



Funded by  
the European Union



Project Acronym	RAISE
Project Name	Research Analysis Identifier SystEm
Project Number	101058479
Topic	HORIZON-INFRA-2021-EOSC-01-04
Type of Action	HORIZON Research and Innovation Actions
Granting Authority	European Research Executive Agency
Project starting date	1 October 2022
Project end date	31 January 2026
Project duration	40 months

## D2.2 Service architecture consumer protection requirements

(Version 3.0, 31/05/2024)

**Disclaimer:** Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Research Executive Agency (REA). Neither the European Union nor the European Research Executive Agency can be held responsible for them.

**Copyright message:** ©RAISE Consortium, 2024. This deliverable contains original unpublished work except where clearly indicated otherwise. Acknowledgement of previously published material and of the work of others has been made through appropriate citation, quotation or both. Reproduction is authorised provided the source is acknowledged.

<b>Deliverable Number</b>	D2.2	
<b>Deliverable Name</b>	Service architecture consumer protection requirements	
<b>Work Package No</b>	2	
<b>Due Date (month)</b>	20	
<b>Submission Date</b>	20	
<b>Lead Beneficiary</b>	UOWM	
<b>Version</b>	3.0	
<b>Status</b>	Final	
<b>Author name(s)</b>	Nikolaos Katertsidis, Athanasios Liatifis, Anna Triantafyllou, Panagiotis Sarigiannidis, Vasiliki Kelli, Dimitrios Pliatsios, Vasileios Vitsas, Georgios Karagiannidis, Aikaterini Karampasi, Nikolaos Lemonas	
<b>Contributor(s)</b>		
<b>Reviewer(s)</b>	Ilektra Makridou (AUTH)	Nikolaos Nikolaidis, Theodoros Maikantis, Alexander Chatzigeorgiou, Apostolos Ampatzoglou (UOM)
<b>Approved by</b>	Evdokimos Konstantinidis (AUTH), Project Coordinator	
<b>Keywords</b>	Security, privacy risks, data protection, consumer requirements, security techniques, access policy	
<b>Type</b>	R – Document, report	
<b>Dissemination level</b>	PU - Public	

The **RAISE** Consortium consists of:

Participant #	Participant organisation name	Short Name	Country
1 COO	ARISTOTELIO PANEPISTIMIO THESSALONIKIS	AUTH	EL
2 BEN	FUNDACION CENTRO DE TECNOLOGIAS DE INTERACCION VISUAL Y COMUNICACIONES VICOMTECH	VICOM	ES
3 BEN	NETCOMPANY-INTRASOFT SA	INTRA	LU
4 BEN	PANEPISTIMIO DYTIKIS MAKEDONIAS	UOWM	EL
5 BEN	UNIVERSITY OF MACEDONIA	UOM	EL
6 BEN	TECREANDO B.V	TECREANDO	NL
7 BEN	WITA SRL	WITA SRL	IT
8 BEN	ETHNIKO KENTRO EREVNAS KAI TECHNOLOGIKIS ANAPTYXIS	CERTH	EL
9 BEN	INNOV-ACTS LIMITED	INNOVACTS	CY
10 BEN	VILABS (CY) LTD	VILABS	CY
11 BEN	KYKLIKI VELTISTOPOIISI IKE	Cyclopt PC	EL
12 BEN	KAROLINSKA INSTITUTET	KI	SE
13 BEN	ATHINA-EREVNITIKO KENTRO KAINOTOMIAS STIS TECHNOLOGIES TIS PLIROFORIAS, TON EPIKOINONION KAI TIS GNOSIS	ATHENA	EL
14 BEN	AINIGMA TECHNOLOGIES	AINIGMA	BE
15 BEN	UNIVERSITEIT HASSELT	UHASSELT	BE
16 BEN	OPENAIRE AMKE	OPENAIRE	EL
17 BEN	CENTRO EUROPEO DI FORMAZIONE E RICERCA IN INGEGNERIA SISMICA	EUCENTRE	IT
18 BEN	ENVE.X SINGLE MEMBER PC	ENVE.X	EL
19 AP	UNIVERSITY OF SOUTHAMPTON	SOTON	UK
20 AP	ROYAL INSTITUTION FOR THE ADVANCEMENT OF LEARNING MCGILL UNIVERSITY	McGill	CA

Revision history			
Version	Date	Modified by	Comments
0.1	05/09/2023	Nikolaos Katertsidis (UOWM)	Table of contents and executive summary
0.3	15/10/2023	Nikolaos Katertsidis (UOWM), Athanasios Liatifis (UOWM), Anna Triantafyllou (UOWM), Vasiliki Kelli (UOWM)	Drafting Section 1
0.5	05/01/2024	Nikolaos Katertsidis (UOWM), Athanasios Liatifis (UOWM), Anna Triantafyllou (UOWM), Dimitrios Pliatsios (UOWM)	Drafting Sections 2 and 3
0.8	20/04/2024	Nikolaos Katertsidis (UOWM), Vasileios Vitsas (UOWM), Georgios Karagiannidis (UOWM), Aikaterini Karampasi (UOWM), Nikolaos Lemonas (UOWM)	Drafting Sections 4 and 5
1.0	15/05/2024	Panagiotis Sarigiannidis (UOWM), Nikolaos Katertsidis (UOWM)	Finalise document
1.5	31/05/2024	Panagiotis Sarigiannidis (UOWM), Nikolaos Katertsidis (UOWM)	Incorporated reviewers' suggestions and other corrections

## Table of Contents

<b>TABLE OF CONTENTS</b>	<b>5</b>
<b>LIST OF FIGURES</b>	<b>5</b>
<b>LIST OF TABLES</b>	<b>6</b>
<b>ABBREVIATIONS</b>	<b>7</b>
<b>EXECUTIVE SUMMARY</b>	<b>10</b>
<b>1 INTRODUCTION</b>	<b>11</b>
1.1 OVERVIEW OF THE RAISE SYSTEM	11
1.2 RAISE SYSTEM ARCHITECTURE AND SERVICES	11
<b>2 SECURITY AND PRIVACY RISKS</b>	<b>13</b>
2.1 HARDWARE LEVEL RISKS	13
2.2 OPERATING SYSTEM LEVEL RISKS	13
2.3 NETWORK LEVEL RISKS	14
2.4 APPLICATION LEVEL RISKS	15
2.5 USER LEVEL RISKS	17
<b>3 REGULATORY COMPLIANCE AND STANDARDS</b>	<b>18</b>
3.1 EU LAWS AND LEGISLATIONS	18
3.1.1 General Data Protection Regulation (GDPR)	18
3.1.2 Network and Information Security Directive (NIS Directive)	19
3.1.3 ePrivacy Directive and ePrivacy Regulation	20
3.1.4 Digital Services Act (DSA) and Digital Markets Act (DMA)	21
3.1.5 Cybersecurity Act	22
3.2 INDUSTRY SECURITY STANDARDS	23
3.2.1 ISO/IEC 27001 - Information Security Management System (ISMS)	23
3.2.2 ISO/IEC 29100 - Privacy Framework	24
3.2.3 NIST Cybersecurity Framework	24
3.2.4 PCI DSS - Payment Card Industry Data Security Standard	26
3.2.5 HIPAA - Health Insurance Portability and Accountability Act	27
3.2.6 CIS Controls and Benchmarks	28
<b>4 RAISE SECURITY REQUIREMENTS</b>	<b>31</b>
<b>5 RAISE SECURITY MEASURES AND BEST PRACTICES</b>	<b>38</b>
5.1 HARDWARE LEVEL	38
5.2 OPERATING SYSTEM LEVEL	38
5.3 NETWORK LEVEL	40
5.4 APPLICATION LEVEL	41
5.5 USER LEVEL	44
<b>6 CONCLUSION</b>	<b>46</b>
<b>7 REFERENCES</b>	<b>47</b>
<b>APPENDIX 1 - INCIDENT RESPONSE PLAN</b>	<b>49</b>

## List of Figures

FIGURE 1: OVERVIEW OF THE RAISE SYSTEM FUNCTIONALITIES	11
FIGURE 2: RAISE SYSTEM ARCHITECTURE AND MODULES	12
FIGURE 3: OVERVIEW OF THE RAISE SECURITY CONTROL MATRICES	31

List of Tables

TABLE 1: REQUIREMENTS OF UNDERLYING HARDWARE INFRASTRUCTURE.....31

TABLE 2: REQUIREMENTS OF UNDERLYING SOFTWARE INFRASTRUCTURE .....32

TABLE 3: REQUIREMENTS OF IDENTITY AND ACCOUNT MANAGEMENT .....33

TABLE 4: REQUIREMENTS OF DATA USAGE AND SHARING.....34

TABLE 5: REQUIREMENTS OF CORE SERVICES AND APPLICATIONS.....35

## Abbreviations

ACL	Access Control List
ARP	Address Resolution Protocol
CIS	Center for Internet Security
CIS-CAT	Center for Internet Security - Configuration Assessment Tool
CSIRT	Computer Security Incident Response Team
DDoS	Distributed Denial of Service
DMA	Digital Markets Act
DoS	Denial of Service
DSA	Digital Services Act
DSP	Digital Service Provider
EC	European Commission
EMI	Electromagnetic Interference
ENISA	European Union Agency for Cybersecurity
EU	European Union
FAIR	Findable, Accessible, Interoperable, Reusable
FTP	File Transfer Protocol
GDPR	General Data Protection Regulation
HHS	Health and Human Services
HIPAA	Health Insurance Portability and Accountability Act
HTML	HyperText Markup Language
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IAM	Identity and Access Management
ICT	Information And Communication Technology
IDS	Intrusion Detection and Prevention System
IPS	Intrusion Prevention System

IRP	Incident Response Plan
ISMS	Information Security Management System
ISO	International Organization for Standardization
JWT	JSON Web Token
LTS	Long Term Support
MFA	Multi-factor Authentication
MitM	Man-in-the-Middle
NCA	National Competent Authority
NIS	Network and Information Security
NIST	National Institute of Standards and Technology
OCR	Office for Civil Rights
OES	Operators of Essential Services
OS	Operating System
OWASP	Open Web Application Security Project
PAM	Pluggable Authentication Modules
PCI DSS	Payment Card Industry Data Security Standard
PCI SSC	Payment Card Industry Security Standards Council
PII	Personally Identifiable Information
PHI	Protected Health Information
RCN	RAISE Certified Node
RCH	RAISE Central Hub
REA	European Research Executive Agency
RBAC	Role-Based Access Control
SMTP	Simple Mail Transfer Protocol
SQL	Structured Query Language
SSH	Secure Shell Protocol
SSO	Single Sign-On



SSRF	Server-Side Request Forgery
TLS	Transport Layer Security
UFW	Uncomplicated Firewall
URL	Uniform Resource Locator
VLAN	Virtual Local Area Network
VLP	Very Large Platform
VPN	Virtual Private Network
WAF	Web Application Firewall
WP	Work Package
XSS	Cross-Site Scripting

### Executive summary

This deliverable analyses all potential threats, breaches and security/privacy risks that are theoretically and practically applicable for all components and actors of the RAISE system including storing and sharing data, accessing applications and services, managing servers and connections, handling channels and other equipment. The aim is to cover all security issues by a reasonable and cost-effective strategy for the entire RAISE system. Thus, deliverable D2.2 includes: 1) a clearly defined set of requirements and restrictions about data and channels protection, liability and user requirements, and 2) a complete set of specifications for security and data protection per subsystem. The security strategy is aligned with the legislations of the EU and the countries involved in the real cases of piloting, as well as industry standards and frameworks. The developed requirements include typical security/privacy risks and threats for each component of the system and what countermeasures will be applied, what protection and security techniques will be integrated in the main architecture and how the data will be protected on the server side. Moreover, privacy requirements on the consumers' side are explored like how the users are authenticated within the whole system, who are the data owners, and who is defining and controlling the access policy and levels.

# 1 Introduction

## 1.1 Overview of the RAISE System

The RAISE system and services are designed to support open and reproducible scientific research by providing a secure, distributed infrastructure for data processing and sharing. The primary goal is to enhance the accessibility and reusability of research data under the FAIR (Findable, Accessible, Interoperable, Reusable) guiding principles, which aligns with modern open science practices. In order to achieve this, RAISE brings the processing algorithm (small size) to the dataset (large size) instead of downloading the dataset to the computer where the processing algorithm is. To increase the processing capacity of the dataset repositories, RAISE borrows the crowdsourcing concept where researchers can easily integrate in the existing workflows computers serving both their datasets and the processing capacity.



**Figure 1: Overview of the RAISE System Functionalities**

Hence, the real value of open data for the research community is not to access them but to process them as conveniently as possible to reduce time-to-result and increase productivity. RAISE promotes a transparent way of sharing and processing data, enabling the research community to publish their work with evidence-based authenticity of the data-analysis performed, ensuring at the same time the accreditation of their work.

## 1.2 RAISE System Architecture and Services

The RAISE system architecture and its components are detailed in the deliverable “D3.1 RAI Cloud services’ specifications” and are depicted in Figure 2. The innovative approach focuses on managing and processing data efficiently and securely, while at the same time adhering to the FAIR principles. Thus, the RAISE system architecture consists of the following main components:

1. **RAI Certified Nodes:** These nodes are distributed and decentralized processing units certified by RAISE. They handle data storage, processing, and execution of scripts while ensuring the data remain secure and private. Each node can be set up easily using Docker,

facilitating the transformation of any computing machine into a certified node without requiring special programming skills.

2. **RAI Central Hub:** This serves as the intermediary interface between the RAISE system's distributed nodes and the users. It hosts the RAISE portal where users can access data and processing tools. It also manages the RAI Registration and Finder services, crucial for managing the identification and retrieval of processed data.
3. **RAI Registration Service:** Used for registering and verifying the integrity of processed results, this module employs a blockchain network, and ensures that data cannot be altered retroactively, enhancing the trustworthiness and reliability of research outputs.

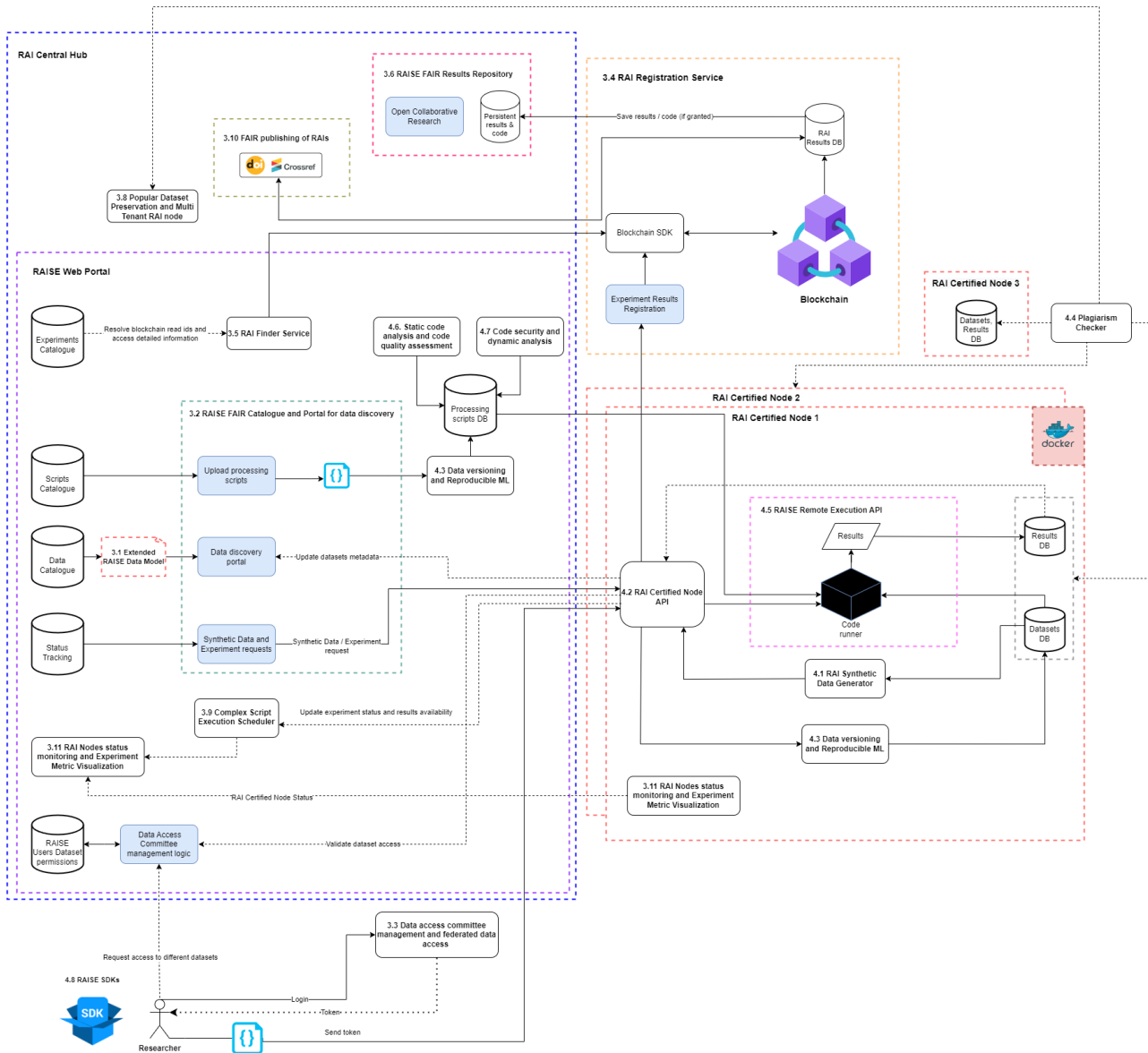


Figure 2: RAISE System Architecture and Modules

The RAISE system is designed to be scalable, secure, and efficient, enabling researchers to share and process data under strict privacy and security standards. It not only supports current research needs, but also adapts to future demands by allowing easy integration of additional resources and technologies.

## 2 Security and Privacy Risks

The RAISE system, as an innovative platform for distributed crowdsourced data processing, faces specific cybersecurity and privacy threats given its design and operational objectives. Understanding these specific threats is critical for implementing effective security measures. Below, a detailed description of various specific threats that the RAISE system may encounter, is presented. The analysis follows a bottom-up approach, since security risks can manifest at various levels of a cloud-based system, from the hardware level to the application level.

### 2.1 Hardware Level Risks

Hardware risks involve the physical components of a system, including servers, workstations, networking equipment, and storage devices, like the ones employed in the RAISE Central Hub and the RAISE Certified Nodes. These risks can lead to severe security vulnerabilities, data breaches, or complete system failures if not properly managed:

- **Physical damage to hardware:** It can occur due to natural disasters (such as floods, earthquakes, and fires), as well as due to human actions such as theft, vandalism, or accidental destruction. Damaged hardware can result in data loss, interruption of services, and costly downtime while repairs or replacements are made.
- **Hardware failures:** Hardware components can fail due to age, manufacturing defects, or poor maintenance. Common failures occur in hard drives, power supplies, and motherboards. Failures can lead to data loss or corruption, system outages, and significant operational disruption.
- **Supply chain attacks:** These occur when malicious modifications are made to hardware components at any point during the design, manufacture, or delivery process. Compromised components can introduce backdoors, allowing attackers to bypass traditional security measures and gain sustained access to enterprise networks.
- **Unauthorized access and theft:** Unauthorized physical access to hardware can lead to theft of devices or data and unauthorized or malicious modifications. Direct access to hardware can allow attackers to bypass network security measures, directly extract data, install malicious hardware like keyloggers, or physically remove devices for data extraction or ransom.
- **Electromagnetic interference and power surges:** Electromagnetic interference (EMI) can cause abnormal operation of IT equipment, while power surges can damage electronic components. These issues can lead to data errors, hardware malfunctions, and premature equipment failure.

Addressing hardware level risks requires a combination of physical security measures, rigorous maintenance routines, careful vendor selection, and strategic planning for hardware lifecycle management.

### 2.2 Operating System Level Risks

Operating System (OS) risks pertain to vulnerabilities and threats that specifically target the underlying software platform managing a computer's hardware resources and providing services for application programs. Since the operating system acts as a bridge between users and the computer's physical components, it is a prime target for various security threats:

- **Unpatched security vulnerabilities:** This involves known vulnerabilities in an operating system that have not been patched or updated. Such vulnerabilities can be exploited by attackers to gain unauthorized access or control over a system. Exploits can lead to data breaches, unauthorized data access, system downtime, and in severe cases, complete system takeover.
- **Configuration errors:** Misconfigurations or inadequate security settings in the operating system can leave the system open to attacks. Common errors include unnecessary services running on the system, open ports, improper permissions, and default settings not being

secured. Poorly configured systems are easier for attackers to exploit, facilitating unauthorized access and potential data loss.

- **Zero-day exploits:** These are previously unknown vulnerabilities in the operating system that have not yet been patched and are unknown to other security professionals. Attackers exploit these vulnerabilities to carry out their malicious intentions. Zero-day exploits are particularly dangerous because there is no prior knowledge of the threat, making detection and prevention difficult.
- **Malware and ransomware:** These are malicious software programs specifically designed to disrupt, damage, or gain unauthorized access to computer systems. Ransomware is a type of malware that encrypts a victim's files, with the attacker then demanding a ransom from the victim to restore access to the data. Malware can steal, delete, encrypt, or alter information; it can also hijack core computing functions and monitor users' computer activity without their permission.
- **Privilege escalation:** This occurs when an attacker gains elevated access to resources that are normally protected from an application or user. The process involves exploiting a bug, design flaw, or configuration oversight in an operating system to gain elevated access to resources. This allows attackers to perform unauthorized actions, such as executing commands, accessing restricted data, and creating accounts with full user rights.
- **Outdated operating systems:** This implies the use of operating systems that are no longer supported by vendors and do not receive security updates. Systems running outdated OS versions are susceptible to a wide range of attacks exploiting unpatched vulnerabilities.

Addressing operating system level risks involves a combination of technical solutions, rigorous processes, and ongoing vigilance.

### 2.3 Network Level Risks

Network level risks encompass a wide array of vulnerabilities and threats that target the infrastructure and protocols governing the communication between devices. As the backbone of an IT environment, the network is a critical asset that, if compromised, can lead to significant disruptions and data breaches:

- **Eavesdropping and interception:** This involves unauthorized listening or interception of network traffic. It can occur in both wired and wireless networks. Attackers might use packet sniffers or similar tools to capture data being transmitted over a network. Eavesdropping can lead to the theft of sensitive information, such as passwords, personal data, etc.
- **Man-in-the-Middle (MitM) attacks:** An attacker secretly intercepts and possibly alters the communication between two parties who believe they are directly communicating with each other. MitM attacks can lead to the interception of sensitive information, session hijacking, and data tampering.
- **Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks:** These are malicious attempts to disrupt the normal functioning of a targeted network by overwhelming the target or its surrounding infrastructure with a flood of Internet traffic. A DoS attack focuses on making a service such as a website unusable by bombarding it with an overwhelming amount of traffic from a single location, or by exploiting a vulnerability to make the server crash. Similarly, DDoS attacks use a multitude of compromised computer systems as sources of attack traffic. Exploited machines can include computers and other networked resources such as IoT devices. As previously indicated, DoS and DDoS can be achieved through various means: 1) **Volume-based attacks:** This involves overwhelming the target with massive amounts of traffic to exhaust the bandwidth; 2) **Protocol attacks:** These attacks consume actual server resources or those of intermediate communication equipment, such as firewalls and load balancers, by exploiting weaknesses in communication protocols; 3) **Application layer attacks:** These are sophisticated attacks that target specific aspects of an

application or server to disrupt service. They require fewer resources than other attacks and are harder to detect.

DoS and DDoS can result in significant downtime, disrupting business operations and damaging system trust.

- **Unauthorized access:** This occurs when an unauthorized user gains access to the network resources. It can be facilitated through weak authentication, ineffective network segmentation, or the exploitation of network services and protocols. Unauthorized access can lead to data breaches, installation of malicious software, and operational disruptions.
- **ARP spoofing:** The Address Resolution Protocol (ARP) is a communication protocol used for discovering the MAC address associated with a given internet IP address. This mapping is a critical function in the Internet protocol suite. Spoofing is a technique whereby an attacker sends fake ARP messages over a local area network. This results in the linking of an attacker's MAC address with the IP address of a legitimate computer or server on the network. ARP spoofing can enable an attacker to intercept, modify, or stop data-in-transit, facilitate DoS attacks, or MitM exploits.
- **Configuration and implementation flaws:** Incorrect configuration or implementation of network devices and services can expose networks to attacks. Flaws such as open ports, unsecured network protocols, or misconfigured firewalls can be exploited to gain unauthorized access or to perform network reconnaissance.

Protecting against network level risks is critical for maintaining the confidentiality, integrity, and availability of data and services. Implementing a robust network security strategy involves a combination of strong technical controls, regular assessments, and continuous monitoring.

## 2.4 Application Level Risks

Application risks refer to vulnerabilities and threats that specifically target software applications, encompassing web applications, desktop applications, and mobile apps. These risks, mainly affecting the RAISE Central Portal and Services, can compromise data integrity, availability, and confidentiality, leading to significant security breaches and loss of trust:

- **Injection flaws:** These occur when an attacker sends untrusted data to an interpreter as part of a command or query. SQL injection, script injection, and command injection are common examples where malicious scripts are injected into otherwise benign and trusted applications. Attackers can use these flaws to bypass authentication, access, modify, or delete data, or execute malicious commands on the server.
- **Broken authentication:** Applications that improperly implement authentication and session management functions may inadvertently allow attackers to compromise passwords, keys, or session tokens, or exploit other implementation flaws to assume other users' identities. Such vulnerabilities can lead to unauthorized access to multiple user accounts, data breaches, and identity theft.
- **Data exposure:** Improper protection of data can lead to its exposure either at rest or in transit. Exposure of sensitive data can result in significant compliance issues, financial loss, and damage to reputation due to loss of user trust.
- **Broken access control:** Restrictions on what authenticated users are allowed to do are often not properly enforced. Attackers can exploit these flaws to access unauthorized functionality and/or data, such as accessing other users' accounts, viewing sensitive files, and modifying other users' data. This can lead to unauthorized information disclosure, modification, or destruction of all data, or performing a business function outside of the user's limits.
- **Security misconfiguration:** This risk covers a wide range of issues due to incorrect security configurations. Common misconfigurations include verbose error messages containing sensitive information, improperly configured HTTP headers, and open cloud storage.



Misconfigurations can make system data vulnerable to unauthorized access and exploitation, facilitating further attacks.

- Cross-Site Scripting (XSS): XSS flaws occur whenever an application includes untrusted data in a new web page without proper validation or escaping, or updates an existing web page with user-supplied data using a browser API that can create HTML or JavaScript. XSS allows attackers to execute scripts in the victim's browser which can hijack user sessions, deface web sites, or redirect the user to malicious sites.
- Insecure deserialization: It occurs when untrusted data is used to abuse the logic of an application, inflict a denial of service (DoS) attack, or execute arbitrary code when the data is deserialized by an application. Even if deserialization flaws do not result in remote code execution, they can be used to perform attacks, including replay attacks, injection attacks, and privilege escalation attacks.

In this context, the Open Web Application Security Project (OWASP), a non-profit foundation that works to improve the security of software, publishes a list of the most critical web application security risks. The OWASP Top 10, as it is known, updates every few years based on the evolving threat landscape and serves multiple purposes: 1) a basic guide for developers and security professionals to ensure the security of the software they develop and deploy; 2) a foundation for developing secure coding practices and methodologies; 3) a reference for organizations to prioritize security risks and incorporate security from the early phases of software development. The most recent version of the OWASP Top 10 list was updated in 2021, and consists of [7]:

- A01:2021-Broken Access Control: Failures of access policies and permissions typically lead to unauthorized information disclosure, modification, or destruction of all data or performing a business function outside the user's limits.
- A02:2021-Cryptographic Failures: They compromise the protection needs of data in transit and at rest, and often lead to sensitive data exposure or system exposure.
- A03:2021-Injection: Attackers exploit vulnerabilities to inject malicious code, usually via user input, which is then executed by the application's interpreter.
- A04:2021-Insecure Design: It focuses on risks related to design and architectural flaws, with a call for more use of threat modeling, secure design patterns, and reference architectures.
- A05:2021-Security Misconfiguration includes vulnerabilities like missing appropriate security hardening across any part of the application stack or improperly configured permissions on cloud services; unnecessary features are enabled or installed; default accounts and their passwords are still enabled and unchanged; error handling reveals stack traces or other overly informative error messages to users, etc.
- A06:2021-Vulnerable and Outdated Components: It refers to using outdated or vulnerable third-party components, which can be exploited to compromise the application. This includes the OS, web / application server, database management system (DBMS), applications, APIs and all components, runtime environments, and libraries.
- A07:2021-Identification and Authentication Failures: Confirmation of the user's identity, authentication, and session management is critical to protect against authentication-related attacks.
- A08:2021-Software and Data Integrity Failures: It focuses on making assumptions related to software updates, critical data, and CI/CD pipelines without verifying integrity.
- A09:2021-Security Logging and Monitoring Failures: This category is to help detect, escalate, and respond to active breaches. Failures of logging and monitoring directly impact visibility, incident alerting, and forensics.
- A10:2021-Server-Side Request Forgery: SSRF flaws occur whenever a web application is fetching a remote resource without validating the user-supplied URL. It allows an attacker to coerce the application to send a crafted request to an unexpected destination, even when protected by a firewall, VPN, or another type of network access control.

Application level risks can be addressed through a combination of proactive prevention, timely detection, and rapid response strategies.



## 2.5 User Level Risks

User level risks encompass vulnerabilities and security threats that are directly related to user actions or behavior. These risks can arise from either inadvertent errors or deliberate actions by users that compromise the security of systems and data. Addressing user level risks is critical because even the most robust technical defenses may be undermined by a single user's mistake or malicious activity. Common types of user level risks include:

- **Phishing attacks:** Phishing involves deceiving users into providing sensitive information such as usernames and passwords by masquerading as a trustworthy entity in electronic communications. Successful phishing can lead to unauthorized access, data breaches, and identity theft.
- **Poor password practices:** Users may employ weak passwords, reuse passwords across multiple accounts, or share passwords with others, all of which weaken security. Easy-to-guess or compromised passwords are a common entry point for attackers seeking unauthorized access.
- **Social engineering:** Manipulative techniques that trick users into breaking security protocols to gain sensitive information or access to systems. Through social engineering, attackers can circumvent traditional security measures by exploiting human psychology rather than technical hacking techniques.
- **Accidental data exposure:** Users may accidentally misconfigure privacy settings, or leave sensitive information exposed to unauthorized parties. Such accidents can lead to data breaches, compliance violations, and loss of trust.

User level risks are particularly challenging to manage because they involve the human element, which is unpredictable and can be manipulated or prone to error. To effectively reduce these risks, a comprehensive approach that includes technology solutions, strict policies and procedures, and ongoing user education and awareness training must be implemented.

### 3 Regulatory Compliance and Standards

#### 3.1 EU Laws and Legislations

The European Union (EU) has several significant legislations and regulations pertaining to security and data protection, aimed at safeguarding individuals' rights and privacy. They set a high standard for global data protection practices and aim to create a safer and more accountable digital environment, while also addressing the challenges posed by the rapidly evolving digital landscape [9]. The following sections present the main of these laws and directives in order to signify the current strategy and policies within the EU. In general, they have a wider scope and fields of application, with the General Data Protection Regulation (GDPR) being the most pertinent to the RAISE system.

##### 3.1.1 General Data Protection Regulation (GDPR)

The General Data Protection Regulation (GDPR) is a comprehensive data protection law that came into effect in the European Union (EU) in 2018. It represents one of the most significant elements of legislation affecting personal data protection and privacy, impacting organizations worldwide that handle or process the personal data of EU residents [10].

GDPR was designed to harmonize data privacy laws across Europe, protect EU citizens' data privacy, and reshape the way organizations across the region approach data privacy. It applies to all organizations operating within the EU and to organizations outside the EU that offer goods or services to individuals in the EU.

The GDPR is built around several key principles that govern the processing of personal data:

- **Lawfulness, Fairness, and Transparency:** Processing must be lawful, fair, and transparent to the data subject.
- **Purpose Limitation:** Data collected for specified, explicit, and legitimate purposes must not be used in any way that's incompatible with those purposes.
- **Data Minimization:** Organizations should only process the personal data that is necessary to achieve its processing purposes.
- **Accuracy:** Personal data must be accurate and kept up to date.
- **Storage Limitation:** Personal data should be kept in a form that permits identification of data subjects for no longer than necessary for the purposes for which the personal data are processed.
- **Integrity and Confidentiality:** Personal data must be processed in a way that ensures appropriate security, including protection against unauthorized or unlawful processing and against accidental loss, destruction, or damage.

GDPR grants several important rights to EU residents to control their personal data, including:

- **Right to Access:** Individuals have the right to know what personal data is being processed and how.
- **Right to Rectification:** Individuals can have incorrect personal data corrected.
- **Right to Erasure (Right to be Forgotten):** Under certain conditions, individuals can request the deletion of their personal data.
- **Right to Restrict Processing:** Individuals can request that their data's processing be restricted.
- **Right to Data Portability:** Individuals can obtain and reuse their personal data for their own purposes across different services.
- **Right to Object:** Individuals have the right to object to the processing of their personal data in certain circumstances, including direct marketing.

- **Rights in relation to automated decision making and profiling:** Individuals have the right to not be subject to a decision based solely on automated processing.

GDPR encourages the integration of data protection from the onset of the designing of systems, rather than as an addition. Failure to comply with the GDPR can result in significant penalties, including fines of up to €20 million or 4% of the worldwide annual revenue of the prior financial year, whichever is higher. The GDPR has set a global benchmark for data protection and privacy, influencing many countries outside the EU to reconsider and tighten their own data protection laws.

### 3.1.2 Network and Information Security Directive (NIS Directive)

The NIS Directive [11] establishes security requirements for operators of essential services (e.g., energy, transportation, healthcare) and digital service providers. It aims to improve the overall cybersecurity posture of critical infrastructures and digital services across the EU. The NIS Directive includes several key provisions aimed at ensuring robust cybersecurity:

#### 1. National Frameworks

- **National NIS Strategies:** Each member state must develop a national strategy for the security of network and information systems, outlining strategic objectives and appropriate policy and regulatory measures.
- **National Competent Authorities (NCAs):** Member states are required to designate one or more national authorities responsible for managing network and information security.
- **Computer Security Incident Response Teams (CSIRTs):** Member states must establish CSIRTs to handle incidents and risks, cooperate and exchange information about risks.

#### 2. Security and Notification Requirements

- **Operators of Essential Services (OES):** Entities in sectors like energy, transport, banking, health, and water supply must take appropriate security measures and notify serious incidents to the relevant national authority.
- **Digital Service Providers (DSPs):** Includes providers of online marketplaces, cloud computing services, and search engines. DSPs are required to take measures to manage the risks posed to their network and information systems and to notify significant incidents to the competent authority.

#### 3. Cross-border Collaboration

- The directive establishes a Cooperation Group to support and facilitate strategic cooperation and the exchange of information among member states. This group also assists member states in building capacity and supports the development of trust and confidence.
- The Network of CSIRTs aims to promote swift and effective operational cooperation on specific network and information system security incidents and sharing information about risks.

In December 2020, the European Commission proposed a revision of the NIS Directive, known as the NIS 2 Directive, to address the evolving landscape of cybersecurity threats and to cover more sectors [12]. The NIS 2 Directive aims to harmonize and increase cybersecurity measures further, enforce stricter supervisory measures, stricter enforcement requirements, and enhance information sharing amongst member states. It was adopted by the European Parliament and the Council in 2022, with member states required to transpose it into national law by October 2024.

The NIS 2 Directive introduces several key enhancements and changes:

1. **Broader Scope:** NIS 2 significantly expands the range of sectors covered by the directive, now including public administration and sectors that rely heavily on ICT, such as waste

management, food, manufacturing, digital infrastructure, and space. This expansion reflects the increasing digitalization of various sectors and the consequent cyber risks.

2. **Mandatory Risk Management Measures:** The directive mandates entities to implement specific technical and organizational measures, including risk analysis, incident handling, business continuity and crisis management, supply chain security, vulnerability handling and disclosure, and policies to assess the effectiveness of cybersecurity risk management measures.
3. **Enhanced Reporting Obligations:** Entities are required to notify relevant authorities of significant cybersecurity incidents within 24 hours of becoming aware of them, followed by a more detailed report later. This rapid reporting aims to ensure that risks are managed effectively across the EU.
4. **Stricter Supervisory Measures:** The directive provides for stricter supervisory measures for national authorities, enhanced enforcement requirements, and aims to harmonize sanctions across member states, setting a framework for how penalties should be determined.
5. **Increased Information Sharing:** There is a strong emphasis on improving information sharing between authorities and across different sectors. This includes sharing information on incidents, risks, and best practices to enhance collective understanding and response to cybersecurity challenges.
6. **Cybersecurity Requirements for Medium and Large Companies:** While the original NIS Directive focused on Operators of Essential Services (OES) and Digital Service Providers (DSPs), NIS 2 applies to all medium and large companies in the specified sectors, increasing the number of businesses that need to comply with stringent cybersecurity practices.

The NIS 2 Directive encourages the use of European cybersecurity certification schemes as proof of compliance with cybersecurity requirements, promoting the use of common standards and practices across the EU.

### 3.1.3 ePrivacy Directive and ePrivacy Regulation

The ePrivacy Directive and the evolving ePrivacy Regulation [13] focus specifically on the privacy of users engaged with electronic communication services, addressing issues such as confidentiality, cookies, email marketing, and the processing of traffic and location data.

Officially known as the "Directive concerning the processing of personal data and the protection of privacy in the electronic communications sector," the ePrivacy Directive was adopted in 2002 and updated by Directive 2009/136/EC. It supplements the general data protection regime and specifically addresses privacy in the electronic communications sector:

- **Confidentiality of Communications:** The directive mandates the confidentiality of communications and related traffic data by service providers.
- **Traffic and Location Data:** It regulates the processing of traffic and location data beyond what is necessary for the transmission of communication or billing.
- **Cookie Usage:** The directive introduced specific rules regarding the use of cookies and similar technologies. Websites must obtain prior informed consent from users before placing cookies on their devices, except for cookies strictly necessary for the delivery of a service explicitly requested by the user.
- **Unsolicited Marketing:** The ePrivacy Directive restricts direct marketing practices via electronic communications (e.g., emails, SMS) and requires prior consent for such communications, except under certain conditions where a contact exists, and the contact details were obtained in the context of a sale.

To address the challenges posed by new technological developments and to align with the General Data Protection Regulation (GDPR), the European Commission proposed replacing the ePrivacy Directive with a new ePrivacy Regulation. Initially proposed in 2017, the regulation is intended to

provide a more harmonized framework for privacy in electronic communications across the EU. The ePrivacy Regulation has not yet been finalized, with ongoing negotiations among EU institutions. According to the EU Commission, the proposal includes the following key changes:

- **Wider Scope:** The regulation aims to apply not only to traditional telecom service providers but also to providers of electronic communications services such as WhatsApp, Facebook Messenger, Skype, and others that offer VoIP, messaging, and email services.
- **Simpler Rules on Cookies:** The regulation seeks to simplify the rules on cookies, reducing the burden on users to manage consent for cookies that are less intrusive and pose little risk to privacy, such as those used for web analytics.
- **Stronger Rules for Electronic Marketing:** It proposes stricter requirements for electronic marketing, including clearer consent mechanisms and strengthened rules for telemarketing calls, including requirements for caller line identification.
- **Protection of Terminal Equipment Information:** The regulation is intended to broaden the requirement for consent not only for storing information but also for accessing information stored in users' terminal equipment.
- **More Effective Enforcement:** Consistent with GDPR, the proposed regulation suggests significant financial penalties for non-compliance, aligning the enforcement mechanisms with those under the GDPR.

### 3.1.4 Digital Services Act (DSA) and Digital Markets Act (DMA)

The Digital Services Act (DSA) and Digital Markets Act (DMA) aim to create a safer digital space where the fundamental rights of all users of digital services are protected, and to establish a level playing field for businesses operating in the digital marketplace [14]. These regulations reflect the EU's efforts to adapt its regulatory framework to the realities of the modern digital economy and society.

Adopted in 2022, the Digital Services Act aims to modernize the legal framework for digital services across the EU by amending the e-Commerce Directive, which had been in place since 2000. The DSA addresses issues related to the responsibilities of digital services that act as intermediaries in their role of connecting consumers with goods, services, and content. Its key provisions include:

- **Transparency Requirements:** The DSA requires online platforms, particularly very large platforms (VLPs), to disclose how their algorithms work, which should help address issues related to transparency in content moderation, advertising, and the functioning of services.
- **Accountability Measures:** It mandates regular independent audits of risk management systems, particularly for VLPs, to ensure compliance with DSA obligations.
- **Enhanced Consumer Safeguards:** The act includes measures to protect consumers from illegal content, goods, and services, and it ensures that users can flag such content easily.
- **Addressing Disinformation:** It compels platforms to take steps to mitigate the spread of disinformation while respecting fundamental rights like freedom of expression.
- **Protections Against Illegal Content:** Platforms are required to swiftly take down illegal content while safeguarding the rights to free expression and due process.
- **Crisis Response Mechanism:** It introduces a crisis response mechanism that platforms need to follow to address the dissemination of misinformation during significant societal events.

Adopted alongside the DSA, the Digital Markets Act focuses on controlling the market power of large online platforms, referred to as "gatekeepers," which serve as critical infrastructure in the digital market. The DMA aims to prevent these gatekeepers from imposing unfair conditions on businesses and consumers, thereby ensuring fair and open digital markets. Its key provisions include:



- **Designation of Gatekeepers:** Platforms qualify as gatekeepers based on specific criteria related to their size, user scope, and market impact. These include companies providing core platform services such as search engines, social networking, and online intermediation services.
- **Prohibited Practices:** The DMA sets out a list of obligations and prohibitions for gatekeepers, including a ban on preferential treatment of their own services over those of competitors on their platforms.
- **Mandatory Data Sharing:** It requires gatekeepers to allow third parties to interoperate with their services in certain situations and mandates sharing of data generated on their platforms with business users.
- **Right to Uninstall:** Users must have the ability to uninstall any software applications that are pre-installed by a gatekeeper.
- **Pro-competitive Measures:** Gatekeepers are prohibited from engaging in practices that close off markets to new entrants or disadvantage rival businesses, such as using data collected on their platforms to compete unfairly with business users.

### 3.1.5 Cybersecurity Act

The Cybersecurity Act, officially enacted in 2019, represents a significant milestone in enhancing cybersecurity across the EU [15]. The act strengthens the EU's cybersecurity framework, primarily by establishing a comprehensive certification framework for ICT products, services, and processes, and by bolstering the role and capabilities of the European Union Agency for Cybersecurity (ENISA). Thus, the main objectives of the Cybersecurity Act are to:

1. **Boost Overall Cybersecurity in the EU:** The act aims to increase trust and security in digital products and services across the internal market by establishing a common cybersecurity certification framework. The framework aims to ensure that certified products, services, and processes sold in EU countries meet consistent and high-level cybersecurity standards. While the certification is voluntary, obtaining certification can serve as a key differentiator and trust mark for ICT products in the European market. The framework categorizes certifications into three levels of assurance – basic, substantial, and high – depending on the level of risk associated with the ICT product's intended use. Each level assesses the resilience of the product against cybersecurity incidents:
  - Basic: Provides a limited degree of confidence in the claimed or asserted cybersecurity qualities of the product.
  - Substantial: Provides a substantial degree of confidence in the claimed cybersecurity qualities, suitable for products facing more serious cybersecurity risks.
  - High: Provides a high degree of confidence, necessary for products that could endanger people's safety or security if compromised.

By creating a unified framework, the Cybersecurity Act aims to prevent fragmentation in the internal market where different countries might have different certification standards for cybersecurity.

2. **Strengthen ENISA:** Unlike its previous temporary mandates, ENISA now has a permanent status, ensuring its continued operation and support within the EU cybersecurity ecosystem. Furthermore, ENISA's role is expanded to include a greater involvement in research, better coordination with national cybersecurity agencies, and more direct involvement in policy development. ENISA is tasked with preparing the technical groundwork for specific certification schemes and assisting the European Commission and member states in the matter of cybersecurity certification of products, services, and processes.

### 3.2 Industry Security Standards

Implementing industry standards and employing specific techniques is critical to establishing a strong foundation for security and data protection in various domains. Their effective application addresses specific security challenges, reduces risks, and fosters a secure and trusted digital environment. The following sections present the main of these standards in order to provide a reference of good practices and processes (see also the subsequent Sections 4 and 5), especially from fields like the financial and health markets (they were some of the first to become digital and consider the handling of sensitive information). Overall, they have scope at the organizational level of an entity, applicable more at the case of a future exploitation of the RAISE system.

#### 3.2.1 ISO/IEC 27001 - Information Security Management System (ISMS)

The ISO/IEC 27001 [16] is a globally recognized standard for the establishment, implementation, maintenance, and continuous improvement of an Information Security Management System (ISMS). It is part of the ISO/IEC 27000 family of standards which are designed to help organizations secure their information assets.

ISO/IEC 27001 specifies a management system that is intended to bring information security under explicit management control. Its primary objective is to help organizations establish and maintain an effective structure to manage their information security. This includes protecting information from unauthorized access, ensuring confidentiality, integrity, and availability of data, and enabling the secure operation of business processes. The key components of ISO/IEC 27001 consist of:

- **Context of the Organization:** This involves understanding the external and internal factors that can impact the security of information, including legal, regulatory, and contractual requirements. It requires defining the scope of the ISMS, which includes identifying stakeholders and their requirements related to information security.
- **Leadership:** Top management must demonstrate leadership and commitment to the ISMS, ensuring that the security policy and security objectives are established and are compatible with the strategic direction of the organization. They must also assign roles and responsibilities for information security throughout the organization.
- **Planning:** This includes identifying, analyzing, and planning to treat information security risks. It requires the organization to establish information security objectives that are measurable and consistent with the information security policy.
- **Support:** The standard requires the organization to provide adequate resources for the ISMS, ensure competent personnel, raise awareness about information security, and manage documented information (policies, procedures, records).
- **Operation:** This involves executing the processes as planned. It includes managing and assessing information security risks, and implementing risk treatment plans to ensure that the information security controls achieve the intended outcomes.
- **Performance Evaluation:** The organization needs to monitor, measure, analyze, and evaluate the information security performance. This often involves regular ISMS audits and reviews of the ISMS by top management to ensure its continuing suitability, adequacy, and effectiveness.
- **Improvement:** ISO/IEC 27001 emphasizes continual improvement of the ISMS. The organization should continually improve the suitability, adequacy, and effectiveness of the ISMS based on the outcomes of audits, reviews, and monitoring of security incidents.
- **Continual Assessment:** Once certified, the organization must undergo regular audits to ensure continual compliance and improvement of the ISMS.

Implementing ISO/IEC 27001 helps organizations manage their information security processes in line with international best practices, thus ensuring the protection of data, building trust with stakeholders, and enhancing the organization's reputation.

### 3.2.2 ISO/IEC 29100 - Privacy Framework

The ISO/IEC 29100 [17] is an international standard, which provides a framework for protecting personal information and ensuring that privacy is maintained in information and communication technology (ICT) environments. This standard was first published in 2011 and serves as a guidance document rather than a certifiable standard like ISO/IEC 27001. The primary objectives of ISO/IEC 29100 are to:

- Provide a privacy framework which specifies a common privacy terminology and defines the actors and their roles in processing personally identifiable information (PII).
- Provide a framework for implementing measures to protect PII in line with privacy principles that are common across countries and organizations.
- Assist organizations in specifying and implementing privacy controls through privacy management within the context of their risk environment.

The standard outlines a set of privacy principles upon which the privacy framework is built. These principles include:

- **Consent and Choice:** Ensuring that PII principals are informed about the collection, use, disclosure, and retention of their PII and have given consent where necessary.
- **Purpose Legitimacy and Specification:** Collecting and processing PII should be for explicit and legitimate purposes, with such purposes specified to the PII principals.
- **Collection Limitation:** Limiting the collection of PII to what is directly relevant and necessary to accomplish the specified purpose.
- **Data Minimization:** Ensuring that PII is adequate, relevant, and not excessive relative to the specified purposes.
- **Use, Retention, and Disclosure Limitation:** PII should not be used, retained, or disclosed for purposes other than those for which it was collected, except with the consent of the PII principal or by the authority of law.
- **Accuracy and Quality:** Maintaining accuracy, completeness, and quality of the PII.
- **Openness, Transparency, and Notice:** Providing PII principals with clear, transparent, and easily accessible information about how their PII is processed and how to comply with applicable privacy laws and regulations.
- **Individual Participation and Access:** Allowing PII principals to access their PII and to correct or delete it if it is inaccurate or processed against these principles.
- **Accountability:** Organizations should be accountable for compliance with these privacy principles and be able to demonstrate such compliance to the relevant authorities.

ISO/IEC 29100 suggests privacy controls in various areas such as consent management, data quality and minimization, and the anonymization of PII. These controls are meant to guide organizations in implementing measures that uphold the privacy of individuals whose PII they process. In addition, the standard emphasizes the need for privacy safeguards across all stages of PII processing. This includes administrative, technical, and physical safeguards to protect PII from unauthorized access, use, disclosure, disruption, modification, or destruction.

ISO/IEC 29100 is applicable to all types and sizes of organizations, including public and private companies, government entities, and not-for-profit organizations, which process PII. It is especially useful for organizations acting as PII controllers or processors and provides guidance on integrating privacy controls into their information security management.

### 3.2.3 NIST Cybersecurity Framework

The National Institute of Standards and Technology (NIST) Cybersecurity Framework is primarily intended for critical infrastructure organizations to manage and mitigate cybersecurity risk based on



existing standards, guidelines, and practices. However, since its first publication in 2014, it has been widely adopted by many types of organizations across sectors due to its flexibility and adaptability.

The primary objective of the NIST Cybersecurity Framework is to provide organizations with a structured and flexible approach to managing cybersecurity risks. The framework aims to help organizations:

- Understand their cybersecurity risks concerning cybersecurity threats.
- Implement a comprehensive approach to reduce cybersecurity risks.
- Communicate internally and externally about their cybersecurity status.

The core of the NIST Cybersecurity Framework is built around five concurrent and continuous functions: Identify, Protect, Detect, Respond, and Recover. These functions provide a high-level, strategic view of the lifecycle of an organization's management of cybersecurity risk and form the backbone of the framework.

- **Identify:** Develop an organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities. This function helps an organization to understand and manage cybersecurity risks to its systems, people, assets, data, and capabilities.
- **Protect:** Develop and implement appropriate safeguards to ensure delivery of critical infrastructure services. This function supports the ability to limit or contain the impact of a potential cybersecurity event.
- **Detect:** Develop and implement appropriate activities to identify the occurrence of a cybersecurity event. This function enables timely discovery of cybersecurity events.
- **Respond:** Develop and implement appropriate activities to take action regarding a detected cybersecurity incident. This function supports the ability to contain the impact of a potential cybersecurity incident.
- **Recover:** Develop and implement appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident. This function supports timely recovery to normal operations to reduce the impact from a cybersecurity incident.

The Framework tiers ("Partial", "Risk Informed", "Repeatable", and "Adaptive") help organizations by providing context on how they view cybersecurity risk management. Tiers describe the degree to which an organization's cybersecurity risk management practices exhibit the characteristics defined in the framework (e.g., risk and threat aware, repeatable, and adaptive).

In addition, profiles are customizations of the Framework core by aligning the Functions, Categories, and Subcategories with the business requirements, risk tolerance, and resources of the organization. They help to establish a roadmap for improving cybersecurity, from a current state to a target state which considers legal and technological changes.

The NIST Cybersecurity Framework offers organizations numerous benefits, including:

- Enhanced understanding of cybersecurity risks.
- Improved cybersecurity posture and risk management.
- Better compliance with existing laws and regulations.
- Improved communication about cybersecurity and risk management with internal and external stakeholders.

In 2024, the National Institute of Standards and Technology released an updated version of the Cybersecurity Framework, known as NIST Cybersecurity Framework (CSF) 2.0. The NIST CSF 2.0 retains the core structure of the original but incorporates updates and enhancements to address the changing cybersecurity landscape, feedback from stakeholders, and advances in best practices. The

framework is applicable to organizations of all sizes and sectors, providing a flexible and scalable approach to managing cybersecurity risks [18].

### 3.2.4 PCI DSS - Payment Card Industry Data Security Standard

The Payment Card Industry Data Security Standard (PCI DSS) is a globally recognized set of security standards designed to ensure that all companies that accept, process, store, or transmit credit card information maintain a secure environment [19]. The PCI DSS is mandated by the major credit card brands but administered by the Payment Card Industry Security Standards Council (PCI SSC), which was launched in 2006, to manage the ongoing evolution of the Payment Card Industry (PCI) security standards with a focus on improving payment account security throughout the transaction process.

The primary objective of PCI DSS is to reduce the risk of debit and credit card data loss by driving businesses to adopt the highest standards of security. By adhering to the PCI DSS, businesses protect sensitive cardholder data and minimize the likelihood of experiencing card payment security issues.

PCI DSS requirements are organized around six control objectives that correspond to twelve core requirements:

#### 1. Build and Maintain a Secure Network and Systems

- Requirement 1: Install and maintain a firewall configuration to protect cardholder data.
- Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters.

#### 2. Protect Cardholder Data

- Requirement 3: Protect stored cardholder data.
- Requirement 4: Encrypt transmission of cardholder data across open, public networks.

#### 3. Maintain a Vulnerability Management Program

- Requirement 5: Protect all systems against malware and regularly update antivirus software or programs.
- Requirement 6: Develop and maintain secure systems and applications.

#### 4. Implement Strong Access Control Measures

- Requirement 7: Restrict access to cardholder data by business need to know.
- Requirement 8: Identify and authenticate access to system components.
- Requirement 9: Restrict physical access to cardholder data.

#### 5. Regularly Monitor and Test Networks

- Requirement 10: Track and monitor all access to network resources and cardholder data.
- Requirement 11: Regularly test security systems and processes.

#### 6. Maintain an Information Security Policy

- Requirement 12: Maintain a policy that addresses information security for all personnel.

Compliance with PCI DSS is enforced by the major credit card brands and is mandatory for all organizations that handle branded credit cards from the major card issuers. The standard applies to all entities that store, process, or transmit cardholder data or sensitive authentication data, including merchants, processors, acquirers, issuers, and service providers.

### 3.2.5 HIPAA - Health Insurance Portability and Accountability Act

The Health Insurance Portability and Accountability Act (HIPAA) is a significant piece of legislation in the United States that was enacted in 1996 [20]. It primarily aims to provide protection for patients' privacy and personal health information and to establish standardized mechanisms for electronic data interchange in healthcare. HIPAA has evolved over the years through subsequent amendments and regulations, notably through the Privacy Rule and the Security Rule, which specifically address the confidentiality and security of health information.

HIPAA was established with multiple goals in mind:

1. **Improve the portability and continuity of health insurance coverage** in the group and individual markets.
2. **Combat waste, fraud, and abuse** in health insurance and healthcare delivery.
3. **Promote the use of medical savings accounts** by introducing tax breaks and other incentives.
4. **Improve access to long-term care services and coverage.**
5. **Simplify the administration of health insurance** through the establishment of standards and requirements for the electronic transmission of certain health information.

HIPAA's regulations are divided into several major rules, each addressing different aspects of healthcare information protection:

- **Privacy Rule:** To safeguard the privacy of individual identifiable health information, known as Protected Health Information (PHI). It applies to health plans, healthcare clearinghouses, and healthcare providers who conduct certain financial and administrative transactions electronically. It requires appropriate safeguards to protect the privacy of PHI and sets limits and conditions on the uses and disclosures that may be made without patient authorization. It also grants patients' rights over their health information, including rights to examine and obtain a copy of their health records, and to request corrections.
- **Security Rule:** To set standards for protecting electronic protected health information (e-PHI). It applies to the same entities as the Privacy Rule and covers electronic health information that those entities create, receive, maintain, or transmit. It requires the implementation of three types of safeguards: administrative, physical, and technical. Entities must conduct risk assessments and implement appropriate security measures to mitigate risks. They must also ensure the confidentiality, integrity, and availability of e-PHI.
- **Enforcement Rule:** To outline the guidelines for investigations into HIPAA compliance violations, compliance reviews, and the procedures for hearings. It includes provisions relating to compliance and investigations, the imposition of civil money penalties for violations, and procedures for hearings.
- **Breach Notification Rule:** To require HIPAA-covered entities and their business associates to provide notification following a breach of unsecured PHI. It requires notifications to individuals, the Secretary of Health and Human Services (HHS), and, in certain circumstances, to the media. Notifications must be provided without unreasonable delay and in no case later than 60 days following the discovery of a breach.
- **Compliance:** HIPAA compliance is enforced by the Office for Civil Rights (OCR) within the U.S. Department of Health and Human Services (HHS). Compliance involves conducting regular risk assessments, implementing effective policies and procedures to safeguard health information, training employees on these policies and procedures, and maintaining proper documentation.

### 3.2.6 CIS Controls and Benchmarks

The Center for Internet Security (CIS) is a non-profit organization that works to safeguard private and public organizations against cyber threats. Founded in 2000, CIS provides a wide range of security benchmarks, resources, and services aimed at enhancing the overall security posture of the connected environment. The organization is widely recognized for its contribution to cyber defense through collaboration and the development of globally accepted and adopted security standards and best practices.

The CIS Controls [21] are a set of 18 actionable and prioritized best practices for cyber defence that provide specific ways to stop today's most pervasive and dangerous attacks. The CIS Controls are mapped to many compliance standards such as the GDPR, NIST, and ISO frameworks, and are divided into three distinct categories:

- **Basic:** Core controls which every organization should implement to ensure basic cybersecurity hygiene.
- **Foundational:** More technical and sophisticated controls that build on the basics to provide broader defence capabilities.
- **Organizational:** Controls that focus on people and processes involved in managing and protecting the information and systems.

The controls are practical and specific, unlike broader standards, making them a valuable resource for organizations looking to quickly improve their security posture. The latest version of the CIS Controls (Version 8) encourages a strategic approach to implementing security measures, emphasizing the importance of understanding the specific threats to an organization and aligning the security controls with those threats. This strategic alignment helps ensure that resources are focused on the most impactful security measures. CIS Controls Version 8 consist of the followings:

#### ***Basic Controls***

##### **1. Inventory and Control of Enterprise Assets:**

- An active management of all hardware devices on the network so that only authorized devices are given access and unauthorized and unmanaged devices are found and prevented from gaining access.

##### **2. Inventory and Control of Software Assets:**

- Automated inventory, tracking, and correction of all software on the network so that only authorized software is installed and can execute, and unauthorized and unmanaged software is found and prevented from installation or execution.

##### **3. Data Protection:**

- Processes and tools to properly manage sensitive data through its lifecycle, ensuring that data is protected from unauthorized access and handling while maintaining confidentiality and integrity.

##### **4. Secure Configuration of Enterprise Assets and Software:**

- Establishing and maintaining secure configurations for all enterprise assets and software, utilizing a rigorous configuration management and change control process to prevent attackers from exploiting vulnerable services and settings.

##### **5. Account Management:**

- Using processes and tools to create, manage, and control the use of enterprise accounts for various system and application access, ensuring that accounts are attributed to authorized users only.

##### **6. Access Control Management:**

- Implementation of processes and tools to assign privileges to users and accounts based on the principle of least privilege and using a secure configuration process.

### **Foundational Controls**

#### **7. Continuous Vulnerability Management:**

- The continuous acquisition, assessment, and action on new information in order to identify vulnerabilities, remediate, and minimize the window of opportunity for attackers.

#### **8. Audit Log Management:**

- The collection, management, and analysis of audit logs to help detect and understand a potential security incident and its impact.

#### **9. Email and Web Browser Protections:**

- Protection against threats that originate from emails and web browsers due to their frequent use as vectors for attackers.

#### **10. Malware Defenses:**

- Control and management of the installation, spread, and execution of malicious code at multiple points in the enterprise.

#### **11. Data Recovery:**

- Processes to ensure proper data backups so the organization can recover from data loss incidents, including storage, testing, and restoration practices.

#### **12. Network Infrastructure Management:**

- Establishment and maintenance of network devices to prevent attackers from exploiting vulnerable network services and settings.

#### **13. Network Monitoring and Defense:**

- The ability to monitor and defend enterprise networks using appropriate tools to detect and respond to anomalies in time.

### **Organizational Controls**

#### **14. Security Awareness and Skills Training:**

- Programs to train all enterprise users, including executives and managers, to understand their roles in maintaining safe cyberspace.

#### **15. Service Provider Management:**

- Processes to manage third-party service providers across the lifecycle to ensure that the third-party products and service providers do not introduce vulnerabilities or weaken the enterprise security posture.

#### **16. Application Software Security:**

- Managing the security lifecycle of all software used by the organization to prevent security vulnerabilities related to software development, deployment, upgrade, and maintenance.

#### **17. Incident Response Management:**

- Established and tested incident response infrastructure for discovering a potential cyber incident, containing the impact, eradicating the incident, and recovering from it.

#### **18. Penetration Testing:**

- Testing the effectiveness of the defenses by simulating real-world attacks that might circumvent existing security measures, identifying vulnerabilities, and learning how to better defend against such attacks.

Furthermore, the CIS Benchmarks [22] are a set of best practice security configuration guides that provide specific, actionable guidance for establishing a secure baseline configuration for various IT systems and applications. They are created through a unique consensus-based process involving a community of cybersecurity professionals and experts from various industries. Key features of the CIS Benchmarks include:

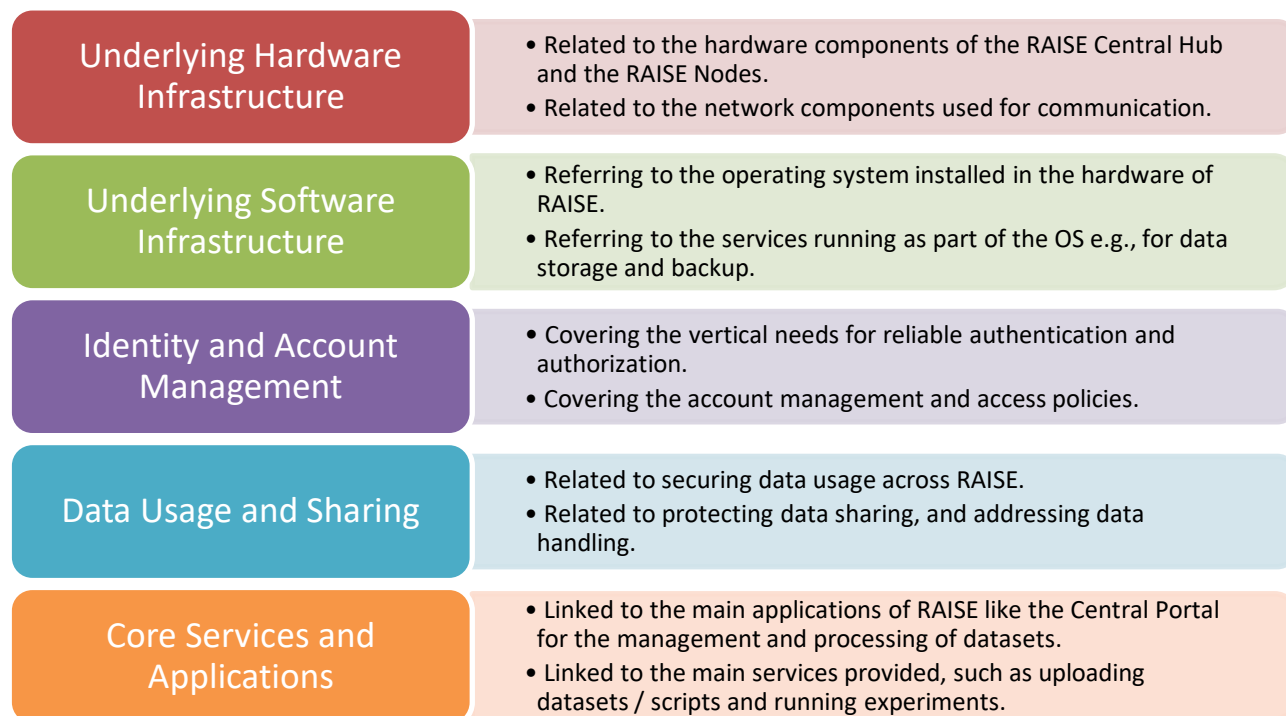
1. **Comprehensive Coverage:** CIS Benchmarks cover a wide range of operating systems, middleware, software applications, and network devices. This includes popular systems like Windows, Linux distributions, macOS, and cloud environments like AWS, Azure, and Google Cloud, as well as mobile operating systems like iOS and Android.
2. **Detailed Guidance:** Each benchmark provides detailed configuration settings that are intended to secure software and systems against known cybersecurity threats. The guidelines include instructions on how to harden operating systems, middleware, applications, and network equipment.
3. **Prioritized Recommendations:** The benchmarks often prioritize recommendations to help organizations focus on implementing the most critical security controls first. This approach helps in gradually enhancing the security posture effectively.
4. **Regular Updates:** CIS Benchmarks are regularly updated to reflect the latest security best practices, technological advancements, and emerging threats. This ensures that the benchmarks remain relevant and effective in a rapidly evolving cybersecurity landscape.
5. **Security Controls Mapping:** Many of the benchmarks include mappings to other standards and frameworks, such as NIST, ISO 27001, and the CIS Controls. This helps organizations that need to comply with multiple standards streamline their compliance efforts.
6. **Automation Support:** CIS provides automated assessment tools that help organizations assess their current configurations against CIS Benchmarks. Tools like the CIS-CAT (Configuration Assessment Tool) provide immediate feedback on compliance with the benchmarks.
7. **Cost-Effectiveness:** As open-source resources, CIS Benchmarks provide an economical solution for organizations seeking to enhance their security without significant investment in proprietary standards or frameworks.

CIS's comprehensive approach to enhancing cybersecurity, through the development and wide distribution of its standards and tools, supports a broad range of sectors including government, academia, and industry, making it a cornerstone of modern cybersecurity defence strategies.



## 4 RAISE Security Requirements

In order to formulate the security requirements and restrictions related to the different aspects of RAISE, a security control matrix (5 in total) was created for each major feature of the RAISE system.



**Figure 3: Overview of the RAISE Security Control Matrices**

The analysis was based on interviews with key stakeholders from the pilot partners; questionnaires to specific experts on the field; and a thorough examination of current standards, techniques and legislations.

**Table 1: Requirements of Underlying Hardware Infrastructure**

COM1 – Underlying Hardware Infrastructure	
<b>General description</b>	<p>Provide redundant infrastructure components that are located in secure housing facilities.</p> <p>Employ measures that protect from a wide range of physical threats, ensuring that the RAISE system's integrity and availability are maintained.</p> <p>Ensure secure and reliable network communication and traffic.</p>
<b>Security and control requirements</b>	
<b>COM1-RQ01</b>	All infrastructure shall be located in data centers / rooms with enhanced access controls to prevent unauthorized physical access to hardware.
<b>COM1-RQ02</b>	Data centers / rooms shall have environmental and power controls to protect hardware from damage.
<b>COM1-RQ03</b>	Employment of surveillance and monitoring systems to detect and record unauthorized access attempts.
<b>COM1-RQ04</b>	Scheduled maintenance and inspections to ensure hardware is operating efficiently and to pre-empt failures.

<b>COM1-RQ05</b>	Redundancy configurations such as RAID setups for data storage and dual power supplies to enhance system reliability.
<b>COM1-RQ06</b>	Fault tolerance measures to ensure system availability in the event of component failure.
<b>COM1-RQ07</b>	Regular updates and patches applied to firmware to protect against vulnerabilities.
<b>COM1-RQ08</b>	Employment of redundant communications links and network paths, with sufficient bandwidth.
<b>COM1-RQ09</b>	Implementation of secure networking equipment, efficiently configured to defend against network-based attacks.
<b>COM1-RQ10</b>	Utilization of Virtual Local Area Networks (VLANs) to logically isolate network traffic for different services.
<b>Success criteria and indicators</b>	
<b>COM1-SC01</b>	System availability is 99% over the measurement period of one month.
<b>COM1-SC02</b>	No security breaches in the employed data centers / rooms.
<b>COM1-SC03</b>	Easy recovery in case of failures in one or more nodes.
<b>COM1-SC04</b>	The system response times guarantee an undisturbed user experience and access to services.
<b>COM1-SC05</b>	All network traffic is secured and suspicious activities are efficiently detected. Protection services at network boundaries detect and mitigate sophisticated attacks.
<b>COM1-SC06</b>	Compliance with relevant standards (e.g., ISO/IEC 27001, NIST) for hardware security and management.

**Table 2: Requirements of Underlying Software Infrastructure**

<b>COM2 – Underlying Software Infrastructure</b>	
<b>General description</b>	<p>Provide a secure software base for the deployment and execution of the RAISE system and services.</p> <p>The RAISE nodes and central hub should employ a reliable Operating System with long term support and software modules that guarantee trustworthiness over time.</p> <p>The RAISE nodes and central hub should implement secure storage of data and files, as well as regularly scheduled backups.</p>
<b>Security and control requirements</b>	
<b>COM2-RQ01</b>	The Operating System shall be hardened following the known industry standards and guidelines.
<b>COM2-RQ02</b>	Only necessary Operating System components and services shall be enabled to minimize attack surfaces.



<b>COM2-RQ03</b>	The Operating System shall be updated and patched regularly to fix vulnerabilities.
<b>COM2-RQ04</b>	Application sandboxing shall be employed to isolate processes and prevent malicious code from affecting system operations.
<b>COM2-RQ05</b>	The principle of least privilege shall be enforced by ensuring that users and applications operate with the minimum level of access necessary.
<b>COM2-RQ06</b>	Administrative access shall be secured with multi-factor authentication and encrypted communication channels.
<b>COM2-RQ07</b>	Comprehensive logging of system and application activity shall be implemented to provide an audit trail for forensic analysis.
<b>COM2-RQ08</b>	Data and files in transit and in storage shall be encrypted using strong protocols.
<b>COM2-RQ09</b>	Real-time security monitoring tools shall be used to detect and respond to potential security incidents.
<b>COM2-RQ10</b>	The backup tool shall protect critical data and system configurations, and provide reliable restore procedures.
<b>Success criteria and indicators</b>	
<b>COM2-SC01</b>	The RAISE nodes and central hub are available and secure with the required technical stack and services.
<b>COM2-SC02</b>	Any security issue is promptly detected and mitigated.
<b>COM2-SC03</b>	Data are strongly encrypted and free from tampering / unauthorized access.
<b>COM2-SC04</b>	Tools are provided to securely access the node resources and deploy system code.
<b>COM2-SC05</b>	Databases are not accessible outside of the intranet (no possible direct external contact).
<b>COM2-SC06</b>	Quick recovery of operating system and applications in the event of failure.
<b>COM2-SC07</b>	Backups are performed following the scheduled program.
<b>COM2-SC08</b>	Compliance with relevant standards and regulations such as GDPR or CIS.

**Table 3: Requirements of Identity and Account Management**

<b>COM3 – Identity and Account Management</b>	
<b>General description</b>	<p>Provide secure identification, authentication and authorization system in line with standard security policies and best practices, in order to ensure the safety of the whole RAISE system.</p> <p>The system should support identity brokering, user federation for single sign-on, and fine-grained authorization policies.</p> <p>The following roles should be implemented: researcher, institute administrator, and system administrator.</p>

<b>Security and control requirements</b>	
<b>COM3-RQ01</b>	The account management system shall provide secure authentication. Passwords and other access authenticators are securely allocated, managed, stored, and transmitted.
<b>COM3-RQ02</b>	Every user shall have one identity. Shared accounts will not be used.
<b>COM3-RQ03</b>	Standard passwords rules: <ul style="list-style-type: none"> <li>• at least eight (8) characters in length,</li> <li>• at least two (2) complexity controls (uppercase letter, lowercase letter, special character),</li> <li>• change periodically,</li> <li>• without reuse of previous password</li> </ul>
<b>COM3-RQ04</b>	Users' accounts shall be locked out after a number of unsuccessful authentication attempts.
<b>COM3-RQ05</b>	The account management system shall support role-based authorization.
<b>COM3-RQ06</b>	All accounts must adhere to the principle of least privilege. The level of access to resources granted to a user account should be commensurate with the privileges required by the owner to perform the corresponding operations.
<b>COM3-RQ07</b>	Privileged user access is administered, approved, and controlled. Administrative responsibilities for user accounts, such as additions, deletions, and modifications, are assigned to the appropriate personnel.
<b>COM3-RQ08</b>	Only authorized users, devices, and processes can access the network and network services.
<b>COM3-RQ09</b>	Session terminations are configured and enforced based on defined thresholds (after a period of inactivity or upon meeting certain predefined conditions).
<b>COM3-RQ10</b>	The account management system shall track sign in counts, timestamps and IP addresses.
<b>Success criteria and indicators</b>	
<b>COM3-SC01</b>	Users can easily login and logout with no effort.
<b>COM3-SC02</b>	Account policies are always adhered to.
<b>COM3-SC03</b>	Access to systems and assets is controlled.
<b>COM3-SC04</b>	Data are continuously protected.
<b>COM3-SC05</b>	No breach was identified regarding the account policies and rules.

Table 4: Requirements of Data Usage and Sharing

## COM4 – Data Usage and Sharing

<b>General description</b>	<p>The RAISE system should promote and enhance confidence on the usage and sharing of datasets.</p> <p>It should include a structured approach to securing data usage and protecting sharing, addressing everything from the handling and classification of data to compliance with data protection laws.</p>
<b>Security and control requirements</b>	
<b>COM4-RQ01</b>	The RAISE system shall classify data accordingly and apply corresponding security controls.
<b>COM4-RQ02</b>	The system shall implement data handling policies that specify procedures for managing data throughout its lifecycle.
<b>COM4-RQ03</b>	Enforce strict access controls based on the principle of least privilege.
<b>COM4-RQ04</b>	Utilize role-based access control (RBAC) to ensure that data access is granted according to user roles and responsibilities.
<b>COM4-RQ05</b>	The system shall encrypt data at rest using strong encryption algorithms.
<b>COM4-RQ06</b>	The system shall encrypt data in transit using secure protocols to protect data integrity and confidentiality.
<b>COM4-RQ07</b>	Use data synthetic techniques where necessary to ensure that real data is not exposed.
<b>COM4-RQ08</b>	Establish a comprehensive auditing and monitoring framework to track data access and sharing activities.
<b>COM4-RQ09</b>	Use automated tools to detect and alert on unauthorized access or anomalous activities involving data.
<b>COM4-RQ10</b>	The system shall include formal data sharing procedures, ensuring that all data sharing complies with applicable legal, regulatory, and ethical standards.
<b>Success criteria and indicators</b>	
<b>COM4-SC01</b>	System users are satisfied with the access control mechanisms.
<b>COM4-SC02</b>	The available datasets in the RAISE system are continuously increased.
<b>COM4-SC03</b>	Minimum unauthorized access incidents are reported.
<b>COM4-SC04</b>	System users are satisfied with the transparency of the data usage and sharing practices.
<b>COM4-SC05</b>	Minimum inquiries and complaints regarding data privacy are reported.

Table 5: Requirements of Core Services and Applications

## COM5 – Core Services and Applications

<b>General description</b>	<p>The RAISE system should provide a rich set of features and services for the management and processing of datasets.</p> <p>It should allow users to securely upload datasets and scripts, run experiments according to their configurations, and access verified results on demand.</p>
<b>Security and control requirements</b>	
<b>COM5-RQ01</b>	The RAISE system shall implement strong authentication mechanisms for all users accessing its core services.
<b>COM5-RQ02</b>	The system shall enforce strict session management policies including session timeouts and secure cookie handling.
<b>COM5-RQ03</b>	Utilize Web Application Firewalls (WAFs) to protect applications from common threats.
<b>COM5-RQ04</b>	Ensure all applications are developed and tested according to OWASP Top 10 security risks mitigation guidelines.
<b>COM5-RQ05</b>	Ensure appropriate storage of data, including protection against unauthorized or unlawful processing and against accidental loss, destruction, or damage.
<b>COM5-RQ06</b>	The system shall employ blockchain technology in order to enhance the security and integrity of stored data.
<b>COM5-RQ07</b>	Use encryption to protect data in transit, employing strong protocols for all communications.
<b>COM5-RQ08</b>	Implement comprehensive logging and monitoring across all services and applications to detect and respond to security incidents.
<b>COM5-RQ09</b>	The system shall employ automated tools to perform code quality and security analysis on the uploaded processing scripts and algorithms.
<b>COM5-RQ10</b>	Automate patch management to ensure all applications and systems are up-to-date with the latest security patches.
<b>Success criteria and indicators</b>	
<b>COM5-SC01</b>	All identified security vulnerabilities are timely mitigated.
<b>COM5-SC02</b>	Reduction in mean time to detect and mean time to respond to security incidents year-over-year.
<b>COM5-SC03</b>	Core services and applications maintain performance benchmarks under varying loads.
<b>COM5-SC04</b>	User satisfaction scores consistently above 85% in regular feedback surveys regarding the usability of the RAISE system.
<b>COM5-SC05</b>	No incidents of data leakage, unauthorized data modification, or access breaches reported.

<b>COM5-SC06</b>	All services and applications comply with relevant standards such as GDPR, ISO/IEC 27001, and any applicable industry-specific regulations.
------------------	---------------------------------------------------------------------------------------------------------------------------------------------

## 5 RAISE Security Measures and Best Practices

Mitigating security risks across different levels of a system involves a combination of best practices, security measures, and adherence to industry standards. The analysis was based on a bottom-up approach, since security risks can manifest at various levels of a distributed system, from the hardware level to the user level.

### 5.1 Hardware Level

As previously indicated, the RAISE system includes multiple infrastructure components, like the RAISE Central Hub and the RAISE Certified Nodes, that are distributed and could be located in various geographical locations. These components require robust physical security measures in their housing facilities in order to prevent unauthorized access and ensure the integrity of the data they process and store. The following list presents a set of appropriate measures mainly for the RAISE Central Hub, and applicable as good practices for the RAISE Certified Nodes:

#### 1. Secure Location:

- Components should be housed in secure areas with controlled access to protect against unauthorized entry.
- Maintain a log of all access to facilities, including timestamps and personnel details.

#### 2. Environmental Controls:

- Employ facilities with climate control systems to maintain optimal operating temperatures and humidity levels to prevent equipment failure.
- Ensure the availability of fire suppression systems that are appropriate for electronic equipment (e.g., gas-based systems).

#### 3. Power Supply Security:

- Employ facilities with redundant power supplies, including uninterruptible power supplies (UPS) and backup generators, to ensure continuous operation.
- Regularly test backup systems to ensure they function properly in the event of a power failure.

#### 4. Physical Anti-Tamper Measures:

- Use locked server racks and cages to prevent unauthorized physical access to the hardware.
- Regularly update security protocols and systems based on the latest threat intelligence.

#### 5. Disaster Recovery Preparedness:

- Develop and regularly test a disaster recovery plan that includes provisions for physical disasters such as fires, floods, or earthquakes.

Implementing these physical security measures will significantly enhance the protection of the RAISE infrastructure against a wide range of physical threats, ensuring that the system's integrity and availability are maintained.

### 5.2 Operating System Level

Operating System (OS) security is critical in ensuring the overall security posture of any IT infrastructure, including the RAISE system. The aim is to leverage the built-in security features of the OS while also applying general security principles to enhance a system's resilience against threats. In the context of RAISE, an OS with Long Term Support (LTS) like the corresponding releases of the Ubuntu Server is recommended. Ubuntu Server LTS [28] is widely recognized for its

stability and extensive support cycle (up to 10 years), making it a preferred choice for environments where long-term reliability and security are crucial. Key security measures at the OS level include:

- **Operating System Hardening** - Operating system hardening involves configuring the OS securely, updating it regularly, and employing best practices to reduce vulnerabilities and attack surfaces:
  - Minimum Necessary Services: Only essential OS services and features are enabled to minimize potential entry points for attackers.
  - Patch Management: Regularly applying security patches and updates to address vulnerabilities. This includes not only the core OS updates but also updates for all installed software. In addition, features like the Unattended Upgrades package of Ubuntu ensure that important security patches are automatically downloaded and installed without needing any manual intervention from an end-user.
  - Secure Configurations: Configuring OS security settings according to industry best practices and security benchmarks, such as those provided by the Center for Internet Security (CIS).
  - Permission Settings: Ensuring that file and service permissions are restricted based on the principle of least privilege, where users and programs are given only those privileges which are essential to perform their intended function. In this context, AppArmor (Application Armor) is a Linux kernel module that helps system administrators restrict programs' capabilities with per-program profiles. Unlike traditional discretionary access control systems, which control access based on user permissions and object owners, AppArmor provides mandatory access control, confining programs to a limited set of resources defined by the security policy. AppArmor profiles are relatively easy to create and maintain. Profiles are written in a straightforward language and stored as simple text files. In addition to manually creating profiles, AppArmor includes a learning mode, which helps the generation of profiles by monitoring an application's activity and proposing rules.
- **Security Monitoring** - Continuous monitoring is vital to detect and respond to potential security incidents in real-time.
  - Log Management: Configuring comprehensive logging of system and application activities. This involves collecting, storing, and regularly reviewing logs to detect unauthorized access or anomalous activities. The Ubuntu OS includes the following main logs: Authorization log, Daemon Log, Debug log, Kernel log and System log.
  - Audit Trails: Maintaining records of system-level activities to facilitate the reconstruction and examination of the sequence of events in investigating an incident. This can be achieved using tools like the Auditd, which is part of the Linux Auditing System. Auditd is a powerful and comprehensive auditing tool integrated into the Linux kernel. It is designed to log and monitor system activities like system calls made by programs, file accesses and modifications, changes to the system time, and user logins. Administrators can configure rules to specify exactly what events to log and what details to record.
- **Access Control** - Managing who can access the operating system and what actions they can perform is foundational to system security.
  - User Account Management: Managing user accounts meticulously to ensure that only authorized users have access to the system. This includes removing or disabling unused accounts and privileges not needed for a user's role.
  - Password Policies: Implementing strong password policies that require complex passwords which must be changed regularly. Ubuntu supports complex password enforcement natively through the Pluggable Authentication Modules (PAM). PAM is a flexible and modular mechanism for authentication management. It is designed to



simplify authentication processes by centralizing authentication policies across various applications that support PAM. System administrators can easily make system-wide changes to authentication mechanisms through a single interface.

- Multi-factor Authentication (MFA): Using MFA wherever possible to add an additional layer of security beyond just usernames and passwords. Tools like Google Authenticator can be integrated into the Ubuntu Server to provide this capability.
- Role-Based Access Control (RBAC): Implementing RBAC to ensure that the ability to access and execute particular functions is dependent on the user's role, thereby enforcing the principle of least privilege.
- **Recovery and Response** - Preparing for potential security incidents with effective recovery and response strategies.
  - Backup and Restore: Regularly scheduled backups of critical data and system configurations, combined with tested restore procedures, to ensure data integrity and availability in the event of data loss or system compromise. Tools like rsync or Bacula [29] can be configured for both local and remote backups. In particular, Bacula is an open-source, enterprise-level computer backup system for heterogeneous networks. It provides for managing backup, recovery, and verification of computer data across a network. Bacula is known for its robust configuration options, allowing precise control over backup and restoration processes.

The above steps emphasize a proactive approach to security, leveraging Ubuntu's features and complementing them with industry best practices to build a secure and robust server environment.

### 5.3 Network Level

Network Level security is designed to protect the integrity, availability, and confidentiality of data as it travels across networks. This level of security is crucial because network vulnerabilities can expose sensitive information to unauthorized access and attacks such as denial-of-service (DoS). The following list presents main security components and strategies employed at the network level:

- **Firewalls:** They act as a barrier between trusted internal networks and untrusted external networks, such as the Internet. Firewalls inspect incoming and outgoing network traffic based on predefined security rules and filter out potentially harmful traffic. They include both hardware and software firewalls, configured to specific needs of the network to provide optimal protection. Regarding software firewalls, UFW (Uncomplicated Firewall) [30] is a popular and user-friendly application for creating and managing iptables firewall rules on Linux systems. It is designed to make it easier for users to configure a firewall using straightforward commands, and to set default policies for incoming and outgoing traffic. Typically, the default setting is to deny all incoming traffic and allow all outgoing traffic, providing a good starting point for securing a system. In addition, UFW allows rules based on applications, and has built-in support for logging. This helps in debugging and understanding incoming and outgoing traffic patterns, as well as checking the status of the firewall.
- **Intrusion Detection and Prevention Systems (IDS/IPS):** IDS monitors network traffic for suspicious activity and known threats, sending alerts when potential security breaches are detected. IPS actively blocks attack attempts and can take immediate action to prevent a breach from occurring, such as blocking traffic from a malicious IP address. In this context, Fail2ban [31] is a well-known software framework that helps protect against unauthorized access to a system and its services. It continuously scans log files and watches for specific patterns corresponding to authentication failures and other potential malicious activities. When an IP address reaches a defined threshold within a set time period, Fail2ban will block the IP address for a specified duration. The service is highly configurable. You can set parameters such as the number of failed attempts to trigger a ban, the duration of the ban, and which services to monitor, including SSH, FTP, SMTP, and more. Apart from banning IP



addresses, Fail2ban can perform other actions such as sending email notifications to administrators when a ban happens or when other defined conditions are met.

- **Encryption:** It utilizes technologies like HTTPS (Hypertext Transfer Protocol Secure) and TLS (Transport Layer Security) to encrypt data as it is transmitted over internal and external networks. This prevents eavesdroppers from intercepting and reading sensitive data. HTTPS is an extension of HTTP, employed extensively in websites and services, and uses TLS to encrypt the data exchanged. TLS provides data integrity through message authentication codes. It ensures that the data sent is not altered in transit.
- **Network Segmentation:** It divides a network into smaller, manageable segments or subnetworks, each serving a specific purpose or containing a particular category of data. Network segmentation limits the spread of cyber threats within networks. If one segment is compromised, others remain protected, isolating potential damage. Typically, it is implemented using subnets and virtual local area networks (VLANs) to control traffic flow and apply security policies more granularly.

By integrating these elements, the RAISE project can establish a comprehensive network security framework that not only defends against external threats but also helps in managing and mitigating internal security risks. This holistic approach is essential for maintaining the integrity and security of data as it flows through the network.

### 5.4 Application Level

Application security refers to the measures and techniques used to protect applications like the RAISE Central Portal from threats throughout the entire application lifecycle. Effective application security encompasses the software and procedural methods to protect applications from external threats and internal vulnerabilities, utilizing strategies and components that make up a robust application security framework:

- **Secure Coding Practices**
  - **Sanitize Inputs:** Ensure that inputs are checked to prevent common vulnerabilities such as SQL injection, cross-site scripting (XSS), and command injection. Inputs should be sanitized to ensure they do not contain malicious code that can be executed by an application.
  - **Use Whitelisting:** Favour whitelisting over blacklisting to explicitly allow only safe and necessary inputs or actions, rather than trying to block known unsafe inputs.
  - **Escape Outputs:** When displaying user input or data fetched from other sources, ensure outputs are encoded to prevent execution in unintended contexts, and guard against XSS attacks.
  - **Prevent Information Leakage:** Ensure that error messages do not provide details that could help an attacker exploit vulnerabilities in the system.
  - **Regular Updates and Patch Management:** Keeping all libraries and frameworks up to date with the latest security patches to mitigate risks from known vulnerabilities.
  - **Use Web Application Firewalls (WAFs):** The primary function of a WAF is to filter, monitor, and block HTTP(S) traffic to and from a web application. A WAF inspects the traffic coming into a web application to detect malicious requests and block them before they reach the server. It uses a set of predefined or dynamically learned security rules to analyse the incoming traffic. These rules can be based on many attributes, including IP addresses, HTTP headers, URL, the method of request, and the content within the request. When a WAF identifies malicious traffic, it can block it and log the details for further inspection. In this field, ModSecurity [32] is a powerful, open-source WAF that acts as a module for the Apache HTTP Server, although it has been adapted for other web servers like Nginx and IIS. ModSecurity operates in real-time, monitoring web traffic at a granular level. It utilizes a robust and flexible rule

engine that allows for a variety of different tests to be performed on HTTP transactions. Users can write their own rules tailored to their specific security needs or use rules from the OWASP Core Rule Set, which provides a generic set of security rules for protecting web applications. Rather than simply blocking every request that matches a rule, ModSecurity supports an anomaly scoring approach where each request can score points for every matched rule. When a configured threshold is reached, the request can then be blocked.

- **Code Reviews:** Employ regular code reviews to detect security vulnerabilities, bugs, and flaws in an application's logic.

- **Authentication and Authorization**

- **Strong Authentication Mechanisms:** Implementing strong single-sign on services and password policies.
- **Least Privilege:** Ensure that accounts and processes operate using the least amount of privilege necessary to perform their tasks. This minimizes potential damage from exploits.
- **Role-Based Access Control (RBAC):** Defining user roles and permissions to control access to resources within the application based on the user's role.
- **Secure Session Management:** Implement secure session management practices, including generating new session identifiers after login and ensuring session expiration.

In this context, Keycloak [33] is an open-source Identity and Access Management (IAM) tool which is used to centralize the authentication and authorization processes for applications and services. Core features of Keycloak include:

1. **Single Sign-On (SSO):** Keycloak supports Single Sign-On, meaning users can log in once and gain access to multiple applications without needing to re-authenticate. This feature enhances user experience and streamlines access across a suite of services.
2. **Multi-factor Authentication (MFA):** It provides strong authentication with an array of configurable options, including OTPs (One-Time Passwords), hardware tokens, and mobile authentication methods.
3. **Social Login:** Keycloak allows users to log in using their existing social media accounts, such as Google, Facebook, Twitter, and more.
4. **User Federation:** It supports user federation, which allows it to integrate with multiple user directories, like LDAP or Active Directory, synchronizing and managing user data centrally.
5. **Identity Brokering:** Keycloak can act as an identity broker between the applications it secures and external identity providers. This feature simplifies the management of user identities across diverse systems.
6. **Fine-grained Authorization:** It provides detailed authorization services, allowing fine-grained permissions and policy settings to manage access control for applications at a detailed level.
7. **Customizable Theming:** The appearance and behavior of login pages and user interfaces can be fully customized to match the look and feel of the parent applications.
8. **Administration Console:** A user-friendly web-based console is provided for managing realms, users, roles, groups, and permissions. This interface makes it easy to configure and administer security settings without the need for deep technical knowledge.

9. **Client Adapters:** Keycloak offers client adapters for various programming languages and frameworks, simplifying the integration of applications with Keycloak for secure authentication and authorization.
10. **Token Exchange and Protocol Support:** It supports OpenID Connect, OAuth 2.0, and SAML 2.0, providing flexibility in terms of protocol support.

Keycloak works by acting as a separate authentication server that applications delegate to for authentication services:

1. **User Access Request:** A user requests access to an application protected by Keycloak.
2. **Redirect to Keycloak:** The application redirects the user to the Keycloak server for authentication. This redirection can include the original application's URL as a callback.
3. **Authentication:** The user logs into Keycloak, which handles the authentication according to its configured security policies.
4. **Token Issuance:** Upon successful authentication, Keycloak issues a security token (JWT, JSON Web Token) back to the application.
5. **Application Access:** The application receives the token, verifies it, and grants access to the user. The application can then use this token to make secure requests to other services on behalf of the logged-in user.
6. **Session Management:** Keycloak manages user sessions and can handle logout requests, session expiration, and even session revocation across all registered applications.

Keycloak can be deployed as a stand-alone server, in a containerized environment using Docker, or within a Kubernetes cluster, making it highly adaptable to various IT environments. Its scalable architecture ensures that it can handle anything from small to enterprise-level user bases efficiently.

- **Data Protection**

- **Data Encryption:** Utilizing encryption both at rest and in transit to protect sensitive data from unauthorized access.
- **Lawfulness, Fairness, and Transparency:** Processing data in a lawful, fair, and transparent manner.
- **Purpose Limitation:** Collecting data only for explicit and legitimate purposes and not further processing it in a way incompatible with those purposes.
- **Integrity and Confidentiality:** Ensuring appropriate storage of data, including protection against unauthorized or unlawful processing and against accidental loss, destruction, or damage. In specific cases, using blockchain technology may offer a unique and robust method to enhance the security and integrity of stored data. Blockchain [34] is a shared, immutable ledger where data is stored in a peer-to-peer network, through transactions that have been validated by a consensus protocol. Open-source implementations like Hyperledger Fabric [35] provide a highly modular and configurable architecture, that include:
  1. **Immutable Ledger:** Once data is recorded on a blockchain, it cannot be altered without the consensus of the network, which typically involves the majority of nodes agreeing to the change. This feature makes it incredibly secure against unauthorized changes and fraud, thereby ensuring the integrity of the data.

2. **Decentralization:** Blockchain's decentralized nature means that the data is not stored in a single location but is instead distributed across multiple nodes. This dispersal eliminates a single point of failure, making it much harder for hackers to compromise the integrity of the data. Even if one or several nodes are attacked, the overall integrity of the data remains secure.
3. **Enhanced Privacy:** Through the use of cryptographic techniques, including public and private keys, blockchain can secure data and ensure that only authorized parties can access it. Each transaction on a blockchain can be seen by having the public key, but only the owner of the corresponding private key can access the full details of the transaction.
4. **Transparency and Traceability:** Every transaction on a blockchain is transparent and recorded on a ledger that all network participants can access. This transparency helps in tracking and verifying the history of data or assets without compromising privacy details.
5. **Smart Contracts:** Smart contracts are self-executing contracts where the terms are directly written into code. They automatically enforce and execute the terms of agreements based on predefined rules. This can be used to manage data access rights and ensure compliance with data protection policies automatically. For example, a smart contract can be programmed to grant data access only when specific conditions are met.

- **Compliance and Regulatory Adherence**

- **Adherence to Regulations:** Ensuring applications comply with relevant legal, regulatory, and compliance requirements, such as GDPR.
- **Use of Secure Frameworks:** Implementing frameworks that promote security, such as the OWASP Top 10, to guide developers on security threats and best practices.
- **Regular Security Audits:** Conducting security audits and penetration testing to simulate potential attacks and identify weaknesses.
- **Incident Response Plan:** Developing a formalized incident response plan to handle security breaches and minimize their impact.

By integrating these elements into the development and deployment processes, RAISE can ensure a proactive approach to application security, significantly reducing the likelihood of successful attacks and the impact of potential security breaches. This comprehensive approach to application security not only protects the technical integrity of the RAISE system, but also safeguards user data and trust.

## 5.5 User Level

User-level security refers to the methods and strategies used to ensure that individual users are given appropriate access to systems and data, based on their specific roles and responsibilities. This type of security is vital to protect information from unauthorized access and to prevent insider threats. User-level security encompasses several components including user authentication, authorization, user activity monitoring, and the management of user permissions:

- **Access Controls:** The first step is verifying the identity of a user attempting to access a system. This typically involves a username and password but can also include multifactor authentication methods. Once authenticated, a user's access to resources is determined based on predefined policies. This process involves checking the user's permissions to ensure they have the right to perform requested actions on specific resources.
- **User Account Management:** Managing user accounts involves several ongoing tasks to ensure that access rights remain appropriate over time:

- **Provisioning and Deprovisioning:** The process of creating user accounts when needed and properly removing or deactivating them when no longer required.
- **Audit and Review:** Regularly reviewing and auditing user roles and permissions to ensure they remain aligned with current requirements and security policies.
- **Password Management:** Enforcing password complexity requirements, setting expiration dates, and implementing regular password changes to maintain security integrity.
- **Data Protection Policies:** Developing clear policies that define how data is handled, who has access to it, and how it is protected. These policies should be communicated to all users and enforced rigorously.
- **User Activity Monitoring:** Monitoring user activities and auditing access logs help in detecting unusual access patterns or policy violations. This is crucial for identifying potential security breaches and ensuring users are only performing authorized actions. With regard to the main functionality of RAISE, automated tools may be employed to detect activities that deviate from normal patterns, and to perform code quality and security analysis on the uploaded processing scripts and algorithms. These tools consist of:
  - A static security analyser – It is responsible for detecting code vulnerabilities and assessing the overall security score of the code. Additionally, it provides extensive information to the users about the identified vulnerabilities and how they can be resolved.
  - A dynamic security analyser – It is tasked with identifying any malicious or harmful behaviour within the user's script by scrutinizing it within a secure environment. This fortifies the robustness and security of the RAISE infrastructure while mitigating the risk of system exploitation through arbitrary code execution.
  - A performance analyser – It monitors the executed code's behaviour from a performance perspective, tracking resource utilization and extracting metrics such as CPU usage, memory consumption, and disk I/O.
- **User Education and Training:** Regularly train users on the importance of security practices, such as recognizing phishing attempts, choosing strong passwords, and securely managing their credentials.

Implementing comprehensive user-level security helps protect from internal threats and accidental data breaches, ensuring that users can access only the data and functions necessary for their roles. By combining strong policies, technical controls, and ongoing user education, the security posture of systems at the user level can be significantly enhanced.

## 6 Conclusion

In recent years, the high advancements of technology and the rapid exchange of information create increased challenges to system security, data protection and user privacy. Organizations and companies worldwide are facing complex issues that arise from connected and distributed applications / systems, stringent regulations, and increasingly sophisticated cyber threats. The alleviation of these issues requires a multi-faceted approach, that includes adopting advanced security technologies, enforcing compliance with regulatory strategies, and fostering a culture of security awareness and best practices among the different stakeholders. Essentially, remaining informed / agile as well as following specific precautions, are key aspects to protecting connected assets and sensitive information from the highly evolving data security and privacy issues.

The RAISE project, given its focus on managing and safeguarding data within a research context, is inherently complex and multifaceted in its security needs. As technology evolves and new threats emerge, the security framework employed by RAISE must be continuously enhanced and adapted, ensuring it remains robust against evolving cyber threats and compliant with stringent data protection regulations. By continuously exploring and integrating new advancements (e.g., advanced encryption techniques, enhanced identity and access management systems, AI-driven security operations, robust data governance and compliance, decentralized security mechanisms), the RAISE project can not only enhance its security framework but also foster a safer and more reliable research environment. Such proactive enhancements are crucial in addressing the dynamic landscape of security threats and maintaining the trust and confidence of all stakeholders involved in or relying on RAISE.



## 7 References

- [1] Diogenes, Y., & Ozkaya, E. (2022). *Cybersecurity - Attack and Defense Strategies* (3<sup>rd</sup> ed.). Packt Publishing.
- [2] Raines, T. (2023). *Cybersecurity Threats, Malware Trends, and Strategies* (2<sup>nd</sup> ed.). Packt Publishing.
- [3] Stallings, W. (2018). *Effective Cybersecurity: A Guide to Using Best Practices and Standards* (1<sup>st</sup> ed.). Addison-Wesley Professional.
- [4] Stallings, W. (2016). *Network Security Essentials: Applications and Standards* (6<sup>th</sup> ed.). Pearson.
- [5] Bhajaria, N. (2022). *Data Privacy: A runbook for engineers* (1<sup>st</sup> ed.). Manning.
- [6] Jarmul, K. (2023). *Practical Data Privacy: Enhancing Privacy and Security in Data* (1<sup>st</sup> ed.). O'Reilly Media.
- [7] The Open Web Application Security Project (OWASP). (2021). *The OWASP Top 10*. Retrieved October 10, 2023, from <https://owasp.org/www-project-top-ten/>
- [8] The European Union Agency for Cybersecurity (ENISA). (2024). *Foresight Cybersecurity Threats For 2030 - Update*. Retrieved March 20, 2024, from <https://www.enisa.europa.eu/publications/foresight-cybersecurity-threats-for-2030-update-2024>
- [9] European Commission. *Data protection - Rules for the protection of personal data inside and outside the EU*. Retrieved September 30, 2023, from [https://commission.europa.eu/law/law-topic/data-protection\\_en](https://commission.europa.eu/law/law-topic/data-protection_en)
- [10] Proton Technologies AG. *Complete guide to GDPR compliance*. Retrieved September 30, 2023, from <https://gdpr.eu/>
- [11] European Commission. (2016). *Directive on Security Network and Information Systems (NIS Directive)*. Retrieved September 30, 2023, from [https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L\\_.2016.194.01.0001.01.ENG&toc=OJ:L:2016:194:TOC](https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG&toc=OJ:L:2016:194:TOC)
- [12] European Commission. (2022). *Directive on measures for a high common level of cybersecurity across the Union (NIS2 Directive)*. Retrieved September 30, 2023, from <https://digital-strategy.ec.europa.eu/en/policies/nis2-directive>
- [13] European Commission. (2017). *Proposal for an ePrivacy Regulation*. Retrieved September 30, 2023, from <https://digital-strategy.ec.europa.eu/en/policies/eprivacy-regulation>
- [14] European Commission. (2022). *The Digital Services Act package*. Retrieved September 30, 2023, from <https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package>
- [15] European Commission. (2019). *The Cybersecurity Act*. Retrieved September 30, 2023, from <https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-act>
- [16] International Organization for Standardization (ISO). (2022). *ISO/IEC 27001 - Information Security Management System (ISMS)*. Retrieved October 10, 2023, from <https://www.iso.org/standard/27001>
- [17] International Organization for Standardization (ISO). (2024). *ISO/IEC 29100 - Privacy Framework*. Retrieved March 20, 2024, from <https://www.iso.org/standard/85938.html>
- [18] National Institute of Standards and Technology. (2024). *The NIST Cybersecurity Framework (CSF) 2.0*. Retrieved March 20, 2024, from <https://www.nist.gov/cyberframework>
- [19] PCI Security Standards Council. (2022). *The Payment Card Industry Data Security Standard*. Retrieved October 12, 2023, from [https://www.pcisecuritystandards.org/document\\_library/?category=pcidss&document=pci\\_dss](https://www.pcisecuritystandards.org/document_library/?category=pcidss&document=pci_dss)



- [20] U.S. Department of Health and Human Services (HHS). (2021). *HIPAA for Professionals*. Retrieved October 12, 2023, from <https://www.hhs.gov/hipaa/for-professionals/index.html>
- [21] Center for Internet Security Inc. *CIS Critical Security Controls*. Retrieved March 30, 2024, from <https://www.cisecurity.org/controls>
- [22] Center for Internet Security Inc. *CIS Benchmarks*. Retrieved March 30, 2024, from <https://www.cisecurity.org/cis-benchmarks>
- [23] Johansen, G. (2022). *Digital Forensics and Incident Response* (3<sup>rd</sup> ed.). Packt Publishing.
- [24] Hoffman, A. (2020). *Web Application Security: Exploitation and Countermeasures for Modern Web Applications* (1<sup>st</sup> ed.). O'Reilly Media.
- [25] Tarandach, I., & Coles, M. (2020). *Threat Modeling: A Practical Guide for Development Teams* (1<sup>st</sup> ed.). O'Reilly Media.
- [26] Anderson, R. (2020). *Security Engineering: A Guide to Building Dependable Distributed Systems* (3<sup>rd</sup> ed.). John Wiley & Sons Inc.
- [27] Ozkaya, E. (2019). *Cybersecurity: A comprehensive guide to getting started in cybersecurity* (1<sup>st</sup> ed.). Packt Publishing.
- [28] Canonical Ltd. *Ubuntu Server*. Retrieved March 30, 2024, from <https://ubuntu.com/server>
- [29] Bacula Community. *The Bacula Open-Source Backup Software*. Retrieved March 30, 2024, from <https://www.bacula.org/>
- [30] Canonical Ltd. *Uncomplicated Firewall*. Retrieved March 30, 2024, from <https://wiki.ubuntu.com/UncomplicatedFirewall>
- [31] Free Software Foundation. *Fail2Ban*. Retrieved April 15, 2024, from <https://github.com/fail2ban/fail2ban>
- [32] OWASP Foundation. *ModSecurity - Open source WAF*. Retrieved April 15, 2024, from <https://github.com/owasp-modsecurity/ModSecurity>
- [33] Cloud Native Computing Foundation. *KEYCLOAK - Open-Source Identity and Access Management*. Retrieved April 15, 2024, from <https://www.keycloak.org/>
- [34] IBM. *What is blockchain?* Retrieved April 15, 2024, from <https://www.ibm.com/topics/blockchain>
- [35] Hyperledger Foundation. *Hyperledger Fabric*. Retrieved April 15, 2024, from <https://www.hyperledger.org/projects/fabric>

## Appendix 1 - Incident Response Plan

Creating an Incident Response Plan (IRP) tailored for the RAISE system involves establishing a framework to effectively identify, manage, respond to, and recover from security incidents. The RAISE IRP is broken out into three phases, the assessment, the response, and the restoration.

**Assessment Phase:** The identification actions evaluating a possible event.

- Incident confirmation and assessment
- Determine the resources needed for recovery
- Form a suitable incident response team

**Response Phase:** The immediate actions following a significant event.

- Implement immediate containment strategies
- Eradication of the cause of the incident
- Develop a strategy for returning affected services and components

**Restoration Phase:** Tasks taken to restore service to previous levels.

- System restoration from backups
- Validation and testing
- Rollout restored system online
- Conduct a post-restoration review

Each of the three phases are further divided to coherent tasks that align with the requirements and objectives of RAISE:

- **Assessment Phase**
  - **Incident Verification:** Confirm that an incident has indeed occurred to avoid false alarms that could lead to unnecessary actions or panic.
  - **Damage Assessment:** Quickly assess the scope and impact of the incident. Evaluate the extent of the damage caused by the incident to determine which components, data, and functionalities have been affected.
  - **Resource Assessment:** Determine the resources needed for recovery, including personnel and technological resources.
  - **Prioritization:** Identify which components and services need to be restored first based on their importance.
  - **Internal Notification:** Inform the relevant internal teams and stakeholders about the incident, and form a suitable incident response team.
  - **External Communication:** Depending on the incident, external parties such as law enforcement, regulators, partners, and affected users may need to be notified.
- **Response Phase**
  - **Short-term Containment:** Implement immediate containment strategies to stop the spread of the incident and limit further damage.

- **Long-term Containment:** Once immediate threats are contained, implement measures to ensure that the threat cannot expand or recur while recovery efforts are underway.
- **Root Cause Analysis:** Identify the root cause of the incident to understand how it happened and how similar incidents can be prevented.
- **Elimination of Threats:** Remove the components responsible for the incident, such as malware, unauthorized access points, or compromised accounts.
- **Evidence Preservation:** Gather and log all relevant data for forensic analysis, which may be used for legal proceedings, regulatory compliance, or to improve security measures.
- **Recovery Strategy:** Develop a strategy for returning affected services and components to full functionality with minimal risk.
- **Restoration Phase**
  - **System Repair and Restoration:** Start the technical process to repair damaged infrastructure, which may involve hardware replacements, software reinstallations, and application of security patches.
  - **Restoration from Backups:** Carefully restore data from backups after verifying their integrity and cleanliness to ensure no remnants of the security threat remain.
  - **System Configuration:** Reconfigure system to match required specifications and security settings, ensuring that all components adhere to the latest security policies and configurations.
  - **Functionality Testing:** Conduct thorough testing of the restored system to ensure it function as expected and meet operational requirements.
  - **Gradual Implementation:** Gradually bring restored system online to monitor performance and catch any unforeseen issues early in a controlled manner.
  - **Monitoring and Adjustment:** Continuously monitor system for any signs of issues during the phased rollout and make necessary adjustments.
  - **Internal Updates:** Keep internal teams informed about the status of restoration efforts, expected timelines, and any potential impacts or limitations during the restoration process.
  - **External Communication:** Update external stakeholders about the restoration progress, especially if the incident had outward-facing consequences or regulatory implications.
  - **Lessons Learned:** Conduct a post-restoration review to assess what went well and what could be improved. Discuss and document any discovered weaknesses in infrastructure, processes, or security posture.
  - **Policy and Process Updates:** Based on the lessons learned, update policies, procedures, and recovery plans to better handle future incidents.
  - **Training and Awareness:** Provide training and updates to relevant staff based on new policies, technologies, or procedures implemented as a result of the incident.
  - **Incident Report:** Prepare a comprehensive incident report that includes the details of the incident, the response actions taken, and the outcomes.

Implementing this Incident Response Plan will help the RAISE partners to effectively manage and mitigate risks associated with security incidents. In addition, regular updates and drills based on this plan will ensure that RAISE remains resilient against evolving security threats.