Triad:

Table 4. ARCHITECTURE

ASSET	THREAT	RISK	ACCESS	SITUATION
		2l	2d, 3a, 3c	1e, 2d, 3g
RESPONSE	**THIRD-PARTIES**	**WORKFORCE**	**ARCHITECTURE**	**PROGRAM**
4c, 4j to 4l	2h		1a to 1k, 2a, 2b, 2d to 2f 2h to 2l, 3a, 3c, 3d, 3f, 3j, 3k 4b, 4d to 4f, 5a to 5h, 6b to 6f	

0.5 THREAT AND VULNERABILITY

An organization's ability to identify, assess and mitigate the security risks associated with the threats and vulnerabilities it faces.
The following practices proposed in the C2M2 maturity model are categorizable within the present category of the AIM Triad:

Table 5. THREAT AND VULNERABILITY

ASSET	THREAT	RISK	ACCESS	SITUATION
1b, 1d, 2b, 2d, 4d, 4h	1a to 1c, 1e to 1g, 1j 2c, 2e, 2g, 2i, 3a to 3f	2a, 2h to 2j, 3d	1c to 1e, 1g to 1j 2a, 2b, 3e, 3f, 3h to 3j	1b, 1c, 2d, 2f 2i, 3b, 3f
RESPONSE	**THIRD-PARTIES**	**WORKFORCE**	**ARCHITECTURE**	**PROGRAM**
1d, 1e, 2i 4k, 4m, 4p	2e, 2g, 2h, 2j, 2k to 2m	1b, 2c	1i, 1j, 2f, 2g, 5f	

0.6 PROGRAM

Refers to an organization's cybersecurity strategy and planning. An effective cyber security program should be aligned with the organization's business objectives, identify critical assets and associated risks, and establish policies and procedures for cyber security management. It should also include the designation of a cybersecurity team and the assignment of clear roles and responsibilities.
The following practices proposed in the C2M2 maturity model are categorizable within the present category of the AIM Triad:

Table 6. PROGRAM

ASSET	THREAT	RISK	ACCESS	SITUATION
5a, 5b, 5d, 5f	3c, 3d	1a to 1f, 1h, 2f, 5b	4a to 4f	
RESPONSE	**THIRD-PARTIES**	**WORKFORCE**	**ARCHITECTURE**	**PROGRAM**
3a, 3e to 3g, 4a 4d, 4e, 4h, 4i 4o, 4p, 5b, 5c	1a, 1b, 1d to 1f 2a to 2c 3a to 3d, 3f	1d, 3a to 3e, 5b	1b, 1h, 6b, 6f	1a to 1e, 1h, 2a 2b, 2e to 2g 3a, 3b, 3f

0.7 WORKFORCE

The set of employees and contractors of an organization who have access to systems and data critical to the operation of the business. This includes workers who handle information technology and security and employees who do not work directly in those areas but still have access to confidential systems and data.
The following practices proposed in the C2M2 maturity model are categorizable within the present category of the AIM Triad:

Table 7. WORKFORCE

ASSET	THREAT	RISK	ACCESS	SITUATION
5b, 5d, 5e	3b, 3e	5b, 5d, 5e	1a to 1c, 1f, 3b 3d to 3g, 4b, 4d, 4e	4b, 4d
RESPONSE	**THIRD-PARTIES**	**WORKFORCE**	**ARCHITECTURE**	**PROGRAM**
3a, 3e, 5b, 5d, 5e	3b, 3d, 3e	1a to 1c, 1f, 2d, 2e 2g, 3a to 3c, 3f, 4a 4c, 4d, 4f, 5a to 5f	6d	3d

0.8 ASSET, CHANGE AND CONFIGURATION

Refers to the management and control of an organization's information technology assets, as well as the management of changes and configurations of these assets. Assets include all systems, applications, data, and network components critical to an organization's business. Asset management involves the identification, classification, and prioritization of assets, as well as the ongoing monitoring and maintenance of assets. In addition, asset management also includes the safe disposal of assets at the end of their life cycle.
The following practices proposed in the C2M2 maturity model are categorizable within the present category of the AIM Triad:

Table 8. ASSET, CHANGE AND CONFIGURATION

ASSET	THREAT	RISK	ACCESS	SITUATION
1a to 1h, 2a, 2c 2e to 2h, 3a to 3e 4a, 4b, 4d, 4f to 4i 5a to 5c, 5e, 5f	1h	2h	1a, 1b, 1e, 1f 2e to 2h, 3a to 3j	1a to 1f, 2c, 2g, 3g
RESPONSE	**THIRD-PARTIES**	**WORKFORCE**	**ARCHITECTURE**	**PROGRAM**
2f, 4b, 4c, 4f 4g, 4i, 4l, 4p	1a to 1f, 2f 2i, 2k to 2m	1b, 1d	1c, 2c, 2k, 3a, 3b 3d, 3e, 3g to 3i, 3k 3l, 4c, 5b, 5c	

0.9 LEGAL AND REGULATORY FRAMEWORK

Refers to laws and regulations governing information security and data privacy in a particular jurisdiction. These laws and regulations may come from various sources, such as government, industry, or the private sector, and compliance with them is mandatory for organizations operating in that jurisdiction.
The following practices proposed in the C2M2 maturity model are categorizable within the present category of the AIM Triad:

Table 9. LEGAL AND REGULATORY FRAMEWORK

ASSET	THREAT	RISK	ACCESS	SITUATION
		2k	4c	3d
RESPONSE	**THIRD-PARTIES**	**WORKFORCE**	**ARCHITECTURE**	**PROGRAM**
2g, 3d, 3j	2a, 2d to 2g	1a		

0.10 INCIDENT DETECTION AND RESPONSE

An organization's ability to detect, respond to, and recover from cybersecurity incidents. This includes early identification of potential security threats, rapid and effective response to incidents, and recovery of affected systems and data.
The following practices proposed in the C2M2 maturity model are categorizable within the present category of the AIM Triad:

Table 10. INCIDENT DETECTION AND RESPONSE

ASSET	THREAT	RISK	ACCESS	SITUATION
4f, 4i	1d, 1l, 1m 2d, 2j		2i, 3i, 3j	1a, 1b, 1d to 1f, 2a 2b, 2e, 2i, 3c, 3d
RESPONSE	**THIRD-PARTIES**	**WORKFORCE**	**ARCHITECTURE**	**PROGRAM**
1a to 1f, 2a to 2i 3b to 3l, 4a 4d to 4i, 4l to 4o 5a to 5f				

0.11 POLICY AND STRATEGY

Refers to an organization's ability to establish clear and effective policies and strategies for information security and cybersecurity management. This includes defining security objectives, identifying risks and threats, and creating policies and procedures to manage and mitigate these risks. The importance of "Policy and Strategy" in a CMM is that well-defined and communicated policies and strategies are the foundation for effective information security and cybersecurity management.
The following practices proposed in the C2M2 maturity model are categorizable within the present category of the AIM Triad:

Table 11. POLICY AND STRATEGY

ASSET	THREAT	RISK	ACCESS	SITUATION
2c, 4c, 5c	3a to 3c, 3f	1a, 1b, 1e, 1g 1h, 4d, 5a, 5c	1a to 1d, 1f to 1j 2a to 2h, 3a to 3j 4a to 4d, 4f	2c, 2i, 3a to 3d 4a to 4d, 4f
RESPONSE	**THIRD-PARTIES**	**WORKFORCE**	**ARCHITECTURE**	**PROGRAM**
1a to 1c, 2a to 2e, 2h 3b, 3d to 3h, 3l, 4a 4h, 4n, 5a, 5c, 5d, 5f	1c, 3a, 3c, 3f	1e, 5a, 5c, 5d, 5f	1a, 1d, 1f, 3c, 6a, 6c	2d, 2h, 3c

0.12 KNOWLEDGE AND CAPABILITIES

Refers to an organization's ability to have a thorough understanding of information security and cybersecurity and to develop and maintain the skills and capabilities necessary to protect the organization's systems and data. The importance of "Knowledge and capabilities" in a CMM lies in the fact that an organization can only be as secure as its personnel's cybersecurity skills and knowledge.
The following practices proposed in the C2M2 maturity model are categorizable within the present category of the AIM Triad:

Table 12. KNOWLEDGE AND CAPABILITIES

ASSET	THREAT	RISK	ACCESS	SITUATION
5d, 5e	3a to 3e	5a, 5e	4a, 4b, 4d, 4e	3c to 3e, 4a, 4e
RESPONSE	**THIRD-PARTIES**	**WORKFORCE**	**ARCHITECTURE**	**PROGRAM**
1a, 2b, 3a, 3d, 3g to 3i 3k, 3o, 5a, 5b, 5e	3e	1e, 4a to 4c, 4e, 4f, 5e	6b, 6d, 6e	3e

0.13 RISK

Refers to an organization's ability to identify, assess and manage the risks associated with information security and cybersecurity. The importance of "Risk" in a CMM is that risk management is essential to ensure that the organization can adequately protect its information assets and minimize the impact of potential security breaches.
The following practices proposed in the C2M2 maturity model are categorizable within the present category of the AIM Triad:

Table 13. RISK

ASSET	THREAT	RISK	ACCESS	SITUATION
1b to 1d, 1f 1g, 2b, 2d 2f, 2g, 5f	1h, 3b, 3f	1c, 1g, 2d, 2e 2h, 3a, 3c, 3f 4a, 4e, 5a, 5f	1d to 1j 2c to 2i 3a to 3h, 4f	1f, 2a, 2g. 2h, 4f
RESPONSE	**THIRD-PARTIES**	**WORKFORCE**	**ARCHITECTURE**	**PROGRAM**
1b, 1c, 1e, 1f 2a to 2e, 2h, 3b 3i, 3l, 4b to 4g 4m to 4p, 5a 5c, 5e, 5f	1a to 1f 2a to 2g, 2i	1c, 1d, 4b	1i, 1j, 2c, 4h 5c to 5e	

1. Asset, Change, and Configuration Management - 36 questions

As presented on the platform, its purpose is: Manage the organization's information technology (IT) and operations technology (OT) assets, including both hardware and software, commensurate with the risk to critical infrastructure and organizational objectives.

The Asset, Change, and Configuration Management (ASSET) domain comprises five objectives:

1. Manage IT and OT Asset Inventory
2. Manage Information Asset Inventory
3. Manage IT and OT Asset Configuration
4. Manage Changes to IT and OT Assets
5. Management Activities for the ASSET domain

1.1 IT and OT Asset Inventory

ASSET-1a

IT and OT assets that are important to the delivery of the function are inventoried, at least in an ad hoc manner. Assets derive their value and importance through their association with the aspects of the function's operations that they support. Identifying and inventorying high-value IT and OT assets helps enable selection and application of appropriate controls. At MIL1, the inventory may be produced in an ad hoc manner. Organizations should consider the different kinds of IT and OT assets that may be within the scope of the self-evaluation, such as:

· virtualized assets

· regulated assets

· assets managed by a third party

· software

· bring your own device (BYOD) assets

- cloud assets (public, hybrid, or private service, software as a service, platform as a service, and infrastructure as a service, etc.)
- mobile assets
- field assets
- assets connected through different networks or communications technologies (e.g., telephone modem, cellular)
- network and communications assets
- backup, spare, and redundant assets, including dormant virtualized assets
- non-operational assets, assets undergoing repair, assets undergoing maintenance
- assets reliant on specific infrastructure such as wireless networks, positioning navigation and timing services, and the Global Position System
- assets that may be considered to be part of the Internet of things or industrial Internet of things
- assets that have the potential to be untracked, unclaimed, or otherwise overlooked, such as legacy assets, communications equipment, and assets supporting multiple groups

An inventory is not meant to imply that a single list is required; multiple repositories, documents, or systems may be used to accomplish this practice. Where appropriate, however, organizations should consider whether inventories may be consolidated to avoid potential risks related to managing multiple repositories.

AIM-Categorization-Tiering: The statement emphasizes the identification and inventory of IT and OT assets, which directly relates to **ASSET, CHANGE AND CONFIGURATION** management practices. This categorization ensures that all critical assets are accounted for, helping in the management and control of these resources. Additionally, understanding the importance of these assets to the function's operations requires a level of **SITUATIONAL AWARENESS**, allowing the organization to detect and understand the significance of each asset in real-time and at different organizational levels.

ASSET-1b

The IT and OT asset inventory includes assets within the function that may be leveraged to achieve a threat objective.
Assets within the function are those that the organization considers as the potential target of the tactics or goals of a threat actor. When considering assets that should be given this designation it is helpful to consider assets that a threat actor might use to accomplish their end-goal, such as

- public-facing assets that may serve as an initial access point
- individual assets that would allow lateral movement within an organization's network
- assets with administrative rights that would enable privilege escalation

Note that identification of this set of assets should be based on an assessment of risk and could be informed by an understanding of the organization's exposure to threats and vulnerabilities, to the extent that these are known.
A threat objective describes the potential action or tactic of a threat actor to achieve a particular outcome or goal by leveraging the assets within the function. The outcome or goal of the threat objective is to negatively impact the organization. Threat objective examples may include data manipulation, IP Theft, damage to property, denial of control, loss of safety, or operational outage.
A threat profile for an asset may include one or more threat objectives which may change over time or in different situations.
Threat objectives are contextual to the organization and the assets within the function. For example, an organization that does not process confidential data may not be concerned about data theft but may be very concerned about an incident that causes an operational outage. Additionally, threat actors may leverage multiple tactics or techniques like those defined in the MITRE ATT&CK frameworks (for Enterprise or Industrial Control Systems) to achieve their goals.
Knowledge of potential threat actors, their threat objectives, and the tools and tactics they may use to achieve their goals should inform the identification of assets within the function.

AIM-Categorization-Tiering: This statement focuses on identifying assets that could be targeted by threat actors, which falls under the **THREAT AND VULNERABILITY** category. The emphasis on maintaining an inventory also aligns with **ASSET, CHANGE AND CONFIGURATION** management. Furthermore, assessing these assets based on the potential threat objectives connects to **RISK** management, as it involves understanding and mitigating the risks associated with these vulnerabilities.

ASSET-1c

Inventoried IT and OT assets are prioritized based on defined criteria that include importance to the delivery of the function.
Prioritization of assets is important for many cybersecurity and operational activities, such as incident response, risk management, threat management, and cybersecurity architecture planning. There are multiple approaches for asset prioritization: forced ranking (sequential list), tiered ranking (e.g., all assets dealing with the flow of gas are tier 1, assets related to efficiency and monitoring are tier 2, and non-critical functions such as public relations and marketing are tier 3). Tiers should be based on defined criteria, such as importance of the asset to the function (e.g., safety, criticality of the asset to the delivery of the function, scarcity of the asset, how dependent other assets are on this asset) or the sensitivity of the data stored or processed by the asset. Prioritizations should be documented and ideally be agreed on by all involved stakeholders. They also should be communicated throughout the organization for use in incident response, risk management, and other relevant activities. As an example, virtualized assets may present increased risk due to issues such as asset sprawl and their unique characteristics (ease of capturing snapshots and storage of dormant virtual machines as files) and thus may pose higher risk to the function. Whatever approach is used, the importance of the asset to the delivery of the function should be one of the prioritization criteria used.

AIM-Categorization-Tiering: Prioritizing IT and OT assets based on their importance to the function is a key aspect of **ASSET, CHANGE AND CONFIGURATION** management. This process ensures that critical assets receive the necessary attention and resources. Additionally, this prioritization is crucial for **RISK** management, as it helps in identifying and addressing the most significant risks associated with the function's critical assets.

ASSET-1d

Prioritization criteria include consideration of the degree to which an asset within the function may be leveraged to achieve a threat objective.
The possibility of an asset being leveraged to achieve a threat objective is added to the criteria for prioritizing IT and OT assets. It is important to consider that a threat actor may have multiple objectives and that those objectives may change over time or in different situations. Including additional criteria beyond those that are used for assets that are important to the delivery of the function will enable a more comprehensive prioritization of the risks to, and impacts associated with, IT and OT assets.

AIM-Categorization-Tiering: Incorporating threat objectives into the prioritization criteria ties directly to **THREAT AND VULNERABILITY** management, as it helps identify assets that could be exploited by threat actors. This approach also aligns with **RISK** management, ensuring that assets posing higher threats are prioritized accordingly. Additionally, this falls under **ASSET, CHANGE AND CONFIGURATION** management, as it involves evaluating and managing assets based on their potential to be leveraged for malicious purposes.

ASSET-1e

The IT and OT inventory includes attributes that support cybersecurity activities (for example, location, asset priority, asset owner, operating system and firmware versions).
Inventory attributes are details about assets that are included in asset inventories to enable management and consistent use of the assets. Including necessary information about assets to support cybersecurity program activities helps ensure that that information is available during periods of operational stress and does not have to be collected while in a state of crisis. For example, incident responders will be able to easily identify the priority, criticality, and location of machines that are affected by a bricking event and have to be replaced. Also, inventory attributes can be used to indicate aspects of assets that may require special attention or treatment, such as systems that use artificial intelligence or machine learning. Examples of potential inventory attributes include physical locations, network locations, importance to delivery of the function, impact if breached, end of life dates, end of support dates, operating system, firmware, versions.

AIM-Categorization-Tiering: The detailed information required in asset inventories, such as location, priority, and operating system versions, supports cybersecurity activities and falls under **ASSET, CHANGE AND CONFIGURATION** management. This comprehensive inventory aids in effective asset management. Furthermore, including specific attributes reflects adherence to cybersecurity **STANDARDS AND TECHNOLOGY**, ensuring that the inventory supports consistent and secure management practices.

ASSET-1f

The IT and OT asset inventory is complete (the inventory includes all assets within the function).
This practice expands the inventory scope of ASSET-1a. Any IT and OT asset that is related to the delivery of the function should be identified and inventoried, along with its attributes. The relationship of assets to business functions should also be included to enable prioritization and development of protection and sustainment strategies. The implementation of the inventory should be proportional to the organization's size, complexity, and risk. For example, for a small, low-complexity firm, a simple spreadsheet may be used for the inventory. For larger, more complex firms, more sophisticated methods such as dedicated asset inventory application are appropriate.

Organizations may consider implementing tools for identifying what devices are connected to networks and identifying new unexpected connections.
Organizations should consider the different kinds of IT and OT assets that may be within the scope of the self-evaluation, such as:

- virtualized assets
- regulated assets
- assets managed by a third party
- bring your own device (BYOD) assets
- cloud assets (public, hybrid, or private service, software as a service, platform as a service, and infrastructure as a service, etc).
- mobile assets
- field assets
- backup, spare, and redundant assets, including dormant virtualized assets
- assets reliant on specific infrastructure such as wireless networks, positioning navigation and timing services, and the Global Position System
- assets that may be considered to be part of the Internet of Things or Industrial Internet of Things

Inventory refers to a complete listing and is not meant to imply that a single list is required; multiple repositories, documents, or systems may be used to accomplish this practice. Where appropriate, however, organizations should consider whether inventories may be consolidated to avoid potential risks related to managing multiple repositories. Asset discovery technologies are increasing in capability and availability and may be leveraged to accomplish this practice.

AIM-Categorization-Tiering: Ensuring a complete inventory of IT and OT assets is fundamental to **ASSET, CHANGE AND CONFIGURATION** management. This comprehensive approach ensures that all assets related to the delivery of the function are identified and managed. Additionally, having a complete inventory aids in **RISK** management by providing a full view of the assets, which is essential for assessing and mitigating risks effectively.

ASSET-1g

The IT and OT asset inventory is current, that is, it is updated periodically and according to defined triggers, such as system changes.
The inventory of assets and significant components should be updated and maintained as assets change throughout their lifecycle to ensure the inventory is complete and accurate. Ensuring that the asset inventory is current might involve change management procedures that require inventory updates any time assets are swapped out or significantly altered. The organization might also conduct inventory reviews, both periodically (such as quarterly or yearly) and based on events (such as changes in organizational structure, major changes in technology infrastructure, and the acquisition and consolidation of another business). Organizations may consider implementing

tools that may enable automated asset discovery and provide a more real-time understanding of inventories.

AIM-Categorization-Tiering: Maintaining an up-to-date inventory of IT and OT assets is crucial for effective **ASSET, CHANGE AND CONFIGURATION** management. Regular updates and defined triggers ensure that the inventory accurately reflects the current state of the assets. This practice is also vital for **RISK** management, as it ensures that any changes in the asset inventory are accounted for, helping to identify and address new risks promptly.

ASSET-1h

Data is destroyed or securely removed from IT and OT assets prior to redeployment and at end of life.
Data is permanently removed (that is, deleted in a way that makes data recovery impossible) from IT assets (computers, scanners, copiers, printers, etc.) and OT assets before they are reused or released for disposal. Selection of data removal and destruction techniques should be commensurate with the organization's cybersecurity requirements. Data removal techniques, including clearing, purging, cryptographic erase, de-identification of personally identifiable information, and destruction, prevent the disclosure of information to unauthorized individuals when such media is reused. Destruction of data might also be achieved through destruction of the media on which it is stored (such as physical destruction of a hard drive). Assets such as mobile devices that are more likely to change location or ownership may require additional activities to ensure data is not accessed by unauthorized individuals. This may include full disk encryption of laptops or remote data removal for mobile devices. Additionally, consider assets that may be out of the direct control of the organization for maintenance, dormant virtual machines, virtual machine backups, and virtual machine snapshots, which may include sensitive data and should be destroyed when no longer needed.

AIM-Categorization-Tiering: The secure removal or destruction of data from IT and OT assets before redeployment or disposal is a key practice in **ASSET, CHANGE AND CONFIGURATION** management, ensuring that assets are properly managed throughout their lifecycle. This practice must comply with established cybersecurity **STANDARDS AND TECHNOLOGY**, preventing unauthorized data access and ensuring data security through methods like cryptographic erasure and physical destruction.

1.2 Information Asset Inventory

ASSET-2a

Information assets that are important to the delivery of the function (for example, SCADA set points and customer information) are inventoried, at least in an ad hoc manner.
Assets derive their value and importance through their association with the aspects of the function's operations that they support. Identifying and inventorying high-value information assets helps enable selection and application of appropriate controls. High-value assets may also include information assets that may create financial, regulatory, or liability risks, such as PII, sensitive operational information, and confidential business information. Organizations should consider the different kinds of IT and OT assets that may contain information that is important to the function, such as:

- virtualized assets (including dormant and backup assets)
- regulated assets

- cloud assets
- bring your own device (BYOD) assets
- field assets
- mobile assets

Organizations should also consider different potential sources of high value information, such as:

- information located off premises
- stored or archived information
- backup data
- information managed by a third party
- information within different classification or sensitivity levels

At MIL1, the inventory may be produced in an ad hoc manner.
An inventory is not meant to imply that a single list is required; multiple repositories, documents, or systems may be used to accomplish this practice. Where appropriate, however, organizations should consider whether inventories may be consolidated to avoid potential risks related to managing multiple repositories.

AIM-Categorization-Tiering: This statement pertains to **ASSET, CHANGE AND CONFIGURATION** management. It emphasizes the identification and inventory of information assets based on their value and importance to the function's operations. Proper inventory management ensures that critical information assets are accounted for, which is crucial for effective asset management. Additionally, this practice aligns with **SITUATIONAL AWARENESS** as it involves understanding the significance of each information asset in relation to the organization's functions.

ASSET-2b

The information asset inventory includes information assets within the function that may be leveraged to achieve a threat objective.
These are assets that may be used in the pursuit of the tactics or goals of a threat actor. It is important to consider that a threat actor may have multiple objectives and that those objectives may change over time or in different situations. Achievement of a threat objective may not cause immediate harm to an organization but would increase the likelihood of the realization of a cyber risk. Identification of assets within the function that may be leveraged to achieve a threat objective should focus on the techniques used by threat actors and the potential for those techniques to be applied to the organization's assets. An example of assets within the function that may be leveraged to achieve a threat objective is information such as personally identifiable information that may cause harm to the organization or its stakeholders if lost, stolen, or disclosed.
Note that identification of this set of assets should be based on an assessment of risk.

AIM-Categorization-Tiering: This statement is associated with **THREAT AND VULNERABILITY** management. It involves identifying information assets that could be targeted by threat actors, which is essential for

understanding potential threats and vulnerabilities. Additionally, this practice relates to **RISK** management as it involves assessing risks based on the potential misuse of these assets. Maintaining an inventory of such assets helps in preparing for and mitigating potential security threats.

ASSET-2c

Inventoried information assets are categorized based on defined criteria that includes importance to the delivery of the function.
Categorization of assets is important for many cybersecurity and operational activities, such as incident response, risk management, threat management, and cybersecurity architecture planning.
Information should be categorized according to its sensitivity, value, criticality, interdependencies with other assets, legal requirements, whether the data is collected by, held by, or shared with a third party, or other scheme, including any scheme that is required by regulation or other compliance factor. Categorization provides another level of important description to an information asset that may affect strategies to protect and sustain it.
These are examples of categorization schemes:

- Confidential, Secret, Top Secret
- Regulated, Unregulated, Public
- Restricted, Private, Public

Whatever scheme is used, the importance of the asset to the delivery of the function should be considered.
Additionally, when identifying categories, consider that many cybersecurity activities generate information assets that need to be protected, such as configuration baseline information, risk registers, and even asset inventories themselves.

AIM-Categorization-Tiering: This statement fits into **ASSET, CHANGE AND CONFIGURATION** management. Categorizing information assets based on their importance helps in organizing and managing them effectively. It also supports **POLICY AND STRATEGY** by providing a structured approach to asset management and protection, ensuring that assets are categorized according to their value, sensitivity, and relevance to organizational functions.

ASSET-2d

Categorization criteria include consideration of the degree to which an asset within the function may be leveraged to achieve a threat objective.
The possibility of an asset within the function being leveraged to achieve a threat objective is added to the criteria used for categorizing information assets. Consideration for the way an asset may be utilized by a threat actor will enable a more comprehensive prioritization of the risks to, and impacts associated with, IT and OT assets. It is important to consider that a threat actor may have multiple objectives and that those objectives may change over time or in different situations.

AIM-Categorization-Tiering: This statement relates to **THREAT AND VULNERABILITY** management. It emphasizes incorporating threat objectives into the criteria for categorizing information assets, which helps in identifying assets at higher risk of being exploited by threat actors. This practice also intersects with **RISK** management, as it involves assessing the potential risks associated with each asset based on its threat profile.

ASSET-2e

The information asset inventory includes attributes that support cybersecurity activities (for example, asset category, backup locations and frequencies, storage locations, asset owner, cybersecurity requirements).
Information asset inventory attributes are details about assets that are included in asset inventories to enable management and consistent use of the assets. Including necessary information about assets to support the cybersecurity program strategy helps ensure that that information is available during periods of operational stress and does not have to be collected while in a state of crisis. For example, response to and recovery from a cybersecurity incident may be expedited if the information asset inventory provides the location of backups for information assets that are important to the delivery of the function (e.g., SCADA set points).Additionally, organizations should consider the different kinds of assets that may be within the scope of the evaluation, such as virtualized assets, regulated assets, cloud assets, and mobile assets.

AIM-Categorization-Tiering: This statement falls under **ASSET, CHANGE AND CONFIGURATION** management. Including detailed attributes in the information asset inventory supports effective management and consistent use of assets. It also aligns with **STANDARDS AND TECHNOLOGY** as it ensures adherence to cybersecurity practices and facilitates proper management of assets based on their attributes and requirements.

ASSET-2f

The information asset inventory is complete (the inventory includes all assets within the function).
This practice expands the inventory scope of ASSET-2a. The level of detail at which information assets are documented in the inventory should be determined with consideration for the importance and sensitivity of the asset to the organization. In many cases, it may be beneficial to consolidate types of information assets into a single entry in the information asset inventory. For example, employee-created assets residing on individual workstations (such as files or databases) may not warrant separate entries in the information asset inventory, unless they have special or critical value to the delivery of the function. The relationship of assets to business functions should also be included to enable prioritization and development of protection and sustainment strategies. The implementation of the inventory should be proportional to the organization's size, complexity, and risk. For example, for a small, lowcomplexity organization, a simple spreadsheet may be used for the inventory. For larger, more complex organizations, more sophisticated methods such as a dedicated asset inventory application is appropriate.

AIM-Categorization-Tiering: This statement is relevant to **ASSET, CHANGE AND CONFIGURATION** management. Ensuring a complete inventory of information assets is fundamental for effective asset management. It also supports **RISK** management by providing a comprehensive view of all assets, which is crucial for identifying and mitigating potential risks.

ASSET-2g

The information asset inventory is current, that is, it is updated periodically and according to defined triggers, such as system changes.
The inventory of information assets should be updated and maintained as assets change throughout their lifecycle to ensure the inventory is complete and accurate. Ensuring that the information asset inventory is current might involve change management procedures that require inventory updates any time assets are significantly altered. The organization might also conduct inventory reviews, both periodically (such as quarterly or yearly) and based on events (such as changes in organizational structure, major changes in critical systems, and the acquisition and

consolidation of another business).

AIM-Categorization-Tiering: This statement pertains to **ASSET, CHANGE AND CONFIGURATION** management. Keeping the inventory current through periodic updates and defined triggers ensures accuracy and relevance. This practice is also important for **RISK** management, as it helps in maintaining an accurate view of assets to address new risks and changes effectively.

ASSET-2h

Information assets are sanitized or destroyed at end of life using techniques appropriate to their cybersecurity requirements.
In this practice, sanitization refers to the removal of sensitive data from an asset in preparation for its reuse. For example, sanitization might involve removing customer-specific information from a slide presentation so that it can be used again. This should be completed in a manner that prevents the disclosure of information to unauthorized individuals when assets are reused.
By contrast, destruction refers to data removal so that it cannot be recovered. This involves permanent removal (that is, deletion in a way that makes recovery impossible, such as cryptographic erase, de-identification of personally identifiable information (PII), and destruction) from IT assets and OT assets when it is no longer needed. The organization must determine which end-of-life actions are appropriate for information assets and create procedures to ensure compliance with retention guidelines that establish when information assets should be retired. Procedures should include all possible locations where copies of the information might be stored, including system logs.

AIM-Categorization-Tiering: This statement relates to **ASSET, CHANGE AND CONFIGURATION** management. Proper sanitization and destruction of information assets at the end of their life cycle are critical for managing data security. It also aligns with **STANDARDS AND TECHNOLOGY**, as it involves implementing appropriate techniques to prevent unauthorized data access and ensure compliance with cybersecurity requirements.

1.3 IT and OT Asset Configurations

ASSET-3a

Configuration baselines are established, at least in an ad hoc manner.
Establishing a baseline for OT, IT, and information assets provides a foundation for managing the integrity of assets as they change over their lifecycle. Establishing point-in-time captures of assets (configuration items) ensures that these assets can be restored to an acceptable form when necessary—after a disruption, when an unauthorized modification has occurred, or under any circumstances where integrity is suspect and provides a level of control over changes that can potentially disrupt the assets' support of organizational services.
Organizations may consider integrity checking mechanisms (manual or automatic) when performing point-in-time captures of assets and asset configurations. Using integrity checking mechanisms to verify point-in-time captures prior to restoration can help ensure they are viable and available.
Documented policies and procedures for the configuration or maintenance of baselines are not required to implement this practice.

AIM-Categorization-Tiering: Establishing configuration baselines is crucial for **ASSET, CHANGE AND CONFIGURATION** management. This practice ensures that a foundational reference is available to manage and verify asset integrity over their lifecycle. By creating point-in-time captures, organizations can restore assets to an acceptable state after disruptions or unauthorized modifications. The use of integrity checking mechanisms aligns with maintaining configuration consistency and control.

ASSET-3b

Configuration baselines are used to configure assets at deployment and restoration.
The organization has procedures in place to ensure that established configuration baselines are applied to assets when they are deployed and restored. These baselines (also referred to as standard builds) support the deployment of assets in a controlled manner.

AIM-Categorization-Tiering: Using configuration baselines during asset deployment and restoration is a core aspect of **ASSET, CHANGE AND CONFIGURATION** management. It ensures that assets are configured in a controlled manner according to predefined standards, supporting both initial deployment and recovery efforts.

ASSET-3c

Configuration baselines incorporate applicable requirements from the cybersecurity architecture (ARCHI-TECTURE-1f).
As part of the cybersecurity architecture, the organization selects and documents requirements for the appropriate level of confidentiality, integrity, and availability of IT, OT, and information assets. These requirements may then be used to drive the development of cybersecurity controls to be applied to assets and systems (such as configuration baselines, network protections, software security). Configuration baseline hardening guidelines, such as the Center for Internet Security Benchmarks or the Department of Defense Security Technical Implementation Guides (STIGs), may provide a starting point for selecting configuration settings that achieve cybersecurity architecture requirements.

AIM-Categorization-Tiering: Incorporating cybersecurity architecture requirements into configuration baselines is integral to both **ASSET, CHANGE AND CONFIGURATION** management and **STANDARDS AND TECHNOLOGY**. This practice ensures that configuration settings meet necessary security standards and align with broader cybersecurity requirements, such as those provided by benchmarks and technical guides.

ASSET-3d

Configuration baselines are reviewed and updated periodically and according to defined triggers, such as system changes and changes to the cybersecurity architecture.
The organization has a defined schedule for reviewing baselines regularly and updating them as needed to ensure they continue to reflect appropriate security and functional requirements.

AIM-Categorization-Tiering: Regular review and update of configuration baselines is a key element of **ASSET, CHANGE AND CONFIGURATION** management. This practice ensures that baselines remain relevant and effective, adapting to system changes and updates in cybersecurity architecture to maintain optimal security and functionality.

ASSET-3e

Asset configurations are monitored for consistency with baselines throughout the assets' lifecycles.
Organizations should monitor asset configurations to ensure that they continue to conform to baselines over time after their deployment. Monitoring for consistency can be done through automated means, such as using a scanning tool that compares the baselines of connected assets to established configuration baselines, or by conducting periodic audits of assets to determine whether unauthorized changes have been made. Tools can also be used to automatically revert assets to baselines.
Automated configuration management or monitoring tools may enable more efficient tracking of asset configurations. Tools that are able to span physical, virtual, mobile, hybrid, and other technology environments should be considered to help ensure adequate coverage of IT and OT assets. These tools may be optimized for specific products. When selecting automation tools, stakeholders with adequate training and experience should be engaged early and careful consideration should be given to ensuring the appropriate fit between automation tools and the products they are intended to integrate with.
Data integrity tools (such as cryptographic checksums) may help in the detection of unauthorized changes to configuration settings, especially when managing virtualized assets. As an example of this, an organization may implement file integrity checks for virtualization platforms to be performed upon boot up and confirm that no unauthorized changes have occurred.

AIM-Categorization-Tiering: Monitoring asset configurations for consistency with baselines is fundamental to **ASSET, CHANGE AND CONFIGURATION** management. This involves ongoing verification that assets conform to established baselines, using tools and techniques to detect unauthorized changes and maintain configuration integrity throughout the asset lifecycle. This practice also involves aspects of **STANDARDS AND TECHNOLOGY**, particularly in the selection and use of automated monitoring tools.

1.4 Changes to IT and OT Assets

ASSET-4a

Changes to assets are evaluated and approved before being implemented, at least in an ad hoc manner.
All proposed changes to inventoried assets are evaluated to understand their priority, benefits, risks, and impacts to functionality and security on the functions they support. Consider that these may differ across different kinds of IT, OT and information assets, such as virtualized assets, regulated assets, assets managed by a third party, bring your own device (BYOD) assets, cloud assets, mobile assets, field assets, assets reliant on specific infrastructure such as wireless networks or the Global Position System, and assets that may be considered to be part of the Internet of Things or Industrial Internet of Things.

AIM-Categorization-Tiering: This practice falls under **ASSET, CHANGE AND CONFIGURATION** management as it involves evaluating and approving changes to assets, which is crucial for managing and controlling these resources. Evaluating changes helps ensure that they are aligned with organizational priorities and do not negatively impact asset functionality or security. The consideration of various asset types and their unique requirements emphasizes the need for effective **SITUATIONAL AWARENESS**, allowing organizations to understand and manage the impacts of changes across different asset categories.

ASSET-4b

Changes to assets are documented, at least in an ad hoc manner.
Any changes made to an inventoried asset are captured in a format that can be easily referenced during troubleshooting or incident response activities. Changes may include the alteration of settings such as routing and port configurations in network devices, the addition or removal of components, and modification of access privileges. Some of the attributes that should be captured include date and time of the change, who made the change, the assets affected by the change, and a description of any risks associated with the change.

AIM-Categorization-Tiering: Documenting changes to assets is an important aspect of **ASSET, CHANGE AND CONFIGURATION** management. This practice ensures that all modifications are recorded and can be referenced when needed for troubleshooting or incident response. Detailed documentation supports effective management and control of assets, providing a historical record of changes that can be critical for maintaining asset integrity and security.

ASSET-4c

Documentation requirements for asset changes are established and maintained.
The organization should define the required information that should be documented when performing changes to IT and OT assets. The requirements should consider what information may be necessary for activities such as troubleshooting or incident response. Additionally, the organization should consider the maintenance of these requirements based on changes to the operating environment.

AIM-Categorization-Tiering: Establishing and maintaining documentation requirements for asset changes falls under **POLICY AND STRATEGY**. Clear documentation requirements ensure that all relevant information is captured, facilitating effective management of changes and supporting troubleshooting and incident response. Maintaining these requirements reflects an ongoing commitment to managing and adapting to changes in the operating environment.

ASSET-4d

Changes to higher priority assets are tested prior to being deployed.
Changes to assets should be tested to ensure continuity of the assets and functions they affect prior to implementing the changes across the enterprise. When possible, testing of proposed changes should be conducted in a test environment or a low-risk production environment. Testing may include stress testing, confirmation that changes were implemented, operability, and load testing. Additionally, organizations may consider whether controls preventing unauthorized changes are necessary for specific types of assets. For example, digital or hardware programming switches should be placed in a mode that does not allow programming during routine operations.

AIM-Categorization-Tiering: Testing changes to higher priority assets is a practice related to **ASSET, CHANGE AND CONFIGURATION** management as it ensures that modifications do not negatively impact critical assets or their functionality. The focus on testing reflects a proactive approach to managing changes and mitigating potential risks associated with asset modifications. Additionally, testing for impact aligns with **THREAT AND VULNERABILITY** management, as it helps identify potential security issues before changes are fully deployed.

ASSET-4e

Changes and updates are implemented in a secure manner.
Procedures and tools used to update assets should incorporate appropriate controls to ensure that unintentional or intentional vulnerabilities or misconfigurations are not introduced as part of asset change processes. This may include use of secure communications protocols, verification methods, such as digital signatures, or other controls.

AIM-Categorization-Tiering: Implementing changes and updates in a secure manner aligns with **STANDARDS AND TECHNOLOGY**, ensuring that asset modifications do not introduce vulnerabilities. This practice reflects adherence to established cybersecurity standards and helps maintain the security and integrity of assets throughout the change process.

ASSET-4f

The capability to reverse changes is established and maintained for assets that are important to the delivery of the function.
This practice describes the development of an ability to roll back changes after they have been applied. This may be achieved through manual or automated methods. This enables an organization to revert to a known good state in the event that a change creates unforeseen or unintended operational or security consequences that cannot be addressed through other means.

AIM-Categorization-Tiering: Establishing the capability to reverse changes is part of **ASSET, CHANGE AND CONFIGURATION** management, providing a safety net for reverting changes that may cause issues. This capability is critical for maintaining asset functionality and security, especially for important assets. It also supports **INCIDENT DETECTION AND RESPONSE** by enabling rapid recovery from changes that result in problems.

ASSET-4g

Change management practices address the full lifecycle of assets (for example, acquisition, deployment, operation, retirement).
Organizational and operational conditions are continually changing, resulting in changes to staff, to the content and use of data, to technology, and so on. These changes can impact important assets throughout their lifecycles. Change management practices should not be limited to changes to operationally deployed assets but should encompass all phases of the lifecycle, including acquisition, deployment, and retirement.
To this end, the organization must define and manage the process for keeping the asset inventory current and ensure that changes to the inventory do not result in gaps in strategies for protecting and sustaining assets. Also, the organization must actively monitor for changes that significantly alter assets, identify new assets, and call for the retirement of assets for which there is no longer a need or whose relative value has been reduced.
Consider that different types of technologies (such as virtualized assets and cloud assets) may have unique lifecycle stages and other distinctive aspects that impact how change management should be implemented.

AIM-Categorization-Tiering: Addressing the full lifecycle of assets in change management practices is a fundamental aspect of **ASSET, CHANGE AND CONFIGURATION** management. This comprehensive approach ensures that all stages of an asset's lifecycle are considered, from acquisition to retirement. Managing changes across the entire lifecycle supports effective asset management and helps maintain asset security and functionality throughout its operational life.

ASSET-4h

Changes to higher priority assets are tested for cybersecurity impact prior to being deployed.
Changes to an asset used in multiple services can meet an immediate need but cause a problem in other applications. Changes should be evaluated in a test environment to identify any impact of the proposed change on other assets and systems. Cybersecurity impact might include any effect on availability of an asset to authorized users, any weakening of protections, or unintended alterations of access control lists. For example, if a vendor pushes a new version of an operating system, the new OS should be tested in a controlled environment to determine whether any applications or services would be affected.

AIM-Categorization-Tiering: Testing for cybersecurity impact before deploying changes relates to **THREAT AND VULNERABILITY** management, as it helps identify potential security risks associated with modifications. This practice ensures that changes do not inadvertently compromise asset security or functionality. It also ties into **ASSET, CHANGE AND CONFIGURATION** management by ensuring that changes are thoroughly evaluated before being fully implemented.

ASSET-4i

Change logs include information about modifications that impact the cybersecurity requirements of assets.
If tests for cybersecurity impact prior to deploying asset changes reveal that cybersecurity requirements (confidentiality, integrity, and availability) will be affected, those impacts should be described in change logs when the assets are changed. For example, if IP addressing schemes are changed within a network appliance, the change log should say something about how the availability of connected devices might be affected.

AIM-Categorization-Tiering: Including information about cybersecurity impacts in change logs is part of **INCIDENT DETECTION AND RESPONSE** management, as it ensures that changes affecting security requirements are documented. This practice supports effective incident response by providing detailed records of how changes might impact asset security. Additionally, this falls under **ASSET, CHANGE AND CONFIGURATION** management by documenting modifications and their effects on cybersecurity.

1.5 Management Activities

ASSET-5a

Documented procedures are established, followed, and maintained for activities in the ASSET domain.
The activities in the ASSET domain are formally documented in some way (such as standard operating procedures, process flow diagrams, RACI charts, and swim lane diagrams). The activities are intentionally designed or described to serve the organization rather than being ad hoc. Documenting procedures helps ensure that they are repeatable and produce expected outcomes. The level of detail included in documentation should be a sufficient to enable consistent performance of domain activities by different people and new employees assuming relevant domain experience and sufficient on-board training.
Also, procedure documentation is made available to and is used by relevant personnel. The documentation is updated as needed to reflect changes in the organizational or operational environment. Additionally, organizations may consider including exceptions processes in documented procedures to ensure that the organization reacts appropriately to unexpected events or situations.

AIM-Categorization-Tiering: The establishment and maintenance of documented procedures for ASSET domain activities fall under **PROGRAM** management. This practice ensures that activities are performed consistently and according to plan, supporting the overall cybersecurity strategy. Documented procedures also support **ASSET, CHANGE AND CONFIGURATION** management by providing clear guidelines for managing and controlling assets, and ensuring that all changes are properly documented and controlled.

ASSET-5b

Adequate resources (people, funding, and tools) are provided to support activities in the ASSET domain.
When determining the adequacy of resources, it may help to consider whether there are any ASSET domain activities not currently being performed that the organization would perform if it had additional people, funding, or tools. An additional consideration may be whether the organization has implemented all practices it has targeted for implementation and whether additional resources are necessary to address potential gaps.
Adequate resources are provided in the form of people, funding, and tools to ensure that ASSET domain practices can be performed as intended. The performance of this practice can be evaluated by determining whether any desired practices have not been implemented due to a shortage of resources.
These are examples of people involved in ASSET domain activities:

- staff responsible for developing and maintaining the asset inventory, including inventory attributes
- staff responsible for configuration management and change management of assets
- owners and custodians of assets

These are examples of tools that might be used in ASSET domain activities:

- asset inventory database management systems
- asset change management software, such as IT automation and orchestration tools for improving the efficiency and consistency of change management activities

Adequacy of resources should be determined on an ongoing basis through regular reviews of the domain program and reviews of domain resources in budgeting activities. It is a common point of concern that there is not enough time to complete cybersecurity program activities. This is addressed primarily through increasing staff and secondarily through increasing funding and tools.
When determining the adequacy of staff, also consider whether the cybersecurity program has sufficient capacity so that the individuals that make up the program can regularly attend training, implement and maintain tools, and respond to incidents while conducting day-to-day operations and meeting the cybersecurity objectives of the organization.

AIM-Categorization-Tiering: Providing adequate resources for ASSET domain activities is crucial for **PROGRAM** management, ensuring that all necessary practices and activities are supported effectively. This practice also relates to **WORKFORCE** management, as it involves allocating human resources and ensuring they have the necessary skills and support. Additionally, this aligns with **ASSET, CHANGE AND CONFIGURATION** management by ensuring that appropriate tools and funding are available to support the management and control of assets.

ASSET-5c

Up-to-date policies or other organizational directives define requirements for activities in the ASSET domain.
Activities in the ASSET domain receive documented guidance and direction from the organization in the form of policies or similar directives. Strategic business objectives drive the development of documented policies or other organizational directives to ensure activities support the accomplishment of the organization's mission.
Policies or other organizational directives for the ASSET domain may contain

- responsibility, authority, and ownership for performing ASSET domain activities, including collecting and documenting asset inventory information
- guidance on asset inventory updating, reconciliation, and change control
- procedures, standards and guidelines for documenting inventory attributes
- responsibility, authority, and mechanisms for protecting information generated in ASSET domain activities (such as inventory information and configuration baseline information) from unauthorized access or dissemination
- requirements for the frequency of inventory updates
- procedures for measuring adherence to policy, exceptions granted, and policy violations

AIM-Categorization-Tiering: The establishment of up-to-date policies and organizational directives for ASSET domain activities falls under **POLICY AND STRATEGY** management. This practice ensures that activities are guided by clear and current policies that align with strategic business objectives. It also supports **ASSET, CHANGE AND CONFIGURATION** management by providing guidelines for managing and controlling assets, including documentation, updates, and security measures.

ASSET-5d

Responsibility, accountability, and authority for the performance of activities in the ASSET domain are assigned to personnel.
The intent of this practice is that specific people (or people in specific roles) are held accountable for ensuring the achievement of expected results of ASSET domain activities and that they are given the appropriate authority to act and to perform their assigned responsibilities.
These are examples of how to formalize responsibility and authority for ASSET domain activities:

- defining roles and responsibilities in policies (see ASSET-5c)
- developing position descriptions and conducting associated performance management activities
- including process tasks and responsibility for these tasks in position descriptions
- developing and implementing contractual instruments (including service level agreements) with external entities to establish responsibility and authority for performing ASSET domain tasks on outsourced functions

· including ASSET domain tasks in measuring performance of external entities against contractual instruments

Additionally, consider how the knowledge developed by personnel within this domain should be managed and shared. This includes determining what processes and tools should be used for knowledge sharing and identifying who will be responsible for making the best use of internal knowledge.

AIM-Categorization-Tiering: Assigning responsibility, accountability, and authority for ASSET domain activities aligns with **PROGRAM** management by ensuring that specific roles and responsibilities are defined and that there is clear accountability. It also supports **WORKFORCE** management by ensuring that personnel are properly assigned and held accountable for their roles. Furthermore, this practice contributes to **KNOWLEDGE AND CAPABILITIES** management by addressing how knowledge is shared and utilized within the domain.

ASSET-5e

Personnel performing activities in the ASSET domain have the skills and knowledge needed to perform their assigned responsibilities.
The organization must identify the skills and knowledge needed to perform ASSET domain activities and identify skill and knowledge gaps in existing personnel. The organization can address gaps either by hiring qualified personnel or training existing personnel. It is important to note that managing and securing many technologies (such as virtualized or cloud-based environments) require specific training in specialized equipment and practices. Care should be taken to ensure that the level of skills and knowledge of personnel managing and securing specialized technologies is commensurate with the importance of and risk posed by those technologies.
Additionally, skill and knowledge assessments should be repeated as operational environments change over time. For example, in the ASSET domain, skills and knowledge are needed for

· developing criteria to use in prioritizing IT and OT assets

· categorizing information assets

· establishing, implementing, and maintaining asset inventories

Additionally, consider how the knowledge developed by personnel within this domain should be managed and shared. This includes determining what processes and tools should be used for knowledge sharing and identifying who will be responsible for making the best use of internal knowledge.

AIM-Categorization-Tiering: Ensuring that personnel have the necessary skills and knowledge for ASSET domain activities is crucial for **WORKFORCE** management, as it involves addressing skill gaps and ensuring staff are properly trained. This practice also supports **KNOWLEDGE AND CAPABILITIES** management by focusing on developing and maintaining the necessary expertise within the organization. Furthermore, it relates to **ASSET, CHANGE AND CONFIGURATION** management by ensuring that personnel are capable of effectively managing and securing assets.

ASSET-5f

The effectiveness of activities in the ASSET domain is evaluated and tracked.
The organization should measure the performance of ASSET activities to ensure they are being performed as

described in plans, policies, and procedures for the ASSET domain. Appropriate metrics should be developed and collected to detect deviations in performance and measure the extent to which ASSET domain activities are achieving their intended purpose.

AIM-Categorization-Tiering: Evaluating and tracking the effectiveness of ASSET domain activities falls under **PROGRAM** management. This practice ensures that activities are monitored and assessed to confirm they meet established goals and standards. It also supports **ASSET, CHANGE AND CONFIGURATION** management by ensuring that asset management practices are effective and aligned with organizational objectives. Additionally, it contributes to **RISK** management by providing insights into the effectiveness of controls and processes in mitigating risks.

2. Threat and Vulnerability Management - 30 questions

As presented on the platform, its purpose is: Establish and maintain plans, procedures, and technologies to detect, identify, analyze, manage, and respond to cybersecurity threats and vulnerabilities, commensurate with the risk to the organization's infrastructure (e.g., critical, IT, operational) and organizational objectives.

The Threat and Vulnerability Management (THREAT) domain comprises three objectives:

1. Reduce Cybersecurity Vulnerabilities
2. Respond to Threats and Share Threat Information
3. Management Activities for the THREAT domain

2.1 Reduce Cybersecurity Vulnerabilities

THREAT-1a

Information sources to support cybersecurity vulnerability discovery are identified, at least in an ad hoc manner.
Information about potential vulnerabilities is available from a wide variety of internal and external sources, such as CISA, appropriate ISACs, industry associations, vendors, federal briefings, and internal assessments. Internal sources typically provide information about vulnerabilities that are unique to the organization and range across all asset types. These sources may provide information about vulnerabilities that the organization has observed or that have been exploited, resulting in disruption to the organization. External or public sources typically provide information that is focused on common technologies that are used by a wide range of organizations.
Vulnerabilities in the traditional sense include software bugs, omission errors, poor code construction, poor configuration, or processing failures. However, other risk exposures can create vulnerabilities that should be identified, processed, and responded to in a similar manner as vulnerabilities that are, for example, reported by software vendors or included in vulnerability catalogs. These types of vulnerabilities might include poor process performance, insider threats, and internal audit findings. These types of vulnerabilities should be included when considering identification of sources for vulnerability discovery.
The identified sources of vulnerability information should align with the organization's vulnerability identification and analysis needs.

AIM-Categorization-Tiering: Identifying information sources to support cybersecurity vulnerability discovery falls under **THREAT AND VULNERABILITY** management. This practice involves gathering information on potential threats and vulnerabilities from various sources, which is essential for proactive vulnerability discovery.

THREAT-1b

Cybersecurity vulnerability information is gathered and interpreted for the function, at least in an ad hoc manner.
The organization should have a process for collecting, cataloging, and filtering vulnerability information from identified sources to separate out information that is relevant to the function.

AIM-Categorization-Tiering: Gathering and interpreting cybersecurity vulnerability information is part of **THREAT AND VULNERABILITY** management. This practice involves processing the gathered information to identify relevant threats and vulnerabilities, which is crucial for understanding and mitigating risks.

THREAT-1c

Cybersecurity vulnerability assessments are performed, at least in an ad hoc manner.
There are many types of assessment techniques that an enterprise can use to discover vulnerabilities, such as internal vulnerability audits and assessments, external-entity assessments, penetration tests, software-based scans, and reviewing the results of internal and external audits. Vulnerabilities can also be discovered from review and capture from the organization's standard list of sources of vulnerability information.

AIM-Categorization-Tiering: Performing cybersecurity vulnerability assessments is a key aspect of **THREAT AND VULNERABILITY** management. This practice involves using various assessment techniques to discover vulnerabilities, which is vital for identifying and addressing security weaknesses.

THREAT-1d

Cybersecurity vulnerabilities that are relevant to the delivery of the function are mitigated, at least in an ad hoc manner
The organization responds to vulnerabilities identified by credible information sources (e.g., government agencies, the software vendor) and takes steps to mitigate those vulnerabilities if they may affect the delivery of services. Vulnerability announcements may include criticality ratings (such as high, medium, low). These should be considered in the context of the overall environment. Even low-scoring vulnerabilities may be relevant and have a significant potential impact when assessed against your IT or OT environment. Response might involve, for example, implementing mitigating controls, applying cybersecurity patches, or tracking patching levels and operating system versions of devices. Advanced cybersecurity techniques such as threat hunting and active defense can provide in-depth information about the IT and OT environment that supports the determination of the relevance of a vulnerability to the organization. It is important to note that implementation of new compensating controls may require allocation of additional resources, such as people, funding, and tools, beyond the current cybersecurity program budget.

AIM-Categorization-Tiering: Mitigating relevant cybersecurity vulnerabilities is part of **INCIDENT DETECTION AND RESPONSE**. This practice involves taking appropriate actions to address identified vulnerabilities to ensure they do not compromise the delivery of services.

THREAT-1e

Cybersecurity vulnerability information sources that collectively address higher priority assets are monitored.
Vulnerability information sources are evaluated to determine the extent to which they provide information on

important assets. Sources providing the most utility and value should be prioritized for increased monitoring and review. The organization should identify additional vulnerability information sources if it determines that existing sources are not providing adequate information for any key assets.

AIM-Categorization-Tiering: Monitoring cybersecurity vulnerability information sources for higher priority assets falls under **THREAT AND VULNERABILITY** management. This practice ensures that the most critical assets are given priority in vulnerability monitoring efforts.

THREAT-1f

Cybersecurity vulnerability assessments are performed periodically and according to defined triggers, such as system changes and external events.
The organization uses established, documented, and structured vulnerability assessment methods to identify known vulnerabilities (that is, vulnerabilities that have been identified by external entities and published in information sources) as well as other potential weaknesses that may be exploited by an adversary. These assessments can be conducted by internal staff or by a third-party entity. Consideration should be given to the perspective of a potential internal or external threat actor. This may aid in identifying potential threat vectors that would otherwise go unnoticed. The organization must decide the appropriate time intervals that it will use to repeat assessments to ensure that it has the most current and accurate vulnerability information.

AIM-Categorization-Tiering: Performing periodic cybersecurity vulnerability assessments according to defined triggers is part of **THREAT AND VULNERABILITY** management. This practice ensures that the organization remains vigilant and updated on potential vulnerabilities by conducting assessments at regular intervals and in response to specific events.

THREAT-1g

Identified cybersecurity vulnerabilities are analyzed and prioritized, and are addressed accordingly.
Vulnerabilities may exist in all types of IT and OT assets, including operating systems, application software, firmware, network devices, mobile devices, IoT devices, and assets residing in the cloud.
Organizations may improve vulnerability management effectiveness through analysis and prioritization. Analysis can aid prioritization in several ways, such as helping to identify the potential impact a vulnerability could have on an organization's security posture. There are several factors important to determining the potential impact of a vulnerability. The attributes of the vulnerability—what it can do, how it is exploited, the potential effects, and the potentially affected assets—should be carefully considered. Additionally, the individual characteristics of the IT and OT environment, the cybersecurity controls in place, and externally determined impact valuation such as NIST National Vulnerability Database (NVD) Common Vulnerability Scoring System (CVSS) scores should also be considered.
Based on the results of analysis, an organization can then prioritize identified vulnerabilities for further action. Activities performed to address vulnerabilities may include implementing software, system, or firmware patches; developing and implementing operational workarounds or other mitigating controls; and developing and implementing new continuity plans or updating existing plans.

AIM-Categorization-Tiering: Analyzing and prioritizing identified cybersecurity vulnerabilities falls under **THREAT AND VULNERABILITY** management. This practice involves assessing the potential impact of

vulnerabilities and determining the appropriate order in which to address them, ensuring effective vulnerability management.

THREAT-1h

Operational impact to the function is evaluated prior to deploying patches or other mitigations.
Proposed patches, particularly those that affect critical assets, should be tested for operational impact prior to installation. Testing patches may help to identify unanticipated effects on the asset or other integrated assets. Organizations may decide to test patches in a test environment when feasible or on a limited number of non-critical production systems prior to enterprise-wide implementation.

AIM-Categorization-Tiering: Pertains primarily to **ASSET, CHANGE AND CONFIGURATION**, as it emphasizes the need for careful management and control of IT assets, including the assessment of changes to these assets. Additionally, it involves **RISK** because it requires identifying and managing the potential risks associated with deploying patches, ensuring that the patches do not introduce new vulnerabilities or issues. Lastly, **STANDARDS AND TECHNOLOGY** is relevant since the practice of testing patches aligns with established standards and best practices for maintaining system integrity and security.

THREAT-1i

Information on discovered cybersecurity vulnerabilities is shared with organization-defined stakeholders.
As cybersecurity vulnerabilities are discovered through vulnerability information sources and assessments, information about vulnerabilities that would be important to relevant stakeholders should be shared with them.

AIM-Categorization-Tiering: Sharing information on discovered cybersecurity vulnerabilities falls under **CULTURE AND SOCIETY**. This practice promotes transparency and ensures that all relevant stakeholders are informed about vulnerabilities and the steps being taken to address them.

THREAT-1j

Cybersecurity vulnerability information sources that collectively address all IT and OT assets within the function are monitored.
Vulnerability information sources should be evaluated to determine the extent to which they provide information for all IT and OT assets within the function. Sources addressing higher priority assets and those deemed of a higher importance may be prioritized for increased monitoring and review.

AIM-Categorization-Tiering: Monitoring cybersecurity vulnerability information sources for all IT and OT assets within the function falls under **THREAT AND VULNERABILITY** management. This practice ensures comprehensive monitoring and protection of all critical assets.

THREAT-1k

Cybersecurity vulnerability assessments are performed by parties that are independent of the operations of the function.
In addition to vulnerability assessments that are conducted internally, the organization should periodically have external parties conduct assessments in order to obtain a completely objective perspective. The assessors should

be external to the function's operations but not necessarily external to the organization.

AIM-Categorization-Tiering: Performing cybersecurity vulnerability assessments by independent parties falls under **STANDARDS AND TECHNOLOGY**. This practice ensures objective and unbiased assessment of vulnerabilities, which is critical for accurate and effective vulnerability management.

THREAT-1l

Vulnerability monitoring activities include review to confirm that actions taken in response to cybersecurity vulnerabilities were effective.
After a response has been made to address a vulnerability (such as deployment of patches), monitoring is conducted to make sure that the response has been effective. Methods to confirm effectiveness will vary depending on resources available to the cybersecurity program and the type of treatment chosen for a vulnerability. For example, if an operating system vendor has disclosed the presence of a vulnerability the organization may choose to remediate the vulnerability and apply a patch. Afterward, a vulnerability scan could be used to confirm that the vulnerability has been resolved on affected systems. Advanced cybersecurity techniques such as threat hunting and active defense also can be used as methods of verification.

AIM-Categorization-Tiering: Including review in vulnerability monitoring activities to confirm the effectiveness of actions taken falls under **INCIDENT DETECTION AND RESPONSE**. This practice ensures that the measures implemented to address vulnerabilities are effective and that the organization remains protected.

THREAT-1m

Mechanisms are established and maintained to receive and respond to reports from the public or external parties of potential vulnerabilities related to the organization's IT and OT assets, such as public-facing websites or mobile applications.
In the event that an individual external to the organization identifies a vulnerability in an IT or OT asset within the organization, it would be beneficial for the organization to be notified. Development of a process that integrates with existing vulnerability management activities would better enable the cybersecurity program in the identification of vulnerabilities. This mechanism should enable the organization to receive communications and take necessary action (e.g., analysis and testing to verify a reported vulnerability exists). The implemented mechanism should complement current vulnerability management activities and organizations should consider if the mechanism would necessitate additional resources. For example, if a bug in a website allows an attacker to access unauthorized information, the individual who discovered the vulnerability sends an email to a specified email address with details about the vulnerability. This capability may be implemented in a variety of ways, such as setting up a web form, a dedicated email address, or through a third-party service.

AIM-Categorization-Tiering: Establishing and maintaining mechanisms to receive and respond to reports from external parties falls under **INCIDENT DETECTION AND RESPONSE**. This practice ensures that the organization can effectively identify and address vulnerabilities reported by external individuals, enhancing overall security posture by incorporating external insights into vulnerability management.

2.2 Respond to Threats and Share Threat Information

THREAT-2a

Internal and external information sources to support threat management activities are identified, at least in an ad hoc manner.
The organization should periodically survey information sources (such as CISA, appropriate ISACs, industry associations, vendors, and federal briefings) to determine their relevance and value in providing threat information. Some analysis may first be necessary to determine what information is most relevant for supporting threat management activities. Additionally, threats affecting similar industry sectors may be relevant to the function and should be considered accordingly.

AIM-Categorization-Tiering: This falls under **SITUATIONAL AWARENESS**, as identifying relevant internal and external sources for threat management activities is essential for maintaining an awareness of potential threats and their implications for the organization.

THREAT-2b

Information about cybersecurity threats is gathered and interpreted for the function, at least in an ad hoc manner.
Threat identification and response begins with collecting useful threat information from reliable sources and determining whether and how that information is relevant in the context of the organization and function. Collection and review of threat information can be done by internal staff, provided as a service through a vendor, or a combination of both. Sources of threat information should address the different kinds of IT, OT, and information assets that are important to the delivery of the function.

AIM-Categorization-Tiering: This practice falls under **SITUATIONAL AWARENESS**, as it involves gathering and interpreting information about threats to ensure the organization stays informed and can respond appropriately.

THREAT-2c

Threat objectives for the function are identified, at least in an ad hoc manner.
Threat objectives are the potential outcomes of threat actor activities that are of concern because they would have negative impacts on the organization. For example, an organization that does not process confidential data may not be concerned about data theft but may be very concerned about an incident that causes an operational outage. Threat actors may leverage multiple tactics or techniques like those defined in the MITRE ATT&CK frameworks (for Enterprise or Industrial Control Systems) to achieve their goals. Threat objective examples may include data manipulation, IP Theft, damage to property, denial of control, loss of safety, or operational outage.

AIM-Categorization-Tiering: Identifying threat objectives is part of **THREAT AND VULNERABILITY**, as it involves understanding the potential outcomes of threat actor activities and how they might impact the organization.

THREAT-2d

Threats that are relevant to the delivery of the function are addressed, at least in an ad hoc manner.
The organization responds to threats identified through the collection and analysis of threat information when

they are determined to have the potential to adversely affect the function. Relevant threats are those that have the means, motive, and opportunity to affect the delivery of services. Threat response might involve, for example, implementing mitigating controls or monitoring threat status.

AIM-Categorization-Tiering: This falls under **INCIDENT DETECTION AND RESPONSE**, as it involves responding to identified threats to ensure the delivery of services is not adversely affected.

THREAT-2e

A threat profile for the function is established that includes threat objectives and additional threat characteristics (for example, threat actor types, motives, capabilities, and targets).
The threat profile can be built from information about threats from reliable sources, both internal (such as results of threat assessments) and external (such as E-ISAC, CISA Central, and government briefings). The threat profile can be used to guide the identification and description of specific threats and can be used as input in the risk analysis process described in the Risk Management domain and in situational awareness activities described in the Situational Awareness domain.
A threat profile may also help to guide identification of assets within the function that may be leveraged to achieve a threat objective as described in the Asset, Change, and Configuration Management domain. Development of a threat profile could occur prior to completion of a self-evaluation or following the completion of a self-evaluation as an activity identified as part of gap analysis and remediation.

AIM-Categorization-Tiering: Establishing a threat profile is part of **THREAT AND VULNERABILITY**, as it involves identifying and documenting potential threats and their characteristics to inform risk analysis and **SITUATIONAL AWARENESS** activities.

THREAT-2f

Threat information sources that collectively address all components of the threat profile are prioritized and monitored.
Threat information sources are evaluated to determine the extent to which they provide information needed in the threat profile. Sources of greater value are prioritized for increased monitoring and greater scrutiny. Sources that do not contribute to addressing components of the threat profile either are eliminated or are given less attention.

AIM-Categorization-Tiering: This practice falls under **SITUATIONAL AWARENESS**, as it involves prioritizing and monitoring information sources that provide valuable threat information relevant to the organization's threat profile.

THREAT-2g

Identified threats are analyzed and prioritized and are addressed accordingly.
Threats must be evaluated to determine which warrant the most and the timeliest attention based on their likely intent, capability, target, and potential to adversely impact the function as described in the threat profile.
Threats should be addressed in order of priority to facilitate an effective response. Actions taken may be to analyze the threat to further understand potential impact, implement controls to mitigate the risk associated with the threat, or to adjust monitoring activities to look for indicators of the threat.

AIM-Categorization-Tiering: Analyzing and prioritizing identified threats is part of **THREAT AND VULNERABILITY**, as it involves evaluating threats and determining the appropriate response based on their potential impact.

THREAT-2h

Threat information is exchanged with stakeholders (for example, executives, operations staff, government, connected organizations, vendors, sector organizations, regulators, Information Sharing and Analysis Centers [ISACs]). Identify what types of threat information you are either willing to and permitted to share or are obligated to report and set up relationships and communications processes to share that information with others. Information sharing activities should adhere to your legal and regulatory requirements. For threat information sharing to be efficient and meaningful, some analysis should be done to ensure that all relevant stakeholders have been identified and are being involved appropriately in threat management activities. A stakeholder mapping technique might aid in accomplishing this.

AIM-Categorization-Tiering: This falls under **CULTURE AND SOCIETY**, as it involves the exchange of threat information with various stakeholders to ensure a coordinated and informed response to threats.

THREAT-2i

The threat profile for the function is updated periodically and according to defined triggers, such as system changes and external events.
The organization should define a schedule for reviewing and updating the established threat profile for the function to ensure that the likely intent, capability, and target of threats currently defined are still accurate and relevant and to add any new threats that have been identified. Given that new threats emerge daily, organizations should consider dedicating resources toward continuous review of threat information and updating of the threat profile if feasible.

AIM-Categorization-Tiering: This practice is part of **THREAT AND VULNERABILITY**, as it involves periodically updating the threat profile to ensure it remains current and relevant in light of new information and changes.

THREAT-2j

Threat monitoring and response activities leverage and trigger predefined states of operation (SITUATION-3g).
Predefined states of operation are distinct operating modes (which typically include specific IT and OT configurations as well as alternate or modified procedures) that have been designed and implemented for the function and can be invoked by a manual or automated process in response to an event, a changing risk environment, or other sensory and awareness data to provide greater safety, resilience, reliability, and/or cybersecurity.
For example, an ISAC publishes a bulletin notifying its members of a successful campaign targeting peer organizations that exploits a previously unknown vulnerability to a technology that is critical to the delivery of the organization's function. Based on this information, existing controls, and risk posture, the organization deems the threat relevant. It invokes a decision process that results in declaration of a high-security operating state that trades off efficiency and ease of use in favor of increased security by blocking remote access and requiring a higher level of authentication and authorization for certain commands. On-going monitoring of internal systems and the threat environment is employed to determine when to return to the normal state of operation.

AIM-Categorization-Tiering: This falls under **INCIDENT DETECTION AND RESPONSE**, as it involves leveraging predefined states of operation to respond to changing threat environments effectively.

THREAT-2k

Secure, near-real-time methods are used for receiving and sharing threat information to enable rapid analysis and action.
Integrating a system of potentially diverse cybersecurity products into a responsive and resilient detection, analysis, response, and information sharing platform requires leveraging cybersecurity automation standards. These systems are intended to ease the burden on analysts by ingesting and enriching data and, in some cases, automatically taking action in response to malicious indicators. Ensuring that components of a larger cybersecurity system share a common taxonomy (e.g., Structured Threat Information Expression (STIX), Trusted Automated Exchange of Indicator Information (TAXII)) and are designed to securely accept, process, and distribute data from a variety of sources and vendors is key to developing a successful cybersecurity platform.

AIM-Categorization-Tiering: This practice falls under **STANDARDS AND TECHNOLOGY**, as it involves using secure, near-real-time methods and standards for receiving and sharing threat information to enable rapid analysis and response.

2.3 Management Activities

THREAT-3a

Documented procedures are established, followed, and maintained for activities in the THREAT domain.
The activities in the THREAT domain are formally documented in some way (such as standard operating procedures, process flow diagrams, RACI charts, and swim lane diagrams). The activities are intentionally designed or described to serve the organization rather than being ad hoc. Documenting procedures helps ensure that they are repeatable and produce expected outcomes. The level of detail included in documentation should be a sufficient to enable consistent performance of domain activities by different people and new employees assuming relevant domain experience and sufficient on-board training.
Also, procedure documentation is made available to and is used by relevant personnel. The documentation is updated as needed to reflect changes in the organizational or operational environment. Additionally, organizations may consider including exceptions processes in documented procedures to ensure that the organization reacts appropriately to unexpected events or situations.

AIM-Categorization-Tiering: It primarily pertains to **THREAT AND VULNERABILITY** because it involves identifying, assessing, and mitigating security risks associated with threats and vulnerabilities. Additionally, it involves **KNOWLEDGE AND CAPABILITIES** as it emphasizes the importance of detailed documentation for enabling consistent performance by personnel, ensuring that the organization's staff have the necessary information to handle threats effectively. Finally, **POLICY AND STRATEGY** is relevant because well-documented procedures align with an organization's broader policies and strategies for managing cybersecurity risks and ensuring consistent and effective threat management.

THREAT-3b

Adequate resources (people, funding, and tools) are provided to support activities in the THREAT domain.
When determining the adequacy of resources, it may help to consider whether there are any THREAT domain activities not currently being performed that the organization would perform if it had additional people, funding, or tools. An additional consideration may be whether the organization has implemented all practices it has targeted for implementation and whether additional resources are necessary to address potential gaps.
Adequate resources are provided in the form of people, funding, and tools to ensure that THREAT domain practices can be performed as intended. The performance of this practice can be evaluated by determining whether any desired practices have not been implemented due to a shortage of resources.
These are examples of people involved in THREAT domain activities:

- staff responsible for collection and analysis of threat information
- staff responsible for developing threat profiles
- staff responsible for performing vulnerability assessments

These are examples of tools that might be used in THREAT domain activities:

- techniques and tools for creating threat profiles
- tools for performing vulnerability assessments
- vulnerability databases

Adequacy of resources should be determined on an ongoing basis through regular reviews of the domain program and reviews of domain resources in budgeting activities. It is a common point of concern that there is not enough time to complete cybersecurity program activities. This is addressed primarily through increasing staff and secondarily through increasing funding and tools.
When determining the adequacy of staff, also consider whether the cybersecurity program has sufficient capacity so that the individuals that make up the program can regularly attend training, implement and maintain tools, and respond to incidents while conducting day-to-day operations and meeting the cybersecurity objectives of the organization.

AIM-Categorization-Tiering: It primarily pertains to **THREAT AND VULNERABILITY**, as it involves ensuring that sufficient resources are allocated to identify, assess, and mitigate security risks. Additionally, it pertains to **WORKFORCE** because it emphasizes the need for sufficient staff to perform threat-related activities and maintain the cybersecurity program. Furthermore, it involves **POLICY AND STRATEGY** since it requires strategic planning to allocate resources effectively, and **KNOWLEDGE AND CAPABILITIES** because adequate funding, tools, and training are essential to develop and maintain the skills necessary for threat management. Finally, **RISK** is relevant as adequate resources are crucial to manage and mitigate potential cybersecurity risks.

THREAT-3c

Up-to-date policies or other organizational directives define requirements for activities in the THREAT domain.
Activities in the THREAT domain receive documented guidance and direction from the organization in the form

of policies or similar directives. Strategic business objectives drive the development of documented policies or other organizational directives to ensure activities support the accomplishment of the organization's mission. Policies or other organizational directives for THREAT domain activities may contain

- responsibility, authority, and ownership for performing THREAT activities
- procedures, standards, and guidelines for collecting and analyzing threat information and creating threat profiles
- lists of individuals and organizations to whom cybersecurity threat information is provided
- guidelines about what cybersecurity threat information can be or must be provided to those individuals and organizations
- requirements for the frequency of updating threat profiles
- guidelines for addressing vulnerabilities
- requirements for the frequency of performing vulnerability assessments
- methods for measuring adherence to policy, exceptions granted, and policy violations
- procedures for the granting and management of exceptions

AIM-Categorization-Tiering: It primarily pertains to **POLICY AND STRATEGY**, as it involves creating and maintaining clear policies to guide threat-related activities. Additionally, it pertains to **THREAT AND VULNERABILITY** because it focuses on identifying, assessing, and mitigating security risks through well-documented guidance. Furthermore, it involves **PROGRAM** since it requires alignment with the organization's strategic objectives and comprehensive planning for cybersecurity management. Lastly, **KNOWLEDGE AND CAPABILITIES** is relevant as the directives ensure that staff have the necessary guidelines to perform threat-related activities effectively.

THREAT-3d

Responsibility, accountability, and authority for the performance of activities in the THREAT domain are assigned to personnel.
The intent of this practice is that specific people (or people in specific roles) are held accountable for ensuring the achievement of expected results of THREAT domain activities and that they are given the appropriate authority to act and to perform their assigned responsibilities.
These are examples of how to formalize responsibility and authority for THREAT domain activities:

- defining roles and responsibilities in policies (see THREAT-3c)
- defining roles and responsibilities that are filled by third party personnel, such as cloud service providers (CSP)
- developing position descriptions and conducting associated performance management activities
- including process tasks and responsibility for these tasks in position descriptions

- developing and implementing contractual instruments (including service level agreements) with external entities to establish responsibility and authority for performing THREAT domain tasks on outsourced functions
- including THREAT domain tasks in measuring performance of external entities against contractual instruments

Additionally, consider how the knowledge developed by personnel within this domain should be managed and shared. This includes determining what processes and tools should be used for knowledge sharing and identifying who will be responsible for making the best use of internal knowledge.

AIM-Categorization-Tiering: It belongs to **THREAT AND VULNERABILITY** because it focuses on assigning roles and responsibilities to personnel for activities related to identifying, assessing, and mitigating security risks. **PROGRAM** because it involves strategic planning and the formalization of responsibilities, ensuring alignment with business objectives and proper governance through policies and contractual agreements. **KNOWLEDGE AND CAPABILITIES** because it addresses the management and sharing of knowledge developed by personnel, emphasizing the importance of processes and tools to leverage internal expertise effectively.

THREAT-3e

Personnel performing activities in the THREAT domain have the skills and knowledge needed to perform their assigned responsibilities.
The organization must identify the skills and knowledge needed to perform THREAT domain activities and identify skill and knowledge gaps in existing personnel. The organization can address gaps either by hiring qualified personnel or training existing personnel. It is important to note that managing and securing many technologies (such as virtualized or cloud-based environments) require specific training in specialized equipment and practices. Care should be taken to ensure that the level of skills and knowledge of personnel managing and securing specialized technologies is commensurate with the importance of and risk posed by those technologies.
Additionally, skill and knowledge assessments should be repeated as operational environments change over time. For example, in the THREAT domain, skills and knowledge are needed for

- tools, techniques, and methods used to collect and analyze threat information
- developing threat profiles
- conducting vulnerability assessments
- evaluating operational impact prior to deploying patches
- interpreting vulnerability information and representing it in ways that are meaningful and appropriate for function stakeholders

Additionally, consider how the knowledge developed by personnel within this domain should be managed and shared. This includes determining what processes and tools should be used for knowledge sharing and identifying who will be responsible for making the best use of internal knowledge.

AIM-Categorization-Tiering: It belongs to **THREAT AND VULNERABILITY** because it focuses on the

skills and knowledge required to effectively identify, assess, and mitigate security risks associated with threats and vulnerabilities. **WORKFORCE** because it addresses the need for personnel with appropriate skills and knowledge to perform their assigned responsibilities, including the hiring and training of qualified personnel. **KNOWLEDGE AND CAPABILITIES** because it emphasizes the importance of having the necessary skills and knowledge to manage and secure technologies, as well as the need for ongoing assessments and knowledge sharing to adapt to changing operational environments.

THREAT-3f

The effectiveness of activities in the THREAT domain is evaluated and tracked.
The organization should measure the performance of THREAT activities to ensure they are being performed as described in plans, policies, and procedures for the THREAT domain. Appropriate metrics should be developed and collected to detect deviations in performance and measure the extent to which THREAT domain activities are achieving their intended purpose.

AIM-Categorization-Tiering: It belongs to **THREAT AND VULNERABILITY** because it focuses on evaluating and tracking the effectiveness of activities aimed at identifying, assessing, and mitigating security risks associated with threats and vulnerabilities. **RISK** because it involves measuring performance to ensure that risk management processes are effectively protecting the organization's information assets and minimizing the impact of potential security breaches. **POLICY AND STRATEGY** because it emphasizes the need for well-defined metrics and performance tracking to ensure that activities align with the organization's established plans, policies, and procedures, thereby supporting the overall cybersecurity strategy.

3. Risk Management - 39 questions

As presented on the platform, its purpose is: Establish, operate, and maintain an enterprise cybersecurity risk management program to identify, analyze, and mitigate cybersecurity risk to the organization, including its business units, subsidiaries, related interconnected infrastructure, and stakeholders.

The Risk Management (RISK) domain comprises five objectives:

1. Establish and Maintain Cyber Risk Management Strategy and Program
2. Identify Cyber Risk
3. Analyze Cyber Risk
4. Respond to Cyber Risk
5. Management Activities for the RISK domain

3.1 Establish and Maintain Cyber Risk Management Strategy and Program

RISK-1a

The organization has a strategy for cyber risk management, which may be developed and managed in an ad hoc manner.
The organization develops, implements, and maintains a cybersecurity risk management strategy that, in its simplest form, includes a list of cyber risk management objectives and related actions, activities, and tasks and a plan

to implement them.
For a C2M2-based program, areas of activity in the strategy could align with objectives in the C2M2 RISK domain and their associated practices. For example, the strategy may include important information about the organization's processes for identifying, analyzing, and responding to cyber risks. Further detail may include the high-level categories into which risks are consolidated, criteria for determining cyber risk priority, and a summary of risk response techniques to be applied to risks, and is the assignment of responsibility for implementation of the strategy.

AIM-Categorization-Tiering: The statement emphasizes the development and management of a cybersecurity risk management strategy, which aligns directly with **POLICY AND STRATEGY**. This categorization ensures that the organization has a clear and effective approach to identifying, analyzing, and responding to cyber risks. Additionally, the assignment of responsibility for implementing the strategy highlights the importance of **PROGRAM** management, ensuring that the risk management objectives are aligned with the organization's business objectives and executed effectively.

RISK-1b

A strategy for cyber risk management is established and maintained in alignment with the organization's cybersecurity program strategy (PROGRAM-1b) and enterprise architecture.
The risk management strategy is kept current and relevant. A risk management strategy focused on mitigating risks of procured software, for example, will likely be out of step with a cybersecurity program goal of increasing internally developed software and an enterprise architecture goal implementing a secure development process.

AIM-Categorization-Tiering: This statement focuses on maintaining the alignment of the cyber risk management strategy with the organization's cybersecurity program strategy and enterprise architecture, which falls under **POLICY AND STRATEGY**. Ensuring that the strategy remains current and relevant to organizational goals also ties into **PROGRAM** management, as it highlights the need for continuous alignment and coordination between various strategic elements.

RISK-1c

The cyber risk management program is established and maintained to perform cyber risk management activities according to the cyber risk management strategy.
The cyber risk management program is typically responsible for ensuring that the cyber risk management objectives as documented in the cyber risk management program strategy are achieved. For example, the cyber risk management program includes activities to ensure that the organization identifies, analyzes, and responds to cyber risks.

AIM-Categorization-Tiering: Establishing and maintaining a cyber risk management program to perform activities according to the strategy is a key aspect of **PROGRAM** management. This ensures that the organization's cyber risk management objectives are achieved through well-defined activities and processes. Additionally, it highlights the importance of **RISK** management by focusing on identifying, analyzing, and responding to cyber risks.

RISK-1d

Information from RISK domain activities is communicated to relevant stakeholders.
The risk management program has procedures that define criteria such as the types of information that should be communicated to stakeholders, methods of communication, and triggers that would require escalation. As the organization identifies, analyzes, and responds to risks, stakeholders should receive updated information on the status of risks. These stakeholders may be internal or external to the organization.

AIM-Categorization-Tiering: Communicating information from risk domain activities to relevant stakeholders relates to **SITUATIONAL AWARENESS**, as it ensures that stakeholders are informed about the current status of risks and any necessary actions. This communication is essential for effective **PROGRAM** management, enabling stakeholders to make informed decisions and respond appropriately to identified risks.

RISK-1e

Governance for the cyber risk management program is established and maintained.
The organization may establish a higher-level risk officer position that provides oversight of risk management or assign the responsibility to someone with sufficient authority in the organization. The officer would be responsible for sponsoring and providing oversight of the policies and procedures for cyber risk management activities. Other responsibilities may include ensuring feedback loops are in place to evaluate the performance of activities or providing reporting to high-level managers on adherence to compliance obligations.

AIM-Categorization-Tiering: Establishing and maintaining governance for the cyber risk management program involves **POLICY AND STRATEGY**, as it includes the oversight and sponsorship of policies and procedures for risk management. This governance ensures that the program operates effectively and aligns with organizational goals. Additionally, it is crucial for **PROGRAM** management, as it involves assigning responsibilities and ensuring continuous evaluation and reporting.

RISK-1f

Senior management sponsorship for the cyber risk management program is visible and active.
Visible and active sponsorship by senior management might include regular communications by senior management about the importance and value of the cyber risk program, organizational support for establishing and implementing governance for managing cyber risk, and funding awards and recognition programs for staff who make significant contributions toward achieving cybersecurity objectives.

AIM-Categorization-Tiering: Visible and active sponsorship by senior management for the cyber risk management program emphasizes the importance of **CULTURE AND SOCIETY**. It shows how senior management promotes and fosters a culture of cybersecurity awareness and support within the organization. This active sponsorship also ties into **PROGRAM** management, as it ensures that the necessary resources and recognition are provided to achieve cybersecurity objectives.

RISK-1g

The cyber risk management program aligns with the organization's mission and objectives.
The cyber risk management program may be a component of an Enterprise Risk Management (ERM) program or

may be a standalone program. If part of an ERM, the cyber risk program should be modeled after the enterprise-wide program to ensure that stakeholders are efficiently engaged and cyber risk information can be more easily integrated into overall ERM activities.
A standalone program should use the cyber risk management strategy, along with the organization's mission and objectives to build the direction of program activities through documents like policies and procedures. Relevant stakeholders should be engaged to ensure the activities of the program are in alignment with operational and business areas of the organization.
Regardless of whether the program is standalone or part of an ERM, the cyber risk program should take the risk appetite of the organization into account when forming program-level activities. The risk appetite of the organization is the amount of risk that the organization is willing to accept, as defined by senior leadership. Certain thresholds or boundaries may be established that would indicate if a risk is greater than organizational acceptance levels.

AIM-Categorization-Tiering: Aligning the cyber risk management program with the organization's mission and objectives is a critical aspect of **POLICY AND STRATEGY**. It ensures that the program supports the broader organizational goals and integrates effectively with other enterprise risk management activities. This alignment also highlights the importance of **RISK** management by considering the organization's risk appetite and ensuring that program-level activities are consistent with this threshold.

RISK-1h

The cyber risk management program is coordinated with the organization's enterprise-wide risk management program.
Alignment of these strategies avoids mismatched expectations between business and technical stakeholders. For example, the enterprise goals of protecting intellectual property and sensitive business data are supported by the cybersecurity goals of minimizing attack surfaces and establishing secure defaults. Cyber risks should be communicated as components or contributors to overall risk and should be communicated in the same terms where possible.
Within an enterprise that has no enterprise risk management functions, this practice may be implemented by aligning risk management practices to enterprise level management functions and ensuring that domain activities are occurring at the enterprise level as appropriate (for example, establishment of strategy, risk management program governance, stakeholder and leadership communication, resourcing, assignment of roles and responsibilities, tracking effectiveness).

AIM-Categorization-Tiering: Coordinating the cyber risk management program with the organization's enterprise-wide risk management program is essential for effective **POLICY AND STRATEGY**. This coordination ensures that cyber risks are integrated into the overall risk management framework and communicated consistently to all stakeholders. It also involves **PROGRAM** management, as it requires aligning risk management practices with enterprise-level management functions and ensuring that domain activities are conducted at the appropriate level.

3.2 Identify Cyber Risk

RISK-2a

Cyber risks are identified, at least in an ad hoc manner.
Identification of cyber risks is a foundational risk management activity. It requires the organization to identify the

types of threats, vulnerabilities, and disruptive events that can pose risk to the operational capacity of assets and services. Identified risks form a baseline from which a continuous risk management process can be established and managed.

AIM-Categorization-Tiering: The statement emphasizes the importance of identifying cyber risks, which aligns with **THREAT AND VULNERABILITY**. This is foundational for the ongoing management of risks and ensuring the operational capacity of assets and services is protected.

RISK-2b

A defined method is used to identify cyber risks.
A defined method is planned in advance, clearly described, made definite, and standardized. Employing a defined method to identify risks will aid the cyber risk management program in producing consistent outputs and better enable effective management of cyber risk. The organization may choose to define their own method or leverage standardized guidance, such as the NIST SP 800-30, Guide for Conducting Risk Assessments.

AIM-Categorization-Tiering: Using a defined method to identify cyber risks emphasizes **STANDARDS AND TECHNOLOGY**. Standardized methods ensure consistency and effectiveness in identifying and managing cyber risks.

RISK-2c

Stakeholders from appropriate operations and business areas participate in the identification of cyber risks.
The involvement of stakeholders from various parts of the organization is beneficial, because different perspectives from throughout the organization will lead to more comprehensive identification of risks. Stakeholders from operational areas may have a better understanding of how a risk could impact an operational process, while stakeholders in a business area may have more visibility into the impact of a risk across services.

AIM-Categorization-Tiering: Engaging stakeholders from various areas emphasizes **CULTURE AND SOCIETY**. This approach ensures that different perspectives contribute to a more comprehensive identification of risks.

RISK-2d

Identified cyber risks are consolidated into categories (for example, data breaches, insider mistakes, ransomware, OT control takeover) to facilitate management at the category level.
Categories of cyber risk are established and may be based on common operational risks such as data breaches, insider mistakes, ransomware, or OT control takeover. The organization should determine the necessary granularity to effectively manage cyber risks. After a cyber risk is identified, it should be assigned to one of the defined categories. The categories will help the organization to more effectively analyze and respond to risks. The cyber risk categories may be a part of a larger taxonomy maintained by the organization's risk management program that also includes key terms and definitions. This capability will help enable organizations to manage risks at the category level but managing risks at the category level is not required for implementation of this practice.

AIM-Categorization-Tiering: Consolidating identified risks into categories aligns with **RISK** management. This helps in more effective analysis and response to cyber risks by managing them at the category level.

RISK-2e

Cyber risk categories and cyber risks are documented in a risk register or other artifact.
The risk register is an inventory of all identified risks and their attributes, such as their risk statements, priorities, risk category (as defined in RISK-2d), and impact evaluation data. The risk register ensures that all identified risks are managed and that all staff involved in risk management activities are using the same risk information. The risk register may be used to manage risks individually or at the category level as defined in RISK-2d. For example, if an analyst identifies new indicators that change a previously identified risk, they can be added to the register and so that the information is available to all risk management stakeholders.

AIM-Categorization-Tiering: Documenting cyber risk categories and risks in a risk register aligns with **RISK** management. It ensures that all identified risks are consistently tracked and managed.

RISK-2f

Cyber risk categories and cyber risks are assigned to risk owners.
The risk owner should be the person who has the authority and authorization within the organization to make decisions about how to respond to specific risk categories and risks and to assign budget for risk responses. Remember that a legitimate (but potentially harmful) response to a risk is to accept the risk. The risk owner must have the authority to accept a risk.
For a risk owner to fully accept a risk, it is important that they understand the risk and the potential impacts that may occur if the risk is realized. To determine if a risk owner has adequate authority for accepting a risk, it may help to consider whether the potential impacts of the risk may extend beyond the scope of her or his authority. It may also help to consider whether the potential risk owner has adequate authority and resources within her or his purview to make appropriate changes if the risk is deemed outside of the organization's risk tolerance.
Assignment of a risk to a risk owner may involve some form of written attestation of their ownership of the risk. Assignment of ownership at the right level of authority helps ensure that risk responses are effectively executed.

AIM-Categorization-Tiering: Assigning cyber risk categories and risks to risk owners relates to **PROGRAM** management. It ensures that the appropriate authority is in place to manage and respond to risks effectively.

RISK-2g

Cyber risk identification activities are performed periodically and according to defined triggers, such as system changes and external events.
Cyber risks that can affect IT, OT, and information assets must be identified and addressed in order to actively manage the resilience of those assets and, more importantly, the services to which the assets are connected. The organization may use a structured risk assessment method to identify these risks according to triggers such as system changes and external events as established in the risk management strategy.
Risk assessments provide the necessary information to determine if identified risks are within the risk tolerances of the organization. Assessments also take existing mitigations and protections into account as part of the process. Risks identified via assessments should be added to the risk register, as recommended in RISK-2e.

AIM-Categorization-Tiering: Performing periodic cyber risk identification activities based on defined triggers aligns with **SITUATIONAL AWARENESS**. This ensures that risks are identified and managed in response to changing conditions and events.

RISK-2h

Cyber risk identification activities leverage asset inventory and prioritization information from the ASSET domain, such as IT and OT asset end of support, single points of failure, information asset risk of disclosure, tampering, or destruction.
The disruption of asset productivity due to operational risk affects the ability of associated functions to meet their mission. Thus, the scope of risk assessments should focus on assets and activities whose disruption has the most potential impact on mission assurance. The asset inventory should include criteria that identifies assets that are most critical to the function.

AIM-Categorization-Tiering: **ASSET, CHANGE AND CONFIGURATION** is relevant because the activities described involve leveraging asset inventory and prioritization information, focusing on the management and control of IT and OT assets, including their end of support and single points of failure. **RISK** is involved as the focus is on cyber risk identification and risk assessments, aiming to understand and mitigate the potential impacts on mission assurance due to operational risks. **THREAT AND VULNERABILITY** is also pertinent because the identification of risks related to the disclosure, tampering, or destruction of information assets is central to assessing and mitigating security threats and vulnerabilities that could disrupt critical functions.

RISK-2i

Vulnerability management information from THREAT domain activities is used to update cyber risks and identify new risks (such as risks arising from vulnerabilities that pose an ongoing risk to the organization or newly identified vulnerabilities).
Vulnerability information sources identified in the THREAT domain should be used in conjunction with the risk management process to identify new risks and update existing risks. For example, a new risk should be identified if a vendor publicly discloses a vulnerability that affects an IT asset.

AIM-Categorization-Tiering: Using vulnerability management information to update and identify new risks aligns with **THREAT AND VULNERABILITY**. This ensures that emerging vulnerabilities are considered in the risk management process.

RISK-2j

Threat management information from THREAT domain activities is used to update cyber risks and identify new risks.
Threat information sources identified in the THREAT domain should be used in conjunction with the risk management process to identify new risks and update existing risks. For example, a new risk should be identified if threat intelligence indicates that a threat actor may be targeting the organization.

AIM-Categorization-Tiering: Utilizing threat management information for updating and identifying new risks also aligns with **THREAT AND VULNERABILITY**. This ensures that threat intelligence is integrated into the risk management process.

RISK-2k

Information from THIRD-PARTIES domain activities is used to update cyber risks and identify new risks.
Information from THIRD-PARTIES activities should be used to identify new risks and update existing risks. For example, if open source information indicates that an equipment supplier has been breached, the organization should consider the impact and log a risk in the risk register.

AIM-Categorization-Tiering: Leveraging information from third parties to update and identify new risks relates to **LEGAL AND REGULATORY FRAMEWORK**. This ensures that third-party risks are incorporated into the organization's risk management activities.

RISK-2l

Information from ARCHITECTURE domain activities (such as unmitigated architectural conformance gaps) is used to update cyber risks and identify new risks.
Periodic or continual evaluation should be leveraged to determine conformance gaps between the organization's systems and networks and the cybersecurity architecture. Gaps in conformance should be logged as risks and remediation plans formed to close the gaps. The remediation plans should include information such as necessary resources to complete remediation and dates by which remediation will be completed.

AIM-Categorization-Tiering: Using information from architecture domain activities to update and identify new risks emphasizes **ARCHITECTURE**. It ensures that architectural gaps are identified and addressed as part of the risk management process.

RISK-2m

Cyber risk identification considers risks that may arise from or impact critical infrastructure or other interdependent organizations.
Dependencies that exist between other critical infrastructure and interdependent organizations should be understood. If a utility service or other dependent service is not available for a significant duration, the organization should have an understanding of how this would impact operations. For example, if a natural disaster is impacting an internet service provider's ability to provide internet services, risks that would stem from degraded communications between geographically dispersed organizational units and how it impacts the function should be considered and logged in the risk register.

AIM-Categorization-Tiering: Considering risks that may arise from or impact critical infrastructure or other interdependent organizations aligns with **SITUATIONAL AWARENESS**. This ensures that external dependencies and their potential impacts are included in the risk management process.

3.3 Analyze Cyber Risk

RISK-3a

Cyber risks are prioritized based on estimated impact, at least in an ad hoc manner.
Potential impact to the organization of identified risks should be evaluated and used to prioritize cyber risks. A higher priority cyber risk should receive greater attention when determining potential mitigations or responses.

Prioritization should focus on criteria deemed important to the enterprise such as safety impacts, operational impacts, and financial impacts (e.g., cost of recovery, potential cost of downtime or lost data). Prioritization may use qualitative methods to indicate relative impact level (e.g., High, Medium, Low).

AIM-Categorization-Tiering: Prioritizing cyber risks based on estimated impact aligns with **RISK** management. This ensures that higher priority risks receive the necessary attention for mitigation or response.

RISK-3b

Defined criteria are used to prioritize cyber risks (for example, impact to the organization, impact to the community, likelihood, susceptibility, risk tolerance).
Potential consequences and other aspects of identified risks should be evaluated and prioritized using the risk criteria in a consistent manner. Risks may be categorized by source, type of threat, or another commonality. This analysis helps determine which risks merit the most attention given the organization's unique operating circumstances, as well as how quickly they should be addressed.
A relative priority should be assigned to each risk (perhaps by category) using a consistent prioritization scheme. The intent of prioritization is to determine the cyber risks that most need attention because of their potential to affect operations. Typical components of an approach for risk prioritization include flow diagrams depicting the prioritization process, inputs to and outputs of the process, a list of relevant stakeholders involved in risk prioritization, and a scheme for ranking risks (high, medium, low, etc.).
Categorization and prioritization of risks help to right-size the number of risks being managed, as well as the amount of time and effort that an organization devotes to the management of identified cyber risks.

AIM-Categorization-Tiering: Using defined criteria to prioritize cyber risks emphasizes **STANDARDS AND TECHNOLOGY**. This ensures that risks are evaluated and prioritized consistently across the organization.

RISK-3c

A defined method is used to estimate impact for higher priority cyber risks (for example, comparison to actual events, risk quantification).
A defined method to estimate the impact of risks and risk categories (e.g., safety impacts, operational disruption, potential cost of downtime, cost of lost data, and cost of recovery) is beneficial since it provides a common comparison point for risks. This method helps identify and prioritize the most critical risks that could impact operations. Mathematical or statistical methods may be used to determine a value such as the potential cost if a risk is realized.

AIM-Categorization-Tiering: Using a defined method to estimate the impact of higher priority risks relates to **RISK** management. It ensures that the most critical risks are identified and prioritized based on their potential impact.

RISK-3d

Defined methods are used to analyze higher priority cyber risks (for example, analyzing the prevalence of types of attacks to estimate likelihood, using the results of controls assessments to estimate susceptibility).
A defined method to analyze risks and risk categories after prioritization ensures that analysis activities are repeatable and produce consistent results. Outputs from organizational processes or continual testing such as controls assessments may help the organization determine the susceptibility to a newly identified vulnerability.

AIM-Categorization-Tiering: Using defined methods to analyze higher priority risks aligns with **THREAT AND VULNERABILITY**. This ensures that risk analysis is consistent and considers susceptibility to new vulnerabilities.

RISK-3e

Organizational stakeholders from appropriate operations and business functions participate in the analysis of higher priority cyber risks.
Organizational stakeholders from appropriate areas of the organization are necessary for comprehensive analysis of prioritized cyber risk categories and cyber risks. Specific stakeholders may be more appropriate for analyzing certain cyber risks or cyber risk categories and provide insight that cannot be gained from others in the organization. Additionally, stakeholders from various parts of the organization will provide different perspectives that will help gain a full understanding of risks and potential mitigations.

AIM-Categorization-Tiering: Involving organizational stakeholders in the analysis of higher priority risks emphasizes **CULTURE AND SOCIETY**. This approach ensures diverse perspectives contribute to a comprehensive understanding and mitigation of risks.

RISK-3f

Cyber risks are removed from the risk register or other artifact used to document and manage identified risks when they no longer require tracking or response.
Once analysis by risk management stakeholders indicates that the realization of a cyber risk is no longer likely or the impact is not material, the risk should be removed from the risk register or other artifact that is used to document and manage identified risks. A defined process for removing risks should be followed that includes archiving analysis information and any lessons learned information that could be leveraged in the management of similar cyber risks in the future.
Cyber risk categories that no longer serve a purpose in the risk management process should also be removed. As the organization remediates the causes of risks, some cyber risk categories may become unnecessary or redundant. Removing cyber risk categories and cyber risks once eliminated or impact is not material will help the organization more efficiently manage remaining risks. For example, the organization may remove a cyber risk related to an operating system if that operating system is no longer in use within the organization.

AIM-Categorization-Tiering: Removing cyber risks from the risk register when no longer necessary aligns with **RISK** management. This ensures efficient management of remaining risks by eliminating redundant or resolved risks.

RISK-3g

Cyber risk analyses are updated periodically and according to defined triggers, such as system changes, external events, and information from other model domains.
Cyber risks that can affect IT, OT, and information assets should be analyzed periodically or according to defined triggers to determine if criteria such as impact or probability have changed. An increased probability of a risk being realized may drive a change to the priority of the cyber risk and a different strategy to mitigate the cyber risk.

For each cyber risk, the organization should assign a date by which the risk must be reevaluated or a defined trigger that would drive reevaluation. Triggers may include a date on which an asset is no longer supported by a vendor or an internal metric that has exceeded a tolerance level.

AIM-Categorization-Tiering: Updating cyber risk analyses periodically and based on defined triggers aligns with **SITUATIONAL AWARENESS**. This ensures that risk analyses remain current and responsive to changing conditions and events.

3.4 Respond to Cyber Risk

RISK-4a

Risk responses (such as mitigate, accept, avoid, or transfer) are implemented to address cyber risks, at least in an ad hoc manner.
Once risks to the function are identified, the organization should decide how to respond to those risks. Response begins with assigning a risk disposition to each risk or risk category, that is, a statement of the organization's intention for addressing the risk. For example, risk mitigation involves taking active steps to minimize the risk; risk transfer is the contractual shifting of a risk from one party to another through a contract, such as through an insurance policy, a liability waiver with a client, or an indemnification agreement with a supplier.
Risk responses should be developed as part of the risk management strategy. Risk responses can vary widely across organizations but typically include:

- risk avoidance—altering operations to avoid the risk while still providing the essential service
- risk acceptance— acknowledgment of the risk but consciously not taking any action (in essence, accepting the potential consequences of the risk)
- risk transfer—assigning the risk to a willing and able entity
- risk mitigation—taking active steps to minimize the risk
- risk monitoring— performing further research and deferring action on the risk until the need to address the risk is apparent

Organizational risk response selection processes should clarify that it is not necessary to mitigate every identified risk. Risk avoidance, acceptance, or transfer should be considered in addition to mitigation.

AIM-Categorization-Tiering: Implementing risk responses to address cyber risks relates to **RISK** management. This includes deciding how to respond to each identified risk through various strategies such as mitigation, acceptance, avoidance, or transfer.

RISK-4b

A defined method is used to select and implement risk responses based on analysis and prioritization.
The organization should develop a defined list of acceptable risk responses and the definition of each response. It may be necessary to define approvals that are necessary for certain risk response strategies, such as accepting a risk. Processes for other risk response strategies such as transference should also be considered to ensure that

cyber risks have an individual responsible for tracking them to closure.

AIM-Categorization-Tiering: Using a defined method to select and implement risk responses based on analysis and prioritization is part of **STANDARDS AND TECHNOLOGY**. This ensures that risk response strategies are consistent and well-documented.

RISK-4c

Cybersecurity controls are evaluated to determine whether they are designed appropriately and are operating as intended to mitigate identified cyber risks.
Cybersecurity control effectiveness should be evaluated by comparing the intended outcome of cybersecurity controls to the actual outcome. The organization may use performance metrics or other defined indicators to identify cybersecurity controls that are not designed appropriately. For example, if a biometric authentication device has a high false negative rate and exceptions are made for personnel access, the configuration of the control should be evaluated to determine if tuning is necessary to improve performance of the device.

AIM-Categorization-Tiering: Evaluating cybersecurity controls to determine their effectiveness relates to **STANDARDS AND TECHNOLOGY**. This ensures that controls are properly designed and functioning as intended to mitigate identified risks.

RISK-4d

Results from cyber risk impact analyses and cybersecurity control evaluations are reviewed together by enterprise leadership to determine whether cyber risks are sufficiently mitigated and risk tolerances are not exceeded.
Unique insight can be gained from the fusion of results from cyber risk impact analyses and cybersecurity control evaluations. For example, enterprise leadership may determine that moving some systems to the cloud increases availability and improves operations of an organization, but a cybersecurity control evaluation finds that misconfigurations of the environment could lead to compromise of confidentiality.

AIM-Categorization-Tiering: Reviewing results from risk impact analyses and control evaluations together by enterprise leadership aligns with **POLICY AND STRATEGY**. This approach ensures that leadership can make informed decisions about risk mitigation and risk tolerance.

RISK-4e

Risk responses (such as mitigate, accept, avoid, or transfer) are reviewed periodically by leadership to determine whether they are still appropriate.
Risk responses and defined methods to implement risk responses should be reviewed periodically to determine if they are still appropriate and effective at managing cyber risk for the organization. Changes in the operational environment such as new technology, new services, or new strategic partnerships may cause the organization to modify existing response strategies, create new response strategies, or retire response strategies.

AIM-Categorization-Tiering: Periodically reviewing risk responses to ensure their appropriateness and effectiveness is part of **RISK** management. This ensures that risk responses remain relevant in the context of changing operational environments.

3.5 Management Activities

RISK-5a

Documented procedures are established, followed, and maintained for activities in the RISK domain.
The activities in the RISK domain, such as risk identification, risk impact estimation, and risk response implementation are formally documented in some way (such as standard operating procedures, process flow diagrams, RACI charts, and swim lane diagrams). The activities are intentionally designed or described to serve the organization rather than being ad hoc. Documenting procedures helps ensure that they are repeatable and produce expected outcomes. The level of detail included in documentation should be a sufficient to enable consistent performance of domain activities by different people and new employees assuming relevant domain experience and sufficient on-board training.
Also, procedure documentation is made available to and is used by relevant personnel. The documentation is updated as needed to reflect changes in the organizational or operational environment. Additionally, organizations may consider including exceptions processes in documented procedures to ensure that the organization reacts appropriately to unexpected events or situations.

AIM-Categorization-Tiering: **RISK** is clearly relevant as the focus is on documenting procedures for risk identification, risk impact estimation, and risk response implementation. **POLICY AND STRATEGY** is involved because establishing, following, and maintaining documented procedures aligns with creating and implementing clear and effective policies and strategies for managing risks. **KNOWLEDGE AND CAPABILITIES** are also pertinent since the documentation and updating of procedures ensure that personnel have the necessary knowledge and can consistently perform risk domain activities, thereby maintaining and enhancing their skills and capabilities.

RISK-5b

Adequate resources (people, funding, and tools) are provided to support activities in the RISK domain.
When determining the adequacy of resources, it may help to consider whether there are any RISK domain activities not currently being performed that the organization would perform if it had additional people, funding, or tools. An additional consideration may be whether the organization has implemented all practices it has targeted for implementation and whether additional resources are necessary to address potential gaps.
Adequate resources are provided in the form of people, funding, and tools to ensure that RISK domain practices can be performed as intended. The performance of this practice can be evaluated by determining whether any desired practices have not been implemented due to a shortage of resources.
These are examples of people involved in RISK domain activities:

- staff responsible for defining risk criteria
- staff responsible for identifying risks
- staff responsible for developing and maintaining a risk taxonomy

These are examples of tools that might be used in RISK domain activities:

- methods for tracking open risks to closure
- techniques for identifying risks, such as interview techniques, questionnaires, and surveys

· quantitative methods for evaluating risk impacts

Adequacy of resources should be determined on an ongoing basis through regular reviews of the domain program and reviews of domain resources in budgeting activities. It is a common point of concern that there is not enough time to complete cybersecurity program activities. This is addressed primarily through increasing staff and secondarily through increasing funding and tools.
When determining the adequacy of staff, also consider whether the cybersecurity program has sufficient capacity so that the individuals that make up the program can regularly attend training, implement and maintain tools, and respond to incidents while conducting day-to-day operations and meeting the cybersecurity objectives of the organization.

AIM-Categorization-Tiering: Providing adequate resources for risk domain activities is part of **WORKFORCE** and **PROGRAM**. This ensures that the necessary people, funding, and tools are available to perform risk management activities effectively.

RISK-5c

Up-to-date policies or other organizational directives define requirements for activities in the RISK domain.
Activities in the RISK domain receive documented guidance and direction from the organization in the form of policies or similar directives. Strategic business objectives drive the development of documented policies or other organizational directives to ensure activities support the accomplishment of the organization's mission.
Policies or other organizational directives for risk management may contain

· responsibility, authority, and ownership for performing RISK domain activities

· procedures, standards, and guidelines for risk management activities, such as identifying sources and categories of risk and determining risk responses

· risk criteria

· list of triggers that initiate risk identification activities

· methods for measuring adherence to policy, exceptions granted, and policy violations

· procedures for the granting and management of exceptions

AIM-Categorization-Tiering: Defining requirements for risk domain activities through up-to-date policies or directives aligns with **POLICY AND STRATEGY**. This provides clear guidance and ensures alignment with organizational objectives.

RISK-5d

Responsibility, accountability, and authority for the performance of activities in the RISK domain are assigned to personnel.
The intent of this practice is that specific people (or people in specific roles) are held accountable for ensuring the achievement of expected results of RISK domain activities and that they are given the appropriate authority to act and to perform their assigned responsibilities.
These are examples of how to formalize responsibility and authority for RISK domain activities:

- defining roles and responsibilities in policies (see RISK-3c)
- developing position descriptions and conducting associated performance management activities
- including process tasks and responsibility for these tasks in position descriptions
- developing and implementing contractual instruments (including service level agreements) with external entities to establish responsibility and authority for performing RISK domain tasks on outsourced functions
- including RISK domain tasks in measuring performance of external entities against contractual instruments

Additionally, consider how the knowledge developed by personnel within this domain should be managed and shared. This includes determining what processes and tools should be used for knowledge sharing and identifying who will be responsible for making the best use of internal knowledge.

AIM-Categorization-Tiering: Assigning responsibility, accountability, and authority for risk domain activities to personnel is part of **WORKFORCE**. This ensures that individuals are clearly designated to manage risk activities and have the authority to do so.

RISK-5e

Personnel performing activities in the RISK domain have the skills and knowledge needed to perform their assigned responsibilities.
The organization must identify the skills and knowledge needed to perform RISK domain activities and identify skill and knowledge gaps in existing personnel. The organization can address gaps either by hiring qualified personnel or training existing personnel. It is important to note that managing and securing many technologies (such as virtualized or cloud-based environments) require specific training in specialized equipment and practices. Care should be taken to ensure that the level of skills and knowledge of personnel managing and securing specialized technologies is commensurate with the importance of and risk posed by those technologies.
Additionally, skill and knowledge assessments should be repeated as operational environments change over time. For example, in the RISK domain, skills and knowledge are needed for

- tools, techniques, and methods used to identify, analyze, mitigate, and monitor operational risks
- developing, implementing, and monitoring risk responses
- managing a risk register
- defining organizational risk criteria

AIM-Categorization-Tiering: Ensuring personnel have the necessary skills and knowledge to perform risk domain activities aligns with **WORKFORCE** and **KNOWLEDGE AND CAPABILITIES**. This ensures that employees are properly trained and capable of managing risks effectively.

RISK-5f

The effectiveness of activities in the RISK domain is evaluated and tracked.
The organization should measure the performance of RISK activities to ensure they are being performed as described in plans, policies, and procedures for the RISK domain. Appropriate metrics should be developed and collected to detect deviations in performance and measure the extent to which RISK domain activities are achieving their intended purpose.

AIM-Categorization-Tiering: Evaluating and tracking the effectiveness of risk domain activities is part of **RISK**. This ensures that risk management activities are effective and align with organizational goals.

4. Identity and Access Management - 35 questions

As presented on the platform, its purpose is: Create and manage identities for entities that may be granted logical or physical access to the organization's assets. Control access to the organization's assets, commensurate with the risk to critical infrastructure and organizational objectives.

The Identity and Access Management (ACCESS) domain comprises four objectives:

1. Establish Identities and Manage Authentication
2. Control Logical Access
3. Control Physical Access
4. Management Activities for the ACCESS domain

4.1 Establish Identities and Manage Authentication

ACCESS-1a

Identities are provisioned, at least in an ad hoc manner, for personnel and other entities such as services and devices that require access to assets (note that this does not preclude shared identities).
Provisioning refers to the creation or registration of identities. This involves identifying the entity and documenting attributes such as role and position in the organization.
Provisioning is performed for persons, devices, systems, and processes, whether internal or external to the organization. Thus, a vendor, agency, or business partner may be registered as an identity by the organization, as could a system or process from an external organization. In some cases, organizations may need to use shared identities, such as group accounts.
A best practice for provisioning is the identity profile. The profile contains all of the relevant information necessary to describe the unique attributes, roles, and responsibilities of the associated entity. The identity profile is generally initiated and approved by the organizational unit or line of business to which the entity belongs and where decisions about use of organizational assets can be made.

AIM-Categorization-Tiering: Can be categorized under **ASSET, CHANGE AND CONFIGURATION**, as it involves managing access to organizational assets by identifying entities and documenting their attributes to ensure authorized access only. It is also related to **WORKFORCE**, since provisioning identities is crucial for

controlling access to systems and data by employees, contractors, and external partners, thereby securing the organization's operations. Furthermore, **POLICY AND STRATEGY** is relevant because effective provisioning of identities is part of broader information security policies and strategies, defining roles and responsibilities and creating identity profiles to establish clear and effective access control policies. Finally, it aligns with **STANDARDS AND TECHNOLOGY**, as identity provisioning typically involves using established standards and technologies to create and manage identities securely, ensuring adherence to recognized cybersecurity standards and enhancing the security of the organization's systems and data.

ACCESS-1b

Credentials (such as passwords, smartcards, certificates, and keys) are issued for personnel and other entities that require access to assets, at least in an ad hoc manner.
Prior to giving personnel and other entities access to organizational assets, the organization should issue credentials to prove that the individual requesting access has the necessary privileges to access the assets. Entities may include individuals (internal or external to the organization) as well as devices, systems, or processes that require access to assets. The privileges associated with those credentials should be in line with the operational requirements.

AIM-Categorization-Tiering: Can be categorized under **ASSET, CHANGE AND CONFIGURATION**, as issuing credentials is part of managing access to critical systems and data, ensuring that only authorized entities can interact with these assets. It also relates to **WORKFORCE**, since managing and issuing credentials is essential for controlling access to systems and data by employees, contractors, and external partners, securing the organization's operations. Additionally, this statement pertains to **STANDARDS AND TECHNOLOGY** because the issuance of credentials often involves established security standards and technologies to protect organizational systems and data. Finally, **POLICY AND STRATEGY** is relevant as issuing credentials should align with the organization's broader information security policies and strategies, ensuring that access control policies are clearly defined and effectively implemented.

ACCESS-1c

Identities are deprovisioned, at least in an ad hoc manner, when no longer required.
When a person, object, or entity ceases to exist in the organization, the associated identity and all of its access privileges and restrictions should be eliminated. The failure to deprovision an identity can result in significant operational risk to an organization because it may provide an identity to which an unauthorized (and perhaps unknown) person, object, or entity can associate. If this occurs and its access privileges have not been terminated, the identity can be stolen along with all of the existing privileges.

AIM-Categorization-Tiering: This also pertains to **WORKFORCE**, as deprovisioning involves managing the access rights of employees, contractors, and external partners, ensuring that only current, authorized personnel can access sensitive systems and data. Additionally, this process aligns with **POLICY AND STRATEGY** because effective deprovisioning is part of an organization's security policies and strategies, ensuring that access control policies are clearly defined and enforced to mitigate risks. Lastly, it is related to **THREAT AND VULNERABILITY** because failing to deprovision identities can lead to significant security risks, such as unauthorized access by former employees or malicious actors, which could compromise the organization's systems and data.

ACCESS-1d

Password strength and reuse restrictions are defined and enforced.
Password strength and reuse requirements may not be supported by all assets within the function. Where feasible, these requirements may be informed by safety and operational considerations, the organization's risk tolerance, the organization's threat profile (THREAT-2e), asset priority, the sensitivity of information, or other considerations.

AIM-Categorization-Tiering: Can be categorized under **STANDARDS AND TECHNOLOGY**, as establishing and enforcing password policies involves using recognized cybersecurity standards and technologies to protect organizational systems and data. This also pertains to **POLICY AND STRATEGY**, as defining password strength and reuse policies is part of an organization's broader security strategies and policies, ensuring clear guidelines are in place to manage and mitigate risks associated with weak or reused passwords. Additionally, this relates to **RISK**, as enforcing strong password policies helps in identifying, assessing, and managing risks associated with information security, ensuring that unauthorized access due to weak passwords is minimized. Finally, it connects to **THREAT AND VULNERABILITY**, as defining and enforcing these restrictions helps to identify, assess, and mitigate security risks associated with password-based threats and vulnerabilities, thereby enhancing the overall security posture of the organization.

ACCESS-1e

Identity repositories are reviewed and updated periodically and according to defined triggers, such as system changes and changes to organizational structure.
Periodic review of identities can help the organization ensure they remain viable and accurate. The periodic review should be performed by the organization with the intent of identifying identities that are no longer valid, are duplicated, or that have changed materially but were not detected by the change management process. Reviews may also uncover identities with invalid roles or responsibilities to which access privileges have been provisioned. Invalid or duplicated identities can result in unauthorized use and modification of information, use of systems and technology, or entry to and use of facilities.

AIM-Categorization-Tiering: It fits under **ASSET, CHANGE AND CONFIGURATION** because it involves the management and control of identity assets, ensuring they are accurate and up-to-date. This is also related to **THREAT AND VULNERABILITY**, as periodic reviews help identify and mitigate potential risks associated with invalid or duplicated identities that could be exploited. Additionally, this connects to **RISK**, as managing identities effectively is crucial for minimizing security breaches and unauthorized access. Finally, **STANDARDS AND TECHNOLOGY** are implicated, as established standards and technologies are employed to review and update identity repositories systematically.

ACCESS-1f

Identities are deprovisioned within organization-defined time thresholds when no longer required.
Deprovisioning should occur as a result of the staff change or termination process. The organization should define a time-based requirement within which the deprovisioning should be done. For example, upon a termination, deprovisioning should occur immediately; for staff transitions to new positions, the time frame might be longer.
For timely deprovisioning to be possible, there must be a process for human resources departments to feed termination information to those who are responsible for maintaining the organization's identity repositories. De-

provisioning may also be the result of corrective actions taken after a review to remedy situations where the time thresholds were not met.

AIM-Categorization-Tiering: It fits under **WORKFORCE** because it involves managing access based on employee status changes, ensuring that only authorized individuals have access to sensitive systems and data. It also relates to **ASSET, CHANGE AND CONFIGURATION** because it requires systematic control and updates of identity assets in response to organizational changes. Additionally, this statement is relevant to **RISK** as timely deprovisioning of identities is crucial for minimizing the risk of unauthorized access and potential security breaches. Finally, it connects to **POLICY AND STRATEGY** since it necessitates clear policies and procedures for managing identity deprovisioning effectively within defined time thresholds.

ACCESS-1g

The use of privileged credentials is limited to processes for which they are required.
Privileged accounts represent higher risk to IT and OT assets. An organization may control the use of privileged credentials through administrative means, such as a policy that restricts the use of a local administrative accounts to required tasks and prohibits use of privileged accounts for day-to-day work functions. Alternatively, an organization may implement technical controls to restrict privileged accounts from accessing resources that do not require elevated privileges.

AIM-Categorization-Tiering: It falls under **POLICY AND STRATEGY** because it involves establishing clear policies and strategies to manage the use of privileged credentials effectively. It is also relevant to **RISK** as controlling privileged accounts is crucial for minimizing the risks associated with unauthorized access and potential security breaches. Additionally, this statement relates to **STANDARDS AND TECHNOLOGY** since it involves implementing technical controls to enforce these policies, ensuring that privileged accounts are used only for their intended purposes. Finally, it connects to **THREAT AND VULNERABILITY** as it addresses the need to mitigate security risks associated with the misuse of privileged credentials.

ACCESS-1h

Stronger credentials, multifactor authentication, or single use credentials are required for higher risk access (such as privileged accounts, service accounts, shared accounts, and remote access).
The requirements for credentials used to access the organization's assets should be commensurate with the risk associated with the assets. If an organization uses a matrix for determining the potential impact and priority of risks, it may develop a companion matrix that specifies credential and authentication requirements for each level of impact. For example, for remote access to a system with risks that could result in significant impact (level 4 of 5) and a high likelihood of occurrence (level 4 of 5), a commensurate requirement might establish that personnel must use strong credentials, multifactor authentication, or single use credentials. In situations where strong credentials (such as MFA) may be warranted, but are precluded by technological limitations, consider implementing the strongest available authentication configurations and implementing compensating controls if deemed appropriate based on risk and operational considerations.
Multifactor authentication (MFA) involves the use of two or more factors to achieve verification of an identity. Factors include (1) something you know, such as a password, (2) something you have, such as a token, (3) something you are, such as a fingerprint, or (4) something that indicates you are where you say you are, such as a GPS token. For the example above, personnel could be required to authenticate using a login ID, a password, and a

token.
Single use credentials may be implemented through a privileged access management (PAM) solution. Functionality provided by a PAM include role-based access to privileged credentials, automated rotation of passwords, integration with MFA, and auditing of privileged credential use.
These are specific examples of access that may pose higher risk to the function:

- privileged accounts
- service accounts
- shared accounts (Use of these should be discouraged in general, but not possible in certain legacy IT and OT assets, where additional controls are appropriate such as stronger credentials as mentioned in this practice, strong physical access controls, or others.)
- remote access
- administrative accounts
- emergency access
- access to sensitive assets
- access to cloud or virtual asset management systems
- cryptographic key management accounts
- backup accounts

(Note that as requirements for stronger or multifactor credentials are established for more of these types of access, the higher the organization moves on the spectrum of maturity.).
Additionally, it is important to note that the word risk is being used in this practice in the general sense of the word and not intended to refer to any specific risks identified in the Risk Management domain of the C2M2. However, organizations should consider access to IT and OT assets and the controls applied to that access during the risk identification, analysis and response activities discussed in the Risk Management domain.

AIM-Categorization-Tiering: It primarily aligns with **STANDARDS AND TECHNOLOGY** as it involves the implementation of established cybersecurity technologies like multifactor authentication and single-use credentials. It also falls under **RISK** since the practice of using stronger credentials and authentication methods is directly tied to managing and mitigating risks associated with unauthorized access to high-risk accounts. Furthermore, the statement relates to **POLICY AND STRATEGY** as it underscores the need for a structured approach to credential management, including the development of matrices to determine authentication requirements based on risk assessments. Lastly, it touches on **THREAT AND VULNERABILITY** by addressing the identification and mitigation of vulnerabilities that can be exploited through weak or inadequate authentication methods.

ACCESS-1i

Multifactor authentication is required for all access, where feasible.
Multifactor authentication may not be supported by all assets within the function. Where feasible, stronger authentication controls, such as multifactor authentication reduce the risk of account misuse resulting from compromised credentials. Where multifactor authentication is not feasible, organizations may consider implementing mitigating controls depending on their risk appetite, threat environment, and operational needs.

AIM-Categorization-Tiering: Primarily, it aligns with **STANDARDS AND TECHNOLOGY** as it involves the implementation of multifactor authentication, an established cybersecurity standard, to protect access to systems and data. It also relates to **RISK** since the practice of using stronger authentication controls is directly tied to managing and mitigating risks associated with compromised credentials. Additionally, this statement pertains to **THREAT AND VULNERABILITY** by addressing the mitigation of security risks that arise from threats like credential compromise. Moreover, it touches on **POLICY AND STRATEGY** as it emphasizes the need for a structured approach to implementing authentication controls, considering the organization's risk appetite and operational needs.

ACCESS-1j

Identities are disabled after a defined period of inactivity, where feasible.
Enforcement of identity deprovisioning based on periods of inactivity can reduce the risk of a dormant account being misused or subject to malicious activity. The period of inactivity must be established by the organization commensurate with potential risk. For example, temporary identities supplied to contractors might be appropriately disabled after a period of 30 days or less. An organization may implement this control by first monitoring last logon timestamp or other attributes to identify potential periods of inactivity. Using this information, identities that have been inactive for a defined period of time can be identified and disabled or removed if no longer needed. The efficiency of this activity may be improved by developing a list of accounts that by nature have long periods of dormancy but are also still necessary to meet operational requirements. While this practice may be enforced by automated means, it is important to carefully consider the impacts to operations prior to implementing automated deprovisioning.

AIM-Categorization-Tiering: Primarily, it aligns with **RISK** since it involves managing the potential risks associated with dormant accounts, reducing the likelihood of misuse or malicious activity. It also relates to **THREAT AND VULNERABILITY** as it addresses mitigating security risks by disabling or removing inactive identities. Additionally, this statement pertains to **STANDARDS AND TECHNOLOGY** by highlighting the use of established cybersecurity practices such as monitoring logon timestamps and automating deprovisioning processes. Finally, it is relevant to **POLICY AND STRATEGY** as it requires the organization to establish clear policies regarding the period of inactivity and implement strategies for identity deprovisioning that consider operational impacts.

4.2 Control Logical Access

ACCESS-2a

Logical access controls are implemented, at least in an ad hoc manner.
Access controls are a key element of the protection provided to assets. Access privileges and restrictions describe

the level and extent of access provided to identities. Access privileges should be commensurate with the various roles represented by an identity.

AIM-Categorization-Tiering: Primarily, it aligns with **ASSET, CHANGE AND CONFIGURATION** as it focuses on the management and control of access to critical assets through logical access controls. This statement also relates to **STANDARDS AND TECHNOLOGY** by emphasizing the importance of implementing established access control standards and technologies to safeguard assets. Additionally, it pertains to **THREAT AND VULNERABILITY** as it involves mitigating risks associated with unauthorized access and ensuring that access privileges are appropriate for the roles represented by an identity. Lastly, it is relevant to **POLICY AND STRATEGY** since it involves defining and enforcing policies for access privileges and restrictions to protect organizational assets.

ACCESS-2b

Logical access privileges are revoked when no longer needed, at least in an ad hoc manner.
Asset owners and custodians are responsible for revoking logical access privileges when no longer required, such as upon an employee's termination or transition to a new role. Generally, staff should maintain the minimum set of privileges needed to perform their assigned responsibilities. Revoking logical access that is no longer required helps prevent aggregation of access privileges.

AIM-Categorization-Tiering: Primarily, it aligns with **ASSET, CHANGE AND CONFIGURATION** as it focuses on the management and control of access privileges to ensure that assets are protected by revoking access when it is no longer necessary. This statement also relates to **STANDARDS AND TECHNOLOGY** by emphasizing the importance of adhering to established access control standards and technologies to safeguard organizational assets. Additionally, it pertains to **THREAT AND VULNERABILITY** as it involves mitigating risks associated with excessive or unnecessary access privileges that could be exploited by malicious actors. Lastly, it is relevant to **POLICY AND STRATEGY** since it involves defining and enforcing policies for the revocation of access privileges to protect organizational assets and ensure that staff have only the access necessary to perform their roles.

ACCESS-2c

Logical access requirements are established and maintained (for example, rules for which types of entities are allowed to access an asset, limits of allowed access, constraints on remote access, authentication parameters).
It is the asset owner's responsibility to ensure that requirements for protecting and sustaining assets are defined for assets under the owner's control, including requirements for controlling logical access (for example, rules for which types of entities are allowed to access an asset, the limits of allowed access, constraints on remote access, and authentication parameters). For example, the logical access requirements for a specific asset might allow remote access by a vendor only during specified and preplanned maintenance intervals and might also require multifactor authentication for such access. As another example, it may be appropriate to apply additional logical access controls (such as peer review) to high-priority assets.
There are several models for access control, such as discretionary access control (DAC), mandatory access control (MAC), role-based access control (RBAC), policy-based access control (PBAC), and attribute-based access control (ABAC). Selection of an access control model will vary based on several factors, such as the operating environment and feasibility of implementation. For example, an organization may choose to implement an access

control model that is supported by current infrastructure, such as RBAC, and plan for future implementation of a more advanced model, such as ABAC, as part of an acquisition of new infrastructure the supports additional access control capabilities.
Advanced security models, such as Zero Trust, may also inform the development of access requirements. For example, implementation of Zero Trust principles may include the ability to collect and use additional information (such as behavioral information, geolocation information, threat intelligence, and other contextual information) as part of access policy enforcement.

AIM-Categorization-Tiering: It mainly falls under **ASSET, CHANGE AND CONFIGURATION** due to its emphasis on managing and controlling access to assets, specifying requirements for logical access, and ensuring asset protection. The responsibilities of asset owners to define and maintain logical access requirements underscore the importance of properly managing and configuring these assets. Additionally, it relates to **STANDARDS AND TECHNOLOGY** as it mentions the use of advanced security models and technologies such as multifactor authentication and Zero Trust principles to enhance access control measures. Furthermore, the statement touches on **POLICY AND STRATEGY** as it involves establishing rules and requirements for access control, which are essential components of an organization's cybersecurity policies and strategies. Lastly, **RISK** is relevant because the selection of appropriate access control models and the implementation of security measures directly influence the management and mitigation of risks associated with unauthorized access and potential security breaches.

ACCESS-2d

Logical access requirements incorporate the principles of least privilege.
The principle of least privilege is a security requirement that establishes limitations on authorized users only to the privileges they require to perform assigned tasks in accordance with their job responsibilities and roles and nothing more. Organizations employ the principle of least privilege when considering the assignment of access rights and controls for specific duties and systems (including specific functions, ports, protocols, and services). The principle of least privilege also applies to information system processes, ensuring that the processes operate at privilege levels no higher than necessary to accomplish required organizational missions and/or functions. Organizations consider the principle of least privilege in the creation of additional processes, roles, and information system accounts as necessary. Organizations also apply the principle of least privilege to the design, development, implementation, and operations of IT and OT systems. Enforcing the principle of least privilege is an important consideration for implementation of Zero Trust principles.

AIM-Categorization-Tiering: Primarily, it falls under **POLICY AND STRATEGY** as it involves establishing clear policies for access rights and controls, ensuring that only necessary privileges are granted in line with job responsibilities and roles. It also relates to **STANDARDS AND TECHNOLOGY** because the enforcement of the least privilege principle requires the use of specific security technologies and access control mechanisms, such as Zero Trust principles, to ensure that processes and systems operate with minimal necessary privileges. Additionally, it is relevant to **ARCHITECTURE** as the design, development, implementation, and operations of IT and OT systems must consider and integrate the least privilege principle to secure the technology infrastructure robustly. Finally, **RISK** is a key category since applying the principle of least privilege helps mitigate risks by limiting access to only what is necessary, thereby reducing the potential impact of security breaches and ensuring better protection of the organization's assets.

ACCESS-2e

Logical access requirements incorporate the principle of separation of duties.
This principle should be included in access requirements to avoid or reduce the potential impact of errors or malicious activities and to prevent potential fraud. For example, the individual requesting access should not also be the person granting access, and the person requesting access should be granted only the minimum set of privileges needed to perform assigned responsibilities. As noted elsewhere in the model, it is important to consider access privileges for devices, systems, and processes that require access to assets and how separation should be applied. For example, systems performing critical safety functions may require additional scrutiny regarding which people or entities may access them, including process control systems they protect.

AIM-Categorization-Tiering: It primarily falls under **POLICY AND STRATEGY** because it involves establishing clear policies that ensure different individuals handle different aspects of access management, thereby minimizing risks and preventing potential fraud. It also relates to **STANDARDS AND TECHNOLOGY** as implementing separation of duties often requires specific access control technologies and systems to enforce these policies effectively. Additionally, the statement is relevant to **RISK** since separating duties helps in mitigating risks associated with errors or malicious activities by distributing responsibilities and privileges among multiple individuals. Finally, it pertains to **ASSET, CHANGE AND CONFIGURATION** because managing and controlling access to critical assets requires careful consideration of who can access what, ensuring that no single individual has complete control over any asset, which helps in maintaining the integrity and security of the organization's information technology assets.

ACCESS-2f

Logical access requests are reviewed and approved by the asset owner.
Privileges for logical access to an asset are assigned and approved by asset owners, custodians, or authorized delegates based on the role of the person, object, or entity that is requesting access. The asset owner or custodian is responsible for granting logical access privileges based on the identity's role and the asset's cybersecurity requirements. Asset owners and custodians must be aware of which particular identities require access to their assets and must validate the requirement with respect to business and cybersecurity requirements before granting approval.

AIM-Categorization-Tiering: It primarily falls under **ASSET, CHANGE AND CONFIGURATION** because it involves managing and controlling access to an organization's assets, ensuring that privileges are assigned based on the role and identity of the person or entity requesting access. The involvement of asset owners and custodians in this process highlights the importance of asset management in maintaining security. Additionally, it relates to **POLICY AND STRATEGY** as it emphasizes the need for clear policies and procedures for reviewing and approving access requests, aligning with the organization's business and cybersecurity requirements. Furthermore, the statement is relevant to **STANDARDS AND TECHNOLOGY** since implementing effective logical access control requires the use of established cybersecurity standards and technologies to protect the organization's systems and data. Finally, **RISK** is also a key category because the review and approval of access requests by asset owners help mitigate risks by ensuring that access is granted only to those who have a legitimate need, thus reducing the potential for unauthorized access and security breaches.

ACCESS-2g

Logical access privileges that pose higher risk to the function receive additional scrutiny and monitoring.
Privileged access, service accounts, shared accounts, and remote access should be subject to stricter control than routine user access. Additional scrutiny might require that access requests are approved by more than one person or an individual with a higher level of authority than standard user access requests. Additional monitoring might entail logging the use of elevated privileges. As an example, in a mature organization, privileged access to shared accounts may be implemented through provisioned credentials that are valid only for the time needed to perform an approved change. Additionally, staff may be monitored through closed-circuit television and screen captures while those credentials are in use.
These are specific examples of access that may pose higher risk to the function:

- privileged accounts
- service accounts
- shared accounts
- remote access
- administrative accounts
- emergency access
- access to sensitive assets
- access to cloud or virtual asset management systems
- cryptographic key management accounts
- backup accounts

Additionally, it is important to note that the word risk is being used in this practice in the general sense of the word and not intended to refer to any specific risks identified in the Risk Management domain of the C2M2. However, organizations should consider access to IT and OT assets and the sufficiency of controls to manage access as potential sources of risk that should be considered in the risk identification, analysis and response activities discussed in the Risk Management domain.

AIM-Categorization-Tiering: It is closely related to **RISK**, as it emphasizes the importance of identifying, assessing, and managing risks associated with elevated access privileges, which can potentially lead to significant security breaches if not properly controlled. This statement also falls under **ASSET, CHANGE AND CONFIGURATION** because it involves the management and control of access to critical information technology assets, ensuring that privileged access is granted and monitored appropriately to protect these assets. Furthermore, the statement relates to **POLICY AND STRATEGY**, as it outlines the need for well-defined policies and procedures to manage high-risk access privileges, including additional approval and monitoring mechanisms to mitigate potential risks. Lastly, it is relevant to **STANDARDS AND TECHNOLOGY**, as implementing strict controls and monitoring for privileged access requires the use of established cybersecurity standards and advanced technologies to log and manage elevated privileges effectively.

ACCESS-2h

Logical access privileges are reviewed and updated to ensure conformance with access requirements periodically and according to defined triggers, such as changes to organizational structure, and after any temporary elevation of privileges.
Constant change in the operational environment creates the potential that at any time the current level of logical access provided to persons, objects, and entities (as reflected in access privileges) may not match the level of need based on current logical access requirements. The organization should define a schedule for regular review of logical access privileges to ensure that the requirements they have set for their assets are being implemented through proper assignment of logical access privileges and implementation of corresponding logical access controls.
Certain temporary events such as projects or incident responses may require granting situation-based privileged logical access. A logical access review should be a necessary step in the closeout process of those events.

AIM-Categorization-Tiering: It is closely related to **RISK**, as it emphasizes the importance of identifying and managing risks associated with access privileges, ensuring that they are appropriate for current needs and operational environments. This statement also falls under **ASSET, CHANGE AND CONFIGURATION**, as it involves the management and control of access to critical information technology assets, ensuring that access levels are periodically reviewed and adjusted according to defined triggers and organizational changes. Furthermore, is relevant to **POLICY AND STRATEGY**, as it outlines the need for establishing clear policies and procedures for the regular review and update of access privileges, including situation-based adjustments during temporary events. Lastly, it is connected to **STANDARDS AND TECHNOLOGY**, as the implementation of proper logical access controls and regular reviews require the use of established cybersecurity standards and technologies to ensure that access requirements are consistently met and updated as needed.

ACCESS-2i

Anomalous logical access attempts are monitored as indicators of cybersecurity events.
Monitoring is done on logical access attempts, and any anomalies detected (such as an attempted login with a user name that doesn't exist within the system) are tagged as requiring further review to determine whether they are indicators of cybersecurity events (rather than user error, for example).

AIM-Categorization-Tiering: Primarily, it is associated with **INCIDENT DETECTION AND RESPONSE**, as it involves the organization's ability to detect and respond to potential cybersecurity incidents by monitoring access attempts and reviewing anomalies. This practice ensures that any suspicious activities are flagged and investigated promptly, helping to prevent security breaches. Additionally, it falls under **SITUATIONAL AWARENESS**, as the organization needs to detect, analyze, and understand cybersecurity risks and threats in real-time, which includes identifying unusual access attempts. Furthermore, this practice aligns with **STANDARDS AND TECHNOLOGY**, as the use of established cybersecurity technologies and standards is crucial for monitoring and detecting anomalies in logical access attempts. Lastly, it pertains to **RISK**, as identifying and managing risks associated with anomalous access attempts is essential for protecting the organization's information assets and minimizing the impact of potential security threats.

4.3 Control Physical Access

ACCESS-3a

Physical access controls (such as fences, locks, and signage) are implemented, at least in an ad hoc manner.
For the purpose of the model, these controls are intended for the protection of IT, OT, and information assets (for example, locks that control entry to a data center). Additionally, it is important to consider that the effectiveness of some types of physical access controls, such as keys and badges, may be significantly impacted by the way in which they are managed and secured.

AIM-Categorization-Tiering: Firstly, it falls under **ARCHITECTURE** as it discusses the design and implementation of security measures like fences, locks, and signage to protect IT, OT, and information assets, which is essential for a secure infrastructure. Secondly, it pertains to **ASSET, CHANGE AND CONFIGURATION** because it involves the management and control of physical access to critical assets such as data centers. Additionally, it is relevant to **RISK** since the effectiveness of these controls, such as keys and badges, directly impacts how well the organization can protect its assets and mitigate potential security breaches. Furthermore, the statement touches on **POLICY AND STRATEGY** as it implies the need for establishing clear policies for managing and securing physical access controls to ensure their effectiveness.

ACCESS-3b

Physical access privileges are revoked when no longer needed, at least in an ad hoc manner.
Asset owners and custodians are responsible for revoking physical access privileges when they are no longer required by whoever (or whatever) they were assigned to, such as upon an employee's termination or transition to a new role. Generally, staff should maintain the minimum set of privileges needed to perform their assigned responsibilities. Revoking physical access that is no longer required helps prevent aggregation of access privileges.

AIM-Categorization-Tiering: Firstly, it falls under **ASSET, CHANGE AND CONFIGURATION** because it involves the management and control of access privileges to physical assets, ensuring that only those who need access have it. Secondly, it pertains to **POLICY AND STRATEGY** as it highlights the importance of establishing clear policies for revoking physical access when no longer needed, which is crucial for effective cybersecurity management. Additionally, it is relevant to **RISK** since revoking unnecessary physical access privileges helps mitigate potential security risks by preventing the accumulation of access privileges that could be exploited. Furthermore, the statement also touches on **WORKFORCE** because it discusses the responsibilities of asset owners, custodians, and staff in managing and maintaining appropriate access privileges.

ACCESS-3c

Physical access logs are maintained, at least in an ad hoc manner.
It is the asset owner's responsibility to ensure that logging of physical access meets the requirements for protecting and sustaining the asset under the owner's control. Logging may be completed via manual means such as a paper log or through automated means such as data collected via physical access control systems.

AIM-Categorization-Tiering: Firstly, it falls under **ASSET, CHANGE AND CONFIGURATION** because it involves the management and control of physical access to assets, ensuring proper logging to protect these assets. Secondly, it pertains to **POLICY AND STRATEGY** as it emphasizes the responsibility of asset owners to ensure

that logging meets the necessary requirements, highlighting the importance of establishing clear policies for logging practices. Additionally, it is relevant to **RISK** since maintaining physical access logs helps in monitoring and mitigating potential security breaches by providing a record of who accessed the assets and when. Furthermore, the statement touches on **ARCHITECTURE** because it includes both manual and automated means of logging, indicating the implementation of infrastructure to support these activities.

ACCESS-3d

Physical access requirements are established and maintained (for example, rules for who is allowed to access an asset, how access is granted, limits of allowed access).
It is the asset owner's responsibility to ensure that requirements for protecting and sustaining assets are defined for assets under the owner's control, including requirements for controlling physical access. For example, physical access requirements for vendor visits to a data center might require issuance of a temporary badge, escorted access, and a staff member monitoring the visitor's activities.

AIM-Categorization-Tiering: Firstly, it falls under **ASSET, CHANGE AND CONFIGURATION** because it involves the management and control of physical access to assets, ensuring that rules for access are clearly defined and maintained. Secondly, it pertains to **POLICY AND STRATEGY** as it highlights the importance of establishing clear policies for who is allowed to access assets, how access is granted, and the limits of allowed access, which are essential for effective cybersecurity management. Additionally, it is relevant to **RISK** since setting and maintaining physical access requirements helps mitigate potential security risks by ensuring that only authorized individuals have access to sensitive assets. Furthermore, the statement also touches on **WORKFORCE** because it discusses the responsibilities of asset owners and staff members in controlling and monitoring physical access, emphasizing the need for proper procedures and oversight.

ACCESS-3e

Physical access requirements incorporate the principle of least privilege.
The principle of least privilege should be incorporated whenever possible when determining physical access requirements to avoid or reduce the potential impact of errors or malicious activities. For example, the person requesting access to a facility should only be granted access to the areas needed to perform assigned responsibilities.

AIM-Categorization-Tiering: Firstly, it falls under **ASSET, CHANGE AND CONFIGURATION** because it involves managing and controlling physical access to assets, ensuring that access is granted only to areas necessary for performing assigned responsibilities. Secondly, it pertains to **POLICY AND STRATEGY** as it emphasizes the need for clear policies that incorporate the principle of least privilege, which is crucial for effective cybersecurity management. Additionally, it is relevant to **RISK** since implementing the principle of least privilege helps in minimizing the potential impact of errors or malicious activities by limiting access to only what is necessary. Moreover, the statement touches on **THREAT AND VULNERABILITY** because it addresses reducing vulnerabilities and mitigating threats through controlled access. Lastly, it is connected to **WORKFORCE** as it involves determining and enforcing access requirements for employees, ensuring that staff only have the minimum privileges needed to perform their tasks.

ACCESS-3f

Physical access requirements incorporate the principle of separation of duties.
The principle of separation of duties should be incorporated whenever possible when determining physical access requirements to avoid or reduce the potential impact of errors or malicious activity. For example, an employee may have physical access privileges to enter a facility but may not have access to a server closet.

AIM-Categorization-Tiering: It primarily falls under **ASSET, CHANGE AND CONFIGURATION** because it involves managing and controlling physical access to organizational assets by ensuring that access is segmented based on roles and responsibilities. Additionally, it pertains to **POLICY AND STRATEGY** as it underscores the importance of establishing clear policies for physical access that incorporate separation of duties, which is fundamental for effective cybersecurity management. This statement is also relevant to **RISK** since implementing the principle of separation of duties helps in mitigating risks by reducing the likelihood of errors or malicious activities through controlled and segmented access. Furthermore, it is connected to **THREAT AND VULNERABILITY** because addressing the potential impact of unauthorized access through the separation of duties is a way to manage and mitigate threats and vulnerabilities. Lastly, it is related to **WORKFORCE** as it involves determining and enforcing physical access requirements for employees, ensuring that staff have access only to the areas necessary for their specific roles, thereby promoting a secure operational environment.

ACCESS-3g

Physical access requests are reviewed and approved by the asset owner.
A procedure exists by which asset owners, custodians, or authorized delegates review and approve requests for assets that they are responsible for. Asset owners and custodians should be aware of which identities require access to their assets and be able to validate the requirement with respect to business and cybersecurity requirements before granting approval.

AIM-Categorization-Tiering: Primarily, it falls under **ASSET, CHANGE AND CONFIGURATION** because it involves managing and controlling access to an organization's critical assets. Ensuring that only authorized personnel have access to these assets is essential for maintaining their integrity and security. Additionally, this statement relates to **POLICY AND STRATEGY** as it underscores the importance of having clear procedures for access requests that align with both business and cybersecurity requirements. Furthermore, this statement is pertinent to **RISK** because reviewing and validating access requests before approval helps mitigate risks by ensuring that access is granted only to individuals who have a legitimate business need, thereby reducing the potential for unauthorized access and security breaches. Lastly, it connects to **WORKFORCE** as it involves the roles and responsibilities of employees in managing access to organizational assets, emphasizing the importance of awareness and accountability among asset owners and custodians.

ACCESS-3h

Physical access privileges that pose higher risk to the function receive additional scrutiny and monitoring.
Facilities or areas of facilities where assets that pose a higher risk to the function reside may have additional or stricter physical access controls. Additional scrutiny might mean that access requests are approved by more than one person or an individual with a higher level of authority than standard access requests. Additional monitoring might entail additional access logging requirements, additional surveillance of the environment, additional badging and escorting requirements for visitors. This may be implemented via an additional access factor(s), additional

logging, or active monitoring by security guards. As an example, an organization may have a general badging system for facility access but also require a PIN to be entered for physical access to a portion of the facility.
Additionally, it is important to note that the word risk is being used in this practice in the general sense of the word and not intended to refer to any specific risks identified in the Risk Management domain of the C2M2. However, organizations should consider access to IT and OT assets and the sufficiency of controls to manage access as potential sources of risk that should be considered in the risk identification, analysis and response activities discussed in the Risk Management domain.

AIM-Categorization-Tiering: Primarily, it falls under **THREAT AND VULNERABILITY** as it emphasizes identifying and mitigating the security risks associated with physical access to high-risk areas. This statement also relates to **ASSET, CHANGE AND CONFIGURATION** because it involves managing and controlling access to critical assets within the organization. Furthermore, the statement is pertinent to **RISK** as it discusses the consideration of risks related to physical access and the implementation of controls to mitigate these risks. Lastly, this statement connects to **POLICY AND STRATEGY** as it outlines the procedures for approving and monitoring access to high-risk areas, demonstrating a strategic approach to managing physical security and aligning it with the organization's broader cybersecurity policies and strategies.

ACCESS-3i

Physical access privileges are reviewed and updated.
Constant change in the operational environment creates the potential that at any time the current level of physical access provided to persons (as reflected in access privileges) may not match the level of need based on current physical access requirements. The organization should define a schedule for regular review of physical access privileges to ensure that the requirements they have set for their assets are being implemented through proper assignment of physical access privileges and implementation of corresponding physical access controls.
Certain temporary events such as projects or incident responses may require granting situation-based privileged physical access. A physical access review should be a necessary step in the closeout process of those events.

AIM-Categorization-Tiering: Firstly, **ASSET, CHANGE AND CONFIGURATION** is relevant because the review and updating of physical access privileges is a crucial part of managing and controlling an organization's information technology assets. This process ensures that access is properly aligned with current operational needs and security requirements. Additionally, **THREAT AND VULNERABILITY** is applicable since the review of physical access privileges is a proactive measure to identify and mitigate potential security risks associated with unauthorized access. **INCIDENT DETECTION AND RESPONSE** is also involved as situation-based privileged physical access may be necessary during incident responses, and a review of such access is vital for securing the environment post-incident. Lastly, **POLICY AND STRATEGY** is important because defining a schedule for regular reviews of physical access privileges reflects the organization's strategic approach to maintaining security through clear policies and procedures.

ACCESS-3j

Physical access is monitored to identify potential cybersecurity events.
Monitoring is done on physical access attempts, and any anomalies detected (such as unapproved access attempts) are tagged as requiring further review to determine whether they are indicators of cybersecurity events (rather than an error, for example).

AIM-Categorization-Tiering: Firstly, **INCIDENT DETECTION AND RESPONSE** is relevant because monitoring physical access attempts and tagging anomalies for further review is a key part of detecting and responding to potential cybersecurity incidents. Additionally, **THREAT AND VULNERABILITY** is applicable since the monitoring of physical access helps in identifying and mitigating security risks associated with unauthorized access attempts. Furthermore, **ASSET, CHANGE AND CONFIGURATION** is involved as the management and control of physical access to critical assets are essential to maintain their security. Finally, **POLICY AND STRATEGY**, because the implementation of systematic monitoring and review procedures reflects the organization's strategic approach to managing cybersecurity risks through well-defined policies and strategies.

4.4 Management Activities

ACCESS-4a

Documented procedures are established, followed, and maintained for activities in the ACCESS domain.
The activities in the ACCESS domain are formally documented in some way (such as standard operating procedures, process flow diagrams, RACI charts, and swim lane diagrams). The activities are intentionally designed or described to serve the organization rather than being ad hoc. Documenting procedures helps ensure that they are repeatable and produce expected outcomes. The level of detail included in documentation should be a sufficient to enable consistent performance of domain activities by different people and new employees (with relevant domain experience and sufficient on-boarding training).
Also, procedure documentation is made available to and is used by relevant personnel. The documentation is updated as needed to reflect changes in the organizational or operational environment. Additionally, organizations may consider including exceptions processes in documented procedures to ensure that the organization reacts appropriately to unexpected events or situations.

AIM-Categorization-Tiering: It emphasizes the importance of documented procedures, which falls under **POLICY AND STRATEGY**, as these procedures establish clear guidelines and strategies for managing the ACCESS domain. The statement also highlights the need for these procedures to be detailed enough to ensure consistent performance, which relates to **KNOWLEDGE AND CAPABILITIES**, as it requires personnel to have the necessary skills and knowledge to follow these procedures. Additionally, the mention of procedures being updated to reflect changes in the organizational or operational environment aligns with the **PROGRAM** category, as it underscores the necessity for a dynamic cybersecurity strategy that adapts to evolving circumstances.

ACCESS-4b

Adequate resources (people, funding, and tools) are provided to support activities in the ACCESS domain.
When determining the adequacy of resources, it may help to consider whether there are any ACCESS domain activities not currently being performed that the organization would perform if it had additional people, funding, or tools. An additional consideration may be whether the organization has implemented all practices it has targeted for implementation and whether additional resources are necessary to address potential gaps.
Adequate resources are provided in the form of people, funding, and tools to ensure that ACCESS domain practices can be performed as intended. The performance of this practice can be evaluated by determining whether any desired practices have not been implemented due to a shortage of resources.
These are examples of people involved in ACCESS domain activities:

- staff responsible for establishing identities and for authorizing and assigning roles to identities
- staff responsible for submitting access requests, and asset owners responsible for reviewing and approving access requests

These are examples of tools that might be used in ACCESS domain activities:

- access request and approval management systems and methods
- access privilege database systems
- tools, techniques, and methods for creating identity profiles, associating specific access privileges with roles, reviewing access privileges, and managing changes to identities

Adequacy of resources should be determined on an ongoing basis through regular reviews of the domain program and reviews of domain resources in budgeting activities. It is a common point of concern that there is not enough time to complete cybersecurity program activities. This is addressed primarily through increasing staff and secondarily through increasing funding and tools.
When determining the adequacy of staff, also consider whether the cybersecurity program has sufficient capacity so that the individuals that make up the program can regularly attend training, implement and maintain tools, and respond to incidents while conducting day-to-day operations and meeting the cybersecurity objectives of the organization.

AIM-Categorization-Tiering: It emphasizes the need for adequate resources, including people, funding, and tools, which aligns with the **PROGRAM** category as it relates to ensuring the cybersecurity program is well-supported and can achieve its objectives. The mention of staffing needs and the roles of various personnel involved in ACCESS domain activities ties into the **WORKFORCE** category, highlighting the importance of having the right people in place to carry out these activities. The focus on implementing desired practices and managing resources effectively connects to **POLICY AND STRATEGY**, as it involves planning and resource allocation to meet the organization's cybersecurity goals. Finally, the consideration of training and maintaining tools points to **KNOWLEDGE AND CAPABILITIES**, emphasizing the need for continuous skill development and the capacity to utilize appropriate tools and methodologies to protect the organization.

ACCESS-4c

Up-to-date policies or other organizational directives define requirements for activities in the ACCESS domain.
Activities in the ACCESS domain receive documented guidance and direction from the organization in the form of policies or similar directives. Strategic business objectives drive the development of documented policies or other organizational directives to ensure activities support the accomplishment of the organization's mission.
Policies or other organizational directives for the ACCESS domain may contain

- responsibility, authority, and ownership for performing ACCESS domain activities, including requesting, approving, and providing access
- rules for access requests that originate from outside of the organization
- procedures, standards, and guidelines for approving and provisioning identity profiles, assigning roles to identities, assigning access privileges to roles, and other ACCESS domain activities

- requirements for the frequency of reviewing and updating identity repositories and reviewing credentials
- time thresholds for deprovisioning identities
- procedures for the granting and management of exceptions
- procedures for measuring adherence to policy, exceptions granted, and policy violations

AIM-Categorization-Tiering: It emphasizes the importance of up-to-date policies and organizational directives that define requirements for activities in the ACCESS domain, aligning with **POLICY AND STRATEGY**, as it highlights the necessity of clear and well-communicated policies to guide these activities. The mention of strategic business objectives driving the development of these policies indicates a connection to the **PROGRAM** category, emphasizing that the directives are designed to support the organization's mission and align with its overarching cybersecurity strategy. Furthermore, the inclusion of specific rules, procedures, and standards for access requests, identity management, and policy adherence touches upon the **LEGAL AND REGULATORY FRAMEWORK** category, as these policies ensure compliance with relevant laws and regulations governing access control and data security.

ACCESS-4d

Responsibility, accountability and authority for the performance of activities in the ACCESS domain are assigned to personnel.
The intent of this practice is that specific people (or people in specific roles) are held accountable for ensuring the achievement of expected results of ACCESS domain activities and that they are given the appropriate authority to act and to perform their assigned responsibilities.
These are examples of how to formalize responsibility and authority for ACCESS domain activities:

- defining roles and responsibilities in policies (see ACCESS-3c)
- developing position descriptions and conducting associated performance management activities
- including process tasks and responsibility for these tasks in position descriptions
- developing and implementing contractual instruments (including service level agreements) with external entities to establish responsibility and authority for performing ACCESS domain tasks on outsourced functions
- including ACCESS domain tasks in measuring performance of external entities against contractual instruments

Additionally, consider how the knowledge developed by personnel within this domain should be managed and shared. This includes determining what processes and tools should be used for knowledge sharing and identifying who will be responsible for making the best use of internal knowledge.

AIM-Categorization-Tiering: It emphasizes the assignment of responsibility, accountability, and authority for activities in the ACCESS domain, which is central to the **PROGRAM** category, as it involves establishing clear roles and responsibilities within the organization's cybersecurity strategy. The statement also aligns with the **WORKFORCE** category, highlighting the importance of having the right personnel in place with the necessary

authority to perform their assigned responsibilities effectively. The inclusion of defining roles and responsibilities in policies and using contractual instruments with external entities connects to the **POLICY AND STRATEGY** category, as these actions ensure a structured and strategic approach to managing the ACCESS domain. Furthermore, the mention of managing and sharing knowledge developed by personnel within the domain aligns with **KNOWLEDGE AND CAPABILITIES**, emphasizing the need for processes and tools that facilitate effective knowledge management and sharing, thus enhancing the organization's overall cybersecurity capabilities.

ACCESS-4e

Personnel performing activities in the ACCESS domain have the skills and knowledge needed to perform their assigned responsibilities.
The organization must identify the skills and knowledge needed to perform ACCESS domain activities and identify skill and knowledge gaps in existing personnel. The organization can address gaps either by hiring qualified personnel or training existing personnel. It is important to note that managing and securing many technologies (such as virtualized or cloud-based environments) require specific training in specialized equipment and practices. Care should be taken to ensure that the level of skills and knowledge of personnel managing and securing specialized technologies is commensurate with the importance of and risk posed by those technologies.
Additionally, skill and knowledge assessments should be repeated as operational environments change over time. For example, in the ACCESS domain, skills and knowledge are needed for

- associating identities with roles and assign appropriate access privileges based on these
- managing identities in a manner appropriate for accessing each type of organizational asset
- tools, techniques, and methods used to manage and maintain identities
- tools, techniques, and methods used to manage access privileges

Additionally, consider how the knowledge developed by personnel within this domain should be managed and shared. This includes determining what processes and tools should be used for knowledge sharing and identifying who will be responsible for making the best use of internal knowledge.

AIM-Categorization-Tiering: It emphasizes the need for personnel performing activities in the ACCESS domain to possess the necessary skills and knowledge, highlighting the organization's responsibility to identify and address any skill and knowledge gaps. This aligns with the **WORKFORCE** category, as it focuses on the qualifications and competencies of employees involved in cybersecurity tasks. Additionally, the requirement for specific training in managing and securing specialized technologies ties into the **KNOWLEDGE AND CAPABILITIES** category, underscoring the importance of continuous learning and adaptation to evolving technological environments. The mention of conducting skill and knowledge assessments as operational environments change also relates to **PROGRAM**, as it involves ongoing evaluation and planning to ensure the organization's cybersecurity strategy remains effective and aligned with its business objectives.

ACCESS-4f

The effectiveness of activities in the ACCESS domain is evaluated and tracked.
The organization should measure the performance of ACCESS activities to ensure they are being performed as described in plans, policies, and procedures for the ACCESS domain. Appropriate metrics should be developed

and collected to detect deviations in performance and measure the extent to which ACCESS domain activities are achieving their intended purpose.

AIM-Categorization-Tiering: It emphasizes the importance of evaluating and tracking the effectiveness of activities in the ACCESS domain, aligning with the **PROGRAM** category, which focuses on the organization's cybersecurity strategy and planning. By measuring performance and ensuring activities are conducted according to established plans, policies, and procedures, the organization demonstrates its commitment to a comprehensive cybersecurity program. This also relates to **POLICY AND STRATEGY**, as it involves setting clear policies and strategic objectives for the ACCESS domain, including the development of appropriate metrics to monitor performance. Furthermore, the emphasis on detecting deviations and ensuring activities meet their intended purpose is crucial for managing **RISK**, as it allows the organization to identify potential vulnerabilities and take corrective actions to mitigate threats to its information assets.

5. Situational Awareness . 28 questions

As presented on the platform, its purpose is: Establish and maintain activities and technologies to collect, analyze, alarm, present, and use operational and cybersecurity information, including status and summary information from the other C2M2 domains, to form a Common Operating Picture (COP).

The Situational Awareness (SITUATION) domain comprises four objectives:

1. Perform Logging
2. Perform Monitoring
3. Establish and Maintain Situational Awareness
4. Management Activities for the SITUATION domain Logging should be enabled based on an asset's potential impact

5.1 Perform Logging

SITUATION-1a

Logging is occurring for assets that are important to the delivery of the function, at least in an ad hoc manner. Enable logging for important assets. Some activities that may be logged include the actions of persons, objects, and entities when they access and use assets, events that can disrupt delivery of the function, changes to assets that deviate from baseline configurations, unexpected assets connecting to networks, and any unexpected or suspicious activity. This may also include unintentionally powered off, deleted, or "resource exhausted" virtualized assets.

AIM-Categorization-Tiering: Relates primarily to **ASSET, CHANGE AND CONFIGURATION** and **INCIDENT DETECTION AND RESPONSE**. This is because logging activities for important assets help in the ongoing monitoring and maintenance of these assets, ensuring any changes or unexpected activities are tracked, which falls under the management and control of an organization's information technology assets. Additionally, this practice aids in the early identification of potential security threats and rapid response to incidents, which are key aspects of detecting, responding to, and recovering from cybersecurity incidents.

SITUATION-1b

Logging is occurring for assets within the function that may be leveraged to achieve a threat objective, wherever feasible.
This practice builds on the logging activities identified in SITUATION-1a to include assets that may be used in the pursuit of threat actor objectives. A threat actor may leverage multiple tactics, such as those defined in the MITRE ATT&CK Framework, to achieve their ultimate threat objective (for example, extortion, data manipulation, IP theft, customer data theft, sabotage). Logging may not be feasible for all types of assets within the function. Where logging is not feasible, organizations may consider implementing mitigating controls, such as limiting physical or logical access.

AIM-Categorization-Tiering: This practice is directly tied to **THREAT AND VULNERABILITY** because it involves identifying and monitoring assets that could be exploited by threat actors to achieve their objectives. Additionally, it is connected to **INCIDENT DETECTION AND RESPONSE** as it emphasizes the importance of logging activities to detect and respond to potential security incidents involving these assets. Furthermore, it pertains to **ASSET, CHANGE AND CONFIGURATION** since it involves the management and control of assets by ensuring proper logging and implementing mitigating controls where logging is not feasible, thereby maintaining the security and integrity of the organization's information technology assets.

SITUATION-1c

Logging requirements are established and maintained for IT and OT assets that are important to the delivery of the function and assets within the function that may be leveraged to achieve a threat objective.
Define logging requirements for all important IT and OT assets. For example, capturing failed login attempts can point to confidentiality issues, unauthorized changes can indicate integrity issues, and log entries on system down time can reveal availability issues. Requirements for logging may differ for different assets, such as operations technology, field devices, mobile devices, and assets that reside in the cloud. For virtual networks, additional tools or processes may be necessary to enable logging of virtual network traffic. Logs from the cloud, including both cloud infrastructure and cloud assets, should be defined by the organization in the logging requirements as applicable. In addition to the types of events to be logged, organizations should consider what logging requirements may be appropriate such as how logs are to be protected, chain of custody considerations, or retention timelines.
Example events that may be logged:

- 1. Operating system and application administration events
    - · account creation and deletion
    - · account privilege assignment
    - · configuration changes or software installation
- 2. Operating system and application usage events
    - · start up, shut down, and failure of services and applications
    - · network connections and failures
    - · successful and unsuccessful log on attempts
    - · application failures

- email and web traffic
- systems and files accessed by users

- 3. Events occurring on network devices such as
  - firewalls
  - switches
  - routers
  - wireless access points

- 4. Events occurring on OT devices such as
  - human machine interfaces (HMIs) and operator workstations
  - protection relays
  - programmable logic controllers (PLCs) and remote terminal units (RTUs)
  - smart meters

AIM-Categorization-Tiering: Establishing and maintaining logging requirements for IT and OT assets ensures proper management and control of these critical assets, which falls under **ASSET, CHANGE AND CONFIGURATION**. Furthermore, defining logging requirements for assets that could be leveraged to achieve a threat objective addresses the identification, assessment, and mitigation of security risks associated with threats and vulnerabilities, aligning with **THREAT AND VULNERABILITY**. Additionally, the use of established logging practices and technologies to capture important events, such as failed login attempts or unauthorized changes, aligns with **STANDARDS AND TECHNOLOGY** by utilizing cybersecurity standards and technologies to protect the organization's systems and data.

SITUATION-1d

Logging requirements are established and maintained for network and host monitoring infrastructure (for example, web gateways, endpoint detection and response software, intrusion detection and prevention systems).
Define logging requirements for all network and host monitoring infrastructure. These requirements may be different from other IT and OT assets as they may provide additional information that could be useful when building a complete understanding of activity within the organization's networks. For example, event logs from a web gateway that show connections to websites that were blocked because they violated the company's policy.

AIM-Categorization-Tiering: Establishing and maintaining logging requirements for network and host monitoring infrastructure ensures that the organization can detect, respond to, and recover from cybersecurity incidents, which aligns with **INCIDENT DETECTION AND RESPONSE**. Furthermore, defining these logging requirements involves the use of established cybersecurity standards and technologies to protect the organization's systems and data, which is related to **STANDARDS AND TECHNOLOGY**. Additionally, it involves the management and control of critical information technology assets, ensuring their configurations and changes are monitored and maintained, which falls under **ASSET, CHANGE AND CONFIGURATION**.

SITUATION-1e

Log data are being aggregated within the function.
Collect log data from different assets and aggregate it in a central repository. Aggregation may be performed within the function or elsewhere in the enterprise depending on several considerations such as enterprise architecture and regulatory requirements. The repository may be a simple log server, or log management infrastructure that includes centralized log servers and log data storage, or a vendor-supported security information and event management (SIEM) system. Doing so makes log data available even when individual assets are offline or destroyed. Aggregation can be especially beneficial for gathering information from operations technology assets with a limited ability to log locally. Additionally, by aggregating log data from various assets, the organization can correlate data to identify patterns and anomalies.

AIM-Categorization-Tiering: The practice of aggregating log data involves designing and implementing a robust technology infrastructure to centralize log data, which aligns with **ARCHITECTURE**. The use of centralized log servers or SIEM systems demonstrates the application of established cybersecurity technologies, linking it to **STANDARDS AND TECHNOLOGY**. The aggregation process also requires the management and control of information technology assets, reflecting **ASSET, CHANGE AND CONFIGURATION**. Finally, centralizing and correlating log data to identify patterns and anomalies is crucial for detecting, responding to, and recovering from cybersecurity incidents, which corresponds to **INCIDENT DETECTION AND RESPONSE**.

SITUATION-1f

More rigorous logging is performed for higher priority assets.
Logging requirements defined in SITUATION-1c and SITUATION-1d are enhanced to include consideration of asset-level risks that have been identified through risk management activities, so that more rigorous logging is performed for higher risk assets. In the context of this practice, more rigorous describes a logging approach that is complete and comprehensive, includes coverage of all key controls, is regularly reviewed and adjusted based on environmental changes, and is persistent and continuous (rather that intermittent and discrete.).
For example, for the management of virtualized assets, the organization may require additional log information to be captured such as user ID, timestamps, and the IP address of the user's terminal. Organizations that have very mature logging capabilities with no opportunity for further implementation of this practice as written should consider a response of fully implemented.
A list of example events that may be logged is provided in the help text for practice SITUATION-1c.

AIM-Categorization-Tiering: The practice of performing more rigorous logging for higher priority assets involves identifying and managing risks associated with different assets, which aligns with **RISK**. The use of enhanced logging requirements demonstrates the application of established cybersecurity standards and technologies, linking it to **STANDARDS AND TECHNOLOGY**. The comprehensive and continuous logging approach is crucial for detecting, responding to, and recovering from cybersecurity incidents, which corresponds to **INCIDENT DETECTION AND RESPONSE**. Additionally, considering asset-level risks and adjusting logging practices accordingly reflects the management and control of information technology assets, highlighting its relevance to **ASSET, CHANGE AND CONFIGURATION**.

5.2 Perform Monitoring

SITUATION-2a

Periodic reviews of log data or other cybersecurity monitoring activities are performed, at least in an ad hoc manner.
Regular review and audit of event logs (manually or by automated tools) is a critical monitoring activity that is essential for situational awareness (e.g., through the detection of cybersecurity events or weaknesses). For example, logs may provide data about changes in the user environment that can result in necessary changes in access privileges or trigger alerts when systems important to the delivery of the function are unavailable. Another example of this is unintentionally powered off, deleted, or "resource exhausted" virtualized assets that may trigger alerts to ensure administrators are aware of system updates or patches that may not have been applied to these systems while they were offline or unable to respond.

AIM-Categorization-Tiering: The regular review and audit of event logs support **SITUATIONAL AWARENESS** by enabling the organization to detect and understand cybersecurity risks and threats in real-time. This practice is crucial for **INCIDENT DETECTION AND RESPONSE** as it ensures early identification and appropriate response to potential security incidents. Furthermore, by identifying changes in the user environment and monitoring the status of virtualized assets, this activity aligns with **RISK** management by assessing and managing the risks associated with information security.

SITUATION-2b

Data and alerts from network and host monitoring infrastructure assets are periodically reviewed, at least in an ad hoc manner.
Anomalous activity is activity that is inconsistent with or deviating from what is usual, normal, or expected. Monitoring should provide the information that the organization needs to determine whether it is being subjected to a cybersecurity event that may require action to prevent organizational impact. This may include, for example, review of network log data to identify unauthorized connections to assets important to the delivery of the function. This may also include observations by control room personnel and other operations staff of unexpected system responses, sensor readings, or other unexplained activity exhibited by operational systems. Part of the intention of this practice is to include people as an element of an organization's overall approach to monitoring its systems.

AIM-Categorization-Tiering: The periodic review of data and alerts supports **SITUATIONAL AWARENESS** by enabling the organization to detect, analyze, and understand cybersecurity risks and threats in real-time. This practice also aligns with **INCIDENT DETECTION AND RESPONSE**, as it ensures that potential security events are identified and acted upon promptly to mitigate organizational impact. Additionally, by involving personnel in monitoring activities and including their observations, this practice fosters a security-conscious culture, linking it to **CULTURE AND SOCIETY** by promoting and integrating cybersecurity awareness among staff.

SITUATION-2c

Monitoring and analysis requirements are established and maintained for the function and address timely review of event data.
Monitoring and analysis requirements define the activities needed to provide information to stakeholders across the function on a regular basis to protect and sustain IT, OT, and information assets essential for the delivery of

the function. The development of requirements should identify key stakeholders and how the monitoring and analysis requirements will satisfy their information needs. Monitoring requirements may be different for assets such as operations technology, field devices, mobile devices, virtualized assets, and assets residing in the cloud. The requirements should describe what data should be collected and how it should be analyzed. Requirements should also specify time parameters for review of collected data and how the data will be distributed.
Requirements should consider:

- type of data and extent of data necessary
- the granularity of data necessary
- the format(s) of the data
- the distribution frequency of the data
- how the data will be distributed
- the retention of the data
- how often reviews should be performed

AIM-Categorization-Tiering: Establishing and maintaining monitoring and analysis requirements support **SITUATIONAL AWARENESS** by ensuring that the organization can detect, analyze, and understand cybersecurity risks and threats in real-time. It also relates to **ASSET, CHANGE AND CONFIGURATION**, as it involves the management and control of different types of assets, ensuring they are monitored appropriately based on their specific characteristics. Additionally, developing and maintaining these requirements is aligned with **POLICY AND STRATEGY**, as it involves defining clear policies and procedures to manage and mitigate risks, ensuring that all stakeholders' information needs are met and that there is a structured approach to monitoring and analysis.

SITUATION-2d

Indicators of anomalous activity are established and maintained based on system logs, data flows, network baselines, cybersecurity events, and architecture and are monitored across the IT and OT environments.
The organization should define and monitor for indicators of anomalous activity that are relevant to its operations. Indicators are signs that an incident may have occurred or may be occurring now. These might include failed login attempts, new device connections, port scanning, large volume file transfers, and availability variances for a system. Indicators may not necessarily be malicious, but they deviate from the norm and warrant additional monitoring.
Indicators of anomalous activity may also be identified through analysis of "near miss" cybersecurity events. These may include events internal to your organization or those occurring externally at another organization. Indicators may not necessarily be malicious, but they deviate from the norm and warrant additional monitoring.

AIM-Categorization-Tiering: Establishing and maintaining indicators of anomalous activity is crucial for **SITUATIONAL AWARENESS** as it enables an organization to detect, analyze, and understand cybersecurity risks and threats in real-time. It also aligns with **THREAT AND VULNERABILITY** because identifying and monitoring these indicators helps an organization assess and mitigate security risks associated with potential threats. Additionally, this practice is related to **ARCHITECTURE** since it involves monitoring various aspects of the organization's technology infrastructure, such as system logs and data flows, to ensure a secure and robust environment.

SITUATION-2e

Alarms and alerts are configured and maintained to support the identification of cybersecurity events.
Monitoring requirements should include specifications for alarms and alerts to aid in the identification of cybersecurity events, such as thresholds, durations, and sources of activity. For example, an alarm might be configured to be triggered when connection requests exceed a specific number that is the established maximum for normal activity, thus indicating the possibility of a denial of service attack.

AIM-Categorization-Tiering: Configuring and maintaining alarms and alerts is critical for **INCIDENT DETECTION AND RESPONSE** as it enables an organization to quickly identify, respond to, and recover from cybersecurity incidents. This practice also aligns with **SITUATIONAL AWARENESS** because it helps an organization detect, analyze, and understand cybersecurity risks and threats in real-time. Furthermore, the use of established criteria and specifications for alarms and alerts relates to **STANDARDS AND TECHNOLOGY**, ensuring that the organization employs recognized standards and technologies to protect its systems and data.

SITUATION-2f

Monitoring activities are aligned with the threat profile (THREAT-2e).
Monitoring requirements should include (among other things) activities that collect information relevant to the function's threat profile. To align monitoring with the threat profile, organizations should review the targeted assets, objectives, and attack methods that may be employed by threat actors and adjust monitoring activities accordingly. For example, if the threat profile includes a threat involving a nation state actor known to use spear phishing, email could be monitored for specific characteristics known to occur in those phishing emails.

AIM-Categorization-Tiering: The statement emphasizes the need to identify, assess, and mitigate security risks associated with specific threats and vulnerabilities, which directly aligns with **THREAT AND VULNERABILITY**. Additionally, by suggesting that monitoring activities should be adjusted according to the threat profile, the statement underscores the importance of real-time detection, analysis, and understanding of cybersecurity risks, thereby aligning with **SITUATIONAL AWARENESS**. Finally, using established criteria and technologies to monitor for specific threat indicators ties into **STANDARDS AND TECHNOLOGY**, as it involves the application of recognized standards and technological practices to enhance cybersecurity measures.

SITUATION-2g

More rigorous monitoring is performed for higher priority assets.
Monitoring requirements defined in SITUATION-2c are enhanced to include consideration of asset-level risks identified through risk management activities, so that more rigorous monitoring is done for higher risk assets (such as assets deemed important to delivery of the function, safety systems, and assets containing sensitive information assets). In the context of this practice, more rigorous describes an approach that is complete and comprehensive, includes coverage of all key controls, is regularly reviewed and adjusted based on environmental changes, and is persistent and continuous (rather that intermittent and discrete.).
For example, the organization may establish requirements to monitor access logs for assets containing sensitive data. Organizations that have very mature monitoring capabilities with no opportunity for further implementation of this practice as written should consider a response of fully implemented.

AIM-Categorization-Tiering: It highlights the importance of identifying, assessing, and managing risks associated with high-priority assets, which directly aligns with **RISK**. The emphasis on continuous and comprehensive monitoring to detect cybersecurity risks in real-time connects to **SITUATIONAL AWARENESS**. Moreover, the statement discusses the necessity of adjusting monitoring requirements based on asset-level risks and environmental changes, which involves managing and controlling critical information technology assets, thus relating to **ASSET, CHANGE AND CONFIGURATION**.

SITUATION-2h

Risk analysis information (RISK-3d) is used to identify indicators of anomalous activity.
Logging activities (SITUATION-1a, SITUATION-1b) and monitoring and analysis requirements (SITUATION-2c) are enhanced to incorporate relevant information from risk analysis activities (RISK-3d). Monitoring staff regularly review the risk analysis information and either modify existing indicators of anomalous activity or develop additional ones based on updates regarding threats, vulnerabilities, and identified risks.

AIM-Categorization-Tiering: It discusses the use of risk analysis information to identify indicators of anomalous activity, reflecting the organization's ability to identify, assess, and manage cybersecurity risks, which aligns with the definition of **RISK**. Additionally, it describes enhancing logging activities, monitoring, and analysis requirements with relevant information from risk analysis, highlighting the organization's ability to detect, analyze, and understand cybersecurity threats in real-time, which aligns with **SITUATIONAL AWARENESS**.

SITUATION-2i

Indicators of anomalous activity are evaluated and updated periodically and according to defined triggers, such as system changes and external events.
Indicators of anomalous activity are reviewed for effectiveness and updated as needed by monitoring staff to ensure they are still meeting the defined monitoring requirements and stakeholder information needs. The review and update should be conducted at a frequency set by the organization that ensures indicators are up to date based on the organization's risk information.
For example, organizations can monitor publicly available sources (e.g., National Vulnerability Database (NVD), CISA Central, and CERT/CC) to gain information on new vulnerabilities and exploits to identify new potential indicators of anomalous activity.

AIM-Categorization-Tiering: It primarily fits under **SITUATIONAL AWARENESS**, as it involves the ongoing detection, analysis, and understanding of cybersecurity risks and threats through the evaluation and updating of indicators. Additionally, it relates to **THREAT AND VULNERABILITY** because it focuses on identifying new vulnerabilities and exploits, as well as mitigating risks by keeping indicators current. Moreover, **POLICY AND STRATEGY** is relevant, as the process of periodic review and updating of indicators aligns with having defined strategies and policies for maintaining effective monitoring requirements. Finally, **INCIDENT DETECTION AND RESPONSE** is applicable, as the proactive review and updating of indicators contribute to the early identification and response to potential security threats.

5.3 Establish and Maintain Situational Awareness

SITUATION-3a

Methods of communicating the current state of cybersecurity for the function are established and maintained.
Methods for effectively communicating the current state of cybersecurity to relevant decision makers might include mechanisms (such as bulletin boards, big screen electronic dashboards, call trees, and satellite phones) and a common language and defined terms for describing cybersecurity information (such as threat levels). These should be regularly evaluated and updated as needed to ensure that they continue to be effective in expressing all cybersecurity conditions.

AIM-Categorization-Tiering: It addresses the establishment and maintenance of methods for communicating the current state of cybersecurity to relevant decision-makers, which reflects an organization's ability to detect, analyze, and understand cybersecurity threats in real-time, aligning with **SITUATIONAL AWARENESS**. Additionally, it involves the creation and evaluation of mechanisms and common language for communication, which is integral to developing clear and effective policies and strategies for information security management, aligning with **POLICY AND STRATEGY**. These categories are justified as they encompass the need for real-time awareness and structured communication to manage cybersecurity effectively.

SITUATION-3b

Monitoring data are aggregated to provide an understanding of the operational state of the function.
Aggregation of monitoring data can be used to determine if the function is operating as expected, including access to shared network resources, bandwidth, and system access controls. The value of this data collection is enhanced by the creation of minimally acceptable and target operational metrics for critical system components, allowing for immediate identification of suboptimal situations and potential degradation of the function. Monitoring data to be aggregated may come from many sources, including those outside of the function in scope for the self-evaluation.

AIM-Categorization-Tiering: It primarily fits under **SITUATIONAL AWARENESS**, as it involves aggregating monitoring data to understand the operational state and detect potential issues in real-time. Additionally, it pertains to **THREAT AND VULNERABILITY**, as the data aggregation helps identify suboptimal situations and potential degradations that may pose security risks. Furthermore, **POLICY AND STRATEGY** is relevant because establishing minimally acceptable and target operational metrics aligns with defining policies and strategies for maintaining optimal system performance and security. Finally, **STANDARDS AND TECHNOLOGY** is applicable, as the process of monitoring and data aggregation leverages established cybersecurity standards and technologies to protect the organization's systems and data.

SITUATION-3c

Relevant information from across the organization is available to enhance situational awareness.
In addition to data collected through monitoring, processes are in place to collect relevant information that may add detail or clarity to situational awareness, or helps to corroborate multiple sources of similar information. Relevant information can include after-action reports from incidents, calls to help desks about suspicious activity, and reports and statistics on phishing attempts. Situational awareness is more complete when it uses multiple sources of information.

AIM-Categorization-Tiering: It primarily fits under **SITUATIONAL AWARENESS**, as it involves gathering and utilizing relevant information from across the organization to enhance the understanding of cybersecurity risks and threats. Additionally, it relates to **INCIDENT DETECTION AND RESPONSE**, since incorporating data from after-action reports, help desk calls, and phishing attempt statistics into situational awareness processes aids in the early identification and effective response to security incidents. Furthermore, **KNOWLEDGE AND CAPABILITIES** is relevant, as leveraging diverse sources of information improves the organization's ability to understand and manage cybersecurity challenges. Finally, **POLICY AND STRATEGY** is applicable because the establishment of processes to collect and integrate relevant information aligns with having well-defined policies and strategies for maintaining comprehensive situational awareness.

SITUATION-3d

Situational awareness reporting requirements have been defined and address timely dissemination of cybersecurity information to organization-defined stakeholders.
Situational awareness reporting requirements should define the development, delivery, and maintenance of situational awareness communications needed for each type of stakeholder. For example, situational awareness communications to law enforcement will differ significantly from those to the board of directors. The plan should address near-term development and delivery and should be adjusted with some regularity in response to new or changing needs and from the assessment of the effectiveness of communications activities.
These are examples of stakeholders for situational awareness reporting:

- organizational leaders
- cybersecurity program leadership and team members
- individuals across the organization for whom a cybersecurity incident would have an impact
- information sharing and analysis centers
- government entities
- law enforcement
- connected organizations
- vendors
- sector organizations (such as trade associations)
- regulators

These are examples of situational awareness reporting requirements:

- the frequency and timing of communications
- special controls over communications (e.g., encryption or secured communications) that are appropriate for some stakeholders

- resources that will be required
- internal and external resources that are involved in supporting the communications process
- internal and external points of contact by role
- communication methods and channels to be used
- The assets, people, and systems (including external systems such as cellular networks) that may be unavailable during response and what backup resources may be needed

AIM-Categorization-Tiering: It is primarily relevant to **SITUATIONAL AWARENESS**, as it involves defining and implementing reporting requirements to ensure timely dissemination of cybersecurity information to stakeholders. Additionally, it fits under **POLICY AND STRATEGY**, since establishing clear reporting requirements and communication plans aligns with defining security objectives and managing risks effectively. **INCIDENT DETECTION AND RESPONSE** is also pertinent, as the development and delivery of situational awareness communications are critical for responding to cybersecurity incidents. Furthermore, **KNOWLEDGE AND CAPABILITIES** is applicable because the process of developing these requirements requires a thorough understanding of the information needs of different stakeholders and the capabilities necessary to meet those needs. Finally, **LEGAL AND REGULATORY FRAMEWORK** is relevant, as communication requirements must comply with laws and regulations governing information security and privacy.

SITUATION-3e

Relevant information from outside the organization is collected and made available across the organization to enhance situational awareness.
In addition to data collected through monitoring and internal information sources, processes are in place to collect information from external organizations that may add detail or clarity to situational awareness. For example, staff may monitor and collect information from a number of resources that provide reliable cybersecurity information, such as forums, vendors, InfraGard, ISACs, and CISA Central. External data is analyzed prior to sharing to ensure shared information is relevant and useful to recipients and to highlight specific areas for attention. The situational awareness information is then shared with appropriate stakeholders such as organizational leadership, incident response personnel, and asset owners.

AIM-Categorization-Tiering: The statement can be categorized under **SITUATIONAL AWARENESS** and **KNOWLEDGE AND CAPABILITIES**. This is because it discusses the collection and dissemination of relevant information from both internal and external sources to enhance situational awareness, which aligns with the organization's ability to detect, analyze, and understand cybersecurity risks and threats in real-time. Additionally, it involves the processes and skills necessary to gather, analyze, and share this information effectively, which relates to the organization's understanding of information security and its ability to develop and maintain the necessary skills and capabilities. These categories are justified as they encompass the need for real-time awareness and the skills to manage and utilize cybersecurity information effectively.

SITUATION-3f

A capability is established and maintained to aggregate, correlate, and analyze the outputs of cybersecurity monitoring activities and provide a near-real-time understanding of the cybersecurity state of the function.

Aggregation of monitoring data typically involves the use of advanced monitoring tools, such as security information and event management (SIEM) systems, to aggregate system logs and network data to enable a more holistic analysis of the environment. While not a requirement for implementation of this practice, organizations may consider aggregation of monitoring data from across functions. Similar to aggregation within a function, sharing and analysis of monitoring data across functions within an organization provides more comprehensive awareness of the organization's operational state and cybersecurity state. This may require implementation of methods to summarize or otherwise simplify the information presented to those reviewing aggregated audit logs (e.g., report reduction).

AIM-Categorization-Tiering: The emphasis on establishing and maintaining a capability to aggregate, correlate, and analyze cybersecurity monitoring outputs reflects the organization's commitment to **SITUATIONAL AWARENESS**, as it aims to provide a near-real-time understanding of its cybersecurity state. The use of advanced monitoring tools, like security information and event management (SIEM) systems, relates to **STANDARDS AND TECHNOLOGY**, highlighting the implementation of established technologies to protect systems and data. Additionally, the practice of aggregating monitoring data to understand potential threats and vulnerabilities further aligns with the **THREAT AND VULNERABILITY** category, as it involves identifying and assessing risks to mitigate security issues.

SITUATION-3g

Predefined states of operation are documented and can be implemented based on the cybersecurity state of the function or when triggered by activities in other domains.
Predefined states of operation are distinct operating modes (which typically include specific IT and OT configurations as well as alternate or modified procedures) that have been designed and implemented for the function and can be invoked by a manual or automated process in response to an event, a changing risk environment, or other sensory and awareness data to provide greater safety, resilience, reliability, and/or cybersecurity.
Defining predefined states of operation typically requires use of detailed architectures or topologies, documentation and detailed understanding of your assets and their priorities (ASSET-1c, ASSET-1d), categories (ASSET-2c, ASSET-2d), and attributes (ASSET-1e, ASSET-2e).
The defined states might include criteria for invoking the state, such as who has the authority to trigger a state change in either direction, checklists that must be completed before moving from a degraded state to an operational state, how long the organization can survive in a particular state, or how the organization will conduct monitoring to determine when the criteria are met. Information from monitoring activities is used to trigger decisions about invoking the predefined states of operation.
For example, if monitoring activities indicate an outage, this might trigger a manual process in which some analysis is done that determines that not all operations can be supported, specific decision makers must sign off on temporarily curtailing nonessential operation, and a predefined state is invoked in which certain assets are shut down.
Other situations might make use of an automated process. For example, based on threat intelligence received through monitoring activities (SITUATION-3f), a ruleset triggers an upgrade of the threat level, which triggers invocation of a predefined state that shuts down critical assets. Another example of predefined states of operations could be limiting communications between IT and OT environments during a cybersecurity incident.
As another example, high-risk situations may be identified that warrant additional logging, such as a safety-related emergency that requires an immediate elevation of access privileges, but they also may increase the verbosity of logging on affected devices.

AIM-Categorization-Tiering: It discusses the documentation and implementation of predefined states of operation based on the cybersecurity state, which involves designing and implementing a secure and robust technology infrastructure, aligning with **ARCHITECTURE**. It also requires a detailed understanding of assets, their priorities, categories, and attributes, reflecting the management and control of information technology assets, which aligns with **ASSET, CHANGE AND CONFIGURATION**. Furthermore, it involves using information from monitoring activities to trigger decisions, reflecting the ability to detect, analyze, and understand cybersecurity threats in real-time, aligning with **SITUATIONAL AWARENESS**.

5.4 Management Activities

SITUATION-4a

Documented procedures are established, followed, and maintained for activities in the SITUATION domain.
The activities in the SITUATION domain are formally documented in some way (such as standard operating procedures, process flow diagrams, RACI charts, and swim lane diagrams). The activities are intentionally designed or described to serve the organization rather than being ad hoc. Documenting procedures helps ensure that they are repeatable and produce expected outcomes. The level of detail included in documentation should be a sufficient to enable consistent performance of domain activities by different people and new employees assuming relevant domain experience and sufficient on-board training.
Also, procedure documentation is made available to and is used by relevant personnel. The documentation is updated as needed to reflect changes in the organizational or operational environment. Additionally, organizations may consider including exceptions processes in documented procedures to ensure that the organization reacts appropriately to unexpected events or situations.

AIM-Categorization-Tiering: The emphasis on establishing, following, and maintaining documented procedures highlights the importance of **POLICY AND STRATEGY**, as it ensures that there are clear and effective guidelines for managing cybersecurity activities. This documentation helps standardize processes and ensures consistency in response, aligning with the need for a comprehensive strategy. The reference to the "SITUATION domain" relates to **SITUATIONAL AWARENESS**, as it involves understanding and managing cybersecurity risks and threats in real-time. By documenting procedures, organizations can maintain a clear understanding of their operational environment and respond effectively to incidents. Additionally, this statement ties into **KNOWLEDGE AND CAPABILITIES**, as having well-documented procedures ensures that personnel have the necessary information and guidance to perform their roles effectively, including new employees who require training and on-boarding.

SITUATION-4b

Adequate resources (people, funding, and tools) are provided to support activities in the SITUATION domain.
When determining the adequacy of resources, it may help to consider whether there are any SITUATION domain activities not currently being performed that the organization would perform if it had additional people, funding, or tools. An additional consideration may be whether the organization has implemented all practices it has targeted for implementation and whether additional resources are necessary to address potential gaps.
Adequate resources are provided in the form of people, funding, and tools to ensure that SITUATION domain practices can be performed as intended. The performance of this practice can be evaluated by determining whether

any desired practices have not been implemented due to a shortage of resources.
These are examples of people involved in SITUATION domain activities:

- staff responsible for reviewing log data
- staff responsible for identifying relevant indicators of anomalous activity

These are examples of tools that might be used in SITUATION domain activities:

- security information and event management (SIEM) systems
- cybersecurity information collection methods, techniques, and tools
- electronic bulletin boards

Adequacy of resources should be determined on an ongoing basis through regular reviews of the domain program and reviews of domain resources in budgeting activities. It is a common point of concern that there is not enough time to complete cybersecurity program activities. This is addressed primarily through increasing staff and secondarily through increasing funding and tools.
When determining the adequacy of staff, also consider whether the cybersecurity program has sufficient capacity so that the individuals that make up the program can regularly attend training, implement and maintain tools, and respond to incidents while conducting day-to-day operations and meeting the cybersecurity objectives of the organization.

AIM-Categorization-Tiering: The emphasis on providing adequate resources such as people, funding, and tools specifically to support activities in the SITUATION domain highlights the organization's focus on **SITUATIONAL AWARENESS**, as it ensures the ability to detect, analyze, and understand cybersecurity risks in real-time. The reference to staff and tools also aligns with the **WORKFORCE** category, emphasizing the need for skilled personnel and appropriate technological resources to effectively carry out cybersecurity functions. Additionally, the consideration of whether resources are sufficient to implement targeted practices and address potential gaps falls under **POLICY AND STRATEGY**, as it involves strategic planning and resource allocation to achieve the organization's cybersecurity objectives. Regular reviews of resource adequacy also underscore the importance of having a well-defined and adaptive strategy for maintaining robust cybersecurity defenses.

SITUATION-4c

Up-to-date policies or other organizational directives define requirements for activities in the SITUATION domain.
Activities in the SITUATION domain receive documented guidance and direction from the organization in the form of policies or similar directives. Strategic business objectives drive the development of documented policies or other organizational directives to ensure activities support the accomplishment of the organization's mission. Policies or other organizational directives for SITUATION activities may contain:

- responsibility, authority, and ownership for performing SITUATION activities
- procedures, standards, and guidelines for SITUATION activities such as logging and monitoring, distribution of data (including distribution media, methods, and channels), and analyzing and deconflicting received cybersecurity information

- guidance about what situational awareness information can be or must be shared with appropriate stakeholders
- situational awareness reporting requirements
- requirements for the frequency of evaluating and updating indicators of anomalous activity
- methods for measuring adherence to policy, exceptions granted, and policy violations
- procedures for the granting and management of exceptions

AIM-Categorization-Tiering: The emphasis on up-to-date policies and organizational directives for activities in the SITUATION domain aligns with **POLICY AND STRATEGY**, as it involves defining clear and effective policies to guide cybersecurity practices. These policies ensure that activities support the organization's strategic business objectives, providing a structured approach to managing cybersecurity. The reference to activities in the SITUATION domain receiving documented guidance, such as logging and monitoring procedures, and the distribution of data, falls under **STANDARDS AND TECHNOLOGY**. Additionally, the focus on situational awareness reporting requirements and methods for measuring adherence to policies ties into **SITUATIONAL AWARENESS**, as it ensures the organization can detect, analyze, and understand cybersecurity risks in real-time.

SITUATION-4d

Responsibility, accountability, and authority for the performance of activities in the SITUATION domain are assigned to personnel.
The intent of this practice is that specific people (or people in specific roles) are held accountable for ensuring the achievement of expected results of SITUATION domain activities and that they are given the appropriate authority to act and to perform their assigned responsibilities.
These are examples of how to formalize responsibility and authority for SITUATION domain activities:

- defining roles and responsibilities in policies (see SITUATION-4c)
- developing position descriptions and conducting associated performance management activities
- including process tasks and responsibility for these tasks in position descriptions
- developing and implementing contractual instruments (including service level agreements) with external entities to establish responsibility and authority for performing SITUATION domain tasks on outsourced functions
- including SITUATION domain tasks in measuring performance of external entities against contractual instruments

Additionally, consider how the knowledge developed by personnel within this domain should be managed and shared. This includes determining what processes and tools should be used for knowledge sharing and identifying who will be responsible for making the best use of internal knowledge.

AIM-Categorization-Tiering: The emphasis on assigning responsibility, accountability, and authority to personnel aligns with **POLICY AND STRATEGY**, as it involves establishing clear roles and responsibilities within

the organization, ensuring that individuals are empowered to act and achieve the expected results in the SITUATION domain. The mention of defining roles and responsibilities in policies and developing position descriptions indicates a structured approach to cybersecurity management, ensuring that all activities are aligned with the organization's objectives. Additionally, the statement relates to **WORKFORCE** as it focuses on the personnel involved, highlighting the importance of clearly defining their roles, responsibilities, and authority. Finally, the aspect of managing and sharing knowledge within the domain connects with **SITUATIONAL AWARENESS**, as it involves ensuring that the organization has the capability to detect, analyze, and understand cybersecurity risks and threats through well-informed and knowledgeable personnel.

SITUATION-4e

Personnel performing activities in the SITUATION domain have the skills and knowledge needed to perform their assigned responsibilities.
The organization must identify the skills and knowledge needed to perform SITUATION domain activities and identify skill and knowledge gaps in existing personnel. The organization can address gaps either by hiring qualified personnel or training existing personnel. It is important to note that managing and securing many technologies (such as virtualized or cloud-based environments) require specific training in specialized equipment and practices. Care should be taken to ensure that the level of skills and knowledge of personnel managing and securing specialized technologies is commensurate with the importance of and risk posed by those technologies.
Additionally, skill and knowledge assessments should be repeated as operational environments change over time. For example, in the SITUATION domain, skills and knowledge are needed for

- tools, techniques, and methods used to collect, record, distribute, and protect monitoring data
- interpreting monitoring data and representing it in ways that are meaningful and appropriate. for stakeholders
- collecting, compiling, and distributing other types of cybersecurity information

Additionally, consider how the knowledge developed by personnel within this domain should be managed and shared. This includes determining what processes and tools should be used for knowledge sharing and identifying who will be responsible for making the best use of internal knowledge.

AIM-Categorization-Tiering: It emphasizes the importance of personnel having the necessary skills and knowledge to perform activities within the SITUATION domain, which aligns with **KNOWLEDGE AND CAPABILITIES**. This category highlights the need for an organization to ensure its staff are well-equipped and trained to handle cybersecurity tasks, especially those involving specialized technologies like virtualized or cloud-based environments. The statement also involves assessing and addressing skill and knowledge gaps, which is crucial for maintaining an effective cybersecurity posture. Additionally, it ties into **SITUATIONAL AWARENESS** as it involves understanding and managing the tools, techniques, and methods necessary for monitoring and analyzing cybersecurity data. This awareness is critical for detecting, analyzing, and responding to potential threats in real-time, ensuring the organization can maintain robust security measures.

SITUATION-4f

The effectiveness of activities in the SITUATION domain is evaluated and tracked.
The organization should measure the performance of SITUATION activities to ensure they are being performed

as described in plans, policies, and procedures for the SITUATION domain. Appropriate metrics should be developed and collected to detect deviations in performance and measure the extent to which SITUATION domain activities are achieving their intended purpose.

AIM-Categorization-Tiering: It emphasizes the need for an organization to evaluate and track the effectiveness of activities within the SITUATION domain, which is a core aspect of **SITUATIONAL AWARENESS**. This involves assessing how well these activities are detecting, analyzing, and responding to cybersecurity risks and threats in real-time. Additionally, the requirement to develop and collect appropriate metrics to measure performance ties into **POLICY AND STRATEGY**, as it underscores the importance of having clear policies and procedures in place to ensure that SITUATION domain activities are aligned with the organization's cybersecurity objectives and are being executed effectively.

6. Event and Incident Response, Continuity of Operations - 49 questions

As presented on the platform, its purpose is: Establish and maintain plans, procedures, and technologies to detect, analyze, and respond to cybersecurity events and to sustain operations throughout a cybersecurity event, commensurate with the risk to critical infrastructure and organizational objectives.

The Event and Incident Response, Continuity of Operations domain comprises five objectives:

1. Detect Cybersecurity Events
2. Analyze Cybersecurity Events and Declare Incidents
3. Respond to Cybersecurity Incidents
4. Address Cybersecurity in Continuity of Operations
5. Management Activities for the RESPONSE domain

6.1 Detect Cybersecurity Events

RESPONSE-1a

Detected cybersecurity events are reported to a specified person or role and documented, at least in an ad hoc manner.

Establish a collection point for reporting actual or suspected cyber events, such as a help desk. Contact information for that person, role, or group should be made known to all of the function's stakeholders. The contact should be someone who has knowledge of cybersecurity practices and issues and who can accurately document reported event information and possibly even do basic troubleshooting. Alternatively or additionally, events might be reported via an internal system such as a virtual help desk on an intranet.

AIM-Categorization-Tiering: It discusses the process of reporting detected cybersecurity events, which involves the ability to detect, respond to, and document incidents, aligning with **INCIDENT DETECTION AND RESPONSE**. It also highlights the need for clear procedures and roles, reflecting the importance of establishing effective policies and strategies, which aligns with **POLICY AND STRATEGY**. Additionally, the requirement for the contact person to have knowledge of cybersecurity practices emphasizes the need for a thorough understanding and skills in cybersecurity, aligning with **KNOWLEDGE AND CAPABILITIES**.

RESPONSE-1b

Criteria are established for cybersecurity event detection (for example, what constitutes a cybersecurity event, where to look for cybersecurity events).
The organization should define cybersecurity event detection criteria that specify what distinguishes cybersecurity events from the multitude of other events. These criteria should relate to the cybersecurity requirements of the IT, OT, and information assets important for the delivery of the function. They allow the organization to focus valuable resources (people, tools, etc.) on events that may potentially affect the productivity of those assets. Regarding "where to look for cybersecurity events," be sure to consider potential events originating from third parties such as cloud resource providers.

AIM-Categorization-Tiering: Defining criteria for detecting cybersecurity events is a critical part of an organization's ability to detect, respond to, and manage such incidents, aligning with **INCIDENT DETECTION AND RESPONSE**. Establishing what constitutes a cybersecurity event and where to look for them involves identifying and assessing risks associated with information security, which aligns with **RISK**. Additionally, the creation of specific detection criteria requires clear policies and strategies to ensure that all relevant aspects are covered and resources are effectively allocated, which aligns with **POLICY AND STRATEGY**.

RESPONSE-1c

Cybersecurity events are documented based on the established criteria.
Anything that is an event according to the criteria defined in RESPONSE-1b should be documented in a consistent manner. The organization should decide what details about events should be documented to enable, for example, (1) decisions about declaring events to be incidents, (2) collection of data for any event metrics the organization might be tracking, and (3) correlation of event information, if the organization is doing that.

AIM-Categorization-Tiering: Documenting cybersecurity events based on established criteria is a critical part of the process for detecting, responding to, and managing such incidents, which aligns with **INCIDENT DETECTION AND RESPONSE**. Establishing what details should be documented involves defining clear policies and strategies to ensure consistency and effectiveness in event handling, which aligns with **POLICY AND STRATEGY**. Additionally, the detailed documentation of events is crucial for assessing and managing risks associated with cybersecurity threats, which aligns with **RISK**.

RESPONSE-1d

Event information is correlated to support incident analysis by identifying patterns, trends, and other common features.
Event correlation may help identify issues that may be more serious than when events are considered independently. For example, brute force attacks can be obfuscated by conducting them from multiple machines, thereby circumventing traditional lockout rules for 3 or 5 failed logins from a single IP address. And the issue is recognized as a more serious issue only when taken in a larger context. Event correlation requires the comparison of two or more events and establishes potential relationships between events.
These are examples of correlation activities:

- Viewing and comparing separate events from the same information source
- Viewing and comparing separate events from different information sources

· Viewing and comparing events over time for common characteristics

AIM-Categorization-Tiering: Correlating event information to support incident analysis by identifying patterns, trends, and common features is essential for understanding and responding to cybersecurity threats in real-time, which aligns with **SITUATIONAL AWARENESS**. By identifying more serious issues that may not be apparent when events are considered independently, the organization can better assess and mitigate security risks associated with threats and vulnerabilities, aligning with **THREAT AND VULNERABILITY**. Additionally, the ability to detect and analyze correlated events is crucial for effective incident detection and response, allowing the organization to respond promptly and accurately to potential security incidents, which aligns with **INCIDENT DETECTION AND RESPONSE**.

RESPONSE-1e

Cybersecurity event detection activities are adjusted based on identified risks and the organization's threat profile (THREAT-2e).
Event detection is largely dependent on the degree to which there is broad awareness of the potential range of events that can affect the organization. One source that is useful for expanding the organization's event awareness is risks that have been identified and are being addressed in the organization risk management process. (See RISK-2a.).
Alerts should be developed to function as early warning indicators for each risk or threat. To adjust event detection activities based on the organization's threat profile, organizations should review the targeted assets, objectives, and attack methods that may be employed by threat actors and tune alerting accordingly. For example, if threat reporting indicates adversaries are targeting certain SCADA systems, existing alerts could be modified to trigger on anomalies that match aspects of that adversarial activity.

AIM-Categorization-Tiering: The primary focus is on **THREAT AND VULNERABILITY**, as it discusses the importance of adjusting event detection activities based on the organization's threat profile, which involves identifying and mitigating risks associated with threats. It also strongly relates to **RISK**, as it emphasizes the need for broad awareness of potential events and the role of risk management processes in expanding event awareness. Furthermore, the statement touches on **INCIDENT DETECTION AND RESPONSE**, highlighting the necessity of developing alerts as early warning indicators for identified risks or threats to ensure rapid and effective responses to potential security incidents.

RESPONSE-1f

Situational awareness for the function is monitored to support the identification of cybersecurity events.
Information collected through situational awareness activities is reviewed and used to help identify cybersecurity events. This information could be collected from multiple sources, including across functions within the organization and outside of the organization.

AIM-Categorization-Tiering: Primarily, it falls under **SITUATIONAL AWARENESS** because it emphasizes monitoring and collecting information to identify cybersecurity events, a core component of understanding risks and threats in real-time. Additionally, it relates to **INCIDENT DETECTION AND RESPONSE**, as the information gathered through situational awareness is reviewed and utilized to detect potential cybersecurity incidents, ensuring early identification and effective response. Finally, it is connected to **RISK**, as the collected information

from various sources aids in identifying and managing risks associated with cybersecurity events, contributing to the organization's overall risk management process.

6.2 Analyze Cybersecurity Events and Declare Incidents

RESPONSE-2a

Criteria for declaring cybersecurity incidents are established, at least in an ad hoc manner.
Criteria for declaring cybersecurity incidents are used to determine whether an event should be treated as an incident and the potential severity of the event. A ranking scale, such as high, medium, and low, may help to communicate incident severity to stakeholders and aid in prioritizing response actions to be taken.
Incident declaration criteria should be developed from experience and may partially be derived from risk evaluation criteria (such as impact thresholds) established as part of Risk Management domain activities. Criteria might be based on the type of event (such as unauthorized access), level of impact (e.g., local versus organization-wide), type of impact (internal systems versus critical external services), compliance obligations (internal-only versus reportable event), or mean time to recovery. For some events, the time between event detection and incident declaration may be immediate, requiring little additional analysis. In other cases, the organization may wish to leverage previously developed criteria to help guide incident declaration.

AIM-Categorization-Tiering: Primarily pertains to **INCIDENT DETECTION AND RESPONSE**, as it discusses the criteria for declaring cybersecurity incidents, which is essential for determining the severity of events and prioritizing response actions. Additionally, it relates to **RISK**, since the criteria for declaring incidents may be derived from risk evaluation criteria established as part of the organization's risk management activities, such as impact thresholds. This connection underscores the importance of **POLICY AND STRATEGY**, as the development and communication of clear incident declaration criteria are foundational for effective cybersecurity management.

RESPONSE-2b

Cybersecurity events are analyzed to support the declaration of cybersecurity incidents, at least in an ad hoc manner.
The analysis of cybersecurity events helps the organization gather additional information for event resolution and to assist in incident declaration, handling, and response. This analysis may consist of categorizing, correlating, and prioritizing events. Through analysis, the organization determines the type and extent of an event (e.g., physical versus technical), whether the event correlates to other events (to determine if they are symptomatic of a larger issue, problem, or incident), and in what order events should be addressed or assigned for incident declaration, handling, and response. Analysis also helps the organization to determine if the event needs to be escalated to other organizational or external staff (outside of the incident management staff) for additional analysis and resolution.

AIM-Categorization-Tiering: It is primarily linked to **INCIDENT DETECTION AND RESPONSE** because it focuses on analyzing cybersecurity events to support the declaration and handling of incidents, which is crucial for effective incident management and response. Additionally, it relates to **RISK**, as the analysis involves determining the type, extent, and correlation of events to assess their impact and prioritize them, which is integral to risk management. This affirmation also pertains to **POLICY AND STRATEGY**, as the processes for categorizing, correlating, and prioritizing events must be well-defined and communicated within the organization to ensure

a systematic approach to incident declaration and response. By analyzing cybersecurity events and potentially escalating them for further resolution, the organization leverages its **KNOWLEDGE AND CAPABILITIES** to maintain a thorough understanding and manage incidents effectively.

RESPONSE-2c

Cybersecurity incident declaration criteria are formally established based on potential impact to the function.
Each organization has many unique factors that must be considered in determining when an event should be declared to be an incident. Through experience, an organization may have a baseline set of types of events that define standard incidents, such as a virus outbreak, unauthorized access to a user account, or a denial-of-service attack. However, in reality, incident declaration may occur on an event-by-event basis.
To guide the organization in determining when to declare an incident (particularly if incident declaration is not immediately apparent), the organization must define incident declaration criteria. Incident declaration criteria should include factors that indicate the potential impact to the function, such as:

- potential safety impacts
- functional impact (priority and scope of impacted assets)
- information impact (impact to information assets)
- recoverability from the incident (resources necessary to recover from the incident)
- the potential cause of the incident (malicious activity vs. unintentional actions)

Additionally, incident declaration criteria should consider impact to the organization's cybersecurity goals, such as:

- potential financial loss
- number of customers affected
- outage of major IT system
- theft of customer information

AIM-Categorization-Tiering: It relates to **INCIDENT DETECTION AND RESPONSE** because it emphasizes the formal establishment of criteria for declaring cybersecurity incidents based on their potential impact, which is essential for effective incident management. It also pertains to **RISK** as it involves evaluating the potential safety, functional, information impacts, recoverability, and causes of incidents, which are critical for assessing and managing cybersecurity risks. Additionally, the affirmation is connected to **POLICY AND STRATEGY**, since defining clear and effective incident declaration criteria aligns with setting strategic policies and objectives for cybersecurity management.

RESPONSE-2d

Cybersecurity events are declared to be incidents based on established criteria.
The cybersecurity incident declaration criteria established according to RESPONSE-2c are used to determine whether an event should be declared to be an incident. Declaring an incident initiates the incident response activities in RESPONSE-3.

AIM-Categorization-Tiering: It primarily pertains to **INCIDENT DETECTION AND RESPONSE**, as it focuses on the use of established criteria to determine when cybersecurity events should be declared as incidents, which is crucial for initiating appropriate incident response activities. Additionally, it relates to **POLICY AND STRATEGY** because the establishment and application of incident declaration criteria are part of a broader strategic framework that defines how an organization manages cybersecurity events. Furthermore, it connects to **RISK** since the criteria for declaring incidents are likely based on assessing the potential impact and risks associated with different events, ensuring that incidents are managed in a way that minimizes harm to the organization.

RESPONSE-2e

Cybersecurity incident declaration criteria are updated periodically and according to defined triggers, such as organizational changes, lessons learned from plan execution, or newly identified threats.
To maximize the investment in the incident detection and response process, incident declaration criteria should be maintained to reflect an organization's evolving risk tolerance and threat environment. Also, updating the criteria based on lessons learned in this process can help the organization to be more efficient and effective in dealing with future events.

AIM-Categorization-Tiering: Primarily pertains to **POLICY AND STRATEGY**, as it involves the periodic updating of cybersecurity incident declaration criteria, reflecting an organization's evolving risk tolerance and threat environment, which is essential for effective cybersecurity management. Additionally, it relates to **INCIDENT DETECTION AND RESPONSE**, since maintaining and updating incident declaration criteria is critical for ensuring that the organization can efficiently detect and respond to cybersecurity incidents. Furthermore, it connects to **RISK**, as the criteria are updated to account for newly identified threats and lessons learned, helping the organization manage its cybersecurity risks more effectively.

RESPONSE-2f

There is a repository where cybersecurity events and incidents are documented and tracked to closure.
Documenting and tracking ensure that an incident is properly progressing through the incident lifecycle and, most important, is closed when an appropriate response and post-incident review have been completed.

AIM-Categorization-Tiering: Primarily pertains to **INCIDENT DETECTION AND RESPONSE**, as it involves the documentation and tracking of cybersecurity events and incidents to ensure they progress through the incident lifecycle and are properly closed after an appropriate response and post-incident review. Additionally, it relates to **ASSET, CHANGE AND CONFIGURATION**, since effective documentation and tracking of incidents are part of the broader management and control of an organization's information technology assets, ensuring they are secure and properly maintained throughout their lifecycle. Furthermore, it connects to **STANDARDS AND TECHNOLOGY**, as the use of standardized processes and technologies is crucial for effectively documenting and tracking incidents.

RESPONSE-2g

Internal and external stakeholders (for example, executives, attorneys, government agencies, connected organizations, vendors, sector organizations, regulators) are identified and notified of incidents based on situational awareness reporting requirements (SITUATION-3d).
Incidents that have been declared and that require a response must be communicated to stakeholders whose involvement is necessary in implementing, managing, and bringing to closure an appropriate and timely solution.
Event and incident notification should be guided by the reporting requirements defined in SITUATION-3d. Miscommunications or inaccurate information about organizational incidents can have dire effects that far exceed the potential damage caused by an incident itself. Therefore, the function must proactively manage communications when incidents are detected and throughout their life cycle.

AIM-Categorization-Tiering: It primarily belongs to **INCIDENT DETECTION AND RESPONSE** because it involves notifying stakeholders about incidents and managing the entire lifecycle of incident communication to ensure proper response and closure. Additionally, it pertains to **SITUATIONAL AWARENESS**, as the reporting and notification process is guided by situational awareness reporting requirements to ensure that stakeholders are informed accurately and timely based on real-time understanding of the incident. Furthermore, it touches on **LEGAL AND REGULATORY FRAMEWORK**, since certain stakeholders such as government agencies and regulators must be notified to comply with legal and regulatory obligations during incident response.

RESPONSE-2h

Criteria for cybersecurity incident declaration are aligned with cyber risk prioritization criteria (RISK-3b).
Aligning incident declaration criteria with the risk criteria established in RISK-3b ensures that the organization is recognizing and addressing incidents that involve risks that the organization is particularly concerned about.

AIM-Categorization-Tiering: First, it pertains to **RISK**, as it directly references the alignment of incident declaration criteria with risk prioritization, highlighting the organization's focus on identifying, assessing, and managing cybersecurity risks effectively. Additionally, it is relevant to **INCIDENT DETECTION AND RESPONSE**, since it emphasizes the criteria for declaring cybersecurity incidents, which are crucial for the timely detection and response to potential threats. Lastly, it relates to **POLICY AND STRATEGY**, as establishing and aligning these criteria reflects a strategic approach to managing and mitigating risks through well-defined policies and procedures. This alignment ensures a coherent and comprehensive approach to incident management and risk mitigation.

RESPONSE-2i

Cybersecurity incidents are correlated to identify patterns, trends, and other common features across multiple incidents.
Correlation of incidents can be done through analysis, incident tracking tools, use of incident categories, and matching terms in logs. For example, system access logs can be checked for system authentication failures, and the IP addresses from those can be correlated with known malicious IP addresses gathered through intelligence sources.

AIM-Categorization-Tiering: First, it is relevant to **SITUATIONAL AWARENESS**, as the correlation of incidents to identify patterns, trends, and common features helps an organization detect, analyze, and understand

cybersecurity risks and threats in real-time. Additionally, it relates to **INCIDENT DETECTION AND RESPONSE**, as using analysis, incident tracking tools, and matching terms in logs enables the organization to detect, respond to, and recover from cybersecurity incidents more effectively. Furthermore, it involves **THREAT AND VULNERABILITY**, as identifying patterns and correlating incidents is essential for assessing and mitigating security risks associated with various threats and vulnerabilities. This comprehensive approach ensures that the organization can recognize and address recurring security issues systematically.

6.3 Respond to Cybersecurity Incidents

RESPONSE-3a

Cybersecurity incident response personnel are identified and roles are assigned, at least in an ad hoc manner.
Identify the roles and responsibilities necessary to perform cybersecurity incident response activities and ensure that staff are assigned to those roles and have the necessary skills. Staff should be provided sufficient autonomy and authority to carry out their duties. The organization may create job descriptions for cybersecurity incident response roles and responsibilities and keep track of skill gaps and gaps in the availability of staff so that suitable personnel can be hired as needed.

AIM-Categorization-Tiering: It is directly related to **PROGRAM**, as it discusses the identification and assignment of roles and responsibilities for cybersecurity incident response, which is a fundamental aspect of an organization's cybersecurity strategy and planning. Additionally, it involves **WORKFORCE**, since it emphasizes the need for staff with the necessary skills and autonomy to perform incident response activities, highlighting the importance of having qualified personnel. Furthermore, it relates to **KNOWLEDGE AND CAPABILITIES**, as ensuring that staff have the necessary skills and addressing skill gaps are crucial for effective incident response. This comprehensive approach ensures that the organization is well-prepared to handle cybersecurity incidents with a competent and well-defined team.

RESPONSE-3b

Responses to cybersecurity incidents are executed, at least in an ad hoc manner, to limit impact to the function and restore normal operations.
Responding to an incident describes the actions the organization takes to prevent or contain the impact of an incident while it is occurring or shortly after it has occurred. The range, scope, and breadth of the response will vary widely depending on the nature of the incident. This may include potential incidents that may occur due to new vulnerabilities or technological advances that have a significant potential impact on the organization, such as vulnerabilities in commonly used technologies (e.g., MS17-010) and emerging technologies that would reduce the effectiveness of current cybersecurity controls (e.g., quantum computing). Incident response may be as simple as notifying users to avoid opening a specific type of email message or as complicated as having to implement service continuity plans that require relocation of services and operations to an off-site provider.
The actions related to incident response might include, for example, containing damage (e.g., by taking hardware or systems offline), communicating to asset owners about the incident, and developing and implementing corrective actions and controls.

AIM-Categorization-Tiering: Firstly, it is relevant to **INCIDENT DETECTION AND RESPONSE**, as it describes the actions taken by the organization to limit the impact of an incident and restore normal operations, including the containment of damage and implementation of corrective actions. Additionally, it involves **RISK**,

as responding to incidents includes addressing potential risks posed by new vulnerabilities or technological advances, which could significantly impact the organization. Lastly, it relates to **POLICY AND STRATEGY**, as the execution of responses, whether ad hoc or planned, reflects the organization's strategic approach to managing and mitigating incidents.

RESPONSE-3c

Reporting of incidents is performed (for example, internal reporting, ICS-CERT, relevant ISACs), at least in an ad hoc manner.
Cybersecurity incident response staff must know what incident information should be reported to various internal and external stakeholders, within what timeframe, and whether there are any constraints (such as legal review of the information to be shared). When possible, assign a single person responsibility for reporting an incident throughout its duration to keep messages consistent as the event evolves. Keep contact information for stakeholders up-to-date. Stakeholders may include personnel, such as public relations team members or legal representatives, that are not involved in the direct response to an incident but must be informed to support the sustainment of the organizational operations.

AIM-Categorization-Tiering: It primarily falls under the category of **INCIDENT DETECTION AND RESPONSE**. This is because it discusses the processes and responsibilities involved in reporting cybersecurity incidents, including the importance of timely and consistent communication with both internal and external stakeholders. Additionally, the need for proper coordination and communication with stakeholders like public relations and legal representatives, who are not directly involved in incident response but are crucial for maintaining organizational operations, underscores the critical role of incident management within an organization's cybersecurity strategy.

RESPONSE-3d

Cybersecurity incident response plans that address all phases of the incident lifecycle are established and maintained.
The organization should create a well-structured and comprehensive plan describing incident management procedures so that response activities will be repeatable, will be performed at the same level of rigor during times of stress, and will have consistent outcomes. The organization may want to consult existing guidance or outside expertise for information about incident management best practices.
These are examples of incident response activities that might be described in the plan:

- containing damage
- collecting evidence
- communicating to stakeholders, including asset owners and incident owners
- communicating with response team members - including backup or out of band communication methods
- developing and implementing corrective actions and controls
- implementing continuity and restoration plans or other emergency actions
- conducting lessons learned reviews

· the types of actions that should be avoided during response

Activities should be included in the plan for all phases of the incident lifecycle (for example, triage, escalation, handling, communication, coordination, and closure). Incident response plans should be comprehensive enough to address the high-level categories of incidents that may affect the organization. Incident response plans should also address potential incidents that may occur due to new vulnerabilities or technological advances that have a significant potential impact on the organization, such as vulnerabilities in commonly used technologies (e.g., MS17-010) and emerging technologies that would reduce the effectiveness of current cybersecurity controls (e.g., quantum computing).
As part of incident response planning organizations may consider what legal agreements may be necessary in different types of response scenarios (e.g., authorization for a federal employee to review a system, agreements related to obtaining assistance from outside organizations) and whether performing legal review in advance is warranted. Additionally, as technology used to complete operational activities continues to shift to more dispersed and mobile options, organizations may consider whether the assets involved in an incident will be physically available during response and what remote response capabilities may be necessary.

AIM-Categorization-Tiering: It is directly linked to **INCIDENT DETECTION AND RESPONSE**, as it discusses establishing and maintaining comprehensive incident response plans that cover all phases of the incident lifecycle. This ensures consistent and effective response activities during times of stress. Additionally, it involves **POLICY AND STRATEGY**, as the development and maintenance of these plans are integral to an organization's overall cybersecurity policies and strategies. Moreover, it touches on **KNOWLEDGE AND CAPABILITIES**, since the organization must have a thorough understanding of incident management best practices and potentially consult external expertise. Lastly, it relates to **LEGAL AND REGULATORY FRAMEWORK**, as the plan considers the necessity of legal agreements and reviews to ensure compliance during different types of response scenarios.

RESPONSE-3e

Cybersecurity incident response is executed according to defined plans and procedures.
The organization should execute incident response based on the defined plans and procedures. This may include responding to actual incidents or potential incidents due to major vulnerabilities.
The organization should consider whether adequate resources will be available to perform the roles identified in the plan. This may require engaging with others prior to an incident to develop requests for technical assistance with law enforcement and government entities, mutual aid agreements with peer organizations, or contracts and retainers with vendors. These agreements may be prepared in advance to allow for immediate activation when response is needed. Additionally, it may be useful to pre-clear access for individuals providing response to avoid delays that may be caused by badging, access provisioning, and mandatory trainings.
Following completion of response to an incident, the organization should conduct reviews or assessments to determine whether the defined plans and procedures are being followed effectively.

AIM-Categorization-Tiering: It primarily belongs to **INCIDENT DETECTION AND RESPONSE** as it describes the execution of incident response plans and procedures. Additionally, it is related to **POLICY AND STRATEGY** since the execution of response activities based on predefined plans and procedures is a crucial part of an organization's overall cybersecurity strategy. The consideration of resource availability and the establishment of agreements with external entities also link it to **PROGRAM**, as it involves strategic planning and

collaboration. Furthermore, ensuring adequate resources and pre-clearance for response personnel touches on **WORKFORCE** because it addresses the need for proper staffing and preparation for incident response roles.

RESPONSE-3f

Cybersecurity incident response plans include a communications plan for internal and external stakeholders.
Cybersecurity incident response activities may require the involvement of stakeholders from across the organization, such as public relations team members and legal representatives. These stakeholders may support activities to mitigate potential reputational harm during and after response to a cybersecurity incident. Organizations should consider the types of communication that may be necessary to keep internal and external stakeholder informed during recovery activities, for example, executives and management teams may need to be informed if specific actions are executed or if the incident response team determines an incident may cause reputational harm to the organization.
Be advised that organizations often have a crisis communications plan in place that is separate and distinct from cybersecurity incident response plans. In this case, the cybersecurity incidence response plan should make reference to and utilize the process defined in the crisis communications plan when executing incident communications to internal and external stakeholders. If such a plan exists, it may be considered an effective substitute for practice RESPONSE-3f but only if it is specifically referenced in the incident response plans.

AIM-Categorization-Tiering: It is primarily associated with **INCIDENT DETECTION AND RESPONSE** as it involves the execution of incident response activities and communication during and after a cybersecurity incident. Additionally, it is related to **POLICY AND STRATEGY** because having a defined communications plan is a part of establishing effective policies and strategies for cybersecurity management. The involvement of various stakeholders, such as public relations and legal representatives, indicates its relevance to **PROGRAM**, highlighting the strategic planning and coordination required for incident response. Lastly, it touches upon **CULTURE AND SOCIETY** as effective communication within and outside the organization helps promote a culture of transparency and awareness regarding cybersecurity incidents.

RESPONSE-3g

Cybersecurity incident response plan exercises are conducted periodically and according to defined triggers, such as system changes and external events.
Proper advanced planning can help an organization establish, document, and staff an incident management capability. Exercises that challenge the viability, accuracy, and completeness of an incident response plan should be part of the planning process. Exercises should be performed under conditions and at a frequency established by the organization. Scenario-based exercises covering multiple scenario types and including external crises (e.g., flood or pandemic) may be helpful in uncovering unexpected cybersecurity impacts that do not stem from cybersecurity incidents. The results of exercises should be documented, along with any relevant information about the organization's level of preparedness to address incidents.
When planning for exercises, organizations should consider coordination with appropriate stakeholders (including third parties or vendors) for the different kinds of information, IT, and OT assets that may be within the scope for exercises such as virtualized assets, regulated assets, cloud assets, and mobile assets. A significant reliance on vendors during steady state operations may indicate an increased need for vendor support during incident response. Additionally, exercises provide an opportunity to identify and communicate the types of actions that should be avoided during response.

Finally, organizations may consider exercising exceptions to normal policies and procedures by including exceptions as part of the exercise scenario script.

AIM-Categorization-Tiering: Primarily, it relates to **INCIDENT DETECTION AND RESPONSE**, as it focuses on testing and validating the organization's ability to respond to cybersecurity incidents effectively. It also pertains to **PROGRAM**, given that it involves strategic planning and coordination to ensure that exercises are well-integrated into the organization's overall cybersecurity strategy. Additionally, **POLICY AND STRATEGY** is relevant since the exercises aim to test and refine the policies and strategies defined in the incident response plan. Finally, **KNOWLEDGE AND CAPABILITIES** is included as these exercises help develop and maintain the skills and capabilities necessary for effective incident response, ensuring that personnel are prepared to handle real incidents.

RESPONSE-3h

Cybersecurity incident lessons-learned activities are performed and corrective actions are taken, including updates to the incident response plan.
Define and implement activities for collecting lessons-learned input from incident response participants after significant incidents, such as hotwash sessions or submission of comments on a team wiki. Participants could provide feedback about how well the incident response plan was followed, any shortcomings in needed resources, and, overall, which incident response actions worked well and which didn't. Make updates to the incident response plan based on lessons learned where appropriate.
Note that the term lessons learned is used in the common, general sense and not as related to definitions used in any specific regulation or guideline.

AIM-Categorization-Tiering: It pertains primarily to **INCIDENT DETECTION AND RESPONSE** because it involves performing activities to gather lessons learned from incident responses and updating the incident response plan accordingly. Additionally, it relates to **KNOWLEDGE AND CAPABILITIES**, as the feedback and lessons learned from participants help improve the organization's understanding and skills in handling cybersecurity incidents effectively. Finally, it also touches on **POLICY AND STRATEGY**, as the updates to the incident response plan based on lessons learned reflect the organization's commitment to continually improving its cybersecurity policies and strategies.

RESPONSE-3i

Cybersecurity incident root-cause analysis is performed and corrective actions are taken, including updates to the incident response plan.
This might involve conducting a formal examination of the causes of the incident, the ways in which the organization responded to it, and the administrative, technical, and physical control weaknesses that may have allowed the incident to occur. The organization can employ commonly available techniques (such as cause-and-effect diagrams) to perform root-cause analysis as a means of potentially preventing future incidents of similar type and impact. Any needed improvements identified through these activities should be made, such as updating the incident response plan or adjusting protection strategies and controls. This type of analysis may also identify higher-level issues within the organization and result in changes to activities in other domains, such as the cyber risk strategy, vulnerability management procedures, or the threat analysis process.
Note that the terms root-cause analysis and corrective action are used in the common, general sense and not as

related to definitions used in any specific regulation or guideline.
Exceptions to policies implemented during response to an incident should be reviewed following recovery for their impact to the cybersecurity control environment (i.e., moving control center operations from on-site only to remote).
Procedures for managing exceptions should include requirements for evaluating changes following return to normal operations including whether changes should remain in place. Additional scrutiny may be valuable for specific change types such as new devices, new applications and changes to access permissions.

AIM-Categorization-Tiering: The statement about performing root-cause analysis of cybersecurity incidents and taking corrective actions primarily falls under **INCIDENT DETECTION AND RESPONSE**, as it involves examining incidents, identifying their causes, and updating response plans to handle future incidents more effectively. Additionally, it relates to **KNOWLEDGE AND CAPABILITIES** because it involves leveraging techniques and expertise to understand and mitigate the causes of incidents, thereby enhancing the organization's ability to prevent similar occurrences in the future. Furthermore, this activity also intersects with **RISK**, as identifying and addressing root causes helps the organization manage and reduce cybersecurity risks by preventing recurring issues and improving overall security measures.

RESPONSE-3j

Cybersecurity incident responses are coordinated with vendors, law enforcement, and other external entities as appropriate, including support for evidence collection and preservation.
An event may become an organizational incident that has the potential to be a violation of local, state, or federal rules, laws, and regulations. This is often not known early in the investigation of an event, so the organization must be vigilant in ensuring that all event and incident evidence is handled properly in case an eventual legal issue, civil or criminal, is raised.
To properly collect, document, and preserve evidence, the organization must have processes for these activities, and the processes must be known to all staff who are involved in any aspect of the incident life cycle. Because it is unpredictable whether an event or incident will result in legal action, an organization must also consider early involvement of legal and possibly law enforcement staff in the incident identification and analysis process to avoid problems with evidence retention, destruction, and tampering.
Note that "other external entities" may include third parties such as cloud resource providers.

AIM-Categorization-Tiering: It primarily falls under **INCIDENT DETECTION AND RESPONSE**, as it involves the process of managing and responding to incidents effectively. Additionally, it relates to **LEGAL AND REGULATORY FRAMEWORK**, given the importance of handling evidence properly to comply with laws and regulations and to support potential legal actions. Moreover, this coordination also involves **CULTURE AND SOCIETY**, as it reflects the organization's commitment to fostering a cybersecurity-aware culture among its employees and external partners, ensuring everyone involved understands the processes and the importance of proper evidence handling in the incident life cycle.

RESPONSE-3k

Cybersecurity incident response personnel participate in joint cybersecurity exercises with other organizations.
If possible, incident response personnel should participate in joint cybersecurity exercises to become familiar with the entities and individuals they would need to work with in a real-world incident, gain experience in response

activities, possibly identify deficiencies in internal response plans, and share their knowledge and experience with others in the community. One example of a joint exercise in the Electric Sector is the Grid Security Exercise (GridEx), the Department of Energy's annual two-day exercise.

AIM-Categorization-Tiering: It pertains to **INCIDENT DETECTION AND RESPONSE**, as these exercises help improve the ability to respond to and recover from incidents. It also relates to **KNOWLEDGE AND CAPABILITIES**, since participating in these exercises allows personnel to gain experience, share knowledge, and improve their skills in cybersecurity response activities. Additionally, it aligns with **CULTURE AND SOCIETY**, as it fosters a collaborative culture and builds relationships with other organizations and stakeholders involved in cybersecurity efforts.

RESPONSE-3l

Cybersecurity incident responses leverage and trigger predefined states of operation (SITUATION-3g).
Effective response requires detailed, in-advance planning for a range of potential threats and incidents. SITUATION-3g defines "predefined states of operation" and describes how they can be used to ensure responses are specific, measured, and appropriate for the level of operational impact of the incident. A typical example of this approach is to have a plan for minimizing network usage to critical systems in the case of degraded network service. Another example is having a game plan ready to shift to a known good state if it becomes apparent that your critical operational data has been corrupted.

AIM-Categorization-Tiering: It pertains primarily to **INCIDENT DETECTION AND RESPONSE**, as it emphasizes the importance of having predefined plans for effectively responding to incidents. Additionally, it relates to **POLICY AND STRATEGY** because it involves advance planning and the establishment of specific operational states for various threat scenarios, ensuring that responses are structured and well-coordinated. Furthermore, it connects to **SITUATIONAL AWARENESS** since understanding and assessing the level of operational impact is crucial for determining the appropriate predefined state of operation to activate during an incident.

6.4 Address Cybersecurity in Continuity of Operations

RESPONSE-4a

Continuity plans are developed to sustain and restore operation of the function if a cybersecurity event or incident occurs, at least in an ad hoc manner.
Continuity plans contain descriptions of the actions the organization will take to sustain and restore operation of the function if a disruption occurs (such as failing over to redundant facilities or initiating manual procedures) and key roles that must be involved. They are generally focused on managing the organizational consequences of disruption based on a range of potential events that can cause disruption. Continuity plans address the most critical business functions of the organization to ensure they continue during different types of emergencies. Organizations may also consider how secure shutdown will be performed as part of continuity planning.

AIM-Categorization-Tiering: Primarily, it falls under **INCIDENT DETECTION AND RESPONSE**, as it involves actions to be taken during and after an incident to ensure operations continue or are restored. Additionally, it is relevant to **POLICY AND STRATEGY**, given that it involves creating structured plans and procedures to manage disruptions. Lastly, it connects to **PROGRAM**, as the development of continuity plans should align with the organization's broader cybersecurity strategy and planning efforts.

RESPONSE-4b

Data backups are available and tested, at least in an ad hoc manner.
This practice is fundamental to restoring operations in the event of data loss or hardware failure. The organization makes accessible, at least in an ad hoc manner, backups of information assets. When identifying information assets to be backed up, organizations should consider data that resides on different types of IT and OT assets, such as virtualized assets, regulated assets, cloud assets, Bring Your Own Device (BYOD) assets, assets managed by a third party, field assets, and mobile assets. Testing is performed for backups to help ensure they are viable and available when needed. Strategies for performing and managing backups should be based on risk to the function or the organization. This practice initiates a progression of practices that continue in MIL2 and are focused on data backups.
Backups of information assets may include:

- operational data
- set points
- configuration files
- storage locations
- copies of important configuration baselines, golden images, hard disk images, and virtual machine images

Backup procedures typically include:

- frequency standards
- retention periods
- authorized storage locations and methods
- encryption and protection requirements; testing standards

AIM-Categorization-Tiering: It primarily falls under **ASSET, CHANGE AND CONFIGURATION**, as it involves managing and maintaining backups of various information assets. Additionally, it is relevant to **RISK**, given that performing and managing backups based on the risk to the organization is crucial for protecting information assets. Lastly, it connects to **STANDARDS AND TECHNOLOGY**, as the use of established standards and procedures for backups, including encryption and protection requirements, is essential for ensuring the security and availability of these backups.

RESPONSE-4c

IT and OT assets requiring spares are identified, at least in an ad hoc manner.
This practice is fundamental to restoring operations in the event of asset loss or failure. The organization identifies, at least in an ad hoc manner, IT and OT assets for which spares may be needed. This practice initiates a progression of practices that continue in MIL2 and are focused on spare or redundant assets.
These are examples of spare or redundant IT and OT assets:

- switches

- routers
- controllers
- sensors
- virtualized assets
- systems on which assets rely, such as communications networks

AIM-Categorization-Tiering: It primarily falls under **ASSET, CHANGE AND CONFIGURATION**, as it involves managing and identifying critical assets and ensuring that spares are available for restoration in case of failure. Additionally, it is relevant to **RISK**, as the practice of having spares helps mitigate the risk of operational disruption due to asset loss or failure. Lastly, it connects to **ARCHIECTURE**, since designing a robust and secure technology infrastructure includes planning for spare or redundant assets to maintain operational continuity.

RESPONSE-4d

Continuity plans address potential impacts from cybersecurity incidents.
Continuity plans address the most critical business functions of the organization to ensure they continue during different types of emergencies. Therefore, to help ensure that continuity plans cover all the actions that need to be taken when certain types of cyber incidents occur, identify types of incidents that might realistically happen to your organization and cause significant disruption. Sources of information may include threat profile information, past incidents, current attack trends, vulnerability information, and cybersecurity alerts. Analysis techniques such as research, brainstorming, subject matter expert interview, and threat modeling may then be applied to identify the likely impacts of those incidents. Impact descriptions should name specific assets that would be affected by each type of incident. Develop as many continuity plans as needed to describe the actions that would need to be taken to deal with potential impacts and sustain operations during the disruption.

AIM-Categorization-Tiering: It primarily falls under **INCIDENT DETECTION AND RESPONSE**, as it involves planning for the detection and recovery from cybersecurity incidents to sustain critical business functions. Additionally, it relates to **RISK**, as it emphasizes identifying and managing the potential risks and impacts of different types of cyber incidents. Lastly, it connects to **PROGRAM**, since developing and implementing continuity plans is a strategic component of an organization's overall cybersecurity program, aligning with business objectives and ensuring resilience during disruptions.

RESPONSE-4e

The assets and activities necessary to sustain minimum operations of the function are identified and documented in continuity plans.
Although organizations perform many activities in support of and related to the delivery of the function, during times of disruption minimum operations can often be performed with a smaller set of those activities. By identifying the subset of critical activities needed to support minimum operations, the organization can prioritize response activities and focus resources on restoring the assets that support those activities first.
Function leaders must first decide what constitutes "minimum operations." They might do this by identifying the operations that most directly affect the ability to achieve the function's primary mission, or which operations their

highest priority customers depend on. IT and OT operations teams should then identify which systems, technologies, data, staff, and processes are associated with maintaining those operations at normal functionality (including any dependencies on external functions or entities). IT and OT teams can then determine how minimum operations could be sustained in different types of degraded conditions (for example, if certain databases, staff, or external data feeds that the operations depend on are not available).
Additionally, organizations should consider what sustaining minimum operations may require in different situations. For example, in a pandemic situation where sudden wide-spread remote work is necessary, individuals may not have physical access to high-priority equipment.

AIM-Categorization-Tiering: Primarily, it falls under **INCIDENT DETECTION AND RESPONSE**, as it involves planning and prioritizing response activities to ensure the continuity of critical operations during disruptions. Additionally, it relates to **RISK**, as it emphasizes identifying and managing the risks associated with sustaining minimum operations under various conditions. Lastly, it connects to **PROGRAM**, since developing continuity plans is a strategic component of an organization's overall cybersecurity program, aligning with business objectives and ensuring resilience during disruptions.

RESPONSE-4f

Continuity plans address IT, OT, and information assets that are important to the delivery of the function, including the availability of backup data and replacement, redundant, and spare IT and OT assets.
Developers of continuity plans should leverage asset inventory and prioritization information (ASSET-1 and ASSET-2 practices) to ensure that continuity plans cover all assets important to the delivery of the function. Details about backups and spares for those assets should be included in the plans, including virtualized asset backups and snapshots captured for recovery purposes. Organizations that are depending on the cloud as a backup location either for on-premise data or cloud data should consider the impact of a cloud event, incident, or vulnerability on the availability of backups.

AIM-Categorization-Tiering: Primarily, it falls under **ASSET, CHANGE AND CONFIGURATION**, as it emphasizes leveraging asset inventory and prioritization information to ensure that all critical assets are covered in the continuity plans, including details about backups and spares. Additionally, it relates to **INCIDENT DETECTION AND RESPONSE**, since having comprehensive continuity plans that include backup and spare assets is essential for responding to and recovering from incidents. Lastly, it connects to **RISK**, as ensuring the availability of backup data and replacement assets helps manage the risks associated with potential disruptions and vulnerabilities, including those related to cloud dependencies.

RESPONSE-4g

Recovery time objectives (RTOs) and recovery point objectives (RPOs) for assets that are important to the delivery of the function are incorporated into continuity plans.
Continuity plans should include information to enable prioritization of assets for recovery in an incident. Inputs to development of RTOs and RPOs include the cost of recovery from an incident, the potential cost of downtime or lost data, regulatory requirements, operational requirements, and recovery solution cost. Where RTOs and RPOs have been defined for any assets important to the delivery of the function, they should be included in any continuity plans that contain recovery steps for those assets.

AIM-Categorization-Tiering: Primarily, it falls under **ASSET, CHANGE AND CONFIGURATION**, as it involves prioritizing and managing critical assets based on their recovery objectives during incidents. Additionally, it pertains to **INCIDENT DETECTION AND RESPONSE**, since defining RTOs and RPOs is crucial for effective response and recovery planning during cybersecurity incidents. Lastly, it is connected to **RISK**, because understanding and incorporating RTOs and RPOs help manage the risks associated with potential downtime, data loss, and regulatory compliance, ensuring the organization can minimize the impact of security breaches effectively.

RESPONSE-4h

Cybersecurity incident criteria that trigger the execution of continuity plans are established and communicated to incident response and continuity management personnel.
A link should be established between incident response and continuity activities. Determine the conditions under which a continuity plan must be executed and ensure that the incident response personnel and owners of continuity plans understand these conditions.

AIM-Categorization-Tiering: Primarily, it falls under **INCIDENT DETECTION AND RESPONSE** because it involves defining and communicating the criteria for initiating continuity plans during incidents, ensuring that response actions are timely and effective. Additionally, it pertains to **POLICY AND STRATEGY**, as establishing clear criteria for incident response and continuity plan execution reflects the organization's strategy for managing cybersecurity incidents and maintaining operational resilience. Moreover, it is connected to **PROGRAM**, since it involves integrating continuity plans with the broader cybersecurity strategy and ensuring that incident response and continuity management personnel are aligned and informed about their roles and responsibilities during an incident.

RESPONSE-4i

Continuity plans are tested through evaluations and exercises periodically and according to defined triggers, such as system changes and external events.
Testing is often the only opportunity for an organization to know whether the plans meet their stated objectives. Testing should be conducted in a controlled environment. The testing program and standards should be enforced to ensure consistency and the ability to interpret results at the organizational level.
Standards for continuity testing can include:

- types of tests (e.g., walkthroughs, tabletops, dependency testing, testing backups and spares)
- required test components
- quality assurance standards
- involvement and commitment of plan stakeholders
- reporting standards
- measurement standards
- test plan maintenance

Testing of backup and storage and related procedures should be done to ensure they are meeting the requirements of the function. Periodic testing of the organization's backup and storage procedures helps ensure continued validity as operational conditions change. Additionally, organizations should consider coordination with appropriate stakeholders for the different kinds of IT, OT, and information assets that may be within the scope for exercises such as virtualized assets, regulated assets, cloud assets, and mobile assets.

AIM-Categorization-Tiering: Primarily, it falls under **INCIDENT DETECTION AND RESPONSE** because it involves testing and evaluating continuity plans to ensure they are effective in responding to incidents. It also pertains to **STANDARDS AND TECHNOLOGY** as the testing process should follow established standards to maintain consistency and reliability. Additionally, it is connected to **ASSET, CHANGE AND CONFIGURATION** since it emphasizes the need to test various IT, OT, and information assets, ensuring their continued validity as operational conditions change. Furthermore, **PROGRAM** is relevant because the periodic testing of continuity plans is part of the broader cybersecurity strategy and planning, ensuring alignment with organizational objectives and the involvement of relevant stakeholders.

RESPONSE-4j

Cybersecurity controls protecting backup data are equivalent to or more rigorous than controls protecting source data.
Ensure that the controls that are being used to protect backup data are at least equivalent to the controls that protect the source data. The organization should select controls that are designed to meet cybersecurity requirements (ARCHITECTURE-1f). The organization may require backup data to have more rigorous cybersecurity controls such as data integrity monitoring or using write once, read many (WORM) technology to prevent modification of data.

AIM-Categorization-Tiering: It primarily relates to **STANDARDS AND TECHNOLOGY** and **ARCHITECTURE**. This is because ensuring that backup data is protected by stringent cybersecurity controls aligns with the use of established cybersecurity standards and technologies to secure an organization's data. Additionally, it pertains to Architecture as it involves designing and implementing robust technology infrastructure to protect both source and backup data, ensuring data integrity and preventing unauthorized modification.

RESPONSE-4k

Data backups are logically or physically separated from source data.
Data backups are stored in a way that reduces or eliminates the risk that a cyber attack that results in alteration or destruction of data could also result in alteration or destruction of that data's backups.

AIM-Categorization-Tiering: It primarily relates to **ARCHITECTURE** and **THREAT AND VULNERABILITY**. This is because ensuring that data backups are stored in a way that reduces the risk of alteration or destruction by cyber attacks involves designing and implementing a robust technology infrastructure to protect critical assets and data. By logically or physically separating backups, the organization mitigates the security risks associated with potential threats and vulnerabilities, ensuring the integrity and availability of essential data. Thus, Architecture addresses the secure design and implementation aspect, while Threat and Vulnerability focuses on the mitigation of risks associated with cyber attacks on data backups.

RESPONSE-4l

Spares for selected IT and OT assets are available.
The organization makes accessible or has procedures to obtain spare or redundant IT and OT assets (as identified in RESPONSE-4c). Testing and routine maintenance (such as patching and configuration updates) are performed for spares and redundancies to help ensure they are viable and available when needed.
These are examples of spare or redundant IT and OT assets:

- switches
- routers
- controllers
- sensors
- virtualized assets
- systems on which assets rely, such as communications networks

AIM-Categorization-Tiering: It belongs to the category **ASSET, CHANGE AND CONFIGURATION** as it refers to the management and control of the organization's information technology assets, including the availability and maintenance of spares and redundant assets. It also involves ongoing monitoring and maintenance, such as patching and configuration updates, to ensure these assets are viable and available when needed. Furthermore, this statement could be related to **INCIDENT DETECTION AND RESPONSE** since having accessible spares and redundant assets is crucial for rapid and effective response to incidents, ensuring minimal disruption to operations. Additionally, **ARCHITECTURE** is relevant as it encompasses designing and implementing a robust technology infrastructure, which includes the availability of spare and redundant systems to protect an organization's assets and data.

RESPONSE-4m

Continuity plans are aligned with identified risks and the organization's threat profile (THREAT-2e) to ensure coverage of identified risk categories and threats.
When developing continuity plans, the organization should review the function's risk categories and threat profile to help ensure that continuity plans are developed for all potential types of cyber incidents. To align continuity planning with the threat profile, organizations should review the targeted assets, objectives, and attack methods that may be employed by threat actors and adjust continuity scenarios to address potential impacts from cybersecurity threats. For example, the threat profile might describe a feasible scenario in which manufacturing control systems are compromised and destructive malware is deployed that causes physical damage to specialized manufacturing equipment. A continuity plan would be developed that contained all the actions necessary to recover the control systems, initiate repair or replacement of the manufacturing equipment affected, and sustain manufacturing operations as much as possible during the disruption.

AIM-Categorization-Tiering: It pertains to the category **THREAT AND VULNERABILITY** as it emphasizes the importance of aligning continuity plans with the organization's threat profile to address identified risks and threats. This involves reviewing risk categories and threat profiles to develop comprehensive continuity plans

for various types of cyber incidents. Additionally, it is related to **RISK** because it involves assessing and managing risks to ensure that continuity plans cover all potential impacts from cybersecurity threats. Moreover, the statement is relevant to **INCIDENT DETECTION AND RESPONSE** as it discusses preparing continuity plans that include actions necessary to recover from incidents, such as repairing or replacing compromised equipment and maintaining operations during disruptions.

RESPONSE-4n

Continuity plan exercises address higher priority risks.
The organization should use information about prioritized risks as determined in RISK-3a to create specific scenarios for which the continuity plans should be tested.

AIM-Categorization-Tiering: It belongs to the category **RISK** because it involves using information about prioritized risks to create specific scenarios for continuity plan exercises. This process ensures that the organization can adequately protect its information assets by addressing higher priority risks. Additionally, it relates to **INCIDENT DETECTION AND RESPONSE** as it emphasizes testing continuity plans through exercises, which is crucial for preparing the organization to effectively detect, respond to, and recover from cybersecurity incidents. Lastly, **POLICY AND STRATEGY** is relevant since it involves establishing clear policies and strategies for continuity planning based on identified risks, ensuring comprehensive management and mitigation of these risks.

RESPONSE-4o

The results of continuity plan testing or activation are compared to recovery objectives, and plans are improved accordingly.
Both continuity plan testing and activation of plans in actual incidents can provide insight about whether plans work as intended. After either a test or an activation of a plan, results should be compared with the plan's recovery objectives, including any defined RTOs and RPOs. Areas where objectives could not be met should be recorded and strategies developed to review and revise the plan. Improvements to the testing process and plans should also be identified, documented, and incorporated into future tests.
Continuity plan testing and activation may also reveal needed improvements due to

- lack of sufficient resources
- lack of appropriate resources
- training gaps for plan staff and stakeholders
- plan conflicts (if multiple plans are tested simultaneously)
- infrastructure shortcomings

AIM-Categorization-Tiering: It belongs to the category **PROGRAM** because it involves evaluating and improving continuity plans, which are key components of an organization's cybersecurity strategy and planning. This process ensures that the continuity plans align with the organization's recovery objectives and business goals. Additionally, it relates to **RISK** as it focuses on comparing the results of continuity plan testing with recovery objectives to identify and manage risks effectively. This helps the organization minimize the impact of potential security breaches. Furthermore, it pertains to **INCIDENT DETECTION AND RESPONSE** since the testing

and activation of continuity plans are crucial for ensuring that the organization is prepared to detect, respond to, and recover from cybersecurity incidents. Lastly, **KNOWLEDGE AND CAPABILITIES** is relevant as it highlights the importance of identifying and addressing training gaps and resource deficiencies during the testing process, which is essential for maintaining effective and resilient continuity plans.

RESPONSE-4p

Continuity plans are periodically reviewed and updated.
The testing and execution of service continuity plans are two sources of potential updates to plans. However, a dynamic operating environment, sources of new threats and risks, and changes such as those in staff, geographical location, and relationships with external entities can require changes to service continuity plans and their corresponding test plans.
These are examples of conditions that may result in changes to continuity plans:

- identification of new vulnerabilities, threats, and risks
- changes to IT, OT, or information assets
- relocation of facilities
- changes in an asset's protective controls
- changes in the plan's stakeholders, including external entities and public agencies

AIM-Categorization-Tiering: It belongs to the category **PROGRAM** because it involves the periodic review and updating of continuity plans, which is essential for maintaining an effective cybersecurity strategy aligned with the organization's business objectives. This ensures that the continuity plans remain relevant and effective in the face of changes in the organization's environment. Additionally, it relates to **RISK** as it emphasizes the need to update continuity plans in response to new vulnerabilities, threats, and risks, thereby helping the organization to better manage and mitigate these risks. Furthermore, it pertains to **ASSET, CHANGE AND CONFIGURATION** since changes in IT, OT, or information assets, as well as other operational shifts, require corresponding updates to continuity plans. Lastly, **THREAT AND VULNERABILITY** is relevant as the identification of new threats and vulnerabilities directly influences the need to revise and improve continuity plans to ensure ongoing protection against emerging risks.

6.5 Management Activities

RESPONSE-5a

Documented procedures are established, followed, and maintained for activities in the RESPONSE domain.
The activities in the RESPONSE domain are formally documented in some way (such as standard operating procedures, process flow diagrams, RACI charts, swim lane diagrams, or similar documentation). The activities are intentionally designed or described to serve the organization rather than being ad hoc. Documenting procedures helps ensure that they are repeatable and produce expected outcomes. The level of detail included in documentation should be a sufficient to enable consistent performance of domain activities by different people and new employees assuming relevant domain experience and sufficient on-board training.
Also, procedure documentation is made available to and is used by relevant personnel. The documentation is updated as needed to reflect changes in the organizational or operational environment. Additionally, organizations

may consider including exceptions processes in documented procedures to ensure that the organization reacts appropriately to unexpected events or situations.
When responding to an incident, or otherwise operating in an abnormal state, it is more likely that exceptions to normal business practices will be necessary. Planning for procedural flexibility increases operational resilience when unexpected situations occur. Incident response planning can support this by helping to define potential operating states that may occur as part of potential crises and reviewing policy from the perspective of operations through different types of crises.
Additionally, defining explicit exception processes further supports flexibility and resilience. Exception process should include after action reviews of exceptions and their impact on security following a return to a normal operating state.

AIM-Categorization-Tiering: It belongs to the category **INCIDENT DETECTION AND RESPONSE** because it involves the establishment, documentation, and maintenance of procedures for activities in the RESPONSE domain, which are critical for ensuring effective and consistent incident response. This process ensures that the organization can respond to incidents in a structured and repeatable manner, thereby improving its ability to detect, respond to, and recover from cybersecurity incidents. Additionally, it relates to **POLICY AND STRATEGY** as it emphasizes the importance of documenting and updating procedures to reflect changes in the organizational or operational environment, which is key to maintaining a robust and adaptable cybersecurity policy. Furthermore, it pertains to **KNOWLEDGE AND CAPABILITIES** since the documentation of procedures ensures that relevant personnel, including new employees, can consistently perform RESPONSE domain activities, thereby enhancing the organization's overall cybersecurity capabilities. Lastly, **RISK** is relevant as the inclusion of exception processes in documented procedures helps the organization manage unexpected events or situations, thereby increasing operational resilience and minimizing the impact of potential security breaches.

RESPONSE-5b

Adequate resources (people, funding, and tools) are provided to support activities in the RESPONSE domain.
When determining the adequacy of resources, it may help to consider whether there are any RESPONSE domain activities not currently being performed that the organization would perform if it had additional people, funding, or tools. An additional consideration may be whether the organization has implemented all practices it has targeted for implementation and whether additional resources are necessary to address potential gaps.
Adequate resources are provided in the form of people, funding, and tools to ensure that RESPONSE domain practices can be performed as intended. The performance of this practice can be evaluated by determining whether any desired practices have not been implemented due to a shortage of resources.
These are examples of people involved in RESPONSE domain activities:

- cybersecurity, business continuity, and IT operations officers, directors, and managers
- staff responsible for training and skill development
- staff responsible for designing and performing cybersecurity awareness activities

These are examples of tools that might be used in RESPONSE domain activities:

- a performance management system that supports establishing performance goals and objectives and evaluating performance against them

- job description templates that reflect standard resilience obligations, roles, and responsibilities, required skills, and specific job requirements (e.g., certifications)
- methods for delivering awareness and training materials, such as user on-demand training
- tools for tracking awareness and training course attendance

Adequacy of resources should be determined on an ongoing basis through regular reviews of the domain program and reviews of domain resources in budgeting activities. It is a common point of concern that there is not enough time to complete cybersecurity program activities. This is addressed primarily through increasing staff and secondarily through increasing funding and tools.
When determining the adequacy of staff, also consider whether the cybersecurity program has sufficient capacity so that the individuals that make up the program can regularly attend training, implement and maintain tools, and respond to incidents while conducting day-to-day operations and meeting the cybersecurity objectives of the organization.

AIM-Categorization-Tiering: It belongs to the category **INCIDENT DETECTION AND RESPONSE** because it focuses on ensuring that adequate resources, such as people, funding, and tools, are provided to support the activities necessary for effective incident response. This ensures that the organization can perform RESPONSE domain practices as intended, thereby improving its ability to detect, respond to, and recover from cybersecurity incidents. Additionally, it relates to **PROGRAM** as it involves evaluating the sufficiency of resources to implement and maintain all targeted practices, which is critical for a well-functioning cybersecurity strategy. Furthermore, it pertains to **WORKFORCE** since the adequacy of personnel involved in RESPONSE activities, including their capacity to attend training and perform their roles effectively, is essential for maintaining a resilient cybersecurity program. Lastly, **KNOWLEDGE AND CAPABILITIES** is relevant as the resources provided, including tools for training and skill development, contribute to the overall capabilities and readiness of the organization to handle cybersecurity challenges.

RESPONSE-5c

Up-to-date policies or other organizational directives define requirements for activities in the RESPONSE domain. Activities in the RESPONSE domain receive documented guidance and direction from the organization in the form of policies or similar directives. Strategic business objectives drive the development of documented policies or other organizational directives to ensure activities support the accomplishment of the organization's mission.
Policies or other organizational directives for RESPONSE domain activities may contain

- 1responsibility, authority, and ownership for performing RESPONSE activities
- procedures, standards, and guidelines for RESPONSE activities such as detecting, logging, reporting, and tracking events, collecting and preserving evidence, triaging events, declaring incidents, and responding to incidents
- requirements for the frequency of updating cybersecurity incident declaration criteria
- criteria for notifying cybersecurity stakeholders of events and incidents
- methods for measuring adherence to policy, exceptions granted, and policy violations

· procedures for the granting and management of exceptions

AIM-Categorization-Tiering: It belongs to the category **POLICY AND STRATEGY** because it involves the creation and maintenance of up-to-date policies or organizational directives that define the requirements for activities in the RESPONSE domain. This ensures that RESPONSE activities are aligned with the organization's strategic business objectives and that they support the accomplishment of the organization's mission. Additionally, it relates to **INCIDENT DETECTION AND RESPONSE** as it provides documented guidance for critical RESPONSE domain activities such as detecting, logging, reporting, and responding to incidents, which are essential for effective incident management. Furthermore, it pertains to **RISK** since the policies include criteria for declaring incidents and notifying stakeholders, which are vital for managing and mitigating risks associated with cybersecurity events. Lastly, **PROGRAM** is relevant as these policies and directives ensure that RESPONSE activities are clearly defined, properly executed, and continuously updated to reflect the evolving operational environment, thereby contributing to a comprehensive and effective cybersecurity program.

RESPONSE-5d

Responsibility, accountability, and authority for the performance of activities in the RESPONSE domain are assigned to personnel.
The intent of this practice is that specific people (or people in specific roles) are held accountable for ensuring the achievement of expected results of RESPONSE domain activities and that they are given the appropriate authority to act and to perform their assigned responsibilities.
These are examples of how to formalize responsibility and authority for RESPONSE domain activities:

· defining roles and responsibilities in policies (see RESPONSE-4c)

· developing position descriptions and conducting associated performance management activities

· including process tasks and responsibility for these tasks in position descriptions

· developing and implementing contractual instruments (including service level agreements) with external entities to establish responsibility and authority for performing RESPONSE domain tasks on outsourced functions

· including RESPONSE domain tasks in measuring performance of external entities against contractual instruments

Additionally, consider how the knowledge developed by personnel within this domain should be managed and shared. This includes determining what processes and tools should be used for knowledge sharing and identifying who will be responsible for making the best use of internal knowledge.

AIM-Categorization-Tiering: It belongs to the category **WORKFORCE** because it involves assigning responsibility, accountability, and authority to specific personnel for the performance of activities in the RESPONSE domain. This ensures that individuals or roles are clearly defined and held accountable for achieving the expected outcomes of RESPONSE activities. Additionally, it relates to **INCIDENT DETECTION AND RESPONSE** as it formalizes the roles and responsibilities necessary for effectively managing and responding to cybersecurity incidents. Furthermore, it pertains to **POLICY AND STRATEGY** since defining roles and responsibilities in policies, developing position descriptions, and establishing performance management activities are critical for

ensuring that RESPONSE activities are executed according to the organization's strategic objectives. Lastly, **KNOWLEDGE AND CAPABILITIES** is relevant as it highlights the importance of managing and sharing the knowledge developed by personnel within the RESPONSE domain, ensuring that internal knowledge is effectively utilized to enhance the organization's overall cybersecurity posture.

RESPONSE-5e

Personnel performing activities in the RESPONSE domain have the skills and knowledge needed to perform their assigned responsibilities.
The organization must identify the skills and knowledge needed to perform RESPONSE domain activities and identify skill and knowledge gaps in existing personnel. The organization can address gaps either by hiring qualified personnel or training existing personnel. It is important to note that managing and securing many technologies (such as virtualized or cloud-based environments) require specific training in specialized equipment and practices. Care should be taken to ensure that the level of skills and knowledge of personnel managing and securing specialized technologies is commensurate with the importance of and risk posed by those technologies.
Additionally, skill and knowledge assessments should be repeated as operational environments change over time. For example, in the RESPONSE domain, skills and knowledge are needed for

- event detection, reporting, and tracking, including service desk activities
- documenting and logging event reports
- collecting and preserving evidence
- technical analysis of events and incidents, including triage
- declaring incidents
- escalating and communicating incidents
- creating, managing, and deploying incident response teams

AIM-Categorization-Tiering: It belongs to the category **KNOWLEDGE AND CAPABILITIES** because it focuses on ensuring that personnel performing activities in the RESPONSE domain possess the necessary skills and knowledge to fulfill their assigned responsibilities. This is crucial for the effective execution of RESPONSE activities and for maintaining a high level of cybersecurity preparedness. Additionally, it relates to **WORKFORCE** as it involves identifying skill and knowledge gaps in existing personnel and addressing these gaps through training or hiring, ensuring that the workforce is adequately equipped to manage and secure specialized technologies. Furthermore, it pertains to **INCIDENT DETECTION AND RESPONSE** since the skills and knowledge required for activities such as event detection, reporting, technical analysis, and incident management are directly related to the organization's ability to effectively detect, respond to, and recover from cybersecurity incidents. Lastly, **RISK** is relevant because ensuring that personnel have the appropriate skills and knowledge to manage and secure critical technologies helps mitigate the risks associated with those technologies, thereby protecting the organization's assets and information.

RESPONSE-5f

The effectiveness of activities in the RESPONSE domain is evaluated and tracked.
The organization should measure the performance of RESPONSE activities to ensure they are being performed as described in plans, policies, and procedures for the RESPONSE domain. Appropriate metrics should be developed and collected to detect deviations in performance and measure the extent to which RESPONSE domain activities are achieving their intended purpose.

AIM-Categorization-Tiering: It belongs to the category **INCIDENT DETECTION AND RESPONSE** because it focuses on evaluating and tracking the effectiveness of RESPONSE domain activities, ensuring that these activities are performed according to established plans, policies, and procedures. This is crucial for the organization's ability to detect, respond to, and recover from cybersecurity incidents effectively. Additionally, it relates to **POLICY AND STRATEGY** as it involves the development and collection of appropriate metrics to measure the performance of RESPONSE activities, ensuring that these activities align with the organization's strategic objectives and are achieving their intended purpose. Furthermore, it pertains to **RISK** because measuring the effectiveness of RESPONSE activities helps identify deviations in performance, allowing the organization to address potential vulnerabilities and minimize the impact of security incidents on its assets and operations.

7. Third-Party Risk Management - 25 questions

As presented on the platform, its purpose is: Establish and maintain controls to manage the cybersecurity risks associated with services and assets that are dependent on external entities, commensurate with the risk to critical infrastructure and organizational objectives.

The Third-Party Risk Management (THIRD-PARTIES) domain comprises three objectives:

1. Identify and Prioritize Third Parties
2. Manage Third-Party Risk
3. Management Activities for the THIRD-PARTIES domain

7.1 Identify and Prioritize Third Parties

THIRD-PARTIES-1a

Important IT and OT third-party dependencies are identified (that is, internal and external parties on which the delivery of the function depends, including operating partners), at least in an ad hoc manner.
Identify and maintain basic information about internal and external parties who may be required for continued performance of the function. Supplier dependencies, for example, might include IT service providers, incident response consultants, and equipment providers. Third parties may support the organization's IT or OT assets and operational activities. Such information should be maintained in a form that is available to those responsible for third-party risk management.

AIM-Categorization-Tiering: It belongs to the category **ASSET, CHANGE AND CONFIGURATION** because it involves identifying and maintaining information about internal and external third-party dependencies that are critical for the continued performance of IT and OT functions. This ensures that the organization has a clear understanding of the assets and external relationships that are essential to its operations. Additionally, it

relates to **RISK** as identifying important third-party dependencies is crucial for managing and mitigating risks associated with relying on external entities for IT and OT functions, thereby protecting the organization's assets and ensuring business continuity. Furthermore, it pertains to **PROGRAM** since maintaining information about third-party dependencies is an important aspect of a comprehensive cybersecurity strategy, ensuring that all critical dependencies are recognized and managed within the broader scope of the organization's risk management and operational plans.

THIRD-PARTIES-1b

Third parties that have access to, control of, or custody of any IT, OT, or information assets that are important to delivery of the function are identified, at least in an ad hoc manner.
Create and maintain a list that provides basic information identifying important internal and external parties that have access to, control of, or custody of any IT, OT, or information assets. For some third parties, such as corporate IT, these important relationships may be entirely internal.

AIM-Categorization-Tiering: It belongs to the category **ASSET, CHANGE AND CONFIGURATION** because it involves identifying and maintaining a list of third parties that have access to, control of, or custody of critical IT, OT, or information assets. This ensures that the organization has a clear understanding of who has control over its essential assets and can manage these relationships effectively. Additionally, it relates to **RISK** as identifying third parties with access to important assets is crucial for managing and mitigating risks associated with external and internal dependencies, helping to protect the organization's assets from potential vulnerabilities. Furthermore, it pertains to **PROGRAM** since creating and maintaining this list is a vital part of a comprehensive cybersecurity strategy, ensuring that all critical relationships are recognized and managed within the broader context of the organization's operational and risk management plans.

THIRD-PARTIES-1c

A defined method is followed to identify risks arising from suppliers and other third parties.
A defined method is planned in advance, clearly described, made definite, and standardized. Employing a defined method to identify risks arising from suppliers and other third parties will aid the organization's risk management processes in producing consistent outputs and better enable effective management of third party risk.

AIM-Categorization-Tiering: It belongs to the category **RISK** because it focuses on using a defined, standardized method to identify risks arising from suppliers and other third parties. This approach is essential for consistent risk management and ensures that the organization can effectively manage potential vulnerabilities introduced by third-party relationships. Additionally, it relates to **POLICY AND STRATEGY** as it involves the development and implementation of a clear, predefined method that aligns with the organization's overall risk management strategy, supporting the consistent and effective management of third-party risks. Furthermore, it pertains to **ASSET, CHANGE AND CONFIGURATION** since managing third-party risks is crucial for protecting the organization's IT, OT, and information assets, ensuring that external dependencies do not compromise the integrity and security of these critical resources.

THIRD-PARTIES-1d

Third parties are prioritized according to established criteria (for example, importance to the delivery of the function, impact of a compromise or disruption, ability to negotiate cybersecurity requirements within contracts).

Prioritization of third parties establishes one or more subsets of entities on which the organization must focus its cybersecurity activities due to defined criteria, such as their importance to the delivery of the function or their role as a critical supplier. The prioritization and criteria should ensure that the prioritization scheme and the list of prioritized third parties are appropriate for the organization's risk environment and tolerance. Failure to prioritize third parties may lead to inadequate protection of important assets and disproportionate attention and resources devoted to third parties with limited potential impact on the function.

AIM-Categorization-Tiering: It belongs to the category **RISK** because it involves prioritizing third parties based on established criteria, such as their importance to the organization's functions and the potential impact of a compromise or disruption. This prioritization is essential for managing risks effectively, ensuring that the organization focuses its cybersecurity efforts on the most critical third-party relationships. Additionally, it relates to **PROGRAM** as it involves developing and applying a systematic approach to third-party prioritization, aligning this process with the organization's overall risk management strategy and ensuring that resources are allocated appropriately. Furthermore, it pertains to **ASSET, CHANGE AND CONFIGURATION** since prioritizing third parties based on their potential impact helps protect the organization's critical assets by ensuring that cybersecurity requirements are negotiated and enforced within contracts for the most important relationships.

THIRD-PARTIES-1e

Escalated prioritization is assigned to suppliers and other third parties whose compromise or disruption could cause significant consequences (for example, single-source suppliers, suppliers with privileged access).
When establishing prioritization criteria, the organization should consider situations where reliance upon a third party could be a single point of failure or the disruption of a third-party service could have significant impact on service delivery. For example, if the organization relies upon a single source for wide area network connectivity at a critical site, this would be a high-priority dependency because disruption of that supply would have the potential to cause significant organizational consequences.

AIM-Categorization-Tiering: It belongs to the category **RISK** because it involves assigning escalated prioritization to suppliers and other third parties whose compromise or disruption could lead to significant consequences. This practice is crucial for managing risks, particularly those that could serve as single points of failure or have a high impact on the organization's operations. Additionally, it relates to **PROGRAM** as it involves establishing clear prioritization criteria that align with the organization's risk management strategy, ensuring that high-priority dependencies are identified and managed with appropriate resources and attention. Furthermore, it pertains to **ASSET, CHANGE AND CONFIGURATION** since managing these high-priority third parties is essential for protecting critical assets and ensuring continuity of operations, particularly in scenarios where reliance on a single source or privileged access could pose substantial risks.

THIRD-PARTIES-1f

Prioritization of suppliers and other third parties is updated periodically and according to defined triggers, such as system changes and external events.
The organization should review prioritization of third parties to ensure that third parties that pose the greatest risk to the function receive adequate attention. This reevaluation of third-party priority may be driven by a defined timeframe or by defined triggers such as the acquisition of a product from a new vendor or open source information about the financial standing of a company.

AIM-Categorization-Tiering: It belongs to the category **RISK** because it involves the periodic updating of supplier and third-party prioritization based on defined triggers, such as system changes and external events, to manage the risks these entities pose to the organization. This ongoing reassessment ensures that the organization remains responsive to changes in its risk environment, focusing attention on those third parties that pose the greatest potential threat. Additionally, it relates to **PROGRAM** as it involves implementing a systematic process for updating third-party prioritization, aligning it with the organization's risk management strategy and ensuring that the process is both dynamic and reflective of current conditions. Furthermore, it pertains to **ASSET, CHANGE AND CONFIGURATION** since regularly updating the prioritization of third parties based on changes in systems or external factors helps protect the organization's critical assets by ensuring that the most significant risks are continually addressed.

7.2 Manage Third-Party Risk

THIRD-PARTIES-2a

The selection of suppliers and other third parties includes consideration of their cybersecurity qualifications, at least in an ad hoc manner.
The cybersecurity qualifications for suppliers and other third parties might include, for example, maintaining a specified level of cybersecurity control implementation, previous cyber incidents involving the third party, background checks for personnel who have access to critical assets, and requirements for reporting breaches and other cybersecurity incidents.

AIM-Categorization-Tiering: It belongs to the category **RISK** because it involves evaluating the cybersecurity qualifications of suppliers and other third parties as part of their selection process. This ensures that the organization mitigates potential risks by choosing partners who meet specified cybersecurity standards and can adequately protect critical assets. Additionally, it relates to **PROGRAM** as it involves incorporating cybersecurity considerations into the selection criteria for third parties, aligning with the organization's broader cybersecurity strategy and objectives. This process ensures that third-party risks are managed from the outset of the relationship, contributing to the overall security posture of the organization. Furthermore, it pertains to **LEGAL AND REGULATORY FRAMEWORK** since considering cybersecurity qualifications during the selection of third parties helps ensure compliance with relevant laws and regulations, as well as with any contractual obligations related to cybersecurity.

THIRD-PARTIES-2b

The selection of products and services includes consideration of their cybersecurity capabilities, at least in an ad hoc manner.
The cybersecurity requirements for products and services might include, for example, ability to disable certain functionality of a product, a clear understanding of components used in a product, and terms of service for a service that meet cybersecurity requirements.

AIM-Categorization-Tiering: It belongs to the category **RISK** because it involves assessing the cybersecurity capabilities of products and services during the selection process, which is crucial for mitigating potential risks associated with their use. This evaluation helps ensure that selected products and services meet the organization's cybersecurity needs and do not introduce vulnerabilities. Additionally, it relates to **STANDARDS AND**

TECHNOLOGY as it requires the organization to consider whether the products and services align with established cybersecurity standards and best practices, ensuring a robust security posture. Furthermore, it pertains to **PROGRAM** since incorporating cybersecurity capabilities into the selection criteria reflects a strategic approach to cybersecurity, ensuring that all technology acquisitions support the organization's broader security objectives and compliance requirements.

THIRD-PARTIES-2c

A defined method is followed to identify cybersecurity requirements and implement associated controls that protect against the risks arising from suppliers and other third parties.
Cybersecurity requirements should be identified according to a defined methodology that is effective and clear. The requirements should include the controls needed to secure the products and services to address cybersecurity risks arising from suppliers and other third parties identified in the RISK domain.. Additional consideration should be given to third parties that are considered by the organization as high priority (THIRD-PARTIES-1c) because they supply, maintain, or operate critical software components that are essential to the operation of the function. The definition of a critical software component may vary widely depending on industry or critical infrastructure sector and may be informed by commonly used frameworks or control sets. For example, NIST provides a definition of critical software under Executive Order 14028 that some organizations may be required to adopt.
Cybersecurity controls should be implemented that reduce the risk that could stem from suppliers and other third parties. The organization may implement operational controls that restrict individuals from a third party such as a maintenance or janitorial service from accessing designed areas of a facility without escort. Technical controls may be necessary for third parties that supply a service like remote maintenance of an asset. The organization may also consider management controls like acqui.itions strategies that obscure the end use of an asset.
The following are examples of the types of requirements to consider:

- controls and procedures for granting access to third parties
- specifications for the governance, protection, and destruction of data
- whether the supplier will be developing software, and if so what secure coding practices must be used
- the knowledge and skills needed to perform the responsibilities assigned to third parties
- cybersecurity training that may be necessary prior to granting access to third parties
- logging, log retention, and monitoring
- incident and vulnerability notification, mitigation, and response coordination including timelines and thresholds
- incident response and information sharing
- controls governing connections to organization systems by third parties
- whether a diversity of software, assets, and suppliers is necessary to lower the risk of broad exploitation of specific vulnerabilities

Sources of information for the development of cybersecurity requirements for suppliers include analysis of previous cyber events (internal, external and "near miss"), brainstorming with internal stakeholders, interviews with cybersecurity experts, industry threat alerts, vulnerability announcements, the results of internal control reviews, vulnerability assessments, penetration tests, and other research.

AIM-Categorization-Tiering: It belongs to the category **RISK** because it involves following a defined method to identify and implement cybersecurity requirements and controls to mitigate risks arising from suppliers and other third parties. This approach ensures that the organization systematically addresses potential threats and vulnerabilities introduced by third parties. Additionally, it pertains to **STANDARDS AND TECHNOLOGY** as it requires the application of cybersecurity standards and the implementation of technical, operational, and management controls to safeguard against third-party risks. Furthermore, it relates to **PROGRAM** since the establishment of a methodical process to identify and implement controls reflects a strategic approach to cybersecurity, aligning with the organization's overall security objectives and ensuring comprehensive risk management.

THIRD-PARTIES-2d

A defined method is followed to evaluate and select suppliers and other third parties.
Using a defined method for evaluation and selection of third parties helps makes that process consistent and repeatable. For example, a part of the defined method could describe how the organization will review supplier responses to requests for proposals (RFPs) to determine if the supplier meets the necessary requirements.
This may include consideration of cybersecurity qualifications, legal standing, financial wellbeing, and relationships to foreign governments. Sources of information may include attestations provided by third parties (e.g., attestation of the suitability and effectiveness of the cybersecurity control environment) and vetting based on track record, information from third party rating services, and open-source information.

AIM-Categorization-Tiering: The statement pertains to the category **CULTURE AND SOCIETY** as it emphasizes the importance of following a consistent and repeatable method to evaluate and select suppliers and third parties, reflecting the organization's commitment to promoting cybersecurity awareness and due diligence among external partners. Additionally, it relates to **LEGAL AND REGULATORY FRAMEWORK** since the evaluation process includes considerations of legal standing and compliance with regulations, which are essential when selecting third parties. Furthermore, **RISK** is relevant as the process involves assessing the cybersecurity qualifications and potential risks associated with suppliers, ensuring that the organization effectively manages risks related to third-party relationships.

THIRD-PARTIES-2e

More rigorous cybersecurity controls are implemented for higher priority suppliers and other third parties.
Not all suppliers expose an organization to the same level of risk. Since contractually imposing specific cybersecurity requirements can result in increased costs, consideration should be taken to ensure cybersecurity requirements are proportional to potential risk. Additional consideration should be given to high priority suppliers (THIRD-PARTIES-1c) because they supply, maintain, or operate critical software components that are essential to the operation of the function. The definition of a critical software component may vary widely depending on industry or critical infrastructure sector and may be informed by commonly used frameworks or control sets. For example, NIST provides a definition of critical software under Executive Order 14028 that some organizations may be required to adopt. The organization should implement more rigorous cybersecurity controls if it is determined that

the financial impact of a potential risk would be greater than the calculated cost of the risk.

AIM-Categorization-Tiering: The statement belongs to the category **RISK** because it involves assessing the level of risk associated with different suppliers and implementing more rigorous cybersecurity controls for higher priority suppliers to mitigate potential risks effectively. It also relates to **THREAT AND VULNERABILITY** as it addresses the need to impose stronger controls on suppliers that manage or provide critical software components, which are essential to the organization's operations and could be targeted by threat actors. Additionally, **LEGAL AND REGULATORY FRAMEWORK** is relevant since the decision to impose specific cybersecurity requirements may be influenced by industry standards or legal frameworks, such as the definition of critical software provided by NIST under Executive Order 14028.

THIRD-PARTIES-2f

Cybersecurity requirements (for example, vulnerability notification, incident-related SLA requirements) are formalized in agreements with suppliers and other third parties.
Requirements in the form of contractual specifications provide the basis for formal agreements that are established to define and govern the relationships between the organization and the actions of external entities, including changes that relate to delivered products or services. For each third-party agreement, the organization should establish a detailed set of specifications that the third party must meet. These should include the cybersecurity requirements that the organization expects the third party to meet. It is important that these specifications be thorough, detailed, definitive, adequate for use as criteria when selecting external entities, suitable as language in agreements with external entities, and appropriate for use as a basis for monitoring the performance of the third party. Ideally, legal and technical staff will work closely together in the development of these requirements. For example, technical staff may face challenges regarding configuration management when there is shared responsibility for the operation of assets. The organization may consider using contract language to ensure responsibility is properly assigned for addressing configuration issues.
Agreement language can be used to specify expectations and requirements for vulnerability or incident notification, including timelines, whether notification is required prior to public disclosure, and communication mechanisms to be used. Such specifications are often documented in service level agreements (SLAs) that are included in requests for proposals (RFPs).
The agreement language should define what constitutes an event, incident, and vulnerability related to the delivery of the product or service. For example, a service outage in one region of the country that might affect other regions could be an event that the service provider should inform the organization about.

AIM-Categorization-Tiering: The statement primarily belongs to the category **LEGAL AND REGULATORY FRAMEWORK** because it discusses the formalization of cybersecurity requirements within contracts and agreements with suppliers and other third parties. This ensures that the organization complies with legal obligations and industry standards when engaging external entities. It also relates to **RISK**, as the formalization of these requirements in agreements helps manage and mitigate potential cybersecurity risks associated with third parties. Additionally, **ASSET, CHANGE AND CONFIGURATION** is relevant since the agreements may include responsibilities for configuration management, ensuring that assets are managed and configured securely, particularly when there is shared responsibility.

THIRD-PARTIES-2g

Suppliers and other third parties periodically attest to their ability to meet cybersecurity requirements.
Agreements with suppliers and other third parties should require attestation that they meet cybersecurity requirements detailed in the agreement terms. Suppliers and third parties should initially attest to meeting these requirements before execution of the agreement, along with periodically attesting that they still meet the cybersecurity requirements. For key suppliers, additional validation of attestations may be considered. This may be performed through monitoring for incidents of note, information from third party rating services, and open-source information.

AIM-Categorization-Tiering: The statement primarily aligns with the **LEGAL AND REGULATORY FRAMEWORK** category, as it focuses on the contractual obligations requiring suppliers and third parties to periodically attest to their compliance with cybersecurity requirements. This ensures that the organization maintains compliance with legal and regulatory standards over time. It also relates to **RISK**, since periodic attestations help manage and mitigate the risks associated with relying on third-party entities by ensuring they continue to meet the necessary cybersecurity standards. Additionally, **THREAT AND VULNERABILITY** is relevant, as monitoring and validating these attestations through various sources helps the organization assess and address potential threats and vulnerabilities that could arise from third-party relationships.

THIRD-PARTIES-2h

Cybersecurity requirements for suppliers and other third parties include secure software and secure product development requirements where appropriate.
The organization should have a standard process for setting secure software and product development requirements for third parties. For suppliers that will be developing software, for example, determine and specify what secure design and coding practices are acceptable, such as the NIST Secure Software Development Framework (SSDF), Building Security In Maturity Model (BSIMM), and Open Web Application Security Project (OWASP). Secure product development requirements might prohibit use of specific components with known cybersecurity issues.
Additional consideration should be given to third parties that are considered by the organization as high priority (THIRD-PARTIES-1c) because they supply, maintain, or operate critical software components that are essential to the operation of the function. The definition of a critical software component may vary widely depending on industry or critical infrastructure sector and may be informed by commonly used frameworks or control sets. For example, NIST provides a definition of critical software under Executive Order 14028 that some organizations may be required to adopt.
This activity is related to the cybersecurity architecture activities associated with selecting vendors based on their secure software development practices (ARCHITECTURE-4b and ARCHITECTURE-4e).

AIM-Categorization-Tiering: This statement primarily aligns with the **ARCHITECTURE** category, as it emphasizes the importance of establishing secure software and product development requirements for suppliers and third parties, particularly in relation to critical software components. Ensuring that third parties adhere to secure design and coding practices is essential to maintaining a robust and secure technology infrastructure. Additionally, it relates to **STANDARDS AND TECHNOLOGY**, since the organization relies on established cybersecurity frameworks and standards, such as the NIST Secure Software Development Framework (SSDF), to define and enforce these requirements. The statement also touches on **THREAT AND VULNERABILITY**, as it involves

mitigating risks associated with using specific components and ensuring that suppliers adhere to secure development practices to prevent potential vulnerabilities.

THIRD-PARTIES-2i

Selection criteria for products include consideration of end-of-life and end-of-support timelines.
Third parties should be selected according to an organized and thorough process and according to explicit specifications and selection criteria. The selection process and criteria should be designed to ensure that the selected entity can fully meet the organization's specifications as established. These criteria should include expected product life and product support periods.

AIM-Categorization-Tiering: This statement aligns with the **ASSET, CHANGE AND CONFIGURATION** category, as it focuses on the management of products by considering their end-of-life and end-of-support timelines during the selection process. Ensuring that selected products have appropriate support periods is crucial for the ongoing maintenance and security of an organization's critical assets. Additionally, it relates to **RISK**, as selecting products without considering their support timelines could expose the organization to risks associated with unsupported or outdated technology, potentially leading to vulnerabilities and security breaches.

THIRD-PARTIES-2j

Selection criteria include consideration of safeguards against counterfeit or compromised software, hardware, and services.
Third parties should be selected according to an organized and thorough process and according to explicit specifications and selection criteria. The selection process and criteria should be designed to ensure that the selected entity can fully meet the organization's specifications as established.
These criteria should include safeguards against counterfeit or compromised software, hardware, and services. For example:

- Will the supplier disclose the existence of all known methods for bypassing computer authentication in the procured product, often referred to as backdoors, and provide written documentation that all such backdoors created by the supplier have been permanently deleted from the system?
- Will the supplier provide summary documentation of the procured product's security features and security-focused instructions on product maintenance, support, and reconfiguration of default settings?

For more examples of vendor procurement criteria that can be derived from procurement language, see the DOE Cybersecurity Procurement Language for Energy Delivery Systems.

AIM-Categorization-Tiering: This statement aligns with the **THREAT AND VULNERABILITY** category, as it emphasizes the importance of selecting third-party products and services that include safeguards against counterfeit or compromised software, hardware, and services. By incorporating these considerations into selection criteria, the organization can better identify and mitigate risks associated with potential threats and vulnerabilities introduced through third-party products. It also relates to **STANDARDS AND TECHNOLOGY**, since evaluating and requiring specific safeguards as part of the selection process ensures that the products and services meet established cybersecurity standards and technological requirements essential for protecting the organization's systems and data.

THIRD-PARTIES-2k

Selection criteria for higher priority assets include evaluation of bills of material for key asset elements, such as hardware and software.
The creation, manufacturing, and assembly of assets supplied by third-parties often comprise many sub-parts and sub-components sourced from other vendors and suppliers. Organizations that acquire these assets from third-parties may unknowingly inherit cyber risks that have not been identified or mitigated.
A bill of materials establishes and itemizes the source of sub-parts and sub-components for acquired assets, including their origin and any additional information that can help the organization establish a determination of inherited risk. Examples of these sub-parts and sub-components could be incorporating software routines from an open source libraries as a component of a software build or the sourcing of parts in a security camera from a known hostile nation-state.

AIM-Categorization-Tiering: This statement is relevant to the **ASSET, CHANGE AND CONFIGURATION** category, as it involves the careful evaluation and management of key asset elements, including hardware and software, through the use of bills of materials. By itemizing the sources of sub-parts and sub-components, organizations can better manage their assets and mitigate potential risks associated with third-party components. It also aligns with **THREAT AND VULNERABILITY**, since understanding the origin of these elements and evaluating them for potential risks helps the organization identify and address vulnerabilities that could be exploited. This process is critical for ensuring that higher priority assets are protected against inherited cybersecurity risks.

THIRD-PARTIES-2l

Selection criteria for higher priority assets include evaluation of any associated third-party hosting environments and source data.
Third parties should be selected according to an organized and thorough process and according to explicit specifications and selection criteria. The selection process and criteria should be designed to ensure that the selected entity can fully meet the organization's specifications as established.
For higher priority assets, these criteria should include the evaluation of associated third-party hosting environments and source data.
Hosting environments and source data can be significant sources of acquired risk. Hosting environments comprise many layers of products and services that are not always under the direct control of hosting providers and may pose unidentified risk to the organization. For example, these may include software packages, open-source code libraries, configurations, and other settings that were used to build a virtual machine that can be deployed in a cloud environment. Similar to a bill of materials, hosting environments should provide documentation of the use of these products and services so that an approximation of acquired risk can be established. In addition, this concept can extend to how hosting organizations store, process, and transmit organizational data. Evaluating the storage locations of data, where it is processed, how it is transmitted, and the controls employed is essential for identifying potential risks to the confidentiality, integrity, and availability of such data.

AIM-Categorization-Tiering: This statement is relevant to the **ASSET, CHANGE AND CONFIGURATION** category, as it emphasizes the importance of evaluating third-party hosting environments and source data for higher priority assets. These evaluations help ensure that the selected entity can meet the organization's specifications, including the management of associated risks from hosting environments and data handling practices. Additionally, it aligns with the **THREAT AND VULNERABILITY** category because assessing the hosting

environments and source data helps identify potential threats and vulnerabilities that could compromise the organization's assets. Understanding these elements is critical to safeguarding the confidentiality, integrity, and availability of organizational data..

THIRD-PARTIES-2m

Acceptance testing of procured assets includes consideration of cybersecurity requirements.
When the third party is responsible for producing or delivering assets to the organization, the monitoring process should include inspection/testing of the assets to ensure that they meet all stated specifications, including cybersecurity requirements.
For example, if there is a requirement to remove all software components that are not required for the operation and/or maintenance of the procured product (games, source code, unused drivers), upon receipt the product could be tested for the inclusion of these components.

AIM-Categorization-Tiering: This statement falls under the **ASSET, CHANGE AND CONFIGURATION** category, as it discusses the importance of acceptance testing to ensure that procured assets meet all specified requirements, including cybersecurity. This process is essential for managing and controlling the organization's assets, ensuring they are configured securely and aligned with the organization's cybersecurity standards. Additionally, it aligns with the **THREAT AND VULNERABILITY** category because acceptance testing helps identify and mitigate potential cybersecurity risks associated with the inclusion of unnecessary or harmful components in procured products.

7.3 Management Activities

THIRD-PARTIES-3a

Documented procedures are established, followed, and maintained for activities in the THIRD-PARTIES domain.
The activities in the THIRD-PARTIES domain are formally documented in some way (such as standard operating procedures, process flow diagrams, RACI charts, and swim lane diagrams). The activities are intentionally designed or described to serve the organization rather than being ad hoc. Documenting procedures helps ensure that they are repeatable and produce expected outcomes. The level of detail included in documentation should be a sufficient to enable consistent performance of domain activities by different people and new employees assuming relevant domain experience and sufficient on-board training.
Also, procedure documentation is made available to and is used by relevant personnel. The documentation is updated as needed to reflect changes in the organizational or operational environment. Additionally, organizations may consider including exceptions processes in documented procedures to ensure that the organization reacts appropriately to unexpected events or situations.

AIM-Categorization-Tiering: This statement falls under the **POLICY AND STRATEGY** category, as it emphasizes the importance of having well-documented procedures that guide activities in the THIRD-PARTIES domain, ensuring they are designed intentionally to serve the organization rather than being handled ad hoc. It also aligns with the **PROGRAM** category, as the documentation and maintenance of these procedures are integral to an organization's overall cybersecurity strategy, enabling consistent performance and supporting the organization's broader objectives. Additionally, this statement is related to the **CULTURE AND SOCIETY** category because it highlights the importance of making procedure documentation accessible to relevant personnel, promoting a culture of adherence to established processes and continuous improvement through regular updates.

THIRD-PARTIES-3b

Adequate resources (people, funding, and tools) are provided to support activities in the THIRD-PARTIES domain.
When determining the adequacy of resources, it may help to consider whether there are any THIRD-PARTIES domain activities not currently being performed that the organization would perform if it had additional people, funding, or tools. An additional consideration may be whether the organization has implemented all practices it has targeted for implementation and whether additional resources are necessary to address potential gaps.
Adequate resources are provided in the form of people, funding, and tools to ensure that THIRD-PARTIES domain practices can be performed as intended. The performance of this practice can be evaluated by determining whether any desired practices have not been implemented due to a shortage of resources.
These are examples of people involved in THIRD-PARTIES domain activities:

- staff responsible for identifying and prioritizing existing suppliers and other third parties
- staff responsible for evaluating proposals and selecting third parties
- staff responsible for establishing formal agreements with third parties
- staff responsible for monitoring the performance of third parties to ensure they are meeting their cybersecurity requirements

These are examples of tools that might be used in THIRD-PARTIES domain activities:

- methods, techniques, and tools for identifying and prioritizing the list of third parties and keeping it up-to-date
- methods, techniques, and tools for identifying and managing risks due to third parties

Adequacy of resources should be determined on an ongoing basis through regular reviews of the domain program and reviews of domain resources in budgeting activities. It is a common point of concern that there is not enough time to complete cybersecurity program activities. This is addressed primarily through increasing staff and secondarily through increasing funding and tools.
When determining the adequacy of staff, also consider whether the cybersecurity program has sufficient capacity so that the individuals that make up the program can regularly attend training, implement and maintain tools, and respond to incidents while conducting day-to-day operations and meeting the cybersecurity objectives of the organization.

AIM-Categorization-Tiering: This statement falls under the **PROGRAM** category, as it emphasizes the need for adequate resources, including people, funding, and tools, to effectively support activities in the THIRD-PARTIES domain. Ensuring that sufficient resources are allocated is crucial for the successful implementation and management of the organization's cybersecurity program, particularly in relation to third-party management. Additionally, it aligns with the **WORKFORCE** category, as the statement highlights the importance of having enough skilled staff to perform necessary tasks, attend training, and manage tools, ensuring that the organization can meet its cybersecurity objectives and maintain operational effectiveness.

THIRD-PARTIES-3c

Up-to-date policies or other organizational directives define requirements for activities in the THIRD-PARTIES domain.
Activities in the THIRD-PARTIES domain receive documented guidance and direction from the organization in the form of policies or similar directives. Strategic business objectives drive the development of documented policies or other organizational directives to ensure activities support the accomplishment of the organization's mission.
Policies or other organizational directives for the THIRD-PARTIES domain activities may contain:

- responsibility, authority, and ownership for performing process activities
- procedures, standards, and guidelines for identifying and prioritizing suppliers and other third parties, managing operational risks resulting from third parties, and monitoring the performance of third parties
- procedures, standards, and guidelines for including cybersecurity requirements in supplier agreements
- requirements for the frequency of reviewing suppliers and other third parties for their ability to meet cybersecurity requirements
- methods for measuring adherence to policy, exceptions granted, and policy violations
- procedures for the granting and management of exceptions.

AIM-Categorization-Tiering: This statement falls under the **POLICY AND STRATEGY** category, as it emphasizes the importance of up-to-date policies or organizational directives that define and guide activities in the THIRD-PARTIES domain. These policies ensure that the organization's strategic business objectives are aligned with its cybersecurity practices, providing clear guidance on responsibilities, procedures, and standards for managing third-party relationships. Additionally, it relates to the **PROGRAM** category, as the development and maintenance of these policies are integral to the overall cybersecurity strategy, ensuring that third-party management supports the organization's mission and addresses operational risks effectively.

THIRD-PARTIES-3d

Responsibility, accountability, and authority for the performance of activities in the THIRD-PARTIES domain are assigned to personnel.
The intent of this practice is that specific people (or people in specific roles) are held accountable for ensuring the achievement of expected results of THIRD-PARTIES domain activities and that they are given the appropriate authority to act and to perform their assigned responsibilities.
These are examples of how to formalize responsibility and authority for THIRD-PARTIES domain activities:

- defining roles and responsibilities in policies (see THIRD-PARTIES-3c)
- developing position descriptions and conducting associated performance management activities
- including process tasks and responsibility for these tasks in position descriptions
- developing and implementing contractual instruments (including service level agreements) with suppliers and other third parties to establish responsibility and authority for performing THIRD-PARTIES domain tasks on outsourced functions

· including THIRD-PARTIES domain tasks in measuring performance of third parties against contractual instruments

Additionally, consider how the knowledge developed by personnel within this domain should be managed and shared. This includes determining what processes and tools should be used for knowledge sharing and identifying who will be responsible for making the best use of internal knowledge.

AIM-Categorization-Tiering: This statement falls under the **WORKFORCE** category, as it focuses on assigning responsibility, accountability, and authority to specific personnel for the performance of activities in the THIRD-PARTIES domain. This ensures that individuals are clearly designated to manage and execute tasks effectively, which is crucial for the organization's operational success and cybersecurity posture. Additionally, it aligns with the **PROGRAM** category, as the formalization of roles and responsibilities through policies, position descriptions, and contractual agreements is essential for the effective implementation and management of the organization's cybersecurity strategy, particularly in relation to third-party management.

THIRD-PARTIES-3e

Personnel performing activities in the THIRD-PARTIES domain have the skills and knowledge needed to perform their assigned responsibilities.
The organization must identify the skills and knowledge needed to perform THIRD-PARTIES domain activities and identify skill and knowledge gaps in existing personnel. The organization can address gaps either by hiring qualified personnel or training existing personnel. It is important to note that managing and securing many technologies (such as virtualized or cloud-based environments) require specific training in specialized equipment and practices. Care should be taken to ensure that the level of skills and knowledge of personnel managing and securing specialized technologies is commensurate with the importance of and risk posed by those technologies. Additionally, skill and knowledge assessments should be repeated as operational environments change over time. For example, in the THIRD-PARTIES domain, skills and knowledge are needed for

· identifying and prioritizing suppliers and other third parties

· tools, techniques, and methods used to identify, analyze, mitigate, and monitor operational risks resulting from third parties

· managing relationships with third parties

· monitoring the performance of third parties

Additionally, consider how the knowledge developed by personnel within this domain should be managed and shared. This includes determining what processes and tools should be used for knowledge sharing and identifying who will be responsible for making the best use of internal knowledge.

AIM-Categorization-Tiering: This statement falls under the **WORKFORCE** category, as it emphasizes the importance of ensuring that personnel performing activities in the THIRD-PARTIES domain possess the necessary skills and knowledge to fulfill their responsibilities effectively. This includes identifying any skill and knowledge gaps and addressing them through training or hiring, which is essential for managing the specific challenges and risks associated with third-party relationships. Additionally, it aligns with the **KNOWLEDGE AND CAPABILITIES** category, as the statement underscores the need for continuous assessment and management of

skills and knowledge, particularly in specialized areas like virtualized or cloud-based environments, to ensure that personnel remain equipped to handle evolving operational environments and technologies.

THIRD-PARTIES-3f

The effectiveness of activities in the THIRD-PARTIES domain is evaluated and tracked.
The organization should measure the performance of THIRD-PARTIES activities to ensure they are being performed as described in plans, policies, and procedures for the THIRD-PARTIES domain. Appropriate metrics should be developed and collected to detect deviations in performance and measure the extent to which THIRD-PARTIES domain activities are achieving their intended purpose.

AIM-Categorization-Tiering: This statement falls under the **PROGRAM** category, as it focuses on the evaluation and tracking of the effectiveness of activities in the THIRD-PARTIES domain, ensuring that these activities are performed in alignment with the organization's plans, policies, and procedures. It also relates to the **POLICY AND STRATEGY** category, as developing and utilizing appropriate metrics to measure performance and detect deviations is essential for assessing whether the organization's strategies in managing third-party relationships are achieving their intended outcomes. This approach ensures continuous improvement and alignment with the organization's overall cybersecurity objectives.

8. Workforce Management - 32 questions

As presented on the platform, its purpose is: Establish and maintain plans, procedures, technologies, and controls to create a culture of cybersecurity and to ensure the ongoing suitability and competence of personnel, commensurate with the risk to critical infrastructure and organizational objectives.

The Workforce Management (WORKFORCE) domain comprises five objectives:

1. Implement Workforce Controls
2. Increase Cybersecurity Awareness
3. Assign Cybersecurity Responsibilities
4. Develop Cybersecurity Workforce
5. Management Activities for the WORKFORCE domain

8.1 Implement Workforce Controls

WORKFORCE-1a

Personnel vetting (for example, background checks, drug tests) is performed at hire, at least in an ad hoc manner. Coordinate with Human Resources staff to ensure that credit checks, criminal background checks, drug tests, verifying credentials and previous employment, and possibly other vetting is performed. In certain cases, you may be able to accept a reciprocal background check from a previous employer (such as the federal government). Also, follow up on anything communicated by someone the candidate gave as a reference that raises concern about the candidate's trustworthiness. The goal is to root out any evidence or indicators that the candidate could end up as an insider threat (e.g., financial instability, criminal history, suspicious or disruptive behavior in previous jobs,

lies).
Vetting may be conducted internally by Human Resources staff or contracted to a vendor, but in either case must be done by personnel who understand all applicable laws and regulations. For outsourced positions, require vendors to perform equivalent vetting of any contractors who will have access to organizational assets.

AIM-Categorization-Tiering: This statement falls under the **WORKFORCE** category, as it addresses the importance of personnel vetting, including background checks and other assessments, to ensure that individuals hired are trustworthy and do not pose an insider threat to the organization. It also relates to the **LEGAL AND REGULATORY FRAMEWORK** category, as the vetting process must comply with all applicable laws and regulations, whether conducted internally or through a vendor. Ensuring proper vetting aligns with the organization's broader cybersecurity objectives by reducing the risk of insider threats and ensuring that both employees and contractors meet the organization's standards for trustworthiness and security.

WORKFORCE-1b

Personnel separation procedures address cybersecurity, at least in an ad hoc manner.
Ensure that personnel who leave do not continue to have access to assets, especially those who have privileged access or access to financial data, PII, or intellectual property. Create procedures to remove, revoke, or disable access to all organizational assets as of the employee's termination date. Start by identifying all of the employee's accounts (including any accounts the employee has with third-party providers, such as company accounts with financial institutions), elevated access of any kind, such as admin or NERC-CIP, all devices in the employee's possession, and all systems, data, and other assets to which the employee has access. Disable all accounts, remove access to all affected assets, remove remote access, and collect the employee's devices, badge, tokens, hard-copy proprietary documents, company credit cards, etc. Coordinate with HR to establish the timing of events and who is responsible for what. For employees with privileged access or access to sensitive data, you may want to monitor their network activity to watch for any evidence of data exfiltration.
For personnel being terminated involuntarily, consider removing, revoking, or disabling all access to assets immediately upon informing the employee of the termination. Escort the employee from the premises immediately after making the announcement. You may also want to examine any systems or computers the employee used for any signs of data exfiltration or compromise.

AIM-Categorization-Tiering: This statement falls under the **WORKFORCE** category, as it focuses on personnel separation procedures that ensure employees leaving the organization do not retain access to critical assets, particularly those with privileged access or access to sensitive data. It also aligns with the **ASSET, CHANGE AND CONFIGURATION** category, as the procedures involve identifying and disabling accounts, revoking access, and securing devices and other assets to prevent unauthorized access after termination. Additionally, it relates to the **THREAT AND VULNERABILITY** category, as the procedures address potential insider threats by ensuring that departing personnel cannot exfiltrate or compromise data, particularly in cases of involuntary termination.

WORKFORCE-1c

Personnel vetting is performed at hire and periodically for positions that have access to assets that are important to the delivery of the function.
For staff who have privileged or trusted access to assets, the vetting described in WORKFORCE-1a (or some ap-

propriate aspects of it) is performed not just at hire but periodically. Doing this helps the organization to discover whether any changes have occurred in the employee's behavior or circumstances that may raise new trust issues.

AIM-Categorization-Tiering: This statement falls under the **WORKFORCE** category, as it emphasizes the importance of ongoing personnel vetting for staff who have privileged or trusted access to critical assets, ensuring that any changes in behavior or circumstances are identified over time. It also relates to the **RISK** category, as periodic vetting helps the organization manage the ongoing risks associated with insider threats by continuously assessing the trustworthiness of individuals in key positions. This proactive approach supports the organization's broader cybersecurity efforts by ensuring that access to important assets is only granted to individuals who consistently meet the organization's standards for security and trust.

WORKFORCE-1d

Personnel separation and transfer procedures address cybersecurity, including supplementary vetting as appropriate.
Potential risks arising from the transfer of personnel should be identified and procedures to mitigate those risks should be established and maintained. For staff who have privileged or trusted access to assets, managing access to and possession of these assets is extremely important for preventing potential disruptions or effects on the resilience of the function. When personnel change positions, their possession of and access to organizational assets (including their access privileges) should be re-evaluated and adjusted as needed. Reassignment of cybersecurity responsibilities may also need to be considered. Organizations may consider additional vetting for employees who transfer to a new position that presents greater risk to the organization.

AIM-Categorization-Tiering: It belongs to the category **RISK** because it involves identifying and mitigating potential cybersecurity risks associated with the separation and transfer of personnel. This process is crucial for ensuring that risks related to access and control of organizational assets are effectively managed. Additionally, it pertains to **PROGRAM** as it involves the establishment and maintenance of procedures that align with the organization's overall cybersecurity strategy, ensuring that personnel transitions are handled in a way that minimizes security risks. Furthermore, it relates to **ASSET, CHANGE, AND CONFIGURATION** as it involves re-evaluating and adjusting access privileges and responsibilities in response to personnel changes, ensuring that the organization's assets remain secure during and after personnel transitions.

WORKFORCE-1e

Personnel are made aware of their responsibilities for protection and acceptable use of IT, OT, and information assets.
Employees and other users of the organization's IT, OT, and information assets should be informed about their own responsibilities for the protection and acceptable use of those assets. The organization should define methods for clearly communicating responsibilities, such as periodic security awareness training and policies. For example, an acceptable use policy, for example, can establish the boundaries of acceptable behaviors when using the organization's systems and data, such as disallowing password syncing and reuse across systems or using personal password vaults to comingle management of both personal and organizational passwords. Organizations may consider supplemental training for users who have access to IT, OT, and information assets with greater protection requirements.
To reinforce expectations of required protection of more sensitive IT, OT, and information assets, organizations

may consider creating goals and objectives for users around protection requirements for these assets.

AIM-Categorization-Tiering: It belongs to the category **KNOWLEDGE AND CAPABILITIES** because it involves educating personnel about their responsibilities for protecting and appropriately using IT, OT, and information assets. Ensuring that employees are aware of and understand their roles in safeguarding these assets is crucial for maintaining organizational security. Additionally, it pertains to **POLICY AND STRATEGY** as it requires the development and communication of clear policies, such as acceptable use policies, to guide user behavior and establish boundaries for the use of organizational systems and data. Furthermore, it relates to **CULTURE AND SOCIETY** since it involves promoting a culture of cybersecurity awareness, where personnel are continuously informed and reminded of their responsibilities, thereby fostering a secure organizational environment.

WORKFORCE-1f

Vetting is performed for all positions (including employees, vendors, and contractors) at a level commensurate with position risk.
Vetting that is described in WORKPLACE-1a and WORKFORCE-1c should be performed for all positions and to a level that reflects the risk associated with each position. The level of risk associated with a position can be due to level of authority (such as CEO), level of responsibility (such as network administrator), or access to assets with significant cost, sensitivity, or criticality to the organization.

AIM-Categorization-Tiering: The statement provided falls under the category of **WORKFORCE**. This is because it emphasizes the importance of conducting thorough vetting processes for all positions, including employees, vendors, and contractors, based on the level of risk associated with each position. The focus on vetting according to position risk highlights the need to ensure that individuals with access to critical systems, sensitive information, or significant authority are properly evaluated, which is a core aspect of managing the security and integrity of the organization's workforce.

WORKFORCE-1g

A formal accountability process that includes disciplinary actions is implemented for personnel who fail to comply with established security policies and procedures.
A disciplinary process is an essential administrative control for enforcing organizational resilience policies. Awareness of the disciplinary process provides staff an additional incentive to comply with the organization's resilience policies and ensures fair and appropriate treatment in the event that wrongdoing is suspected. From the organization's perspective, a formalized disciplinary process provides a preplanned response to suspected infractions of cybersecurity policy that is designed to address all relevant concerns while protecting the organization to the fullest extent possible.
The disciplinary process should be formalized and documented. It should ensure fair treatment of staff in compliance with all applicable regulations and agreements, protect the organization's interests, and include a range of acceptable responses that correspond to the seriousness of the infraction.
Revise the disciplinary process as needed.

AIM-Categorization-Tiering: The statement provided belongs to the category of **CULTURE AND SOCIETY**. This is because the implementation of a formal accountability process, including disciplinary actions, directly

impacts the organizational culture by enforcing adherence to security policies and procedures. The statement emphasizes the importance of maintaining a culture of compliance and responsibility within the organization. By formalizing and documenting the disciplinary process, the organization fosters a culture where employees are aware of the consequences of non-compliance, thus promoting a secure and resilient environment. The focus on fair treatment and adherence to regulations also highlights the organization's commitment to upholding its values and societal responsibilities.

8.2 Increase Cybersecurity Awareness

WORKFORCE-2a

Cybersecurity awareness activities occur, at least in an ad hoc manner.
Conduct activities to improve personnel's understanding of cyber risks, cybersecurity-related laws and regulations to which the organization is subject, and cybersecurity policies, procedures, and requirements. Topics can be general, for all personnel (such as event reporting), or specifically for certain roles (such as social engineering risks that affect financial services staff). All cybersecurity employees should be aware of the cybersecurity program strategy (PROGRAM-1a), so briefings about it should be included in awareness activities. Some awareness communications may be necessary with business partners, such as how PII is handled and how compliance with standards is achieved.
Cybersecurity awareness activities might include cybersecurity-focused emails from acknowledged experts, quarterly refreshers, lunch and learn sessions, posters, and a dedicated intranet site where news about current cybersecurity events and relevant articles, memos, alerts, etc. are posted.
These are examples of cybersecurity awareness topics: email phishing and other social engineering tactics; recognizing indicators of insider threats; event and incident identification; classification and handling of data; acceptable use policies; identity management, including cloud accounts; account authorities; remote connectivity; and mobile device security.

AIM-Categorization-Tiering: The statement provided belongs to the category of **CULTURE AND SOCIETY**. This is because it emphasizes the importance of conducting cybersecurity awareness activities to improve personnel's understanding of cyber risks, relevant laws and regulations, and organizational policies. These activities contribute to fostering a culture of security awareness within the organization, which is essential for protecting against cybersecurity threats. By educating employees and business partners about various cybersecurity topics and the organization's program strategy, the organization promotes a culture that values and prioritizes cybersecurity.

WORKFORCE-2b

Cybersecurity awareness objectives are established and maintained.
Objectives for cybersecurity awareness activities are based on awareness needs that define the messages that need to be communicated regarding cybersecurity to staff and other internal and external stakeholders. For some topics, awareness needs may be consistent across the function's entire population; for others, different stakeholders may have different awareness needs. All of these groups should be identified and their awareness needs documented.
Sources of awareness needs include:

- cybersecurity requirements that specify how assets are to be protected and sustained; organizational policies that attempt to enforce and reinforce acceptable behaviors or implement necessary controls across the

enterprise, such as keeping payroll data confidential

- vulnerabilities under watch or that are being actively managed
- laws and regulations to which the organization is subject because of its industry, geographical location, or type of business
- maintaining security while using specific types of technology that pose increased cyber risk, such as email and mobile devices

Awareness needs are temporal and may change as a result of changes in technology, policy, strategy, and risks being managed. A routine process to maintain and update awareness needs should be put in place.

AIM-Categorization-Tiering: The statement provided belongs to the category of **CULTURE AND SOCIETY**. This is because it focuses on establishing and maintaining cybersecurity awareness objectives, which are crucial for fostering a culture of security within an organization. By identifying and addressing the specific awareness needs of different stakeholders, the organization ensures that the relevant messages regarding cybersecurity are effectively communicated. This approach helps to instill a culture where cybersecurity is valued and prioritized, aligning with the organization's overall security goals. Additionally, regularly updating these objectives in response to changes in technology, policy, and risks further reinforces the organization's commitment to cultivating a strong cybersecurity culture.

WORKFORCE-2c

Cybersecurity awareness objectives are aligned with the defined threat profile (THREAT-2e).
To align cybersecurity awareness objectives with the defined threat profile, analyze the threat profile to understand the targeted assets, objectives, and attack methods that may be employed by threat actors. This supports identification of the types and extent of awareness efforts necessary to address threats relevant to function. For example, if the threat profile includes a threat involving spear phishing, awareness content could be created on that topic.

AIM-Categorization-Tiering: The statement provided belongs to the category of **THREAT AND VULNERABILITY**. This is because aligning cybersecurity awareness objectives with the defined threat profile directly involves understanding and addressing the specific threats and vulnerabilities that an organization faces. By analyzing the threat profile, the organization can tailor its awareness efforts to focus on relevant risks, such as spear phishing, ensuring that employees are informed and prepared to mitigate these specific threats. This approach ensures that cybersecurity awareness is both targeted and effective, enhancing the organization's overall security posture.

WORKFORCE-2d

Cybersecurity awareness activities are conducted periodically.
This practice builds on the cybersecurity awareness activities described in WORKFORCE-2a to include execution of these activities according to organizationally defined periods. For example, this may include awareness activities that are required as part of new employee onboarding, as well as annual refresher activities.

AIM-Categorization-Tiering: The statement provided belongs to the category of **WORKFORCE**. This is because conducting periodic cybersecurity awareness activities is directly related to the continuous education and

training of an organization's employees and contractors, ensuring they are aware of cybersecurity policies, risks, and best practices. By incorporating these activities into processes like onboarding and annual refreshers, the organization ensures that its workforce remains knowledgeable and vigilant, thereby supporting the overall cybersecurity posture. Periodic awareness efforts are essential to maintaining and enhancing the cybersecurity skills and awareness of all personnel who have access to critical systems and data.

WORKFORCE-2e

Cybersecurity awareness activities are tailored to job role.
Cybersecurity awareness activities may be tailored for specific jobs roles. For example, more advanced social engineering awareness training may be considered for higher risk roles, such as organizational leadership or roles that have the authority to approve financial transactions.

AIM-Categorization-Tiering: The statement provided belongs to the category of **WORKFORCE**. This is because tailoring cybersecurity awareness activities to specific job roles directly impacts the employees and contractors within an organization. By customizing training based on the responsibilities and risks associated with different roles, such as providing advanced social engineering awareness for high-risk positions, the organization ensures that its workforce is better equipped to handle the specific cybersecurity challenges they may face. This approach enhances the overall security posture by ensuring that each role receives the appropriate level of awareness and training necessary to protect the organization's systems and data.

WORKFORCE-2f

Cybersecurity awareness activities address predefined states of operation (SITUATION-3g).
Cybersecurity awareness communications requirements should include providing information about predefined states of operation. For example, awareness communications could include information about when and why a shift from the normal state of operation to a high-security operating mode may be invoked in response to a declared cybersecurity incident of sufficient severity.

AIM-Categorization-Tiering: The statement provided belongs to the category of **SITUATIONAL AWARENESS**. This is because addressing cybersecurity awareness activities that include predefined states of operation requires the organization to detect, analyze, and understand the different levels of operation and associated risks in real-time. By communicating when and why shifts from normal operations to high-security modes are necessary in response to cybersecurity incidents, the organization enhances its ability to maintain vigilance and effectively manage its cybersecurity posture, thereby reinforcing its overall situational awareness across various operational states.

WORKFORCE-2g

The effectiveness of cybersecurity awareness activities is evaluated periodically and according to defined triggers, such as system changes and external events, and improvements are made as appropriate.
The organization should have a documented process to evaluate the effectiveness of awareness activities. Typically, assessing effectiveness is done by having employees fill out evaluations after awareness activities. It's more challenging to evaluate the effectiveness of other awareness mechanisms such as posters or regular communications.
These are examples of methods that can be used to evaluate the effectiveness of awareness activities:

- questionnaires or surveys designed to measure people's awareness of specific topics
- focus groups to elicit the level of awareness of a group of people after an awareness activity and to gather improvement recommendations
- selective interviews to inquire about awareness and any changes in behavior that may have occurred as a result of awareness activities
- behavioral measures to objectively evaluate shifts in behavior after an awareness activity—for example, evaluating the strength of passwords before and after a password-awareness activity
- observations, evaluations, and benchmarking activities conducted by external entities

AIM-Categorization-Tiering: Evaluating the effectiveness of cybersecurity awareness activities involves fostering a culture of continuous improvement in cybersecurity practices within the organization, which is a key aspect of **CULTURE AND SOCIETY**. Additionally, the process of evaluating and improving awareness activities directly impacts the knowledge and behavior of the organization's employees, which aligns with the **WORKFORCE** category, as it pertains to the cybersecurity competence of the employees who have access to critical systems and data.

8.3 Assign Cybersecurity Responsibilities

WORKFORCE-3a

Cybersecurity responsibilities for the function are identified, at least in an ad hoc manner.
Identify the roles and activities needed to meet the needs of the function's cybersecurity program. This would include typical cybersecurity roles such as security administrator, network administrator, and chief information security officer (or a similar role) and their assigned activities. Cybersecurity responsibilities are not restricted to traditional cybersecurity or IT roles. For example, operations engineers, human resources specialists, and procurement specialists typically have cybersecurity roles, and these roles may be performed by third parties. It may be useful to consider consulting industry best practices or frameworks, such as the NICE Cybersecurity Workforce Framework (NIST Special Publication 800-181) for help in identifying and describing fundamental cybersecurity responsibilities.

AIM-Categorization-Tiering: Iidentifying and assigning cybersecurity responsibilities within an organization involves defining the roles and activities necessary for an effective cybersecurity program, which aligns with **PROGRAM**. Additionally, recognizing that cybersecurity responsibilities extend beyond traditional IT roles to include various employees across different functions relates directly to the **WORKFORCE** category, as it emphasizes the involvement of all employees, including those in non-traditional cybersecurity roles, in maintaining the organization's security posture.

WORKFORCE-3b

Cybersecurity responsibilities are assigned to specific people, at least in an ad hoc manner.
Assign personnel to the cybersecurity responsibilities identified in WORKFORCE-3a. These may be full-time roles or just a small set of responsibilities given to someone whose primary role is in a different area. The main goal is to ensure that some specific person (or persons) is accountable for each of the activities needed to implement the function's cybersecurity program.

AIM-Categorization-Tiering: Assigning specific personnel to cybersecurity responsibilities involves integrating these roles into the organization's broader cybersecurity program, which falls under **PROGRAM**. It also directly impacts the **WORKFORCE** category by specifying how individuals, whether in full-time roles or part-time capacities, are designated with cybersecurity duties to support the organization's security initiatives.

WORKFORCE-3c

Cybersecurity responsibilities are assigned to specific roles, including external service providers.
Clearly assigning cybersecurity responsibilities to roles establishes expectations for the tasks that personnel in those roles will perform. These roles may be explicitly cybersecurity-focused (network administrator, help desk, CISO, etc.) or may be other roles that contribute to cybersecurity activities. These responsibilities should also be specified in formal agreements with external entities, such as Internet service providers, security as service providers, cloud service providers, and IT/OT service providers.

AIM-Categorization-Tiering: The assignment of cybersecurity responsibilities to specific roles, including external service providers, falls under **PROGRAM** as it involves defining and organizing the roles necessary to implement the organization's cybersecurity strategy effectively. It also pertains to **WORKFORCE** since it addresses the roles and responsibilities of both internal staff and external service providers, highlighting the need to clarify these duties to ensure proper execution of cybersecurity tasks and responsibilities.

WORKFORCE-3d

Cybersecurity responsibilities are documented.
Cybersecurity responsibilities should be clearly documented (in job descriptions or performance criteria, for example) so that staff members know their responsibilities and can plan their performance accordingly. The definition of cybersecurity responsibilities in the job description establishes the foundation for performance management and measurement of the staff member's commitment to helping the organization sustain operational resilience.

AIM-Categorization-Tiering: The statement belongs to the category of **PROGRAM**. Documenting cybersecurity responsibilities is a crucial aspect of a cybersecurity program because it involves establishing clear roles and expectations for personnel. This documentation ensures that staff members understand their specific duties related to cybersecurity, which is essential for aligning individual performance with the organization's overall cybersecurity strategy and objectives. By integrating these responsibilities into job descriptions or performance criteria, the organization lays the groundwork for effective performance management and supports the sustainability of operational resilience.

WORKFORCE-3e

Cybersecurity responsibilities and job requirements are reviewed and updated periodically and according to defined triggers, such as system changes and changes to organizational structure.
Responsibilities and requirements for a job should be reviewed and updated on a predetermined basis, using one or more triggers such as time elapsed, personnel changes, and process changes. Those triggers ensure that the responsibilities and requirements of the role adapt to changes in organizational risk, organizational processes, or the threat landscape. Keeping job responsibilities and requirements up-to-date helps ensure that personnel have a

clear understanding of the roles they play in the cybersecurity of the organization.

AIM-Categorization-Tiering:It belongs to the category of **PROGRAM**. Reviewing and updating cybersecurity responsibilities and job requirements periodically is a key aspect of a cybersecurity program. This practice ensures that the roles and responsibilities related to cybersecurity remain relevant and aligned with changes in organizational structure, risk, and processes. By incorporating defined triggers, such as system changes and personnel adjustments, the organization ensures that its cybersecurity program adapts to evolving threats and operational needs. This ongoing adjustment supports the overall effectiveness of the cybersecurity strategy and helps maintain clarity in personnel roles and expectations.

WORKFORCE-3f

Assigned cybersecurity responsibilities are managed to ensure adequacy and redundancy of coverage, including succession planning.
Resource planning and analysis should be conducted to determine staffing requirements for cybersecurity activities. Periodic budgeting should ensure adequate funding for those requirements. Staffing needs should include training and availability of backup personnel, at least for critical tasks. Succession planning should involve higher level managers to identify potential successors and to ensure they are mentored and trained to take roles in the future contingent on vacancies that have not yet occurred.

AIM-Categorization-Tiering: It falls under the category of **WORKFORCE**. Managing assigned cybersecurity responsibilities to ensure adequacy and redundancy, including succession planning, is crucial for maintaining a robust cybersecurity posture. This involves evaluating and planning for staffing needs, budgeting for necessary resources, and preparing backup personnel for critical tasks. Succession planning ensures that there are qualified individuals ready to step into key roles as needed, thus supporting the ongoing effectiveness of the cybersecurity program and ensuring that the organization remains resilient against potential disruptions.

8.4 Develop Cybersecurity Workforce

WORKFORCE-4a

Cybersecurity training is made available to personnel with assigned cybersecurity responsibilities, at least in an ad hoc manner.
Ensure that personnel in assigned responsibilities in WORKFORCE-3b have the knowledge and skills needed to perform those responsibilities. Conduct cybersecurity training internally or include funding in the cybersecurity program budget for personnel to take training from vendors. If training is provided internally, it should be relevant to the types of activities identified in WORKFORCE-3a. Additionally, as noted in the help text for WORKFORCE-3a, cybersecurity responsibilities are not restricted to traditional cybersecurity or IT roles. For example, operations engineers, human resources specialists, and procurement specialists typically have cybersecurity roles, and these roles may be performed by third parties.
Training might include attendance at conferences that provide deep dive sessions, vendor-specific training on tools used, and certificate programs. Payment for external training and certificate programs might be done only on a reimbursement basis after successful completion.

AIM-Categorization-Tiering: The emphasis on providing cybersecurity training to personnel with assigned responsibilities aligns with **WORKFORCE** because it ensures that employees with critical roles are equipped

with the necessary skills and knowledge. Additionally, the focus on relevant and effective training to enhance personnel's abilities highlights the importance of **KNOWLEDGE AND CAPABILITIES**. Proper training and skill development are essential to maintaining a competent workforce capable of addressing cybersecurity challenges effectively.

WORKFORCE-4b

Cybersecurity knowledge, skill, and ability requirements and gaps are identified for both current and future operational needs, at least in an ad hoc manner.
To identify gaps, you first might create a skills inventory to identify and document the current skill set of the organization's personnel. This inventory provides a snapshot of current capabilities and can be used to diagnose resource shortages and gaps against both your current and future workforce needs.
The skills inventory is compared to the identified cybersecurity responsibilities for the function (WORKFORCE-3a) to identify skills that the organization does not possess. The resulting skill gap provides insight into the current and future skill needs of the organization. These skill gaps may prevent the organization from performing adequately in managing cyber risks and may result in additional risk.

AIM-Categorization-Tiering: Identifying and addressing cybersecurity knowledge, skill, and ability requirements, and gaps relates directly to **KNOWLEDGE AND CAPABILITIES** because it involves assessing and developing the skills necessary to protect the organization's systems and data. Additionally, evaluating skill gaps is crucial for **RISK** management, as it helps in identifying potential vulnerabilities and addressing them to prevent inadequate management of cybersecurity risks and mitigate associated risks.

WORKFORCE-4c

Identified cybersecurity knowledge, skill, and ability gaps are addressed through training, recruiting, and retention efforts.
An organization can address knowledge, skill, and ability gaps identified in WORKFORCE-4b in a number of ways: existing staff may be trained to acquire new skills, new staff may be hired to acquire the necessary skills, or the skills may be acquired by outsourcing the work that requires them. As gaps are closed, the skills inventory should be updated to ensure that recruiting and training efforts are aligned with current needs.

AIM-Categorization-Tiering: Addressing identified cybersecurity knowledge, skill, and ability gaps through training, recruiting, and retention aligns with **KNOWLEDGE AND CAPABILITIES** because it focuses on enhancing the skills and understanding of personnel to effectively manage cybersecurity. Additionally, the efforts to recruit, train, and retain personnel to address these gaps directly relate to **WORKFORCE**, as it involves managing and developing the organization's human resources to meet its cybersecurity needs.

WORKFORCE-4d

Cybersecurity training is provided as a prerequisite to granting access to assets that are important to the delivery of the function.
New personnel and personnel transferred into new positions are trained in cybersecurity principles, requirements, and best practices before they are allowed access to IT, OT, and information assets. The training may include cybersecurity training specific to the responsibilities of the position or specific to the assets that will be accessed in the position (such as supply chain security or cloud security training), as well as general cybersecurity training

that applies to all personnel.

AIM-Categorization-Tiering: Providing cybersecurity training as a prerequisite to granting access to critical assets aligns with **WORKFORCE** because it directly involves the management and development of personnel who have access to key systems and data. This approach ensures that both new and transferred employees are adequately trained in cybersecurity principles and practices relevant to their roles, which is essential for maintaining the security and integrity of the organization's assets.

WORKFORCE-4e

The effectiveness of training programs is evaluated periodically, and improvements are made as appropriate.
A process should exist to determine the effectiveness of training for meeting the training needs of staff involved in the cybersecurity program.
These are examples of methods used to assess training effectiveness:

- testing in the training context
- post-training surveys of training participants
- post-training surveys of training participants' managers about their satisfaction with the impact of the training on participants' ability to perform their cybersecurity responsibilities
- assessment mechanisms embedded in training materials

Document suggested improvements to the training plan based on the evaluation of the effectiveness of training activities and implement improvements when feasible.

AIM-Categorization-Tiering: Evaluating the effectiveness of training programs and making improvements addresses the need to ensure that personnel possess the necessary skills and knowledge to effectively perform their cybersecurity roles. By assessing and enhancing training methods and materials, an organization maintains and develops the required capabilities of its staff to manage and respond to cybersecurity challenges effectively. This aligns with **KNOWLEDGE AND CAPABILITIES** because it focuses on improving the skills and knowledge base of the workforce, which is critical for robust cybersecurity management.

WORKFORCE-4f

Training programs include continuing education and professional development opportunities for personnel with significant cybersecurity responsibilities.
The broad range of skills necessary to adequately perform the competencies required in the cybersecurity program requires extensive and ongoing training. Due to the critical nature of these program responsibilities, it is important that opportunities for cybersecurity personnel to get training are planned for and budgeted for.

AIM-Categorization-Tiering: The statement falls under the **WORKFORCE** category because it focuses on the training and development of personnel who have significant cybersecurity responsibilities within the organization. Providing continuing education and professional development opportunities ensures that these employees maintain and enhance their skills, which is critical for effectively managing and securing the organization's systems and data. Additionally, this statement relates to the **KNOWLEDGE AND CAPABILITIES** category as

it emphasizes the importance of developing and maintaining the necessary skills and knowledge in cybersecurity personnel, which is vital for protecting the organization's assets. The planned and budgeted approach to training further underscores the organization's commitment to strengthening its cybersecurity posture through a well-prepared and capable workforce.

8.5 Management Activities

WORKFORCE-5a

Documented procedures are established, followed, and maintained for activities in the WORKFORCE domain.
The activities in the WORKFORCE domain are formally documented in some way (such as standard operating procedures, process flow diagrams, RACI charts, and swim lane diagrams). The activities are intentionally designed or described to serve the organization rather than being ad hoc. Documenting procedures helps ensure that they are repeatable and produce expected outcomes. The level of detail included in documentation should be a sufficient to enable consistent performance of domain activities by different people and new employees assuming relevant domain experience and sufficient on-board training.
Also, procedure documentation is made available to and is used by relevant personnel. The documentation is updated as needed to reflect changes in the organizational or operational environment. Additionally, organizations may consider including exceptions processes in documented procedures to ensure that the organization reacts appropriately to unexpected events or situations.

AIM-Categorization-Tiering: This statement falls under the **WORKFORCE** category, as it emphasizes the importance of establishing, following, and maintaining documented procedures for activities within the workforce domain. Proper documentation ensures that workforce-related activities are consistently performed, supporting the organization's overall cybersecurity posture by providing clear guidance to employees and new hires. Additionally, this statement aligns with the **POLICY AND STRATEGY** category because the creation and maintenance of these documented procedures reflect a strategic approach to managing workforce activities, ensuring they are aligned with the organization's security objectives and can adapt to changes in the organizational or operational environment.

WORKFORCE-5b

Adequate resources (people, funding, and tools) are provided to support activities in the WORKFORCE domain.
When determining the adequacy of resources, it may help to consider whether there are any WORKFORCE domain activities not currently being performed that the organization would perform if it had additional people, funding, or tools. An additional consideration may be whether the organization has implemented all practices it has targeted for implementation and whether additional resources are necessary to address potential gaps.
Adequate resources are provided in the form of people, funding, and tools to ensure that WORKFORCE domain practices can be performed as intended. The performance of this practice can be evaluated by determining whether any desired practices have not been implemented due to a shortage of resources.
These are examples of people involved in WORKFORCE domain activities:

- cybersecurity, business continuity, and IT operations officers, directors, and managers
- staff responsible for training and skill development
- staff responsible for designing and performing cybersecurity awareness activities

These are examples of tools that might be used in WORKFORCE domain activities:

- a performance management system that supports establishing performance goals and objectives and evaluating performance against them
- job description templates that reflect standard resilience obligations, roles, and responsibilities, required skills, and specific job requirements (e.g., certifications)
- methods for delivering awareness and training materials, such as user on-demand training
- tools for tracking awareness and training course attendance

Adequacy of resources should be determined on an ongoing basis through regular reviews of the domain program and reviews of domain resources in budgeting activities. It is a common point of concern that there is not enough time to complete cybersecurity program activities. This is addressed primarily through increasing staff and secondarily through increasing funding and tools.
When determining the adequacy of staff, also consider whether the cybersecurity program has sufficient capacity so that the individuals that make up the program can regularly attend training, implement and maintain tools, and respond to incidents while conducting day-to-day operations and meeting the cybersecurity objectives of the organization.

AIM-Categorization-Tiering: This statement primarily falls under the **WORKFORCE** category, as it emphasizes the need to provide adequate resources—people, funding, and tools—to support activities within the workforce domain. Ensuring that the workforce is properly resourced is crucial for the effective performance of cybersecurity-related tasks, training, and awareness activities, which are essential to maintaining the organization's security posture. Additionally, this statement also aligns with the **PROGRAM** category because it involves strategic planning and resource allocation to ensure that all workforce-related practices are implemented as intended. Adequate resourcing is a key element in the successful execution of a cybersecurity program, ensuring that the workforce can meet the organization's cybersecurity objectives while also allowing for ongoing training and development.

WORKFORCE-5c

Up-to-date policies or other organizational directives define requirements for activities in the WORKFORCE domain.
Activities in the WORKFORCE domain receive documented guidance and direction from the organization in the form of policies or similar directives. Strategic business objectives drive the development of documented policies or other organizational directives to ensure activities support the accomplishment of the organization's mission.
Policies or other organizational directives for WORKFORCE domain activities may contain

- responsibility, authority, and ownership for performing WORKFORCE activities
- procedures, standards, and guidelines for WORKFORCE activities such as training, vetting, and awareness
- descriptions of the function's cybersecurity responsibilities
- list of the triggers that initiate review and update of cybersecurity responsibilities and job requirements

- training and awareness attendance requirements
- requirements for the frequency of evaluating the effectiveness of cybersecurity awareness activities
- methods for measuring adherence to policy, exceptions granted, and policy violations
- procedures for the granting and management of exceptions.

AIM-Categorization-Tiering: The **POLICY AND STRATEGY** category is relevant because the statement emphasizes the importance of having up-to-date policies and directives that define and guide activities within the WORKFORCE domain. These policies ensure that the workforce activities are aligned with the organization's strategic business objectives and support the overall mission. Establishing clear policies and directives is fundamental to effective cybersecurity management and strategy. The **WORKFORCE** category is also applicable because the statement directly pertains to the activities within the workforce domain, specifically focusing on how these activities are guided by documented organizational policies. It underscores the importance of having structured and well-defined procedures, standards, and guidelines that address various workforce-related activities such as training, vetting, and awareness. This helps ensure that the workforce is well-prepared, accountable, and capable of fulfilling their cybersecurity responsibilities in alignment with organizational goals.

WORKFORCE-5d

Responsibility, accountability, and authority for the performance of activities in the WORKFORCE domain are assigned to personnel.
The intent of this practice is that specific people (or people in specific roles) are held accountable for ensuring the achievement of expected results of WORKFORCE domain activities and that they are given the appropriate authority to act and to perform their assigned responsibilities.
These are examples of how to formalize responsibility and authority for WORKFORCE domain activities:

- defining roles and responsibilities in policies (see WORKFORCE-5c)
- developing position descriptions and conducting associated performance management activities
- including process tasks and responsibility for these tasks in position descriptions
- developing and implementing contractual instruments (including service level agreements) with external entities to establish responsibility and authority for performing WORKFORCE domain tasks on outsourced functions
- including WORKFORCE domain tasks in measuring performance of external entities against contractual instruments

Additionally, consider how the knowledge developed by personnel within this domain should be managed and shared. This includes determining what processes and tools should be used for knowledge sharing and identifying who will be responsible for making the best use of internal knowledge.

AIM-Categorization-Tiering: The **WORKFORCE** category is relevant because the statement focuses on assigning responsibility, accountability, and authority to personnel for activities within the workforce domain. This

involves defining specific roles and ensuring that individuals are equipped to carry out their responsibilities effectively, which is a core aspect of workforce management in cybersecurity. The **POLICY AND STRATEGY** category is also applicable because the statement discusses the formalization of these roles and responsibilities through organizational policies, position descriptions, and contractual agreements. These elements reflect the need for clear policies and strategic planning to ensure that workforce activities align with the organization's cybersecurity objectives and that accountability is maintained at all levels.

WORKFORCE-5e

Personnel performing activities in the WORKFORCE domain have the skills and knowledge needed to perform their assigned responsibilities.
The intent of this practice is that specific people (or people in specific roles) are held accountable for ensuring the achievement of expected results of WORKFORCE domain activities and that they are given the appropriate authority to act and to perform their assigned responsibilities.
These are examples of how to formalize responsibility and authority for WORKFORCE domain activities:

- defining roles and responsibilities in policies (see WORKFORCE-5c)
- developing position descriptions and conducting associated performance management activities
- including process tasks and responsibility for these tasks in position descriptions
- developing and implementing contractual instruments (including service level agreements) with external entities to establish responsibility and authority for performing WORKFORCE domain tasks on outsourced functions
- including WORKFORCE domain tasks in measuring performance of external entities against contractual instruments

AIM-Categorization-Tiering: The **WORKFORCE** category is relevant because the statement focuses on ensuring that personnel in the workforce domain have the necessary skills and knowledge to perform their responsibilities, which directly impacts the effectiveness of workforce management in cybersecurity. The **KNOWLEDGE AND CAPABILITIES** category is applicable because the statement emphasizes the importance of equipping personnel with the required knowledge and skills, which is crucial for maintaining a secure environment. Ensuring that personnel are knowledgeable and capable aligns with the broader goal of protecting the organization's systems and data through a well-informed and skilled workforce.

WORKFORCE-5f

The effectiveness of activities in the WORKFORCE domain is evaluated and tracked.
The organization should measure the performance of WORKFORCE activities to ensure they are being performed as described in plans, policies, and procedures for the WORKFORCE domain. Appropriate metrics should be developed and collected to detect deviations in performance and measure the extent to which WORKFORCE domain activities are achieving their intended purpose.

AIM-Categorization-Tiering: The **WORKFORCE** category is relevant because the statement directly addresses the evaluation and tracking of activities related to the organization's personnel, which is essential for maintaining

effective workforce management in cybersecurity. The **POLICY AND STRATEGY** category applies because the effectiveness of workforce activities is measured against the standards set by the organization's plans, policies, and procedures. Evaluating and tracking these activities ensures that they align with the organization's strategic objectives and cybersecurity policies, thereby supporting the overall security posture of the organization.

9. Cybersecurity Architecture - 58 questions

As presented on the platform, its purpose is: Establish and maintain the structure and behavior of the organization's cybersecurity controls, processes, and other elements, commensurate with the risk to critical infrastructure and organizational objectives.

The Cybersecurity Architecture (ARCHITECTURE) domain comprises six objectives:

1. Establish and Maintain Cybersecurity Architecture Strategy and Program
2. Implement Network Protections as an Element of the Cybersecurity Architecture
3. Implement IT and OT Asset Security as an Element of the Cybersecurity Architecture
4. Implement Software Security as an Element of the Cybersecurity Architecture
5. Implement Data Security as an Element of the Cybersecurity Architecture
6. Management Activities for the ARCHITECTURE domain

9.1 Establish and Maintain Cybersecurity Architecture Strategy and Program

ARCHITECTURE-1a

The organization has a strategy for cybersecurity architecture, which may be developed and managed in an ad hoc manner.
There is a desired outcome for the cybersecurity architecture strategy and general agreement on how to achieve it. For example, the architecture strategy may be focused on preventing unauthorized access, and there is consensus on the design decisions concerning proposed authentication and authorization solutions.

AIM-Categorization-Tiering: The statement primarily belongs to the category of **ARCHITECTURE**. It refers to the organization's strategy for developing and managing its cybersecurity architecture, including design decisions related to authentication and authorization solutions. This involves creating a secure and robust infrastructure to protect the organization's assets and data. The statement also touches on the alignment of this strategy with the organization's goals, which implies an element of **POLICY AND STRATEGY**, as it involves setting clear objectives and achieving consensus on implementation methods within the cybersecurity architecture framework.

ARCHITECTURE-1b

A strategy for cybersecurity architecture is established and maintained in alignment with the organization's cybersecurity program strategy (PROGRAM-1b) and enterprise architecture.
The cybersecurity architecture strategy is kept current and relevant. A cybersecurity architecture strategy for protecting legacy mainframe systems, for example, will likely be out of step with a cybersecurity program goal of accommodating secure mobile devices and an enterprise architecture goal of moving to the cloud and providing

data as an enterprise-wide asset.

AIM-Categorization-Tiering: The statement primarily belongs to the category of **ARCHITECTURE**, as it discusses the establishment and maintenance of a cybersecurity architecture strategy that aligns with both the organization's cybersecurity program and enterprise architecture. The focus is on ensuring that the architecture strategy remains current and relevant, particularly when dealing with evolving technologies such as secure mobile devices and cloud-based solutions. Additionally, the statement also relates to **PROGRAM** because it emphasizes the alignment of the cybersecurity architecture with the broader cybersecurity program strategy, ensuring that both are coordinated to meet the organization's overall security objectives.

ARCHITECTURE-1c

A documented cybersecurity architecture is established and maintained that includes IT and OT systems and networks and aligns with system and asset categorization and prioritization.
The cybersecurity architecture is documented so that it can be communicated to and reviewed by important stakeholders. The cybersecurity architecture supports reasoning about asset prioritization and important architectural safeguards concerning the interactions among IT and OT assets. For example, design decisions concerning trust boundaries need to be documented in terms of the architectural elements involved and the information exchanges among them. The cybersecurity architecture should include appropriate considerations for assets used in the delivery of the function or that may increase cyber risk to the function, including mobile assets, personal computing and networking equipment used for remote connectivity, field devices, VoIP, badging and other physical access systems, and digital signage.

AIM-Categorization-Tiering: The statement belongs to the category of **ARCHITECTURE** because it describes the establishment and maintenance of a documented cybersecurity architecture that encompasses IT and OT systems, ensuring alignment with asset categorization and prioritization. The focus on documenting the architecture for communication and review by stakeholders further emphasizes the structured design and implementation of secure infrastructure. Additionally, the statement touches on **ASSET, CHANGE AND CONFIGURATION**, as it involves considerations for various assets, including mobile and remote connectivity devices, and emphasizes the need for architectural safeguards in their interactions, reflecting the importance of managing and prioritizing these assets within the cybersecurity framework.

ARCHITECTURE-1d

Governance for cybersecurity architecture (such as an architecture review process) is established and maintained that includes provisions for periodic architectural reviews and an exceptions process.
There is sufficient oversight of the cybersecurity architecture or equivalent cybersecurity architecture governance function to prevent architectural drift—the discrepancy between the documented architecture and the implemented architecture. For example, proposed changes to the architecture are subject to review and approval, and exceptions are approved with knowledge of the risks and consequences.

AIM-Categorization-Tiering: The statement primarily belongs to the **ARCHITECTURE** category, as it focuses on the governance and oversight of the organization's cybersecurity architecture, ensuring that the design and implementation of the technology infrastructure remain aligned and secure. The governance process, including periodic architectural reviews and an exceptions process, is crucial for maintaining a robust security posture

and preventing architectural drift. Additionally, this statement is related to the **POLICY AND STRATEGY** category, as it involves establishing and maintaining governance processes, policies, and procedures that guide the review, approval, and management of changes to the architecture, ensuring they are conducted with an understanding of the associated risks and consequences.

ARCHITECTURE-1e

Senior management sponsorship for the cybersecurity architecture program is visible and active.
Visible and active sponsorship by senior management might include regular communications by senior management about the importance and value of the cybersecurity architecture, organizational support for establishing and implementing governance for cybersecurity architecture (such as an architecture review process), and funding awards and recognition programs for staff who make significant contributions toward achieving cybersecurity objectives.

AIM-Categorization-Tiering: The statement belongs to the **ARCHITECTURE** category, as it emphasizes the importance of senior management actively sponsoring and supporting the cybersecurity architecture program. This involvement is crucial for ensuring that the design and implementation of the organization's technology infrastructure are secure and aligned with business objectives. Additionally, this statement relates to the **CULTURE AND SOCIETY** category, as the visible and active sponsorship from senior management helps to cultivate a culture of cybersecurity awareness and prioritization within the organization, reinforcing the value of a strong security posture across all levels of the organization.

ARCHITECTURE-1f

The cybersecurity architecture establishes and maintains cybersecurity requirements for the organization's assets.
Select and document requirements for the appropriate level of confidentiality, integrity, and availability of IT, OT, and information assets. A common expression of these requirements are organizational policies associated with the selection and implement of controls for the organization's assets.

AIM-Categorization-Tiering: The statement belongs to the **ARCHITECTURE** category, as it emphasizes the role of cybersecurity architecture in defining and maintaining security requirements for the organization's assets, including IT, OT, and information assets. This involves selecting and documenting requirements related to confidentiality, integrity, and availability, which are fundamental aspects of a secure technology infrastructure. Additionally, it relates to the **POLICY AND STRATEGY** category, as the establishment of these requirements and their expression through organizational policies are critical to ensuring that appropriate controls are selected and implemented to protect the organization's assets in line with its overall security strategy.

ARCHITECTURE-1g

Cybersecurity controls are selected and implemented to meet cybersecurity requirements.
The cybersecurity architecture includes design decisions—tactics—to implement cybersecurity requirements defined in ARCHITECTURE-1f. For example, confidentiality —the requirement not to disclose sensitive information to unauthorized parties— may be realized by a control that ensures no credit card information is retained by a web-based user interface after a payment transaction has completed. As another example, confidentiality and integrity may be addressed by placing additional encryption controls on external connections such as cellular,

satellite, or city fiber provided by an external entity. Selected controls are documented in the cybersecurity architecture.

AIM-Categorization-Tiering: The statement belongs to the **ARCHITECTURE** category because it emphasizes how cybersecurity architecture incorporates design decisions, or tactics, to implement cybersecurity requirements. These design decisions involve selecting and implementing specific controls to address requirements such as confidentiality and integrity, which are fundamental to a secure technology infrastructure. Additionally, this statement also relates to the **STANDARDS AND TECHNOLOGY** category, as it involves the use of established cybersecurity controls and technologies, such as encryption, to protect the organization's systems and data. The documentation of these selected controls within the cybersecurity architecture further reinforces their alignment with industry standards and best practices.

ARCHITECTURE-1h

The cybersecurity architecture strategy and program are aligned with the organization's enterprise architecture strategy and program.
Alignment of these strategies avoids mismatched expectations between business and technical stakeholders. For example, the enterprise goals of protecting intellectual property and sensitive business data are supported by the cybersecurity goals of minimizing attack surfaces and establishing secure defaults.

AIM-Categorization-Tiering: It aligns with **PROGRAM** because it discusses the alignment of the cybersecurity architecture strategy and program with the organization's enterprise architecture strategy and program, emphasizing the importance of integrating cybersecurity initiatives with broader business objectives. This ensures that the cybersecurity program supports the organization's overall goals, such as protecting intellectual property and sensitive business data. Additionally, it falls under **ARCHITECTURE** because the statement highlights the role of cybersecurity architecture in minimizing attack surfaces and establishing secure defaults, which are key elements in designing and implementing a secure technology infrastructure. The alignment of these strategies helps avoid mismatched expectations between business and technical stakeholders, ensuring cohesive and effective cybersecurity management.

ARCHITECTURE-1i

Conformance of the organization's systems and networks to the cybersecurity architecture is evaluated periodically and according to defined triggers, such as system changes and external events.
The cybersecurity architecture is treated as a resource that helps maintain an organization's security posture. Periodic evaluations of conformance to the cybersecurity architecture are a risk-reduction technique. For example, a proposed repurposing or virtualization of a server is a design decision that should be assessed for its effect on the architecture. Evaluations should include devices that may increase cyber risk to the function, such as mobile assets, personal computing and networking equipment used for remote connectivity, field devices, VoIP, badging and other physical access systems, and digital signage. Advanced cybersecurity techniques such as threat hunting and active defense may aid in identifying non-conforming systems or networks.

AIM-Categorization-Tiering: It aligns with **ARCHITECTURE** because it emphasizes the importance of periodically evaluating conformance to the cybersecurity architecture, treating it as a resource to maintain the organization's security posture. The reference to advanced cybersecurity techniques such as threat hunting and

active defense directly relates to **THREAT AND VULNERABILITY**, as these techniques help identify non-conforming systems or networks that could introduce security risks. Additionally, the periodic evaluations and assessments of design decisions, such as the repurposing or virtualization of servers, highlight the organization's efforts in managing and mitigating risks, which is central to the **RISK** category.

ARCHITECTURE-1j

The cybersecurity architecture is guided by the organization's risk analysis information (RISK-3d) and threat profile (THREAT-2e).
Risk analysis output such as prioritized risk categories, and threat profile information such as targets in certain types of attacks, are potential sources of information on the likely architectural tactics needed to detect, resist, react to, and recover from attacks. To align the cybersecurity architecture with the threat profile, organizations may review the targeted assets, objectives, and attack methods that may be employed by threat actors and adjust the cybersecurity architecture accordingly. For example, maintaining an audit trail is a tactic to support accountability and recovery from attacks, and providing redundant servers is a tactic to support availability and business continuity.

AIM-Categorization-Tiering: It aligns with **RISK** because the cybersecurity architecture is informed by the organization's risk analysis, which prioritizes risks and influences architectural decisions. It relates to **THREAT AND VULNERABILITY** as the architecture is also guided by the threat profile, which identifies targets and attack methods, leading to adjustments in the architecture to address these vulnerabilities. Lastly, the statement is inherently tied to **ARCHITECTURE** because it discusses how the architecture is designed and adapted based on risk and threat information, employing tactics such as maintaining audit trails and providing redundant servers to enhance security and ensure business continuity.

ARCHITECTURE-1k

The cybersecurity architecture addresses predefined states of operation (SITUATION-3g).
The design of the cybersecurity architecture should account for necessary requirements to support predefined states of operation that may need to be engaged by the organization. For example, monitoring requirements may need to be built into the architecture to help support decisions to shut down assets if there are indicators of a potential outage. As another example, if a safety-related incident occurs and a temporary elevation of privileges is required, the system could automatically increase the verbosity of logging.

AIM-Categorization-Tiering: It aligns with **ARCHITECTURE** because it discusses how the cybersecurity architecture is designed to address predefined states of operation, such as monitoring requirements and automatic adjustments during incidents. This reflects the importance of a secure and robust infrastructure that can adapt to various operational scenarios. Additionally, it relates to **SITUATIONAL AWARENESS** as the architecture includes mechanisms to detect and respond to specific situations, such as potential outages or safety incidents, thereby enabling the organization to make informed decisions in real-time.

9.2 Implement Network Protections as an Element of the Cybersecurity Architecture

ARCHITECTURE-2a

Network protections are implemented, at least in an ad hoc manner.
Protections are implemented that meet the desired outcomes in the cybersecurity architecture strategy. In the context of the ARCHITECTURE domain, the implementation of these protections are based upon standardized requirements that are documented in a cybersecurity architecture. Since this practice may be performed in an ad hoc manner, they may in general align with these requirements, but may not be implemented according to a documented process or procedure.

AIM-Categorization-Tiering: The statement belongs primarily to the category of **ARCHITECTURE**, as it discusses the implementation of network protections based on the cybersecurity architecture strategy, even if done in an ad hoc manner. This involves ensuring that the protections align with standardized requirements outlined in the cybersecurity architecture, which is key to designing and maintaining a secure technology infrastructure. The reference to potentially undocumented processes also connects to the category of **STANDARDS AND TECHNOLOGY**, as it highlights the use of established cybersecurity standards to guide the implementation of protections, despite the lack of formalized procedures.

ARCHITECTURE-2b

The organization's IT systems are separated from OT systems through segmentation, either through physical means or logical means, at least in an ad hoc manner.
This is a minimal approach, ranging from firewalls to remote access servers (a.k.a. jump boxes). Segmentation is an architectural tactic that provides a first line of defense aimed at containing the spread of attacks and preventing traversal of bad actors across systems (e.g., Web-facing systems, IT systems, and OT systems). Segmentation may include separation, implementation of trust zones, implementation of demilitarized zones (DMZs), or other architectural tactics.

AIM-Categorization-Tiering: The statement belongs primarily to the category of **ARCHITECTURE**, as it describes the use of segmentation as an architectural tactic to separate IT and OT systems, either physically or logically, to protect an organization's assets and data. This tactic is crucial for creating a secure and robust infrastructure, serving as a first line of defense against potential cybersecurity threats. Additionally, the mention of implementing trust zones and demilitarized zones (DMZs) highlights the use of **STANDARDS AND TECHNOLOGY**, as these are established methods for enhancing security through well-known cybersecurity practices.

ARCHITECTURE-2c

Network protections are defined and enforced for selected asset types according to risk and priority (for example, internal assets, perimeter assets, assets connected to the organization's Wi-Fi, cloud assets, remote access, and externally owned devices).
Network protections should be designed to enforce defined controls based on different asset types. The decision to implement stricter controls may be based on factors like the trust of certain asset types or the sensitivity of information that may be accessed by an asset type. For example, remote connections could present greater risk and would be subject to additional protections.
Alternatively, IT assets that only operate on the internal network may be more trusted and therefore require less

rigorous network protections.

AIM-Categorization-Tiering: The statement belongs to the category of **ASSET, CHANGE AND CONFIGURATION**, as it focuses on defining and enforcing network protections based on the types of assets and their associated risks and priorities. This involves the management and control of various assets within the organization, ensuring that appropriate network protections are implemented according to the risk level and importance of each asset type. Additionally, it also relates to **RISK** because the decision to implement different levels of network protections is based on the assessment of risks associated with different asset types, such as remote access and perimeter assets.

ARCHITECTURE-2d

Assets that are important to the delivery of the function are logically or physically segmented into distinct security zones based on asset cybersecurity requirements.
This practice expands on ARCHITECTURE-2b to include assets important to delivery of the function. The practice goes on to note that the segmentation should be based on defined cybersecurity requirements. Criteria for creation of different security zones may be based on several factors. These are some examples of factors:

- specific safety, reliability, and security requirements
- importance of the asset to the function
- the tasks performed by the asset
- whether the asset is managed by a third party
- who has access to the asset
- whether remote access to the asset is enabled
- the degree of trust associated with the asset
- applying cybersecurity controls to groups of assets
- limiting the impacts of potential cyber intrusions

Additionally, these criteria should be clearly documented in the cybersecurity architecture or in a similar document. This helps those not privy to the original decision-making process understand why each criterion is needed. For example, OT assets that have unique characteristics (e.g., those that depend on insecure legacy software or have high availability requirements) may require a specific cybersecurity architecture design to achieve the operational goals of the organization. Additionally, organizations should consider standards and guidelines when planning for segmentation.

AIM-Categorization-Tiering: The statement primarily belongs to the category of **ARCHITECTURE**, as it discusses the segmentation of assets into distinct security zones based on defined cybersecurity requirements, which is a key aspect of designing and implementing a secure infrastructure. The segmentation is intended to protect critical assets and ensure that cybersecurity controls are applied appropriately based on the importance and characteristics of the assets. Additionally, this statement relates to **STANDARDS AND TECHNOLOGY** because it emphasizes the need to consider cybersecurity standards and guidelines when planning for segmentation, ensuring that the architecture aligns with established best practices and technological requirements.

ARCHITECTURE-2e

Network protections incorporate the principles of least privilege and least functionality.
Network segments should be designed to separate activities that present a greater risk to the organization. For example, the administration of network infrastructure should be done on a separate management network that is restricted to only specific administrative accounts and uses stronger authentication techniques like multifactor authentication. Similarly, the organization may restrict management of OT devices to specific workstations on the same logical network.

AIM-Categorization-Tiering: The statement belongs to the category of **ARCHITECTURE** because it discusses the design and implementation of network segments that separate activities based on risk, which is a fundamental aspect of building a secure and robust infrastructure. By incorporating the principles of least privilege and least functionality, the architecture ensures that only necessary access is granted, minimizing potential security risks. Additionally, the statement relates to **STANDARDS AND TECHNOLOGY** as it emphasizes the use of established cybersecurity principles, such as least privilege and multifactor authentication, to enforce security controls effectively within the network infrastructure.

ARCHITECTURE-2f

Network protections include monitoring, analysis, and control of network traffic for selected security zones (for example, firewalls, allowlisting, intrusion detection and prevention systems [IDPS]).
Network protections include capabilities to monitor, analyze, and control network traffic. Different security zones may require increased levels of network protections based on cybersecurity requirements. For example, if the organization has a network segment for devices that connect via a guest Wi-Fi access point, network traffic may not be heavily monitored but there would be increased control to ensure it does not cross over to the internal network. As another example, a management network may be heavily monitored, actions performed on the network may be subject to increased analysis, and access may be strictly controlled.

AIM-Categorization-Tiering: The statement belongs to the category of **ARCHITECTURE** because it discusses the design and implementation of network protections that include monitoring, analysis, and control of network traffic, which are crucial aspects of building a secure infrastructure. The use of different security zones, each with tailored protections such as firewalls and intrusion detection systems, emphasizes the need for a robust security architecture. Additionally, the statement relates to **THREAT AND VULNERABILITY** as it focuses on the ability to detect and control potential security threats through the careful monitoring and management of network traffic within distinct security zones.

ARCHITECTURE-2g

Web traffic and email are monitored, analyzed, and controlled (for example, malicious link blocking, suspicious download blocking, email authentication techniques, IP address blocking).
Network protections should include capabilities to monitor, analyze, and control web traffic and email. The web and email are common vectors that attackers use to attempt to gain credentials or other sensitive information from users. Phishing and watering hole attacks are commonly used to distribute malware or obtain user credentials that are leveraged in the early stages of the kill chain. The organization may consider protections such as monitoring links and attachments in emails, quarantining suspicious downloads, and using DNS filtering to reduce the chance of attackers using these attack vectors to gain a foothold on the network.

AIM-Categorization-Tiering: The statement belongs to the category of **STANDARDS AND TECHNOLOGY** because it focuses on the use of established cybersecurity technologies, such as email authentication techniques, malicious link blocking, and IP address blocking, to monitor, analyze, and control web traffic and email. These technologies are essential in protecting an organization's systems and data from common cyber threats like phishing and malware distribution. Additionally, the statement relates to **THREAT AND VULNERABILITY** as it addresses the need to mitigate security risks associated with web traffic and email, which are common vectors for cyberattacks.

ARCHITECTURE-2h

All assets are segmented into distinct security zones based on cybersecurity requirements.
This practice expands on ARCHITECTURE-2d to include all assets. The practice goes on to note that the segmentation should be based on defined cybersecurity requirements. Criteria for creation of different security zones may be based on several factors. These are some examples of factors:

- specific safety, reliability, and security requirements
- importance of the asset to the function
- the tasks performed by the asset
- whether the asset is managed by a third party
- who has access to the asset
- whether remote access to the asset is enabled
- the degree of trust associated with the asset
- applying cybersecurity controls to groups of assets
- limiting the impacts of potential cyber intrusions
- the characteristics of the network (e.g., guest wireless network)

Additionally, these criteria should be clearly documented in the cybersecurity architecture or in a similar document. This helps those not privy to the original decision-making process understand why each criterion is needed. For example, OT assets that have unique characteristics (e.g., those that depend on insecure legacy software or have high availability requirements) may require a specific cybersecurity architecture design to achieve the operational goals of the organization. Additionally, organizations should consider standards and guidelines when planning for segmentation. It is important to note, there are several ways to implement this practice including application of a zero trust model.

AIM-Categorization-Tiering: The statement belongs primarily to the category of **ARCHITECTURE** because it discusses the design and implementation of a secure technology infrastructure through the segmentation of assets into distinct security zones based on cybersecurity requirements. This approach ensures that different assets are protected according to their specific needs, which is a fundamental aspect of a robust security architecture. Additionally, the statement also relates to **STANDARDS AND TECHNOLOGY**, as it mentions the importance of

considering standards and guidelines when planning for segmentation. This ensures that the architecture adheres to established cybersecurity best practices and technologies.

ARCHITECTURE-2i

Separate networks are implemented, where warranted, that logically or physically segment assets into security zones with independent authentication.
The cybersecurity requirements of certain assets may require isolation through logical or physical segmentation from other organizational networks. In addition, these networks should include an independent authentication scheme that is not shared with other organizational systems. An organization may utilize this type of segmentation for critical OT assets.

AIM-Categorization-Tiering: The statement belongs primarily to the category of **ARCHITECTURE** because it discusses the implementation of separate networks that logically or physically segment assets into security zones with independent authentication. This approach is a core aspect of designing and implementing a secure technology infrastructure to protect critical assets. The segmentation of networks based on cybersecurity requirements and the use of independent authentication schemes are essential elements of a robust security architecture, ensuring that critical assets are appropriately isolated and protected from potential threats.

ARCHITECTURE-2j

OT systems are operationally independent from IT systems so that OT operations can be sustained during an outage of IT systems.
OT systems should be architected in such a way that they are able to continue operations when there is an outage or disruption to IT systems. The organization should not only implement manual backup processes, but these processes should be tested to ensure that they function as expected.
OT systems refer to assets that operate on the OT network segment. These assets might resemble traditional IT assets, except that they support OT operations. When considering this practice, be aware that OT systems are sometimes dependent on IT systems that operate on a separate IT network segment. The intent in this practice is to ensure that service delivery or production activities supported by OT systems can be sustained if IT systems are unavailable for any reason.

AIM-Categorization-Tiering: The statement primarily belongs to the category of **ARCHITECTURE** because it discusses the need to design OT (Operational Technology) systems in a manner that ensures their operational independence from IT systems. This architectural approach is essential for maintaining the continuity of OT operations even during outages or disruptions in IT systems. Ensuring that OT systems can sustain operations independently involves careful design and implementation of a robust infrastructure that separates OT from IT while providing necessary backup processes to support continuous functionality.

ARCHITECTURE-2k

Device connections to the network are controlled to ensure that only authorized devices can connect (for example, network access control [NAC]).
Network connections should be controlled by the organization at the device level. This may be achieved through a solution like network access control that does not allow devices that do not meet specific security requirements to connect to the network.

AIM-Categorization-Tiering: The statement belongs to the category **ASSET, CHANGE AND CONFIGURATION** because it involves the management and control of an organization's devices that are critical to the business's network infrastructure. By controlling device connections to the network, the organization ensures that only authorized devices, which meet specific security requirements, can connect, thereby maintaining the security and configuration of its technological assets. Additionally, this action also aligns with the principles of **ARCHITECTURE**, as it involves designing and implementing secure infrastructure controls, such as Network Access Control (NAC), to protect the organization's assets and data at the network and system level.

ARCHITECTURE-2l

The cybersecurity architecture enables the isolation of compromised assets.
This practice expands on the implementation of architectural tactics such as network segmentation (ARCHITECTURE-2a) and restricting network to authorized devices (ARCHITECTURE-2k). The cybersecurity architecture may include monitoring that enables the organization to detect if an asset is compromised and isolate it on a logically separate network. This could enable incident responders to perform analysis on the system in a safe environment, while not impacting other production networks.

AIM-Categorization-Tiering: The statement belongs to the category **ARCHITECTURE** because it describes the design and implementation of a secure technology infrastructure that isolates compromised assets to protect an organization's overall system. The use of architectural tactics, such as network segmentation and restricting access to authorized devices, reflects the principles of security architecture, which involve protecting network and system integrity. Additionally, this practice ensures that compromised assets can be safely analyzed without affecting the production environment, further demonstrating the importance of a robust and well-designed cybersecurity architecture.

9.3 Implement IT and OT Asset Security as an Element of the Cybersecurity Architecture

ARCHITECTURE-3a

Logical and physical access controls are implemented to protect assets that are important to the delivery of the function, where feasible, at least in an ad hoc manner.
Cybersecurity controls are implemented to manage the risks associated with unauthorized and/or inappropriate levels of access to IT, OT, and information assets, including physical assets. Logical controls may be administrative (e.g., policies, procedures), operational (e.g., system maintenance, capacity management), and technical (e.g., authentication schemes, system logging). Physical controls may also be administrative (e.g., policies, procedures), operational (e.g., fences, locks, signage), and technical (e.g., electronic badge readers, motion detectors, entry point logging).

AIM-Categorization-Tiering: It relates to **ASSET, CHANGE AND CONFIGURATION** because it involves the implementation of logical and physical access controls to protect critical assets, ensuring that these assets are managed and monitored effectively to prevent unauthorized access. The statement also aligns with **ARCHITECTURE**, as it describes the design and implementation of security measures, including administrative, operational, and technical controls, to create a robust infrastructure that safeguards both IT and physical assets essential to the organization's functions.

ARCHITECTURE-3b

Endpoint protections (such as secure configuration, security applications, and host monitoring) are implemented to protect assets that are important to the delivery of the function, where feasible, at least in an ad hoc manner.
Endpoint protections refer to cybersecurity controls applied directly to IT and OT assets. These controls should be focused on prevention of endpoint security risks such as exploits, attacks and inadvertent data leakage caused by human error. Endpoint protections may include configuration hardening, configuration policies and rules, endpoint detection and response software, anti-malware software, monitoring software agents, data loss prevention tools, host-based intrusion detection and firewalls, and other protections.

AIM-Categorization-Tiering: It relates to **ASSET, CHANGE AND CONFIGURATION** because it discusses the implementation of endpoint protections, which are critical for managing and safeguarding an organization's IT and OT assets, including their secure configuration and ongoing monitoring. Additionally, it aligns with **STANDARDS AND TECHNOLOGY** as the use of security applications, configuration policies, and various protective tools are established cybersecurity technologies aimed at protecting assets from risks like exploits, attacks, and data leakage.

ARCHITECTURE-3c

The principle of least privilege (for example, limiting administrative access for users and service accounts) is enforced.
Accounts should be created and configured consistent with the principle of least privilege. The principle of least privilege is a security requirement that establishes limitations on authorized users only to the privileges they require to perform assigned tasks in accordance with their job responsibilities and roles and nothing more. The principle of least privilege also applies to information system processes, ensuring that the processes operate at privilege levels no higher than necessary to accomplish required organizational missions and/or functions.
In the context of this practice, it is imperative that organizations also apply the principle of least privilege when designing, developing, and implementing IT and OT systems, and ensuring that the mechanisms and controls used to implement the principle of least privilege are feasible and operate as designed. The design and construction of Zero Trust architectures, for example, must establish the principle of least privilege as a key requirement to meet the key objectives of this authentication approach.

AIM-Categorization-Tiering: It aligns with **POLICY AND STRATEGY** because enforcing the principle of least privilege is a fundamental security requirement that must be clearly defined and communicated as part of an organization's cybersecurity policies and strategies to ensure that access privileges are restricted according to job responsibilities and roles. Additionally, the statement is relevant to **ARCHITECTURE** as the principle of least privilege is crucial in the design and implementation of secure systems, such as Zero Trust architectures, to ensure that processes and users operate at the minimum privilege level necessary, thus protecting the organization's assets and data.

ARCHITECTURE-3d

The principle of least functionality (for example, limiting services, limiting applications, limiting ports, limiting connected devices) is enforced.
Assets should be configured to provide only essential capabilities and to restrict unnecessary functionality. For example, if a system is configured to operate as an email server, ports not associated with this service should be

closed and applications/services should be disabled if they do not support the sending and receiving of email.

AIM-Categorization-Tiering: It aligns with **ARCHITECTURE** because enforcing the principle of least functionality is integral to designing and implementing a secure and robust technology infrastructure that minimizes potential attack surfaces by disabling unnecessary services, applications, and ports. Additionally, the statement is relevant to **ASSET, CHANGE AND CONFIGURATION** as it emphasizes the need to configure and manage IT assets to provide only essential capabilities, ensuring that unnecessary functionalities are restricted, which is crucial for effective asset management and control.

ARCHITECTURE-3e

Secure configurations are established and maintained as part of the asset deployment process where feasible.
Secure configuration of assets should be considered prior to deployment in a production environment where feasible. The organization should consider measures such as applying patches, enabling host-based protections, configuring logging to support higher-level analysis, and disabling unnecessary default accounts prior to deploying an asset.

AIM-Categorization-Tiering: The statement belongs to the category **ASSET, CHANGE AND CONFIGURATION**. This categorization is justified because it emphasizes the importance of establishing and maintaining secure configurations as part of the asset deployment process. The focus on applying patches, enabling host-based protections, configuring logging, and disabling unnecessary default accounts before deploying an asset aligns directly with the principles of effective asset management and control. These actions ensure that assets are securely configured and prepared for production, thereby minimizing potential vulnerabilities and ensuring ongoing security throughout the asset's lifecycle.

ARCHITECTURE-3f

Security applications are required as an element of device configuration where feasible (for example, endpoint detection and response, host-based firewalls).
0Security applications should be an element of device configuration where feasible. The organization should consider protections such as endpoint detection and response solutions that monitor and respond to malicious activity and provide logs to a higher level0 analysis platform. Host-based firewalls are another consideration for device configuration as they can be configured to allow only essential communication.

AIM-Categorization-Tiering: The statement belongs to the category **ARCHITECTURE**. This categorization is justified because it emphasizes the importance of integrating security applications, such as endpoint detection and response solutions and host-based firewalls, into the device configuration process. These measures are essential components of a secure technology infrastructure, as they help monitor and respond to malicious activity and ensure that only essential communication is allowed. By incorporating these security applications, the organization strengthens its overall security architecture, protecting its assets and data from potential threats.

ARCHITECTURE-3g

The use of removeable media is controlled (for example, limiting the use of USB devices, managing external hard drives).
Removeable media should be controlled and restricted as necessary to reduce risk. The organization may consider

technical controls to restrict the use of removeable devices on systems where there is not a business purpose, operational controls that restrict use of removeable media by policy, or a combination of both.

AIM-Categorization-Tiering: The statement belongs to the category **ASSET, CHANGE AND CONFIGURATION**. This categorization is justified because it emphasizes the need to manage and control removable media, such as USB devices and external hard drives, as part of the organization's information technology assets. By implementing technical and operational controls to restrict the use of removable media, the organization ensures that only essential and secure configurations are maintained, thereby protecting critical systems and data from unauthorized access or potential security breaches.

ARCHITECTURE-3h

Cybersecurity controls are implemented for all assets within the function either at the asset level or as compensating controls where asset-level controls are not feasible.
This practice extends the architectural tactics for cybersecurity controls beyond assets that are important to the delivery of the function to include all assets used for the delivery of the function. The practice also requires that cybersecurity controls be implemented at the asset level where feasible. Compensating controls should be implemented in situations where an asset does not support cybersecurity controls at the asset level to sufficiently reduce risk. For example, if an asset does not support encrypted communications, no direct connections should be permitted with the device and all communications should be routed through an intermediary device.

AIM-Categorization-Tiering: The statement belongs to the category **ASSET, CHANGE AND CONFIGURATION**. This categorization is justified because the focus is on implementing cybersecurity controls for all assets involved in a function, either directly at the asset level or through compensating controls when direct implementation is not feasible. This practice is essential for managing and controlling an organization's information technology assets, ensuring that all assets are adequately protected and that alternative measures are in place to mitigate risks when direct controls cannot be applied.

ARCHITECTURE-3i

Maintenance and capacity management activities are performed for all assets within the function.
Maintenance and capacity management support operational goals by helping to ensure the availability of assets important to the delivery of the function. Organizations should plan for adequate maintenance to be performed with as little impact on operations as possible. This may include performance of preventative maintenance to avoid unanticipated equipment failure, as well as the scheduling of maintenance for planned outage windows or other off-peak operational hours. Capacity management planning requires an understanding of future operational needs of the organization and adequate budget, equipment, and tools to meet those needs. This may require advanced planning and engagement with budgeting processes and organizational leadership to develop and communicate appropriate justification for necessary resources.

AIM-Categorization-Tiering: The statement belongs to the category **ASSET, CHANGE AND CONFIGURATION** because it discusses the management and control of an organization's assets through maintenance and capacity management activities. This includes ensuring that assets are available and operational, which is critical to supporting the organization's functions. The planning and scheduling of maintenance, as well as the capacity management to meet future operational needs, are key aspects of managing the organization's assets, aligning

directly with the category's focus on asset management and maintenance.

ARCHITECTURE-3j

The physical operating environment is controlled to protect the operation of assets within the function.
Protection of the operating environment is important for continued operation of assets used for the delivery of the function. Physical and environmental protections should be implemented that support the sustainability of the operating environment. Consideration of these requirements will help prevent instability of the function or other cascading impacts.

AIM-Categorization-Tiering: The statement belongs to the category **ARCHITECTURE** because it emphasizes the importance of controlling and protecting the physical operating environment to ensure the continued operation and security of assets within the function. Implementing physical and environmental protections is a key aspect of designing and maintaining a secure and robust technology infrastructure, which aligns with the focus of security architecture on safeguarding an organization's assets and data from potential disruptions or cascading impacts.

ARCHITECTURE-3k

More rigorous cybersecurity controls are implemented for higher priority assets.
Assets designated as higher priority through the prioritization process in ASSET-1c likely pose a greater risk to the function or process sensitive data and should be subject to more rigorous cybersecurity controls. ARCHITECTURE-1c notes that a cybersecurity architecture would be in alignment with additional security objectives for higher priority assets. Examples of more rigorous cybersecurity controls include enhanced monitoring of access, additional authentication factors, or a change management process with additional testing and approvals.

AIM-Categorization-Tiering: It discusses the implementation of more rigorous cybersecurity controls for higher priority assets, which involves the management and prioritization of critical assets. The mention of enhanced monitoring, additional authentication factors, and change management processes with extra testing and approvals relates to the control and configuration of assets, directly aligning with **ASSET, CHANGE AND CONFIGURATION**. Additionally, the reference to aligning cybersecurity architecture with additional security objectives for higher priority assets ties into the design and implementation of a secure technology infrastructure, which is central to **ARCHITECTURE**.

ARCHITECTURE-3l

Configuration of and changes to firmware are controlled throughout the asset lifecycle.
Through the lifecycle of an asset, it may be necessary to change or update the firmware for reasons such as enabling specific functionality or improving performance. Where possible, the organization should carefully test changes to firmware prior to deployment, because these changes could also cause unanticipated behavior of the asset or other connected assets.

AIM-Categorization-Tiering: It focuses on the control and management of firmware configuration and changes throughout the asset lifecycle. The emphasis on testing changes before deployment to avoid unanticipated behavior highlights the importance of careful management and monitoring of assets, which directly aligns with the

focus of **ASSET, CHANGE AND CONFIGURATION** on the ongoing control, configuration, and maintenance of an organization's critical assets.

ARCHITECTURE-3m

Controls (such as allowlists, blocklists, and configuration settings) are implemented to prevent the execution of unauthorized code.
In addition to the secure configuration measures in ARCHITECTURE-3e, the organization should implement controls to prevent the execution of unauthorized software and code. The organization may use a blocklist policy to explicitly define applications that are not permitted or use an allowlist policy that specifies a limited set of applications that are permitted. Additionally, the organization may choose to block the execution of code such as JavaScript or macro code on assets.

AIM-Categorization-Tiering: It discusses the implementation of technical controls, such as allowlists, blocklists, and configuration settings, to prevent the execution of unauthorized code. These measures are essential cybersecurity standards and technologies used to protect an organization's systems and data. The reference to secure configuration measures further aligns with the use of **STANDARDS AND TECHNOLOGY** to enforce and maintain a secure operating environment.

9.4 Implement Software Security as an Element of the Cybersecurity Architecture

ARCHITECTURE-4a

Software developed in-house for deployment on higher priority assets is developed using secure software development practices.
Secure software development practices are codified in several frameworks such as, the NIST Secure Software Development Framework (SSDF), Building Security In Maturity Model (BSIMM), or the Open Web Application Security Project (OWASP). Selection of secure development practices from established frameworks should include consideration of the organization's operational needs, risk appetite, and the threat environment. Security should be a consideration in each phase of the software development lifecycle, including requirements definition, design, development, testing, and maintenance.
Organizations should also consider the risks inherent in the use of less formal software development processes, such as no-code development platforms. For example, open-source content management systems typically have templates and other plugins that are created by third parties and could introduce risk to the organization.

AIM-Categorization-Tiering: It emphasizes the use of secure software development practices that are based on established frameworks, such as the NIST Secure Software Development Framework (SSDF) and OWASP. These practices ensure that software developed in-house for higher priority assets adheres to recognized cybersecurity standards and technologies. Additionally, the statement highlights the importance of security considerations throughout the software development lifecycle, which aligns with the principles of **STANDARDS AND TECHNOLOGY** to protect the organization's systems and data.

ARCHITECTURE-4b

The selection of procured software for deployment on higher priority assets includes consideration of the vendor's secure software development practices.

The organization may enforce secure software development practices with vendors through various means such as contractual requirements and technical testing of vendor code. The organization may specify secure design and coding practices from vendors such as those identified in established standards including the NIST Secure Software Development Framework (SSDF), Building Security In Maturity Model (BSIMM), and Open Web Application Security Project (OWASP). This can be done by observing the behavior of the application and inferring the vendor's coding practices, or by running some tests to uncover insecure practices such as buffer overflow, SQL injection, and poor authentication. Beyond that, the cybersecurity architecture can facilitate the integration and interoperability of procured system components (for example, by providing secure interfaces to third-party software).
Additional consideration should be given to high priority suppliers (THIRD-PARTIES-1c) because they supply, maintain, or operate critical software components that are essential to the operation of the function. The definition of a critical software component may vary widely depending on industry or critical infrastructure sector, and may be informed by commonly-used frameworks or control sets. For example NIST provides a definition of critical software under Executive Order 14028 that some organizations may be required to adopt.
This activity is related to the cybersecurity architecture activities associated with selecting vendors based on their secure software development practices (THIRD-PARTIES-2h and ARCHITECTURE-4e).

AIM-Categorization-Tiering: The statement belongs primarily to the category **STANDARDS AND TECHNOLOGY** because it emphasizes the importance of using established cybersecurity standards and frameworks, such as the NIST Secure Software Development Framework (SSDF) and OWASP, when selecting procured software for deployment on higher priority assets. The organization ensures that vendors adhere to secure software development practices through technical testing and contractual requirements, reflecting the use of technology and standards to protect the organization's systems. Additionally, the integration and interoperability of procured components through secure interfaces touch upon the design principles associated with **ARCHITECTURE**, as it involves ensuring that the cybersecurity architecture supports secure deployment and operation of third-party software.

ARCHITECTURE-4c

Secure software configurations are required as part of the software deployment process for both procured software and software developed in-house.
Prior to deployment of software on an asset, configuration settings should be reviewed to ensure that they align with cybersecurity requirements for the asset. Misconfiguration of software could introduce vulnerabilities that could be leveraged by an attacker.

AIM-Categorization-Tiering: The statement primarily belongs to the category **ASSET, CHANGE AND CONFIGURATION** because it emphasizes the importance of managing and controlling the configuration settings of software—whether procured or developed in-house—before deployment on an asset. Ensuring secure software configurations as part of the deployment process is crucial for preventing vulnerabilities that could arise from misconfigurations, thereby protecting the organization's critical systems and data. This activity also aligns with maintaining secure configurations throughout the lifecycle of the assets, which is a key aspect of this category.

ARCHITECTURE-4d

All software developed in-house is developed using secure software development practices.
This practice extends the architectural tactics for secure software development practices noted at MIL1. This practice requires that secure software development practices are used for all software that is developed in-house.

AIM-Categorization-Tiering: The statement belongs to the category **ARCHITECTURE** because it emphasizes the importance of integrating secure software development practices into the design and implementation of in-house software, which is a critical component of a secure technology infrastructure. By ensuring that all in-house software development follows secure practices, the organization strengthens its overall security architecture, protecting its assets and data from potential vulnerabilities that could arise from insecure coding or design. This approach is essential to maintaining a robust and secure technology infrastructure.

ARCHITECTURE-4e

The selection of all procured software includes consideration of the vendor's secure software development practices.
This practice extends the architectural tactics for selection of procured software noted at MIL1. This practice requires that the organization consider the software development practices of vendors for all procured software. The organization may specify secure design and coding practices from vendors such as those identified in established standards including the NIST Secure Software, Development Framework (SSDF), Building Security In Maturity Model (BSIMM), and Open Web Application Security Project (OWASP).
Additional consideration should be given to high priority suppliers (THIRD-PARTIES-1c) because they supply, maintain, or operate critical software components that are essential to the operation of the function. The definition of a critical software component may vary widely depending on industry or critical infrastructure sector and may be informed by commonly used frameworks or control sets. For example, NIST provides a definition of critical software under Executive Order 14028 that some organizations may be required to adopt.
This activity is related to the cybersecurity architecture activities associated with selecting vendors based on their secure software development practices (THIRD-PARTIES-2h and ARCHITECTURE-4b).

AIM-Categorization-Tiering: The statement primarily belongs to the category **STANDARDS AND TECHNOLOGY** because it emphasizes the importance of considering established secure software development practices, such as those from NIST, BSIMM, and OWASP, when selecting procured software. Additionally, it relates to the category **ARCHITECTURE** as it involves architectural tactics for vendor selection based on secure development practices, ensuring that critical software components are protected. The focus on secure software development practices and vendor assessment aligns with the organization's overall cybersecurity strategy and infrastructure.

ARCHITECTURE-4f

The architecture review process evaluates the security of new and revised applications prior to deployment.
New and revised applications may introduce changes to the interfaces, behavior, and interactions of cybersecurity architectural elements. Such changes are subject to review and approval by an architecture review board or similar authoritative organizational entity.

AIM-Categorization-Tiering: The statement belongs to the category **ARCHITECTURE** because it involves

the evaluation of the security of new and revised applications within the organization's technology infrastructure. The architecture review process ensures that any changes introduced by these applications, including interfaces, behavior, and interactions, are carefully assessed to maintain a secure and robust environment. This evaluation is essential for protecting the organization's assets and data, which are central to the architecture's role in cybersecurity.

ARCHITECTURE-4g

The authenticity of all software and firmware is validated prior to deployment.
The authenticity of software, particularly software downloaded from the internet, should be verified prior to execution within organizational systems. The authenticity of software can be verified by ensuring that it is digitally signed or by comparing a hash of the software to one published by the vendor. Firmware should also be verified for authenticity through similar steps like comparing a hash of the binary to one provided by the vendor.

AIM-Categorization-Tiering: The statement belongs to the category **STANDARDS AND TECHNOLOGY** because it involves the use of established methods, such as digital signatures and hash comparisons, to validate the authenticity of software and firmware before deployment. These practices ensure that the software and firmware meet security standards and are not tampered with, thus protecting the organization's systems and data from potential cybersecurity threats. Verifying authenticity is a critical step in maintaining a secure technology infrastructure.

ARCHITECTURE-4h

Security testing (for example, static testing, dynamic testing, fuzz testing, penetration testing) is performed for in-house-developed and in-house-tailored applications periodically and according to definted triggers, such as system changes and external events.
Software security testing provides validation and verification that the software performs as expected under normal operating conditions and does not contain control weaknesses or vulnerabilities that could pose additional risk to the organization.
Security testing should be a consideration in each phase of the software development lifecycle, including requirements definition, design, development, testing, and maintenance.

AIM-Categorization-Tiering: It fits within **STANDARDS AND TECHNOLOGY** because it describes the use of various security testing methods, such as static, dynamic, fuzz, and penetration testing, to ensure that in-house-developed and tailored applications meet established cybersecurity standards. Additionally, it relates to **RISK** as the testing aims to identify and mitigate potential control weaknesses or vulnerabilities that could increase the organization's exposure to cybersecurity risks. These practices are essential for maintaining secure systems and minimizing potential threats throughout the software development lifecycle.

9.5 Implement Data Security as an Element of the Cybersecurity Architecture

ARCHITECTURE-5a

Sensitive data is protected at rest, at least in an ad hoc manner.
Authentication techniques (e.g., credential management, digital certificates, biometric identification, multifactor

authentication), authorization techniques (e.g., access control mechanisms), and protection techniques (e.g., encryption and data masking) are typical architectural tactics for protecting sensitive data at rest. Applying multiple techniques is not required for implementation of this practice. Data at rest may include data stored within dormant virtualized assets.

AIM-Categorization-Tiering: It fits within **ARCHITECTURE** because it discusses the implementation of various architectural tactics, such as authentication, authorization, and protection techniques, to secure sensitive data at rest. These techniques are fundamental components of a secure and robust technology infrastructure. Additionally, it relates to **STANDARDS AND TECHNOLOGY** as it involves the use of established cybersecurity practices like encryption and data masking, which are essential for protecting an organization's systems and data in accordance with cybersecurity standards.

ARCHITECTURE-5b

All data at rest is protected for selected data categories.
Information can be categorized (as referenced in ASSET-2c) according to several security considerations including sensitivity, value, criticality, or legal requirements. This practice extends the architectural tactics for data at rest noted in ARCHITECTURE-5a, such as authentication (e.g., credential management, digital certificates, biometric identification, multifactor authentication), authorization (e.g., access control mechanisms), and protection (e.g., encryption and data masking). Architectural data protection tactics may also include, for example, the use of a secure data access layer instead of permitting direct access to data stores.

AIM-Categorization-Tiering: It fits within **ARCHITECTURE** because it discusses architectural tactics such as authentication, authorization, and protection to secure data at rest. The statement is also related to **ASSET, CHANGE AND CONFIGURATION** since it involves the categorization of data based on security considerations like sensitivity and criticality, which are key aspects of managing and controlling information technology assets. Additionally, it touches on the **LEGAL AND REGULATORY FRAMEWORK** category as it considers legal requirements when categorizing and protecting data, ensuring compliance with applicable laws and regulations.

ARCHITECTURE-5c

All data in transit is protected for selected data categories.
Cryptographic protocols and data masking are examples of typical architectural tactics for protecting sensitive data in transit and promoting secure data sharing. Depending on the data category, additional protections such as the use of a virtual private network may be necessary.

AIM-Categorization-Tiering: It falls under **ARCHITECTURE** because it discusses architectural tactics like cryptographic protocols, data masking, and the use of virtual private networks to protect sensitive data in transit. The statement also relates to **ASSET, CHANGE AND CONFIGURATION** since it involves the management and configuration of data protection measures based on specific data categories. Additionally, it addresses **RISK** by highlighting the need to assess and manage the risks associated with transmitting sensitive data, ensuring that appropriate protections are applied depending on the data category.

ARCHITECTURE-5d

Cryptographic controls are implemented for data at rest and data in transit for selected data categories.
This practice builds on ARCHITECTURE-5a, ARCHITECTURE-5b, and ARCHITECTURE-5c by introducing cryptographic controls. The cybersecurity architecture supports the establishment and maintenance of cryptographic controls for protection of data at rest or in transit. This includes the selection, retirement, and replacement of cryptographic controls to keep pace with changes in technology (such as quantum computing). It embodies design decisions and rationales about the desired level of encryption. For example, some cryptographic algorithms perform better than others, and so there are tradeoffs concerning strength of encryption versus system performance and ease of maintenance. There are also design considerations for data at rest, such as full disk encryption, file-based encryption, and container-based encryption. Data at rest may include data stored within dormant virtualized assets. The term "selected data categories" is used in this practice to signify that organizations should explicitly select the types of data that are required to be encrypted during transit. For example, the organization may elect not to encrypt OT signals on an isolated network but may require encryption for all data in transit in a web-facing application.

AIM-Categorization-Tiering: It is primarily related to **ARCHITECTURE** because it discusses the design and implementation of cryptographic controls for protecting data at rest and in transit, including considerations such as encryption methods and system performance. It also pertains to **STANDARDS AND TECHNOLOGY** as it involves the use of cryptographic standards and technologies to safeguard data, ensuring that these controls are maintained and updated in response to technological changes like quantum computing. Additionally, it touches on **RISK** by addressing the need to carefully select and manage encryption methods based on the risk associated with different data categories, ensuring that the organization's security measures are appropriate for the level of threat faced.

ARCHITECTURE-5e

Key management infrastructure (that is, key generation, key storage, key destruction, key update, and key revocation) is implemented to support cryptographic controls.
Examples of architectural tactics for management of public/private key pairs and certificates include operating system and browsersupported key stores, remote key servers, and cryptographic tokens and smart cards. Maintenance of key management infrastructure includes consideration of changes in technology that may impact security (such as quantum computing).

AIM-Categorization-Tiering: It primarily relates to **ARCHITECTURE** because it involves the design and implementation of a key management infrastructure to support cryptographic controls, which is a critical aspect of building a secure and robust technology environment. The inclusion of key generation, storage, and revocation tactics is central to establishing a secure infrastructure. It also pertains to **STANDARDS AND TECHNOLOGY** as it refers to the use of established cryptographic standards and technologies, such as key stores, remote key servers, and cryptographic tokens, to ensure the effective management of cryptographic keys. Additionally, the statement touches on **RISK** by considering the impact of evolving technologies, like quantum computing, on the security of cryptographic controls, highlighting the need for ongoing assessment and adjustment of key management practices to mitigate potential risks.

ARCHITECTURE-5f

Controls to restrict the exfiltration of data (for example, data loss prevention tools) are implemented.
Examples of controls to restrict the exfiltration of data include architectural tactics such as authentication and authorization, restricting remote access (including restricting use of cloud services), and monitoring user activity (e.g., for high-volume uploads of data to external systems).

AIM-Categorization-Tiering: It relates to **ARCHITECTURE** because it involves the implementation of controls, such as data loss prevention tools, that are part of a secure and robust technology infrastructure designed to protect an organization's assets and data. The mention of specific architectural tactics like authentication, authorization, and monitoring user activity highlights the role of security architecture in preventing unauthorized data exfiltration. Additionally, it pertains to **THREAT AND VULNERABILITY** as these controls are essential for identifying, assessing, and mitigating the risks associated with potential threats to data security, particularly those related to unauthorized data exfiltration.

ARCHITECTURE-5g

The cybersecurity architecture includes protections (such as full disk encryption) for data that is stored on assets that may be lost or stolen.
Examples of controls to protect data in the event of physical asset loss include encryption (e.g. full disk encryption) or applications that would allow the organization to initiate a remote erasure of the data on the device. Implementation of these controls should be based on the categories of data that are stored on a device.

AIM-Categorization-Tiering:The statement relates to the category **ARCHITECTURE** as it describes the implementation of secure technology infrastructure, specifically focusing on the protection of data through controls like full disk encryption and remote erasure. These measures are designed to safeguard assets, particularly in the event of physical loss or theft, which is a key aspect of security architecture. By emphasizing the importance of data protection based on the categorization of data, the statement also indirectly addresses the concept of secure design and implementation, which falls under the category.

ARCHITECTURE-5h

The cybersecurity architecture includes protections against unauthorized changes to software, firmware, and data. For example, the cybersecurity architecture enforces the use of cryptographic controls such as digital certificates and rejects software or firmware updates that have not been cryptographically signed.

AIM-Categorization-Tiering: The statement relates to the category **ARCHITECTURE** as it describes the design and implementation of a secure technology infrastructure that includes protections against unauthorized changes to software, firmware, and data. Specifically, the use of cryptographic controls such as digital certificates and the enforcement of cryptographic signatures for updates are measures that ensure the integrity and security of the organization's assets. These controls are fundamental aspects of a robust security architecture, which aims to protect data and systems from unauthorized alterations, thereby maintaining the organization's overall cybersecurity posture.

9.6 Management Activities

ARCHITECTURE-6a

Documented procedures are established, followed, and maintained for activities in the ARCHITECTURE domain. The activities in the ARCHITECTURE domain are formally documented in some way (such as standard operating procedures, process flow diagrams, RACI charts, and swim lane diagrams). The activities are intentionally designed or described to serve the organization rather than being ad hoc. Documenting procedures helps ensure that they are repeatable and produce expected outcomes. The level of detail included in documentation should be a sufficient to enable consistent performance of domain activities by different people and new employees assuming relevant domain experience and sufficient on-board training.
Also, procedures documentation is made available to and is used by relevant personnel. The documentation is updated as needed to reflect changes in the organizational or operational environment. Additionally, organizations may consider including exceptions processes in documented procedures to ensure that the organization reacts appropriately to unexpected events or situations.

AIM-Categorization-Tiering: It emphasizes the need for documented procedures and formal documentation within the architecture domain, ensuring that activities are systematically designed and executed. This documentation supports the secure and robust implementation of technology infrastructure. Additionally, the statement ties into **POLICY AND STRATEGY** because it highlights the importance of establishing, maintaining, and updating procedures as part of the organization's broader cybersecurity management strategy. The consistent and intentional design of these procedures ensures alignment with organizational objectives and the ability to adapt to changes, which are critical elements of effective policy and strategy.

ARCHITECTURE-6b

Adequate resources (people, funding, and tools) are provided to support activities in the ARCHITECTURE domain.
When determining the adequacy of resources, it may help to consider whether there are any ARCHITECTURE domain activities not currently being performed that the organization would perform if it had additional people, funding, or tools. An additional consideration may be whether the organization has implemented all practices it has targeted for implementation and whether additional resources are necessary to address potential gaps.
Adequate resources are provided in the form of people, funding, and tools to ensure that ARCHITECTURE domain practices can be performed as intended. The performance of this practice can be evaluated by determining whether any desired practices have not been implemented due to a shortage of resources.
These are examples of people involved in ARCHITECTURE domain activities:

- staff responsible for developing cybersecurity architecture strategy
- staff responsible for evaluating conformance of the organization's systems and networks to the cybersecurity architecture
- staff involved in designing and implementing network segmentation strategies
- staff responsible for establishing and maintaining cryptographic controls

These are examples of tools that might be used in ARCHITECTURE domain activities:

- security testing (dynamic testing, fuzz testing, etc.) tools and methods
- tools and methods for conducting data controls validation
- key management tools

Adequacy of resources should be determined on an ongoing basis through regular reviews of the domain program and reviews of domain resources in budgeting activities. It is a common point of concern that there is not enough time to complete cybersecurity program activities. This is addressed primarily through increasing staff and secondarily through increasing funding and tools.
When determining the adequacy of staff, also consider whether the cybersecurity program has sufficient capacity so that the individuals that make up the program can regularly attend training, implement and maintain tools, and respond to incidents while conducting day-to-day operations and meeting the cybersecurity objectives of the organization.

AIM-Categorization-Tiering: It primarily relates to **ARCHITECTURE** because it discusses the allocation of resources, including people, funding, and tools, to ensure that the organization's cybersecurity architecture is effectively implemented and maintained. The statement also aligns with **PROGRAM** because it addresses the strategic planning and evaluation of resource adequacy within the cybersecurity program, ensuring alignment with organizational objectives. Additionally, it connects to **KNOWLEDGE AND CAPABILITIES** by emphasizing the importance of having a well-trained and adequately staffed workforce to perform domain activities, attend training, and maintain the necessary tools and methods, which are crucial for achieving the cybersecurity objectives.

ARCHITECTURE-6c

Up-to-date policies or other organizational directives define requirements for activities in the ARCHITECTURE domain.
Activities in the ARCHITECTURE domain receive documented guidance and direction from the organization in the form of policies or similar directives. Strategic business objectives drive the development of documented policies or other organizational directives to ensure activities support the accomplishment of the organization's mission.
Policies or other organizational directives for ARCHITECTURE domain activities may contain

- responsibility, authority, and ownership for performing ARCHITECTURE domain activities, such as conducting architectural reviews and managing key management infrastructure
- requirements for adhering to the cybersecurity architecture
- procedures, standards, and guidelines for implementing network segmentation
- procedures, standards, and guidelines for implementing a defined software development process
- requirements for the frequency of architectural reviews
- methods for measuring adherence to policy, exceptions granted, and policy violations
- procedures for the granting and management of exceptions

AIM-Categorization-Tiering: It is primarily related to **POLICY AND STRATEGY** because it discusses the creation and implementation of up-to-date policies or organizational directives that define requirements for activities, which are crucial for ensuring that cybersecurity strategies are aligned with business objectives and that activities support the organization's mission. Additionally, it connects to **ARCHITECTURE** as it involves defining and enforcing policies specific to the ARCHITECTURE domain, including responsibilities, standards, and procedures essential for maintaining a secure and robust technology infrastructure.

ARCHITECTURE-6d

Responsibility, accountability, and authority for the performance of activities in the ARCHITECTURE domain are assigned to personnel.
The intent of this practice is that specific people (or people in specific roles) are held accountable for ensuring the achievement of expected results of ARCHITECTURE domain activities and that they are given the appropriate authority to act and to perform their assigned responsibilities.
These are examples of how to formalize responsibility and authority for ARCHITECTURE domain activities:

- defining roles and responsibilities in policies (see ARCHITECTURE-5c)
- developing position descriptions and conducting associated performance management activities
- including process tasks and responsibility for these tasks in position descriptions
- developing and implementing contractual instruments (including service level agreements) with external entities to establish responsibility and authority for performing ARCHITECTURE domain tasks on outsourced functions
- including ARCHITECTURE domain tasks in measuring performance of external entities against contractual instruments

Additionally, consider how the knowledge developed by personnel within this domain should be managed and shared. This includes determining what processes and tools should be used for knowledge sharing and identifying who will be responsible for making the best use of internal knowledge.

AIM-Categorization-Tiering: It is related to **ARCHITECTURE** because it involves assigning responsibility, accountability, and authority for activities that are directly tied to the design and implementation of a secure technology infrastructure. The statement also connects to **WORKFORCE** as it discusses the formalization of roles and responsibilities, which ensures that the personnel responsible for these activities are appropriately designated and managed. Additionally, the mention of knowledge sharing and management within this domain relates to **KNOWLEDGE AND CAPABILITIES**, highlighting the importance of ensuring that personnel have the necessary skills and resources to perform their tasks effectively and to leverage internal knowledge.

ARCHITECTURE-6e

Personnel performing activities in the ARCHITECTURE domain have the skills and knowledge needed to perform their assigned responsibilities.
The organization must identify the skills and knowledge needed to perform ARCHITECTURE domain activities

and identify skill and knowledge gaps in existing personnel. The organization can address gaps either by hiring qualified personnel or training existing personnel. It is important to note that managing and securing many technologies (such as virtualized or cloud-based environments) require specific training in specialized equipment and practices. Care should be taken to ensure that the level of skills and knowledge of personnel managing and securing specialized technologies is commensurate with the importance of and risk posed by those technologies. Additionally, skill and knowledge assessments should be repeated as operational environments change over time. For example, in the ARCHITECTURE domain, skills and knowledge are needed for

- designing a cybersecurity architecture
- evaluating conformance of systems and networks to the cybersecurity architecture
- managing key management infrastructure
- implementing network segmentation

Additionally, consider how the knowledge developed by personnel within this domain should be managed and shared. This includes determining what processes and tools should be used for knowledge sharing and identifying who will be responsible for making the best use of internal knowledge.

AIM-Categorization-Tiering: It is directly related to **ARCHITECTURE** because it discusses the skills and knowledge required to perform activities within the architecture domain, such as designing cybersecurity architectures, managing key infrastructure, and implementing network segmentation. It also pertains to **KNOWLEDGE AND CAPABILITIES** because it emphasizes the need for personnel to possess the necessary knowledge and skills to effectively carry out their responsibilities, including identifying and addressing skill gaps through training or hiring, and ensuring that knowledge is properly managed and shared as operational environments evolve.

ARCHITECTURE-6f

The effectiveness of activities in the ARCHITECTURE domain is evaluated and tracked.
The organization should measure the performance of ARCHITECTURE activities to ensure they are being performed as described in plans, policies, and procedures for the ARCHITECTURE domain. Appropriate metrics should be developed and collected to detect deviations in performance and measure the extent to which ARCHITECTURE domain activities are achieving their intended purpose.

AIM-Categorization-Tiering: It is related to **ARCHITECTURE** because it focuses on evaluating and tracking the effectiveness of activities within the architecture domain, which includes ensuring that the design and implementation of the technology infrastructure are aligned with the organization's security goals. It also pertains to **PROGRAM** because the evaluation and tracking of these activities require the establishment of metrics and performance measurements, which are critical components of a well-defined cybersecurity program. These metrics help ensure that ARCHITECTURE activities are performed according to the plans, policies, and procedures established by the organization's cybersecurity strategy.

10. Cybersecurity Program Management - 24 questions

As presented on the platform, its purpose is: Establish and maintain an enterprise cybersecurity program that provides governance, strategic planning, and sponsorship for the organization's cybersecurity activities in a manner

that aligns cybersecurity objectives with the organization's strategic objectives and the risk to critical infrastructure.

The Cybersecurity Program Management (PROGRAM) domain comprises three objectives:

1. Establish Cybersecurity Program Strategy
2. Establish and Maintain Cybersecurity Program
3. Management Activities for the PROGRAM domain

10.1 Establish Cybersecurity Program Strategy

PROGRAM-1a

The organization has a cybersecurity program strategy, which may be developed and managed in an ad hoc manner.
The organization develops, implements, and maintains a cybersecurity program strategy that, in its simplest form, includes a list of cybersecurity objectives and related actions, activities, and tasks and a plan to implement them. For a C2M2-based program, areas of activity in the strategy could align with C2M2 domains and objectives. For example, one area of activity would be identifying and responding to cyber risks that affect the function's assets and services. Further detail would describe how this activity is to be accomplished (again, aligning with C2M2 practices, but providing more details about how the practices are to be implemented in the function, such as use of a particular risk management framework).

AIM-Categorization-Tiering: The statement belongs to the category **PROGRAM** because it describes the development, implementation, and maintenance of a cybersecurity program strategy that aligns with the organization's objectives. This includes defining cybersecurity goals, planning related actions, and ensuring that the strategy is implemented effectively. The statement emphasizes the creation of a structured approach to managing cybersecurity activities, which is central to a well-defined and effective cybersecurity program.

PROGRAM-1b

The cybersecurity program strategy defines goals and objectives for the organization's cybersecurity activities.
In its simplest form, the cybersecurity program strategy should include a list of goals and objectives and at least a high-level plan for the actions, activities, and tasks that must be performed to meet them. These objectives should support the achievement and ongoing improvement of an appropriate cybersecurity posture and support the accomplishment of overall organizational strategic objectives.
These are examples of a cybersecurity goal and related objectives:

- Goal: Minimize the impact of cybersecurity incidents on customers.
- Objectives:
  - Maintain commitment to customers by safeguarding their sensitive information from cyber risk and responding competently and appropriately to minimize impact when incidents occur
  - Support the availability of services through the quick detection of cybersecurity incidents that may lead to service interruptions and by expeditiously responding to those events

AIM-Categorization-Tiering: The statement belongs to the category **PROGRAM** because it emphasizes the definition of goals and objectives within the organization's cybersecurity strategy. The strategy outlines the necessary actions, activities, and tasks to achieve these objectives, which are essential for maintaining and improving the organization's cybersecurity posture. This alignment of cybersecurity goals with the organization's overall strategic objectives is a key component of an effective cybersecurity program.

PROGRAM-1c

The cybersecurity program strategy and priorities are documented and aligned with the organization's mission, strategic objectives, and risk to critical infrastructure.
The cybersecurity program strategy is developed as part of the organization's strategic business planning and specifically addresses the actions, activities, and tasks that must be performed to support achievement of the organization's strategic objectives and to manage risks to critical infrastructure within the organization's risk tolerances and appetite.

AIM-Categorization-Tiering: The statement belongs to the category **PROGRAM** because it describes how the organization's cybersecurity program strategy and priorities are documented and aligned with the organization's mission and strategic objectives. This alignment ensures that the cybersecurity efforts are integrated into the overall business strategy, addressing risks to critical infrastructure within the organization's risk tolerances and appetite. The emphasis on the strategic planning process and risk management highlights the role of a comprehensive cybersecurity program in supporting the organization's broader goals.

PROGRAM-1d

The cybersecurity program strategy defines the organization's approach to provide program oversight and governance for cybersecurity activities.
Governance is a process of providing strategic direction for the organization while ensuring that it meets its obligations, appropriately manages risk, and efficiently uses finances and human resources to ensure that the cybersecurity program supports and sustains strategic objectives. Governance is focused on providing oversight of the cybersecurity program, not performing or managing process tasks to completion. For example, the process of overseeing the identification, definition, and inventorying of high-value assets is a governance task, while performing these tasks is part of asset management.
Program oversight and governance might be achieved through

- a formal cybersecurity oversight committee
- establishing C2M2 as standard for cybersecurity program evaluation
- identifying and documenting the areas of the organization and the assets that are within the purview of the cybersecurity program and those that are not
- identifying whether data governance and data protection are to be managed as part of the cybersecurity program or separately

AIM-Categorization-Tiering: The statement belongs to the category **PROGRAM** because it discusses the strategic oversight and governance of cybersecurity activities within an organization. This includes ensuring that the cybersecurity program aligns with the organization's strategic objectives, effectively manages risk, and

efficiently utilizes resources. The focus on governance, such as the establishment of oversight committees and the definition of high-value assets, underscores the importance of structured planning and strategic direction within a comprehensive cybersecurity program.

PROGRAM-1e

The cybersecurity program strategy defines the structure and organization of the cybersecurity program.
The program strategy should contain an organization chart or some other descriptive document which includes the cybersecurity program's structure, the roles in the program, and key activities associated with those roles. For example, a table could be used to describe departments (such as Security Operations Center), sub functions within departments (such as vulnerability management), activities of the sub function (such as scanning for, analyzing, and addressing vulnerabilities), and, if applicable, any organization that the sub function is contracted out to (such as Corporate IT).

AIM-Categorization-Tiering: The statement belongs to the category **PROGRAM** because it addresses the structure and organization of the cybersecurity program within an organization. The emphasis on defining roles, key activities, and the overall organization of the cybersecurity functions directly relates to the strategic planning and alignment of the cybersecurity program with the organization's objectives. By detailing the structure, departments, and functions within the cybersecurity program, the statement underscores the importance of having a clear and organized approach to cybersecurity management.

PROGRAM-1f

The cybersecurity program strategy identifies standards and guidelines intended to be followed by the program.
Standards or guidelines are identified to inform the implementation of practices in the cybersecurity program that will have implications for activities in all C2M2 domains. These may simply be the reference sources the organization consulted when developing the plan for performing the practices. They should include any standards or guidelines required by policy. If the organization is using C2M2 to guide its cybersecurity program activities, C2M2 could be one of the guidelines identified in the program strategy.
Other examples of standards and guidelines are

- National Institute of Standards and Technology (NIST) SP 800 guidelines such as 800-53, 800-124, 800-61, 800-82, 800-30
- NIST Framework for Improving Critical Infrastructure Cybersecurity (CSF)
- Zero trust security models (for example, NIST SP 800-207)
- the Center for Internet Security (CIS) Critical Security Controls
- Control Objectives for Information and Related Technologies (COBIT)
- International Organization for Standardization (ISO)
- DOE Cybersecurity Procurement Language for Energy Delivery Systems

AIM-Categorization-Tiering: The statement belongs to the category **STANDARDS AND TECHNOLOGY** because it focuses on the identification and application of cybersecurity standards and guidelines that inform the implementation of practices within the cybersecurity program. The emphasis on referencing specific standards and frameworks, such as NIST guidelines, CIS Controls, and ISO standards, underscores the importance of established cybersecurity standards in guiding the organization's cybersecurity efforts and ensuring the protection of its systems and data.

PROGRAM-1g

The cybersecurity program strategy identifies any applicable compliance requirements that must be satisfied by the program (for example, NERC CIP, TSA Pipeline Security Guidelines, PCI DSS, ISO, DoD CMMC).
Compliance requirements are typically imposed on the organization by local, state, or federal governments. Different compliance requirements may apply to some but not all assets in-scope for the cybersecurity program. The cybersecurity program should be aware of what compliance requirements must be fulfilled by the program and the scope of each requirement. Listing compliance requirements in the cybersecurity program strategy helps ensure that cybersecurity program stakeholders know what they are held accountable for. For example, a strategy might include a statement that compliance to PCI DSS is required by the cybersecurity program. Organizations should consider the differences in legal and regulatory requirements within the areas in which they operate and how they may conflict with global IT, enterprise-wide IT, or cybersecurity controls.
Some examples of compliance requirements that organizations may need to satisfy include:

- North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) Standards
- Transportation Security Administration (TSA) Pipeline Security Guidelines
- Payment Card Industry Data Security Standards (PCI DSS)
- International Organization for Standardization (ISO)
- Department of Defense Cybersecurity Maturity Model Certification (DoD CMMC)
- California Consumer Privacy Act (CCPA)
- Health Insurance Portability and Accountability Act of 1996 (HIPAA)
- State- and local-level cybersecurity and privacy laws

AIM-Categorization-Tiering: The statement belongs to the category **LEGAL AND REGULATORY FRAMEWORK** because it focuses on the identification and management of compliance requirements that the organization's cybersecurity program must satisfy. This category encompasses the laws, regulations, and standards that govern information security and data privacy, ensuring that the organization adheres to mandatory guidelines imposed by various governmental and regulatory bodies. The emphasis on different compliance requirements, such as PCI DSS, NERC CIP, and HIPAA, highlights the necessity for the cybersecurity program to be aware of and fulfill these obligations to maintain legal and regulatory compliance.

PROGRAM-1h

The cybersecurity program strategy is updated periodically and according to defined triggers, such as business changes, changes in the operating environment, and changes in the threat profile (THREAT-2e).
The organization should have a documented process to ensure that certain types of changes trigger an update of the cybersecurity program strategy. An example of a business change that would necessitate an update would be a change in the business that increases its exposure to cyber events, such as entering a new line of business. An example of a change in the operating environment that might necessitate an update would be the acquisition of a new customer management system that uses sensitive information. An example of a change in the threat profile of a utility company that might necessitate an update would be threat reporting that indicates increased cyber-attack activity targeting utilities.

AIM-Categorization-Tiering: The statement belongs to the category **PROGRAM** because it focuses on the need for a cybersecurity program strategy to be updated periodically in response to specific triggers, such as business changes, changes in the operating environment, and changes in the threat profile. This reflects the organization's approach to ensuring that its cybersecurity strategy remains aligned with its evolving business objectives and risk landscape. By documenting a process for updating the strategy based on these triggers, the organization demonstrates its commitment to maintaining an effective and adaptive cybersecurity program that is responsive to internal and external changes.

10.2 Establish and Maintain Cybersecurity Program

PROGRAM-2a

Senior management with proper authority provides support for the cybersecurity program, at least in an ad hoc manner.
Having material support from senior management is necessary for implementing a cybersecurity program. The fundamental forms of support are providing resources (people, tools, and funding) and authority to perform cybersecurity activities. To provide such support, the senior managers themselves must have sufficient and relevant authority.

AIM-Categorization-Tiering: The statement belongs to the category **PROGRAM** because it emphasizes the importance of senior management's support in implementing a cybersecurity program. This support is critical for providing the necessary resources, such as personnel, tools, and funding, as well as the authority needed to carry out cybersecurity activities effectively. The involvement of senior management with proper authority ensures that the cybersecurity program is aligned with the organization's strategic goals and has the backing required for successful execution. This alignment and resource allocation are key aspects of a well-structured and effective cybersecurity program.

PROGRAM-2b

The cybersecurity program is established according to the cybersecurity program strategy.
The cybersecurity program is typically responsible for ensuring that the cybersecurity objectives as documented in the cybersecurity program strategy are achieved. For example, the cybersecurity program includes activities to ensure that adequate staff will be available to fulfill the requirements of the program strategy.

AIM-Categorization-Tiering: The statement belongs to the category **PROGRAM** because it describes the establishment of the cybersecurity program in alignment with the cybersecurity program strategy. This category focuses on the strategic planning and execution of cybersecurity efforts, ensuring that the program's activities, including staffing and resource allocation, are designed to meet the objectives outlined in the program strategy. The alignment between the program and the strategy is crucial for achieving the organization's cybersecurity goals effectively.

PROGRAM-2c

Senior management sponsorship for the cybersecurity program is visible and active.
Visible and active sponsorship by senior management might include regular communications by senior management about the importance and value of cybersecurity activities, organizational support for establishing and implementing policies or other organizational directives to guide the program, funding awards and recognition programs for staff who make significant contributions toward achieving cybersecurity objectives, and ensuring that cybersecurity concepts are included in contracts with suppliers and business partners.

AIM-Categorization-Tiering: The statement belongs to the category **CULTURE AND SOCIETY** because it highlights the role of senior management in visibly and actively supporting the cybersecurity program. This support manifests through regular communications, funding, recognition programs, and integration of cybersecurity concepts into organizational practices. These actions reflect how senior management's culture and values influence and promote the importance of cybersecurity within the organization, impacting how employees, suppliers, and partners perceive and engage with cybersecurity efforts.

PROGRAM-2d

Senior management sponsorship is provided for the development, maintenance, and enforcement of cybersecurity policies.
Polices are an expression of senior managers' level of commitment to the cybersecurity program. Lack of visible endorsement of cybersecurity policies by senior managers typically renders policies less effective because stakeholders may assume that the policies are not being enforced or that they are simply meant to be used as a guideline rather than a requirement. Senior managers should communicate the importance of cybersecurity policies to the mission and well-being of the organization and express their intention to hold stakeholders responsible for compliance.

AIM-Categorization-Tiering: The statement belongs to the category **POLICY AND STRATEGY** because it addresses the role of senior management in supporting and enforcing cybersecurity policies. Effective cybersecurity policies are essential components of an organization's strategy, and their development, maintenance, and enforcement reflect the commitment and direction provided by senior management. This support ensures that policies are taken seriously, enforced properly, and aligned with the organization's cybersecurity objectives, which are crucial for effective policy implementation and overall security management.

PROGRAM-2e

Responsibility for the cybersecurity program is assigned to a role with sufficient authority.
It's important that the role that is made responsible for executing the cybersecurity program (such as a chief information security officer) has the necessary and sufficient authority within the organization to carry out program

activities and to obtain the necessary resources to support the program.

AIM-Categorization-Tiering: The statement belongs to the category **PROGRAM** because it highlights the necessity of assigning responsibility for the cybersecurity program to a role with adequate authority. This ensures that the individual or team responsible for the program has the power to implement cybersecurity activities effectively, secure necessary resources, and drive the program's success. The authority of this role is crucial for the execution of the cybersecurity strategy and achieving the program's objectives, which are central to effective cybersecurity management and planning.

PROGRAM-2f

Stakeholders for cybersecurity program management activities are identified and involved.
Stakeholders of the cybersecurity program are identified and involved in the performance of practices. This could include stakeholders from within the function, from across the organization, or from outside the organization, depending on how the organization implemented the practices. Stakeholders might include project managers, business process owners, and owners of affected assets and services, as well as staff involved in cybersecurity activities. Identification of stakeholders and their appropriate involvement should be documented in some way, such as in position descriptions or team charters.

AIM-Categorization-Tiering: The statement belongs to the category **PROGRAM** because it focuses on identifying and involving stakeholders in the management of the cybersecurity program. Effective cybersecurity program management requires recognizing the relevant stakeholders, which may include internal and external individuals, and ensuring their active participation in the program's activities. This involvement is essential for the successful execution of the cybersecurity strategy and for addressing the needs and responsibilities related to cybersecurity practices. Proper documentation of stakeholders and their roles further supports the alignment and effectiveness of the cybersecurity program.

PROGRAM-2g

Cybersecurity program activities are periodically reviewed to ensure that they align with the cybersecurity program strategy.
There should be a process in place to periodically evaluate cybersecurity program activities to ensure that they continue to support the goals and objectives of the cybersecurity program strategy. Activities that don't contribute to the accomplishment of those goals and objectives should be evaluated to determine whether they should be continued. Any gaps in fulfillment of the objectives should also be addressed.

AIM-Categorization-Tiering: The statement belongs to the category **PROGRAM** because it emphasizes the need for ongoing evaluation of cybersecurity program activities to ensure they remain aligned with the overarching cybersecurity program strategy. Regular reviews are essential for assessing whether these activities are effectively supporting the program's goals and objectives. This process helps identify and address any gaps or inefficiencies, ensuring that the program continues to meet its strategic objectives and adapt as necessary.

PROGRAM-2h

Cybersecurity activities are independently reviewed to ensure conformance with cybersecurity policies and procedures, periodically and according to defined triggers, such as process changes.

The purpose of this practice is to provide additional assurance that cybersecurity activities are being performed as specified by the organization's cybersecurity policies and procedures. The evaluation must be independent; that is, conducted by reviewers from outside the cybersecurity program under direction from the organization's governing body). Those directly involved in program activities cannot perform the evaluation or render an opinion on the program's effectiveness. Such evaluations may be done through internal and external audits, post-event reviews, and capability appraisals and should be initiated by and accountable to the board of directors or a similar group. Advanced cybersecurity techniques such as threat hunting and active defense can be used to provide insight into the performance of the overall cybersecurity program.

AIM-Categorization-Tiering: The statement belongs to the category **POLICY AND STRATEGY** because it focuses on ensuring that cybersecurity activities align with and conform to established cybersecurity policies and procedures. The emphasis is on conducting independent reviews, often through audits or evaluations by external parties, to verify adherence to these policies and to provide additional assurance of their effectiveness. This practice ensures that the cybersecurity strategy remains effective and that any discrepancies are addressed, reflecting a commitment to maintaining a high standard of policy compliance and strategic alignment.

PROGRAM-2i

The cybersecurity program addresses and enables the achievement of legal and regulatory compliance, as appropriate.
The organization should have personnel who are responsible for ensuring that it is aware of all regulatory compliance obligations that it is subject to from governments and other sources. Cybersecurity program objectives should align with and support the meeting of any of those obligations that are relevant to cybersecurity, and the program should develop and implement the proper procedures and activities to ensure compliance in a timely and accurate manner.

AIM-Categorization-Tiering: The statement belongs to the category **LEGAL AND REGULATORY FRAMEWORK** because it focuses on ensuring that the cybersecurity program is designed to meet legal and regulatory compliance obligations. This involves having dedicated personnel responsible for understanding and addressing compliance requirements from various regulatory bodies. The emphasis is on aligning the cybersecurity program's objectives with these obligations and developing procedures to ensure timely and accurate compliance, reflecting the importance of adhering to legal and regulatory standards in the organization's cybersecurity efforts.

PROGRAM-2j

The organization collaborates with external entities to contribute to the development and implementation of cybersecurity standards, guidelines, leading practices, lessons learned, and emerging technologies.
In addition to maintaining awareness of any industry cybersecurity standards that the organization is obligated to comply with (such as the North American Energy Reliability Corporation Critical Infrastructure Protection standard), the organization should assign responsibility to selected personnel to contribute to industry efforts to develop cybersecurity practices or guidelines. For example, the Payment Card Industry practices were developed by stakeholders in the credit card industry for voluntary implementation.

AIM-Categorization-Tiering: The statement belongs to the category **STANDARDS AND TECHNOLOGY** because it emphasizes the organization's role in collaborating with external entities to develop and implement

cybersecurity standards, guidelines, leading practices, and emerging technologies. This involves actively participating in industry efforts to establish and refine cybersecurity practices, which is crucial for aligning with established standards and incorporating advanced technologies. The focus on contributing to the development of cybersecurity practices and guidelines reflects the importance of adhering to and influencing industry standards and technological advancements.

10.3 Management Activities

PROGRAM-3a

Documented procedures are established, followed, and maintained for activities in the PROGRAM domain.
The activities in the PROGRAM domain are formally documented in some way (such as standard operating procedures, process flow diagrams, RACI charts, and swim lane diagrams). The activities are intentionally designed or described to serve the organization rather than being ad hoc. Documenting procedures helps ensure that they are repeatable and produce expected outcomes. The level of detail included in documentation should be a sufficient to enable consistent performance of domain activities by different people and new employees assuming relevant domain experience and sufficient on-board training.
Also, procedure documentation is made available to and is used by relevant personnel. The documentation is updated as needed to reflect changes in the organizational or operational environment. Additionally, organizations may consider including exceptions procedures in documented practices to ensure that the organization reacts appropriately to unexpected events or situations.

AIM-Categorization-Tiering: The statement belongs to the category **PROGRAM** because it focuses on the establishment, adherence, and maintenance of documented procedures specifically for activities within the cybersecurity program domain. The documentation of procedures, such as standard operating procedures and process flow diagrams, is crucial for ensuring that program activities are consistent, repeatable, and align with organizational objectives. This category encompasses the strategic and planning aspects of cybersecurity, including the creation and maintenance of procedures to manage and oversee cybersecurity activities effectively.

PROGRAM-3b

Adequate resources (people, funding, and tools) are provided to support activities in the PROGRAM domain.
When determining the adequacy of resources, it may help to consider whether there are any PROGRAM domain activities not currently being performed that the organization would perform if it had additional people, funding, or tools. An additional consideration may be whether the organization has implemented all practices it has targeted for implementation and whether additional resources are necessary to address potential gaps.
Adequate resources are provided in the form of people, funding, and tools to ensure that PROGRAM domain practices can be performed as intended. This includes both initiation and ongoing maintenance of a cybersecurity program. The performance of this practice can be evaluated by determining whether any desired practices have not been implemented due to a shortage of resources.
These are examples of people involved in PROGRAM domain activities:

- staff responsible for collection and analysis of threat information
- staff responsible for developing threat profiles
- staff responsible for performing vulnerability assessments

These are examples of tools that might be used in PROGRAM domain activities:

- techniques and tools for creating threat profiles
- tools for performing vulnerability assessments
- vulnerability databases

Adequacy of resources should be determined on an ongoing basis through regular reviews of the domain program and reviews of domain resources in budgeting activities. It is a common point of concern that there is not enough time to complete cybersecurity program activities. This is addressed primarily through increasing staff and secondarily through increasing funding and tools.
When determining the adequacy of staff, also consider whether the cybersecurity program has sufficient capacity so that the individuals that make up the program can regularly attend training, implement and maintain tools, and respond to incidents while conducting day-to-day operations and meeting the cybersecurity objectives of the organization.

AIM-Categorization-Tiering: The statement belongs to the category **PROGRAM** because it focuses on the allocation and adequacy of resources (people, funding, and tools) necessary to support and maintain activities within the cybersecurity program domain. The emphasis is on ensuring that sufficient resources are available to perform and sustain program activities effectively, address potential gaps, and achieve the organization's cybersecurity objectives. This includes evaluating whether additional resources are needed for implementing and maintaining program practices, which is central to the planning and strategic management aspects of a cybersecurity program.

PROGRAM-3c

Up-to-date policies or other organizational directives define requirements for activities in the PROGRAM domain.
Activities in the PROGRAM domain receive documented guidance and direction from the organization in the form of policies or similar directives. Strategic business objectives drive the development of documented policies or other organizational directives to ensure activities support the accomplishment of the organization's mission.
Policies or other organizational directives for PROGRAM domain activities may contain

- responsibility, authority, and ownership for performing PROGRAM activities
- sponsorship statements, such as statements reflecting higher level managers' commitment to managing cybersecurity
- list of triggers that initiate independent review of cybersecurity activities
- methods for measuring adherence to policy, exceptions granted, and policy violations
- procedures for the granting and management of exceptions

AIM-Categorization-Tiering: The statement belongs to the category **POLICY AND STRATEGY** because it discusses the establishment of up-to-date policies or organizational directives that define and guide the requirements for activities within the PROGRAM domain. These policies ensure that the PROGRAM domain's activities align with the organization's strategic business objectives, providing clear responsibilities, authority, and ownership. This category is essential for establishing effective and well-communicated policies and strategies that form the foundation of a robust cybersecurity management framework.

PROGRAM-3d

Responsibility, accountability, and authority for the performance of activities in the PROGRAM domain are assigned to personnel.
The intent of this practice is that specific people (or people in specific roles) are held accountable for ensuring the achievement of expected results of PROGRAM domain activities and that they are given the appropriate authority to act and to perform their assigned responsibilities.
These are examples of how to formalize responsibility and authority for PROGRAM domain activities:

- defining roles and responsibilities in policies
- developing position descriptions and conducting associated performance management activities
- including process tasks and responsibility for these tasks in position descriptions
- developing and implementing contractual instruments (including service level agreements) with external entities to establish responsibility and authority for performing PROGRAM domain tasks on outsourced functions
- including PROGRAM domain tasks in measuring performance of external entities against contractual instruments

Additionally, consider how the knowledge developed by personnel within this domain should be managed and shared. This includes determining what processes and tools should be used for knowledge sharing and identifying who will be responsible for making the best use of internal knowledge.

AIM-Categorization-Tiering: The statement belongs to the category **WORKFORCE** because it discusses the assignment of responsibility, accountability, and authority to personnel for performing activities within the PROGRAM domain. Ensuring that specific roles are defined and that individuals are empowered to act within these roles is critical to the effective management of cybersecurity tasks. This process involves defining roles, responsibilities, and performance expectations, which are essential aspects of managing the cybersecurity workforce and ensuring that they have the necessary authority to fulfill their duties.

PROGRAM-3e

Personnel performing activities in the PROGRAM domain have the skills and knowledge needed to perform their assigned responsibilities.
The organization must identify the skills and knowledge needed to perform PROGRAM domain activities and identify skill and knowledge gaps in existing personnel. The organization can address gaps either by hiring qualified personnel or training existing personnel. It is important to note that managing and securing many technologies (such as virtualized or cloud-based environments) require specific training in specialized equipment and practices. Care should be taken to ensure that the level of skills and knowledge of personnel managing and securing specialized technologies is commensurate with the importance of and risk posed by those technologies.
Additionally, skill and knowledge assessments should be repeated as operational environments change over time. For example, in the PROGRAM domain, skills and knowledge are needed for

- developing a cybersecurity program strategy and structure

· developing, disseminating, and enforcing policy

· providing adequate resources for implementing the cybersecurity program strategy

Additionally, consider how the knowledge developed by personnel within this domain should be managed and shared. This includes determining what processes and tools should be used for knowledge sharing and identifying who will be responsible for making the best use of internal knowledge.

AIM-Categorization-Tiering: The statement belongs to the category **KNOWLEDGE AND CAPABILITIES** because it emphasizes the importance of ensuring that personnel in the PROGRAM domain possess the necessary skills and knowledge to perform their responsibilities effectively. This involves identifying skill gaps, providing training, and ensuring that employees are equipped to manage and secure specialized technologies. Continuous assessment and improvement of knowledge and skills are crucial to maintaining a robust cybersecurity posture, particularly as operational environments evolve. Therefore, ensuring that personnel have the required capabilities is fundamental to the successful implementation of cybersecurity strategies.

PROGRAM-3f

The effectiveness of activities in the PROGRAM domain is evaluated and tracked.
The organization should measure the performance of PROGRAM activities to ensure they are being performed as described in plans, policies, and procedures for the PROGRAM domain. Appropriate metrics should be developed and collected to detect deviations in performance and measure the extent to which PROGRAM domain activities are achieving their intended purpose.

AIM-Categorization-Tiering: The statement belongs to the category **PROGRAM** because it emphasizes the importance of evaluating and tracking the effectiveness of cybersecurity activities within the PROGRAM domain. This involves measuring performance against established plans, policies, and procedures to ensure that these activities are effectively supporting the organization's cybersecurity strategy. By developing and collecting appropriate metrics, the organization can detect deviations and assess whether PROGRAM domain activities are achieving their intended purpose, ensuring alignment with broader business objectives.

Acknowledgments

Funded (partially) by Dirección de Investigación, Universidad de La Frontera, Grant PP24-0027.

References

[1] Hochstetter-Diez J, Diéguez-Rebolledo M, Fenner-López J, Cachero C (2023) Aim triad: A prioritization strategy for public institutions to improve information security maturity. *Applied Sciences* 13(14):8339.

[2] US Department of Energy (2024) Cybersecurity capability maturity model (c2m2). Online resource Available at https://www.energy.gov/ceser/cybersecurity-capability-maturity-model-c2m2.