

Introduction into Security



NYENRODE
BUSINESS UNIVERSITEIT

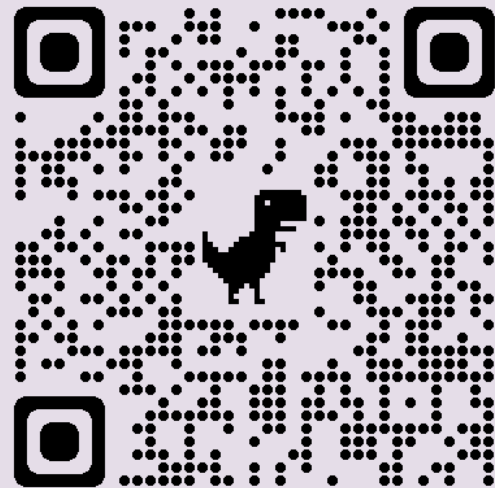
AXVECO

Xebia
Security



2022-05

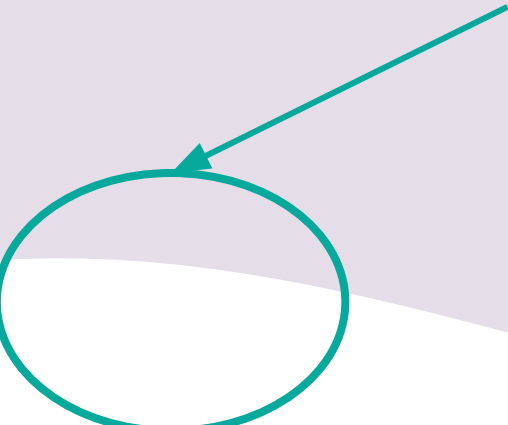
GOOGLE PRESENTATION LINK



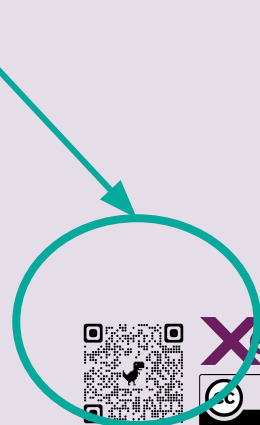
HOUSEKEEPING

1. Make & share notes for you exam.
2. Ask questions all the time, always.
3. 50 min content, 10 min break, 50 min content

Location for optional
(open access) reading



QR Code to the Google
Presentation of this slide





WHY

JESUS
DIED
SO I COULD
LIVE

TOPICS

1. Introduction of you and me
2. What defines security
3. Chaos Theorie (VUCA/ Cynefin)
4. Foundation for Security in Enterprise Design
5. Foundation for Security in IT
6. Security specific tools:
CIA & ROSI
7. The big impact of GDPR (et al)

Q&A during the session!





Edzo Botjes
Antifragility Architect
Variety Engineer
Trusted Advisor

<https://www.edzob.com>

Apply



2021 - now Xebia
2006 - 2020 Sogeti
1992 - 2006 *your IT guy*

Consultancy for
7 Sectors,
30 Clients,
40+ Assignments
Infra to business strategy

Share



@Edzob
(.com, LinkedIn, Twitter)

Multiple whitepapers
Thesis with 1500+ reads
40+ Blogs
Quoted in Books and Theses.

Teaching Enterprise
Architecture (MSc) at
Utrecht University
of Applied Sciences
2022 -

Research



PhD student
Information
Security
2021-2027

MSc
Enterprise
Architecture
2020

BSc
Business
Information
Systems
2006

ASc
Computer
Science
2003





Edzo Botjes
Antifragility Architect
Variety Engineer
Trusted Advisor

<https://www.edzob.com>

Internships
2005 - 2006

BAARSMA • WINES

heart
for vital let

Consultant @ Sogeti
2006 - 2020



Ministerie van Financiën



Ziggo

VISMA | raet

AIRFRANCE / KLM
Martinair CARGO

VfPf

KAS BANK
CORPORATE BANKING

LINDORFF

AIRFRANCE KLM

IGNITION

sogeti
Part of Capgemini



NYENRODE
BUSINESS UNIVERSITEIT



ProRail

HAN UNIVERSITY
OF APPLIED SCIENCES

mborijn//land

Raad voor Rechtsbijstand

Consultant @ Xebia
2021 -

Witteveen + Bos

Syntess
Software

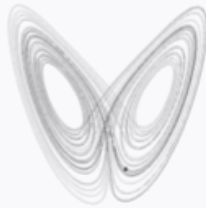
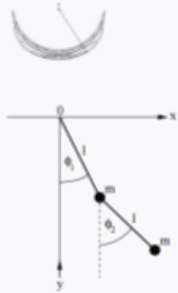
nationale
nederlanden

sdworx

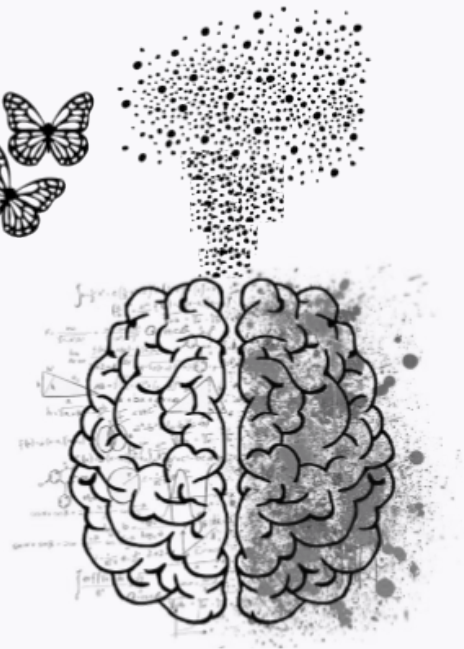
ASML

Xebia

My personal journey into security



$$\begin{aligned}\frac{dx}{dt} &= \sigma(y - x), \\ \frac{dy}{dt} &= x(\rho - z) - y, \\ \frac{dz}{dt} &= xy - \beta z.\end{aligned}$$





910 950
FT 497, 498, 499, 699
FT Silver Streak

ALHAMBRA

EL MONTE

ROSEMEAD

SOUTH EL MONTE

MONTEREY PARK

MONTEBILLO

WHITTIER

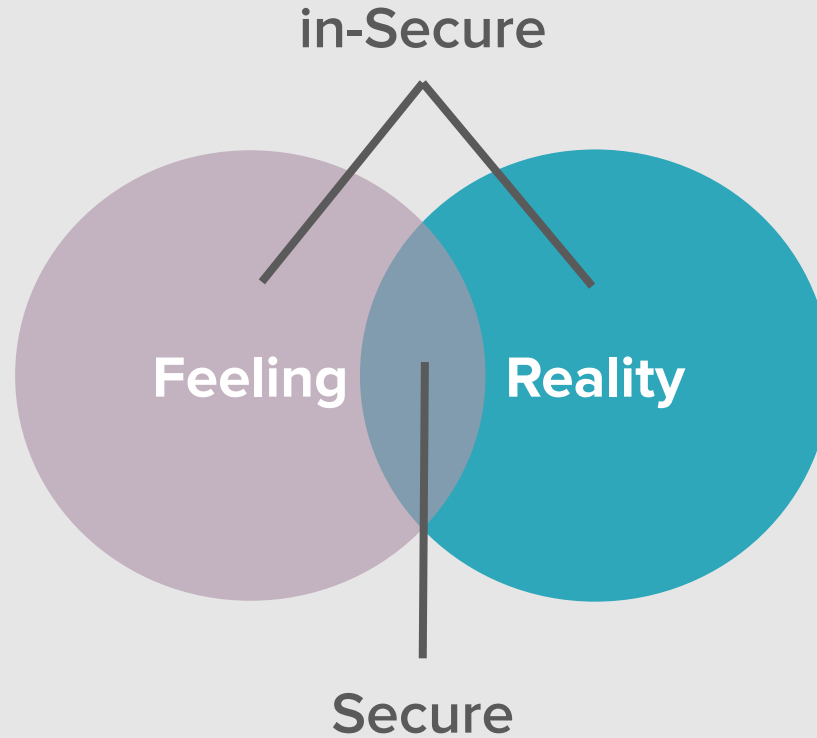


The map is not the territory

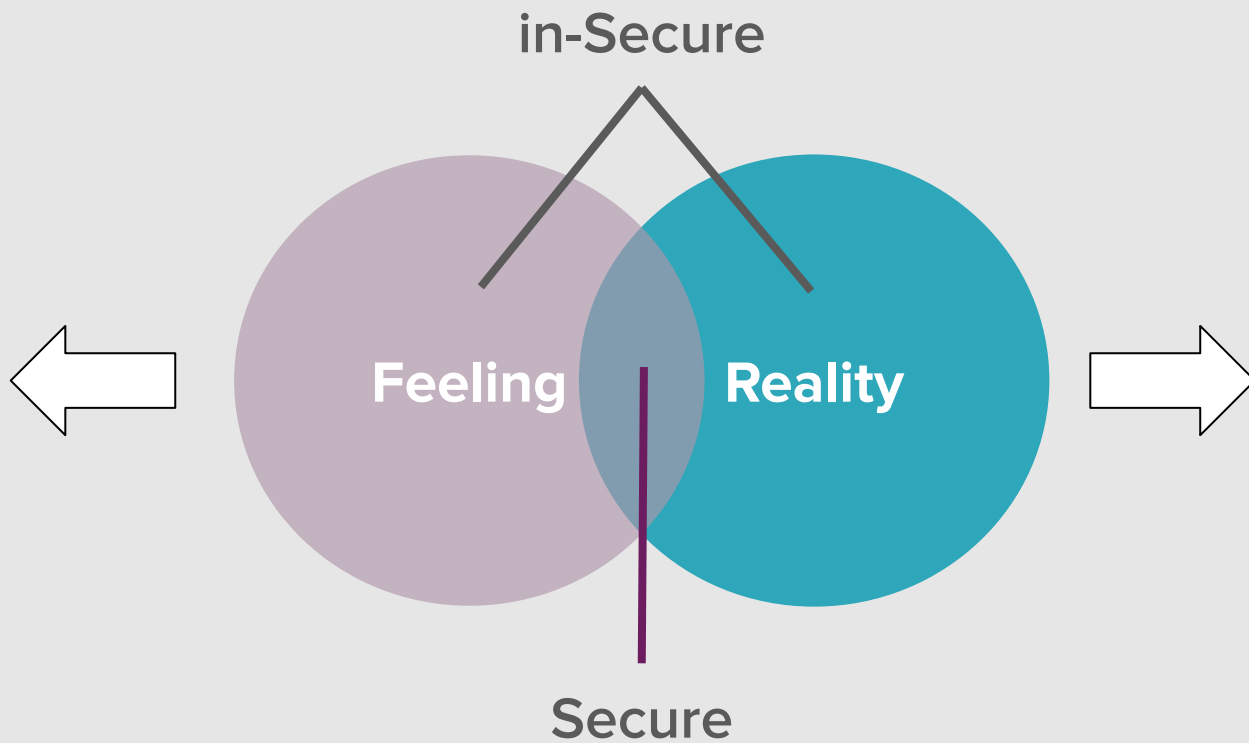
SECURITY



How we define secure



The story of two continuous forces



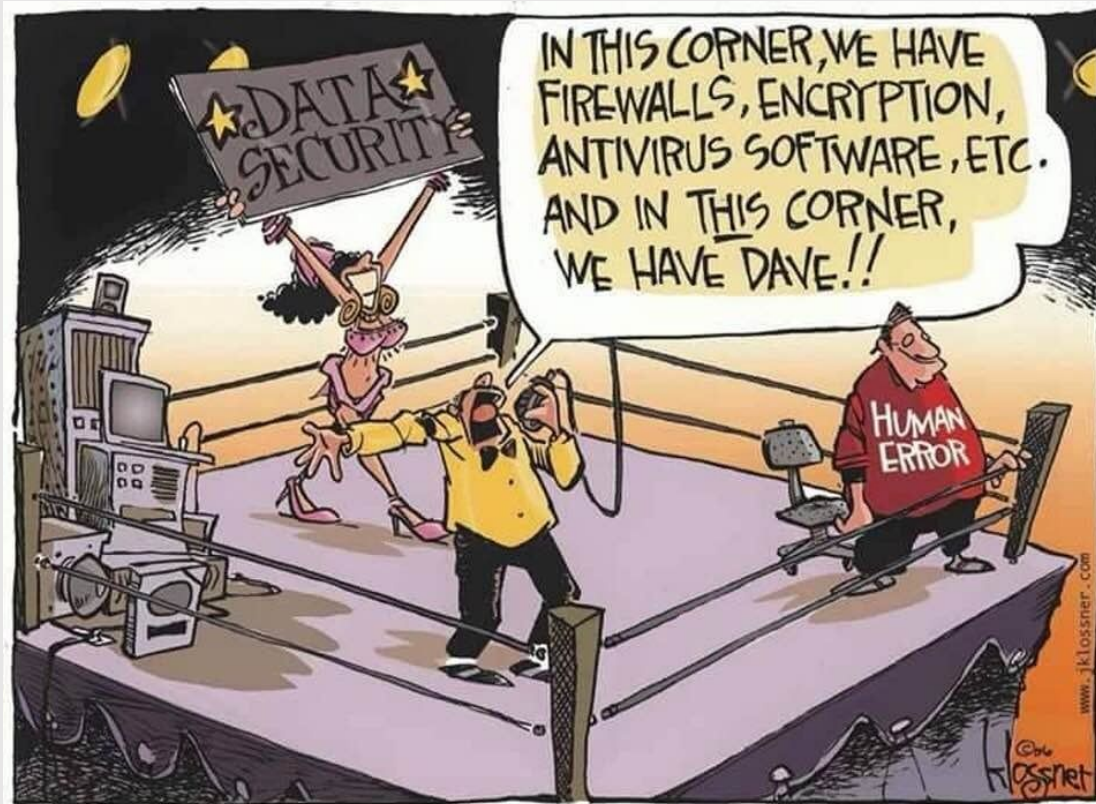
The human factor

The State of Cloud Security Risk, Compliance, and Misconfigurations



CloudHealth
by vmware

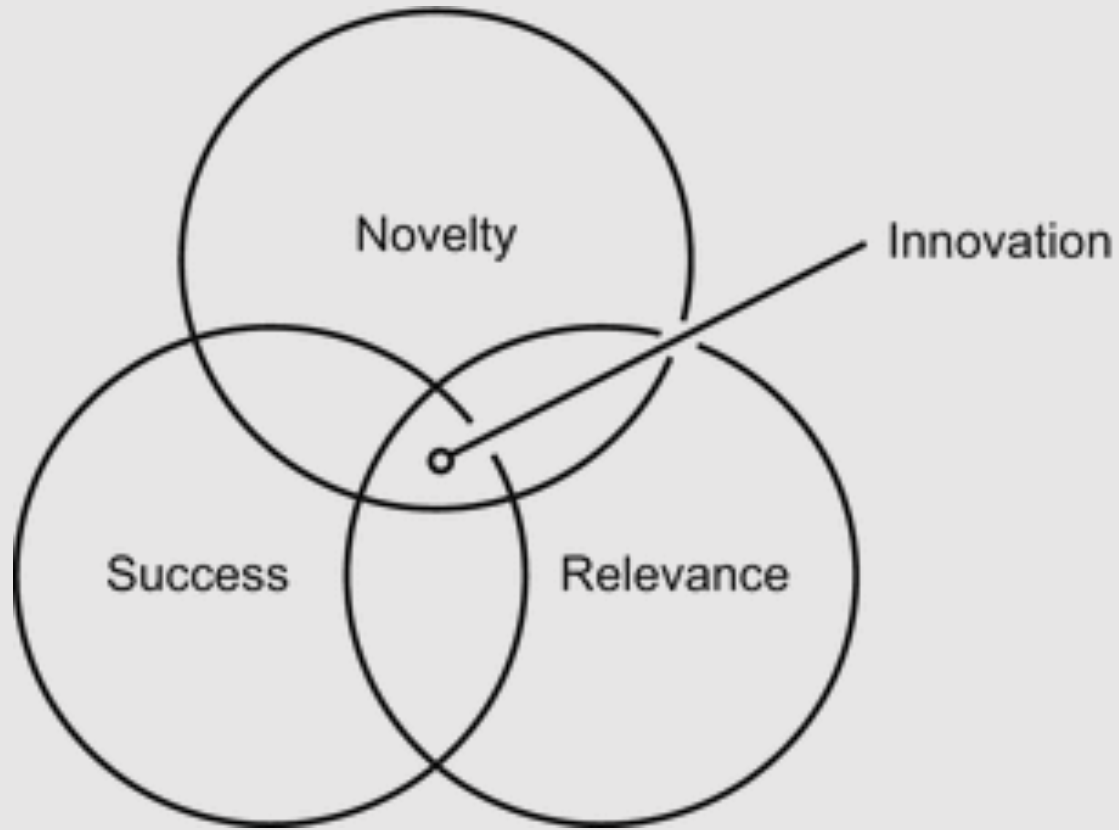
cloud security
alliance®



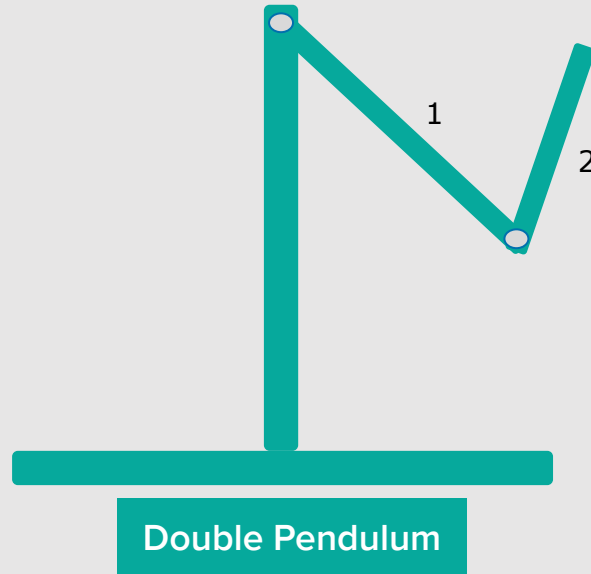
Xebia



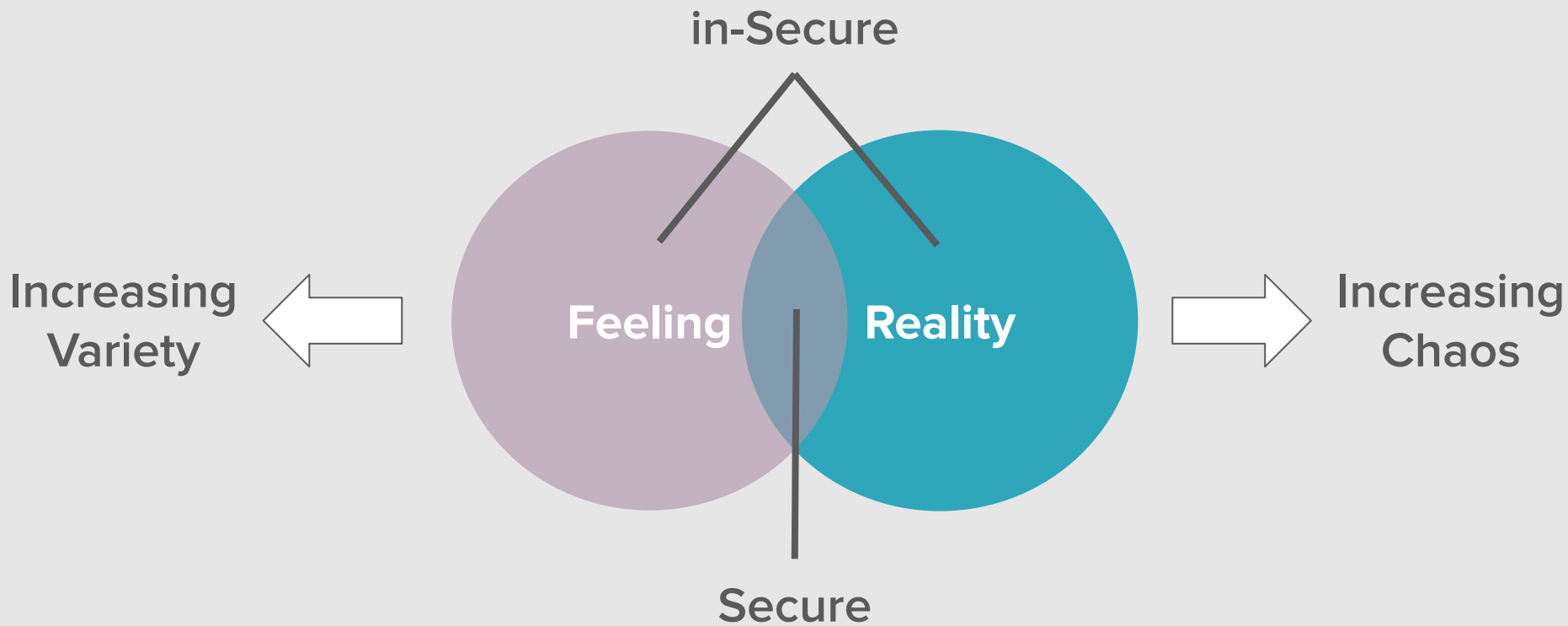
Innovation drives change in reality

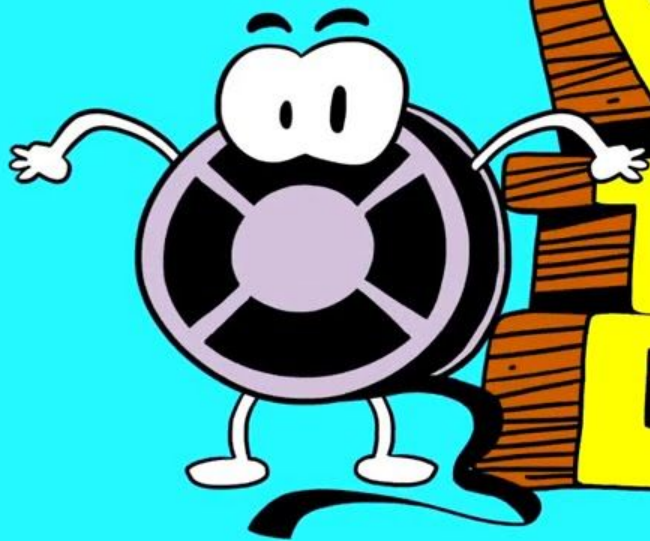


Reality is unpredictable

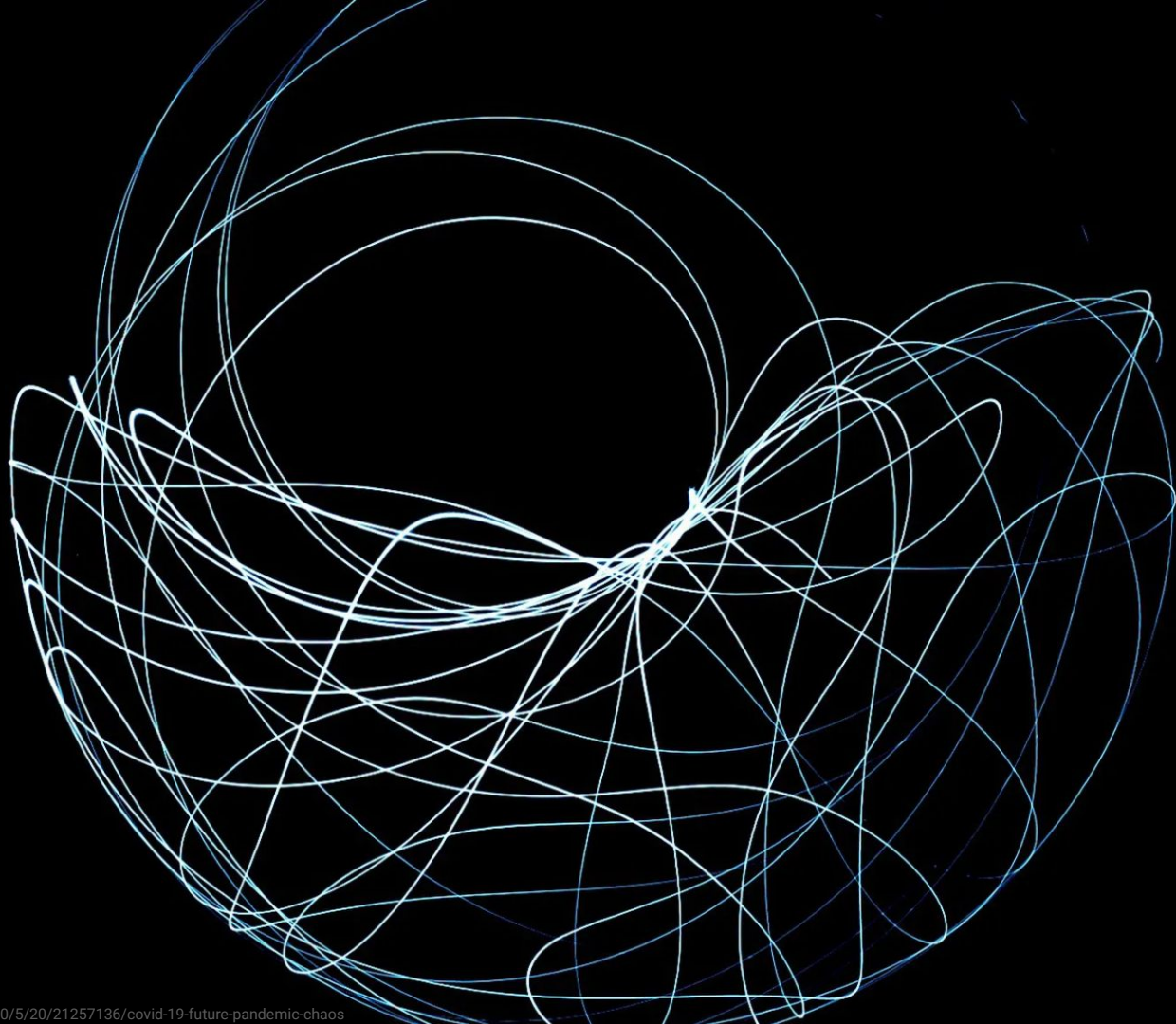


The continuous security challenge





**NO ONE
KNOWS
WHAT
THEY'RE
DOING**



Thus we are in the age of VUCA

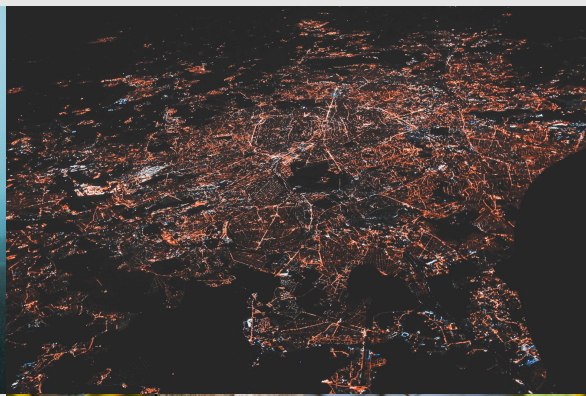
Volatility



Uncertainty



Complexity



ISO 31.000
<https://doi.org/10.1016/j.bushor.2014.01.001>
<https://hbr.org/2014/01/what-vuca-really-means-for-you>
<https://link.springer.com/book/10.1007/978-3-319-16689-0>
https://en.wikipedia.org/wiki/Volatility_uncertainty_complexity_and_ambiguity

Ambiguity



Security is all about how to deal with your VUCA world.

Next up a mental model to put VUCA in a corner,
then concrete ways to improve security in your organization(s).



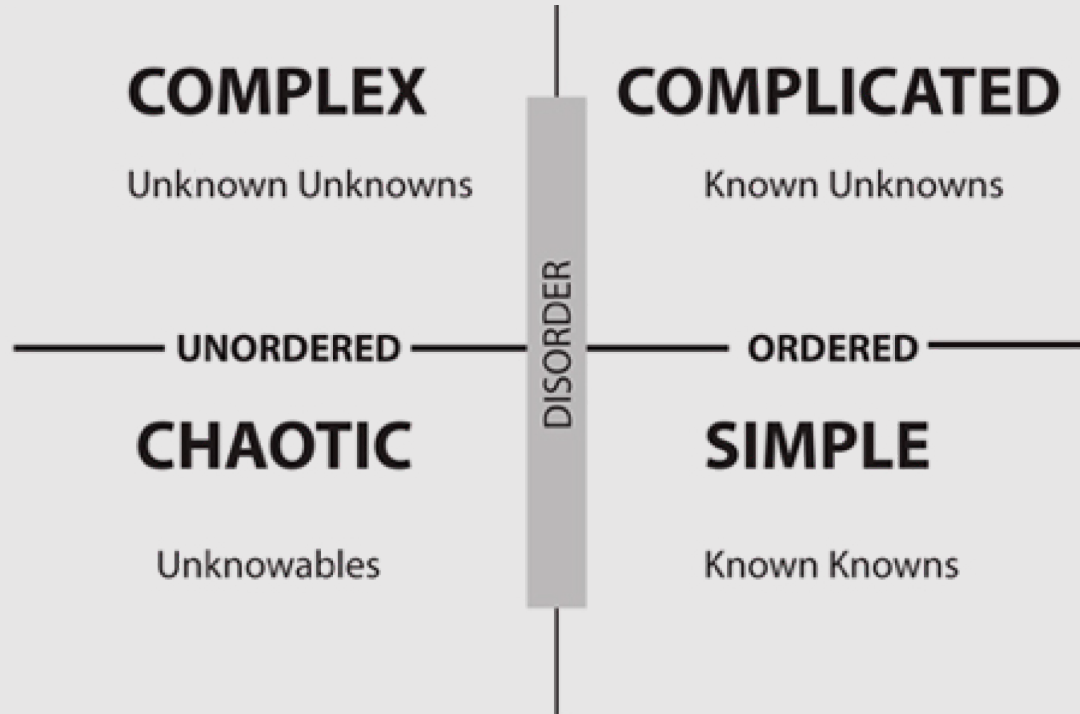
Xebia



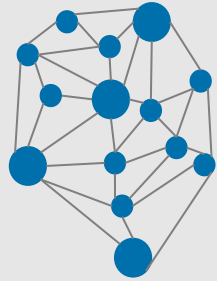
NOT ALL IS CHAOS



Not all is chaos, Cynefin to make sense.



Not all is chaos, Cynefin to make sense.



Holistic
approach

COMPLEX

Unknown Unknowns

UNORDERED

CHAOTIC

Unknowables

DISORDER

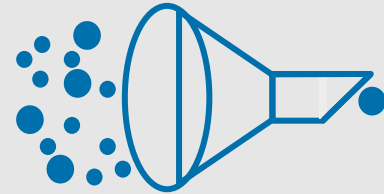
COMPLICATED

Known Unknowns

ORDERED

SIMPLE

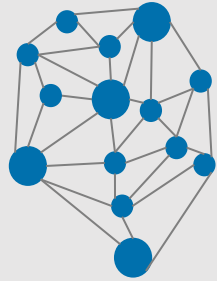
Known Knowns



Reductionistic
approach



Not all is chaos, Cynefin to make sense.



Holistic
approach

COMPLEX

Unknown Unknowns

Probe - Sense - Respond

UNORDERED

CHAOTIC

Unknowables

Act - Sense - Respond

DISORDER

COMPLICATED

Known Unknowns

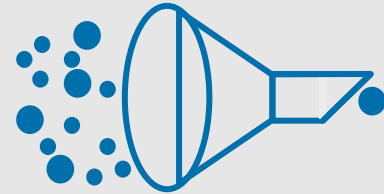
Sense - Analyze - Respond

ORDERED

SIMPLE

Known Knowns

Sense - Categorize - Respond



Reductionistic
approach





**BUILD A COMPANY
OR
JOIN A COMPANY**

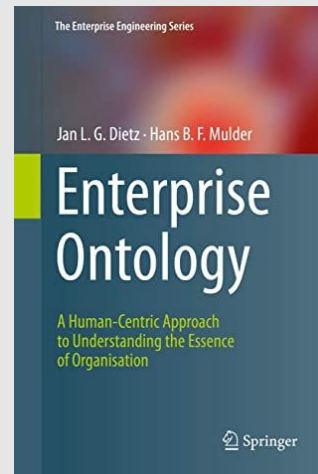
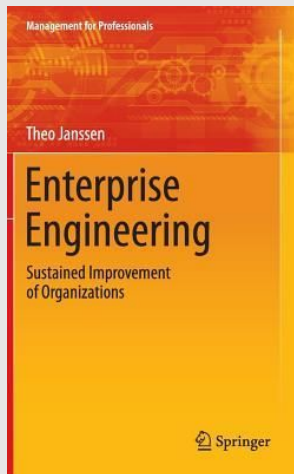
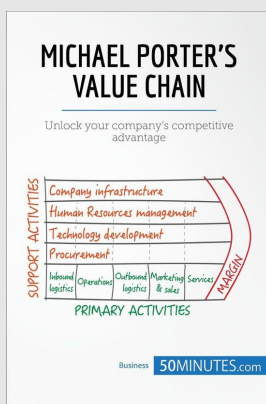
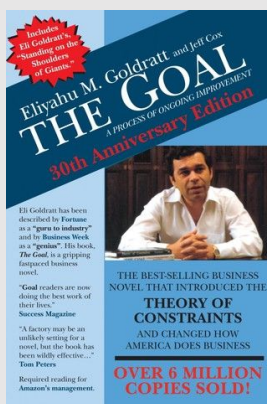
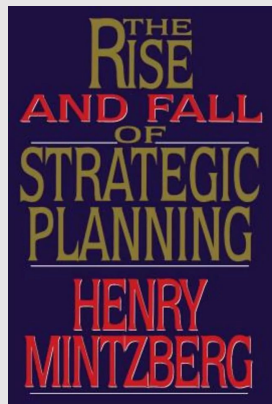
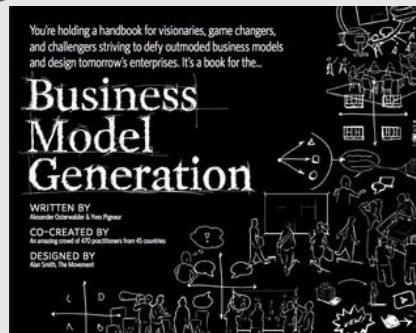
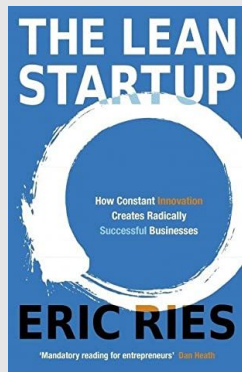
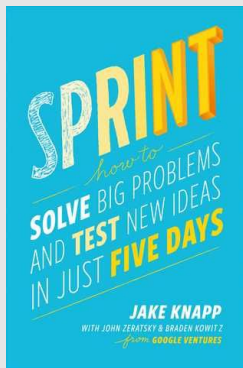
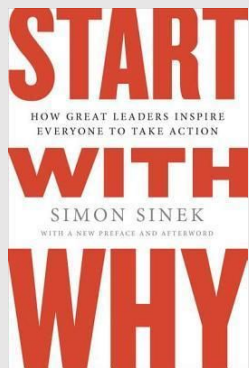
BOOK BINGO



Xebia



How to build/ change a company



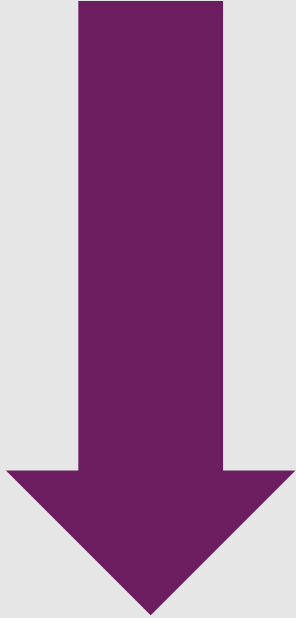
How to build/ change a company **BOILS DOWN TO ...**



PEOPLE

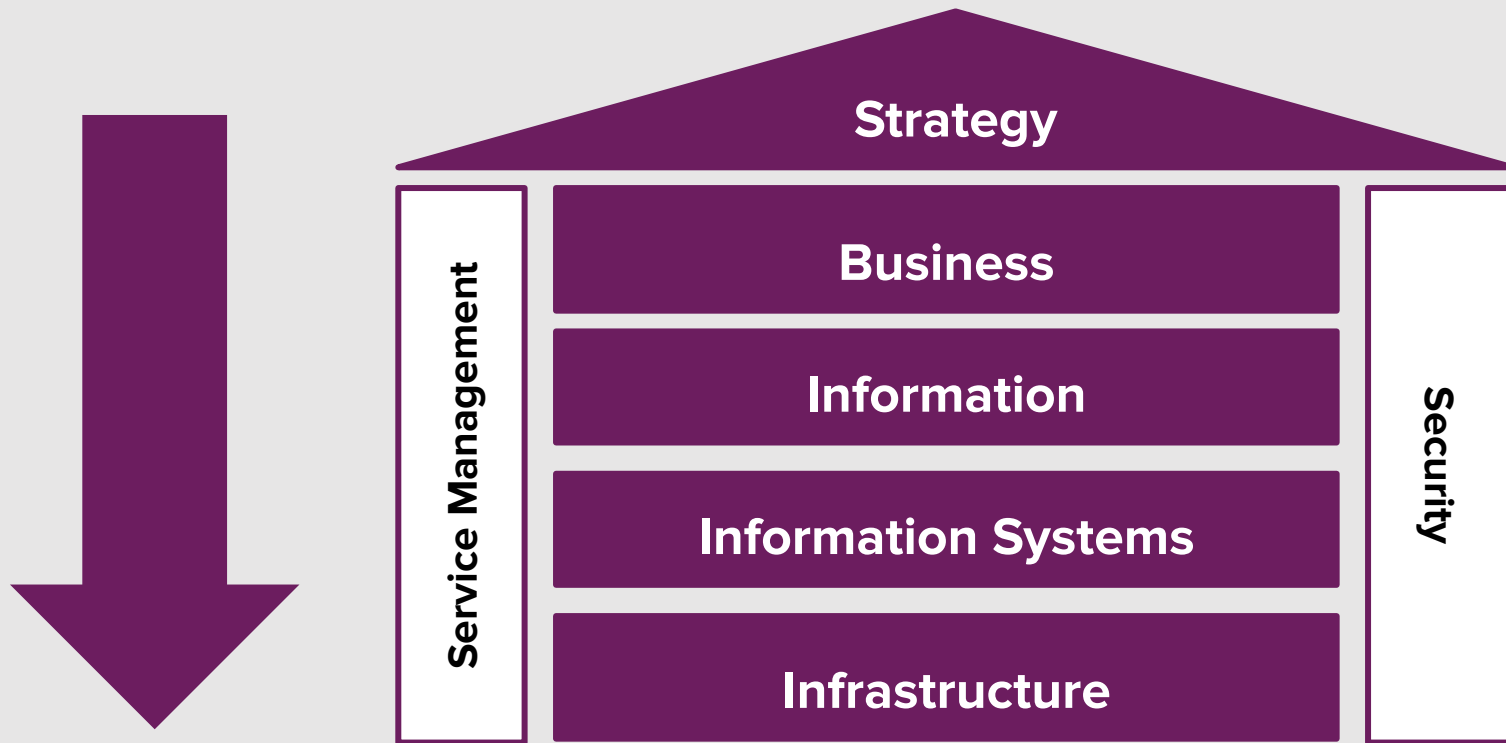
PROCESS


TECHNOLOGY



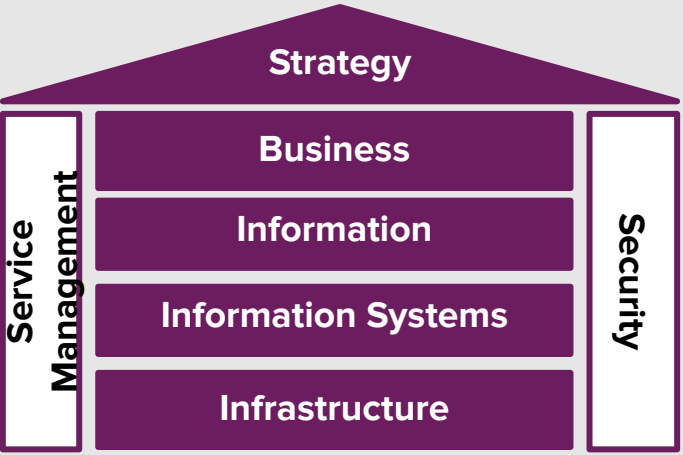
All Enterprise Models **BOILS DOWN TO ...**



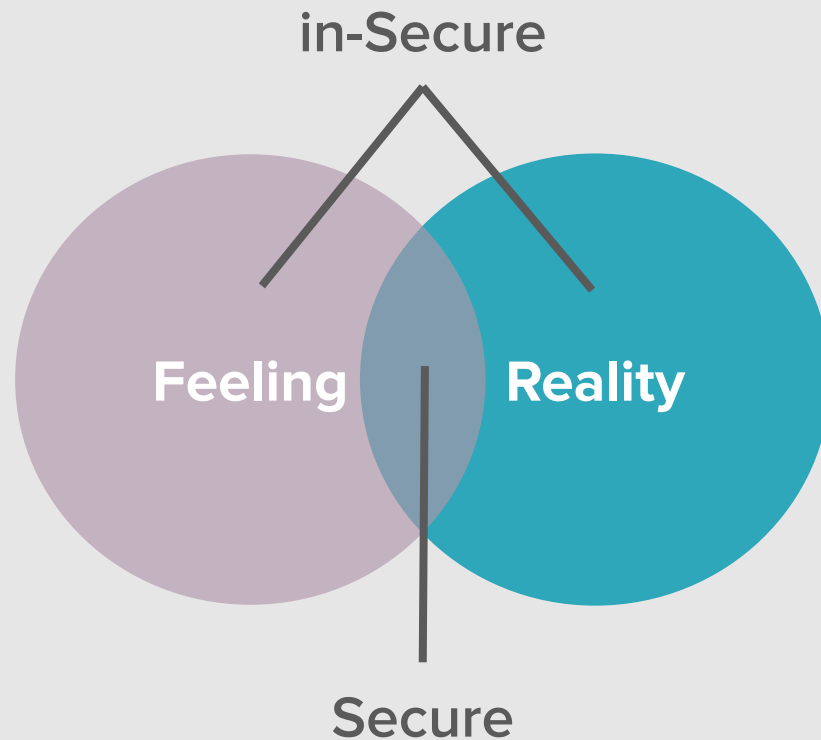
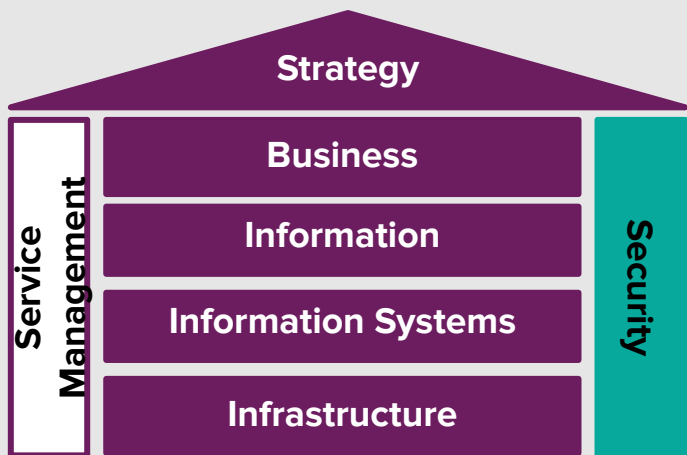




SECURITY IN ALL LAYERS



Security is active on all layers



Security is active on all layers, some examples

Business Modelling

Enterprise Design
Resilient Organisation
Antifragile Organisation

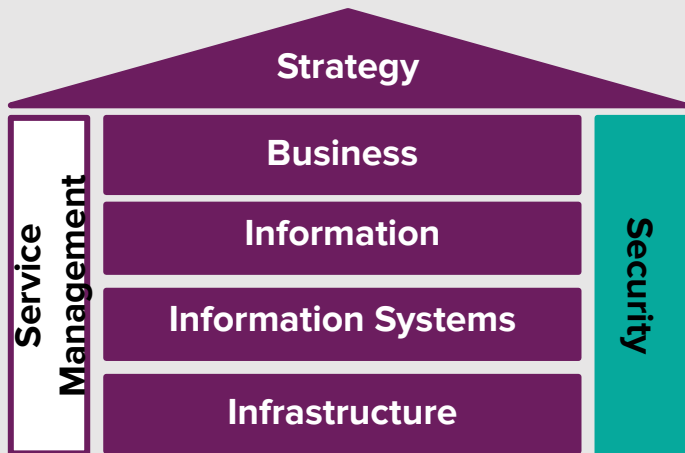
Business Continuity Management

Risk Management
Compliance

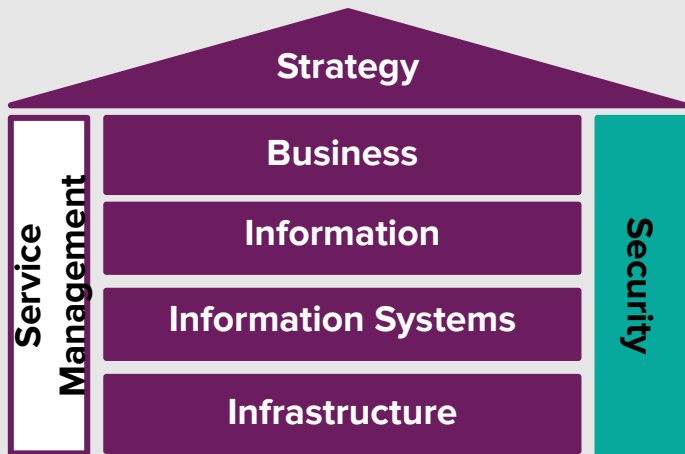
Information Security

Cyber Security
IT Security
Application Security

Infrastructure Security
Physical Security
Operational Security
Asset Security
Network and Telecom Security



Security is active on all layers, and attracts people that like order

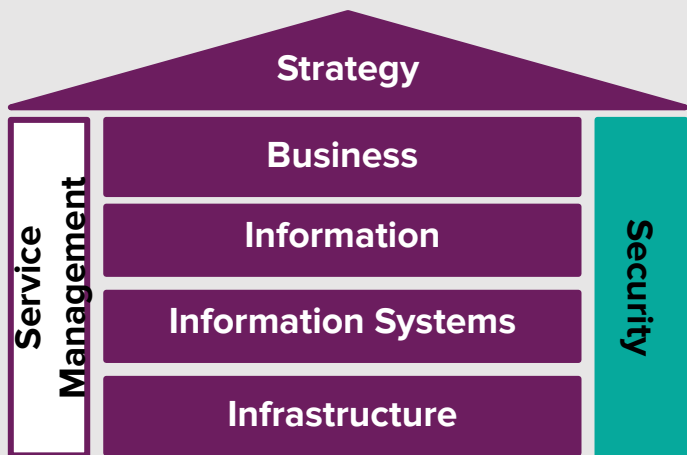


People trying to order all the security things:

1. <https://pauljerimy.com/security-certification-roadmap>
2. <https://www.securecontrolsframework.com>
3. <https://privacyplan.net/privacy-datasets/privacy-legislation-grid>



Security is active on all layers, bla bla bla bla



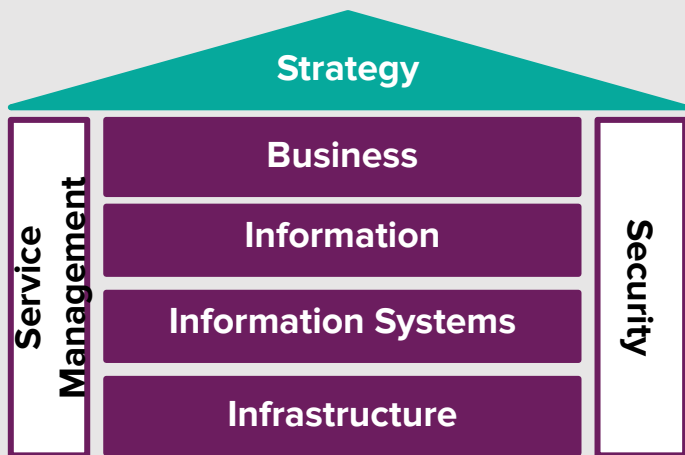
Xebia



EVERY COMPANY



Strategy



In the strategy layer, security is present as Risk Management.

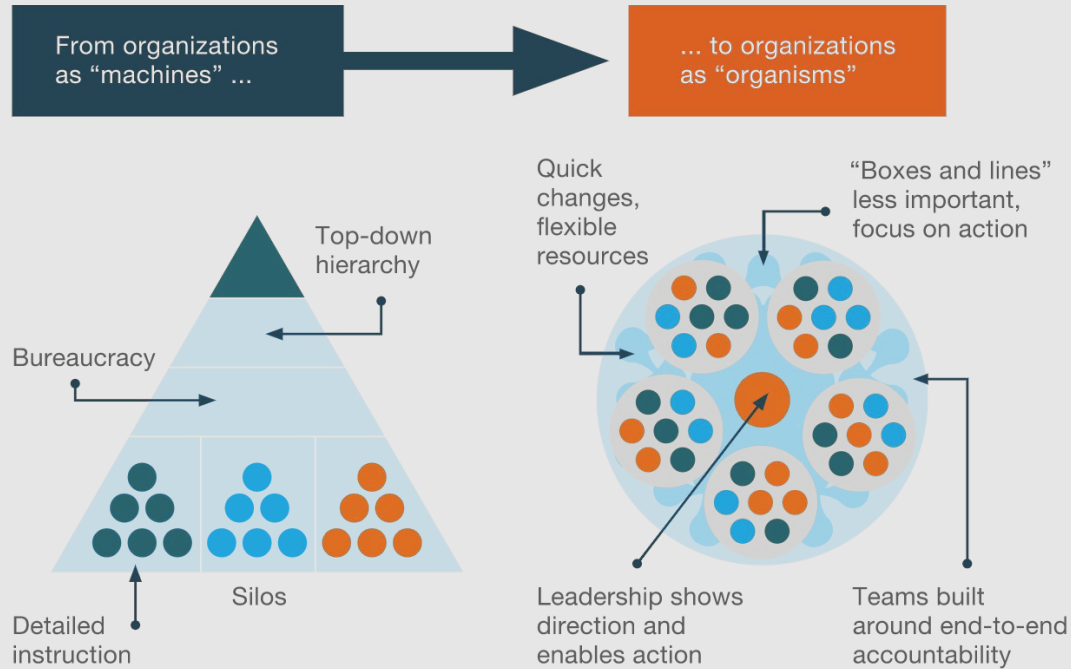
Key Questions are:

1. Where is my organisation strategy fragile? *PEST/ SWOT*
2. How do I want to respond? *RESILIENCE*
3. What is my risk appetite?



The agile organization is dawning as the new dominant organizational paradigm.

Rather than organization as machine, the agile organization is a living organism



McKinsey&Company



27000: "risk is chance or probability of loss"

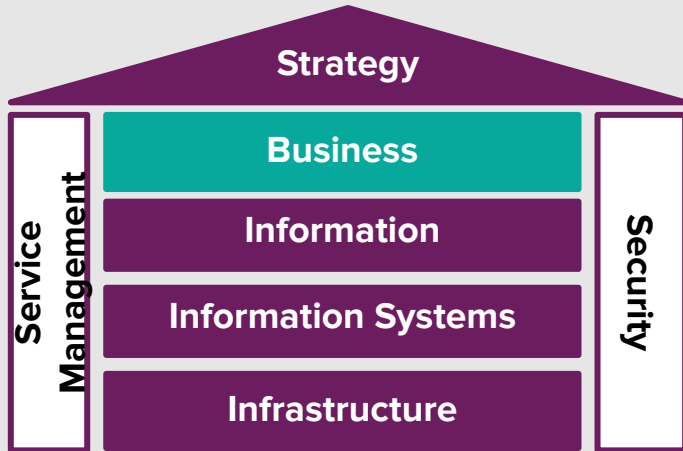
31000: "risk is the effect of uncertainty on objectives"

31000: “Risk management is the identification, assessment, and prioritization of risks (effect of uncertainty on objectives, whether positive or negative) followed by effective and economic application of resources to minimize, monitor, control, and assure the probability and/or consequence of negative events or to maximize opportunities.“

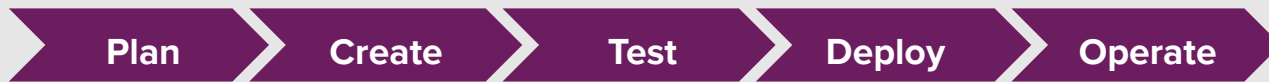
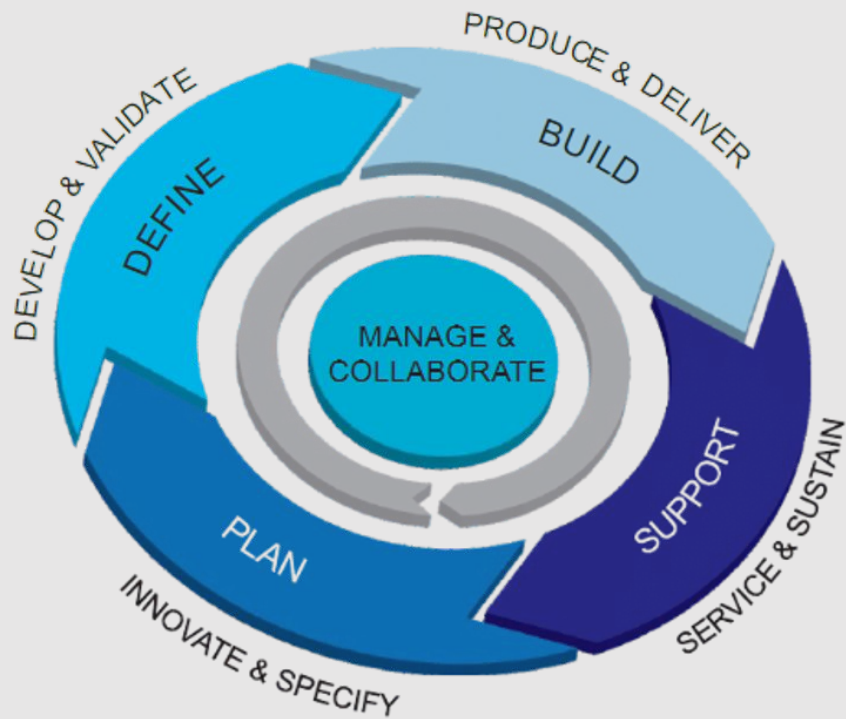
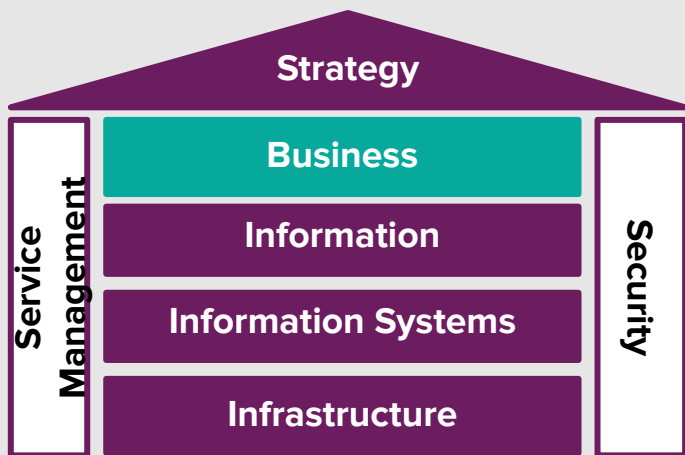
“The risk assessment and treatment process in ISO 27001 aligns with the principles and generic guidelines provided in ISO 31000.”



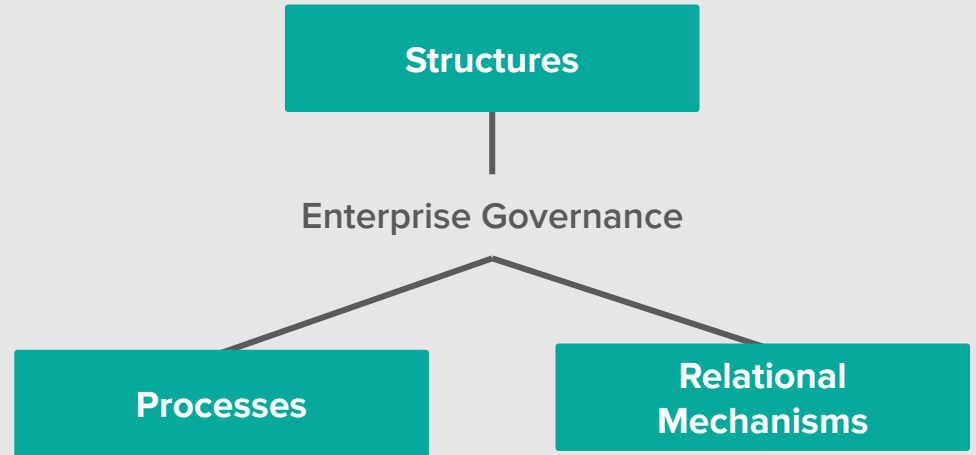
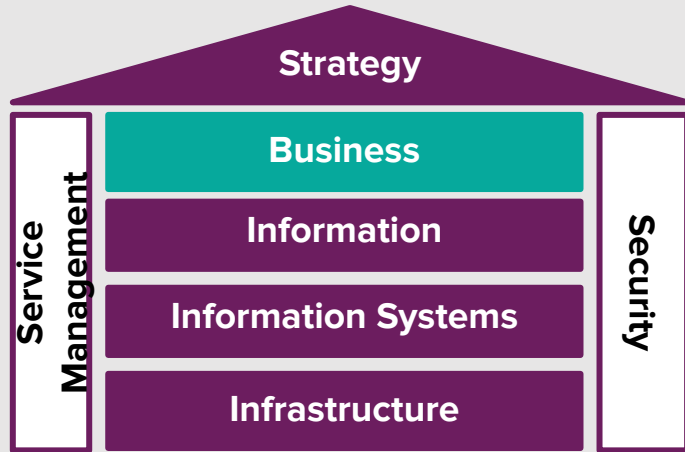
Business that delivers via processes products and services



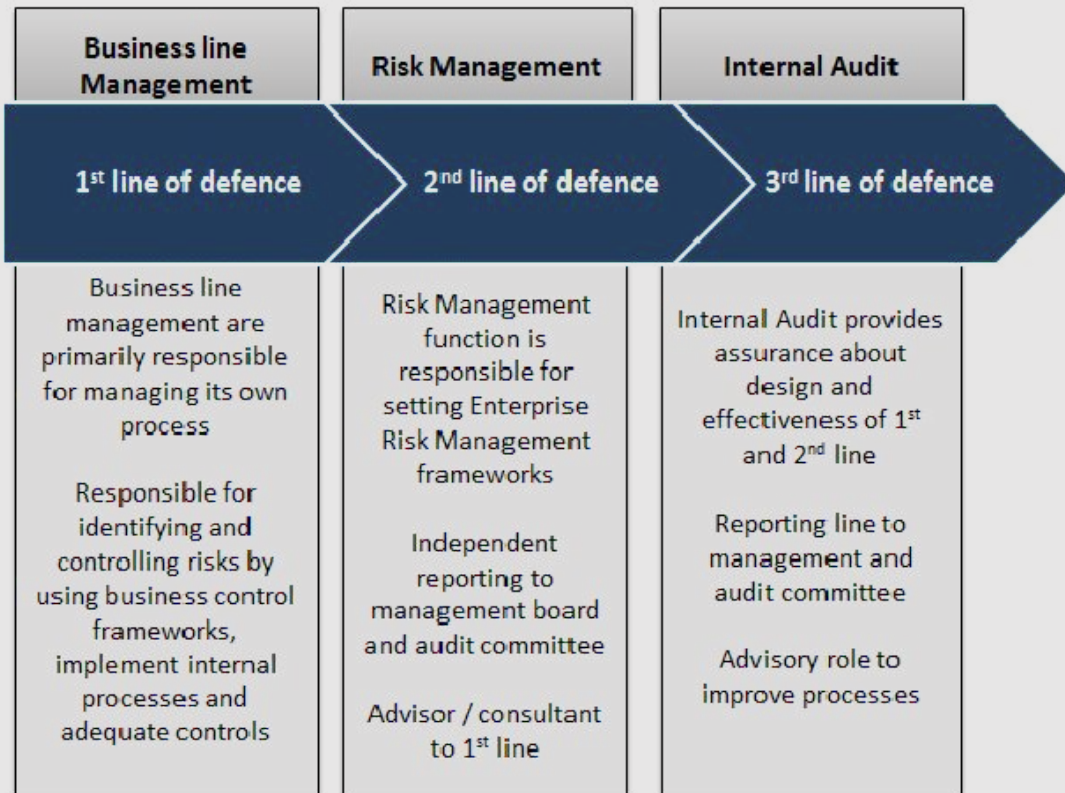
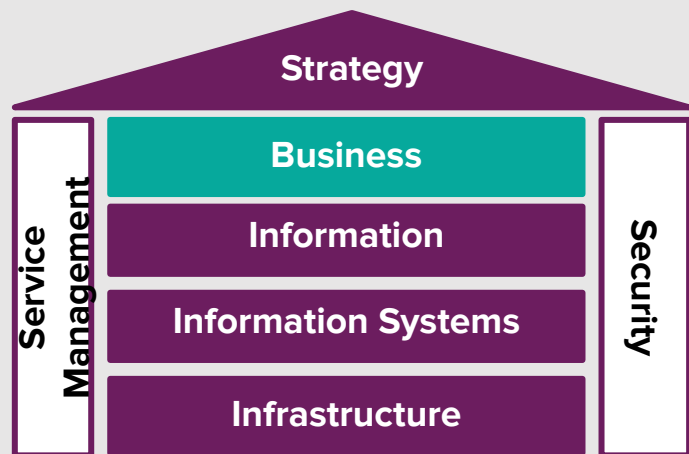
Business is responsible for the product life cycle



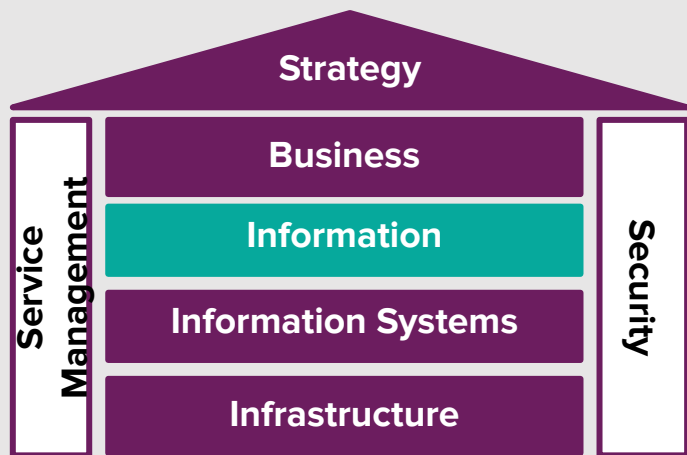
Business that organizes itself via Enterprise Governance



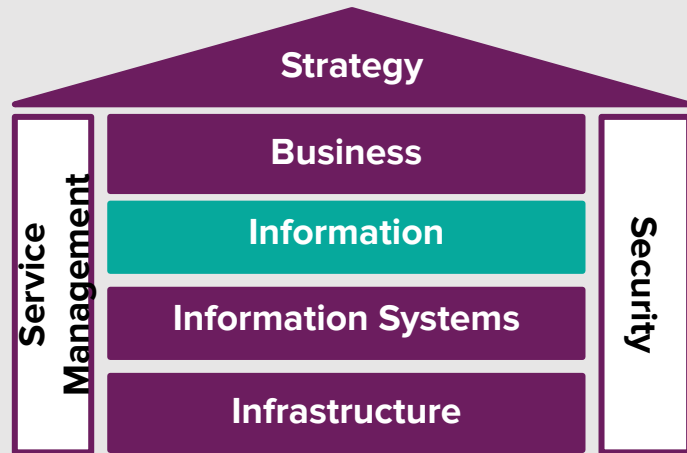
Three levels of defence for quality assurance in your business



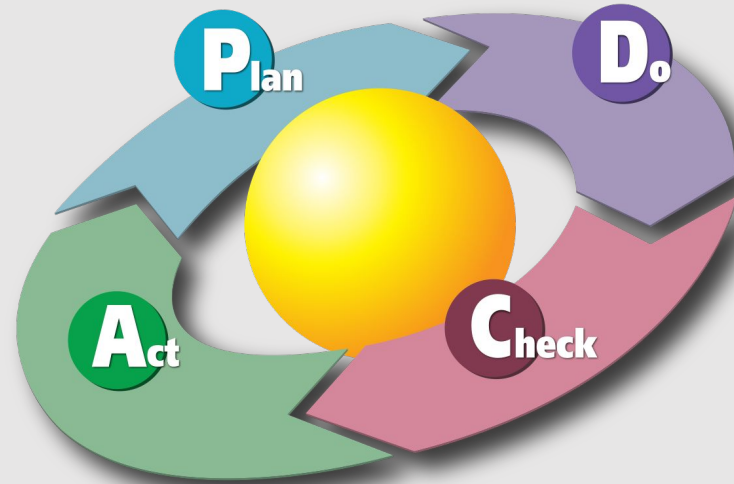
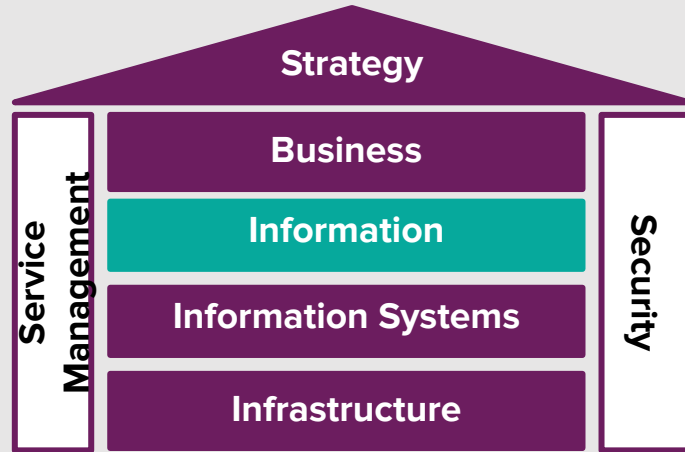
Information needed in process to deliver products and services



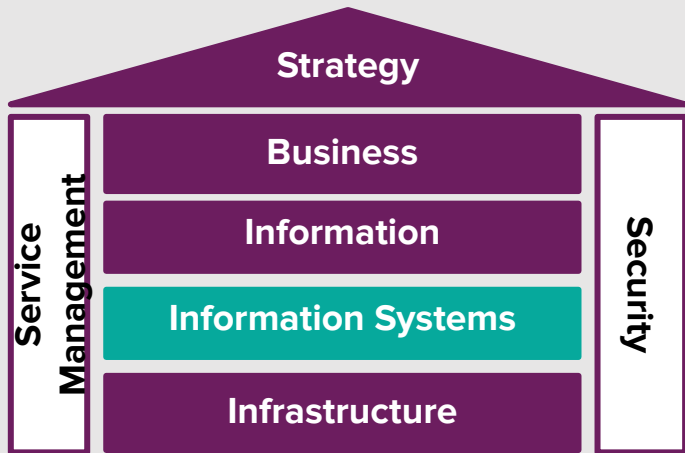
Information quality can lead to for example: identity mix-ups



Best way to improve (information) quality is the Deming Circle



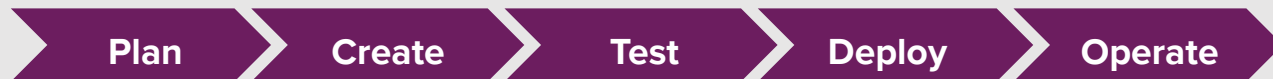
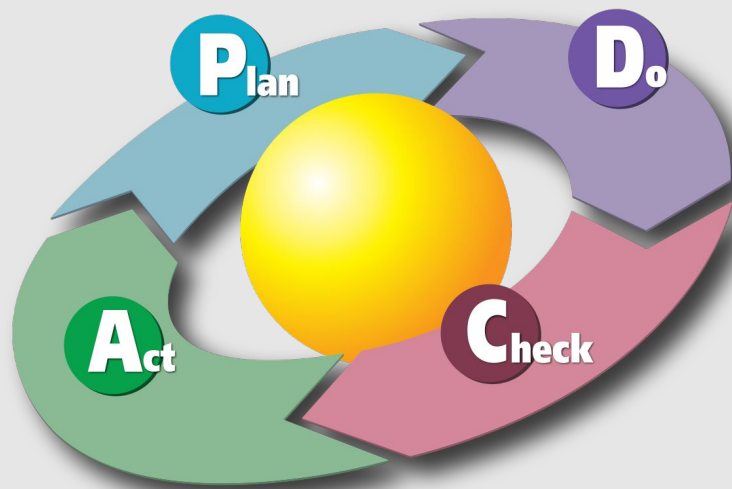
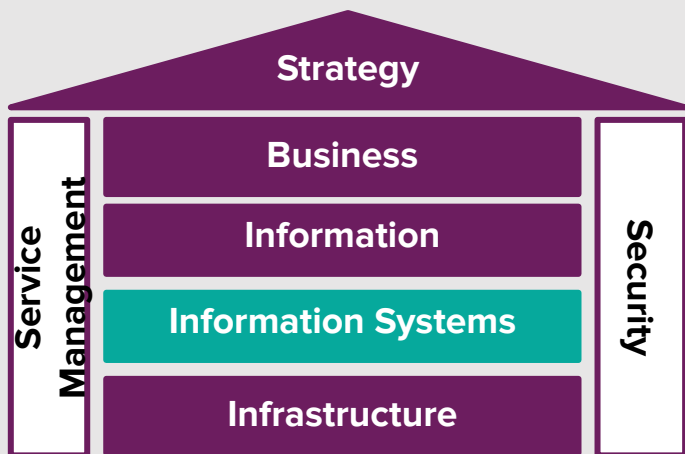
Information Systems needed to store, sort and deliver information



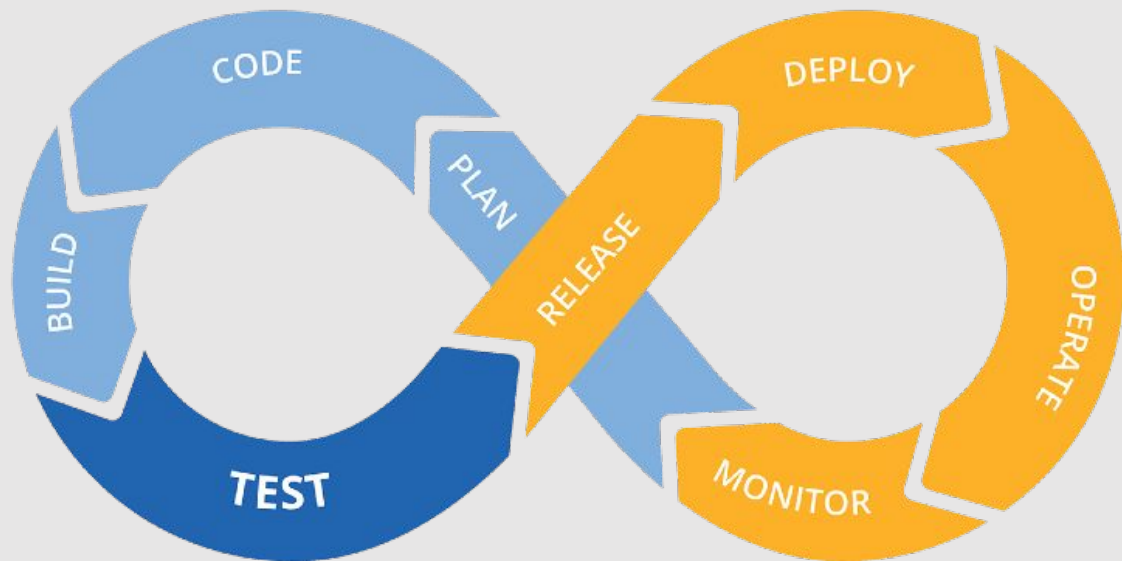
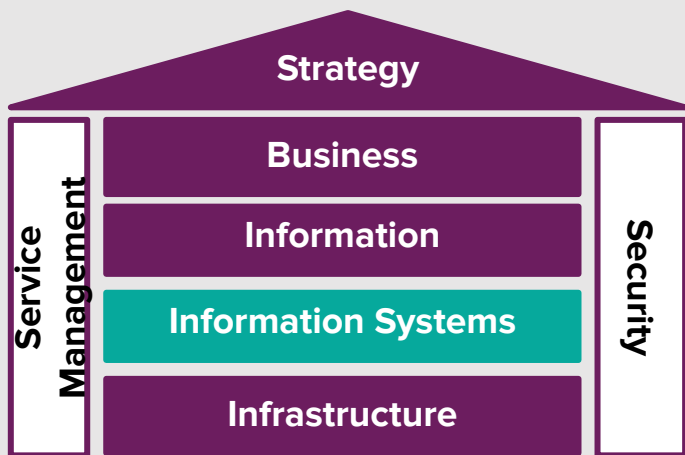
Xebia



Improve IT systems (security) by Deming + Product LifeCycle



Deming and Product LifeCycle combined as Software LifeCycle



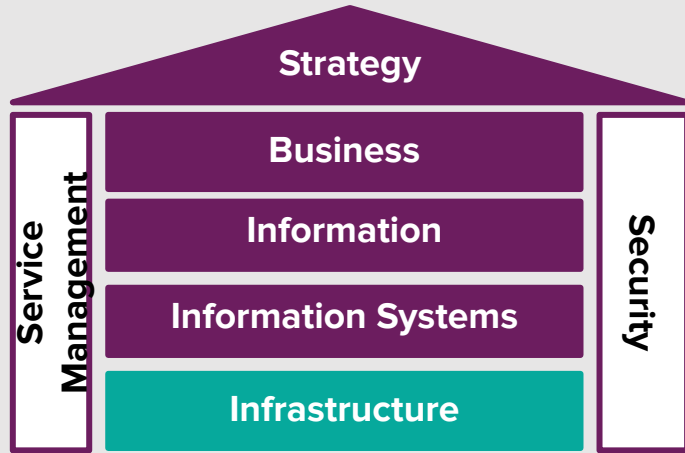
1 <https://www.linkedin.com/pulse/governance-cloud-world-david-das-neves>

2 <https://www.linkedin.com/pulse/devsecops-paradoxon-david-das-neves>

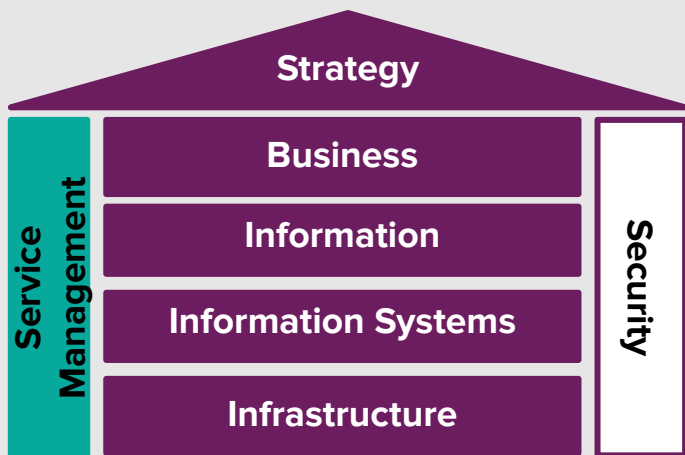
3 <https://xebia.com/the-shift-left-fallacy>



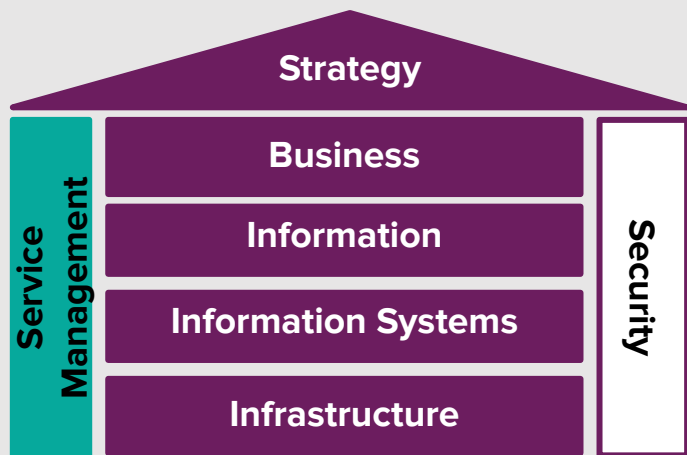
Infrastructure where informations systems can run and live



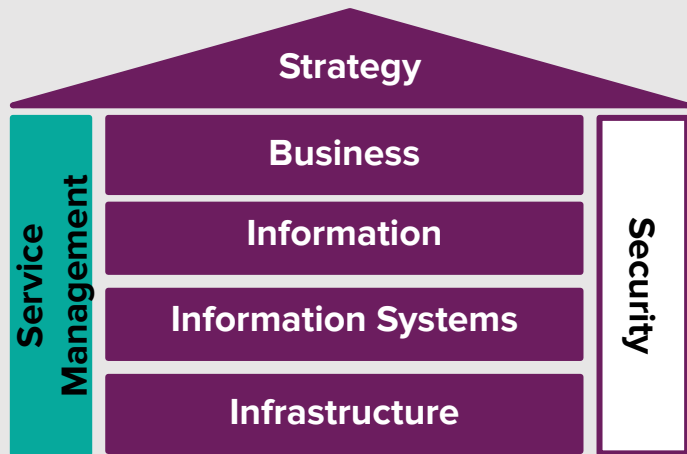
Service Management is active on all layers



Service Management is active on all layers - Facilitate Buildings



Service Management is active on all layers - Facilitate Learning



SECURITY TOOLS



CIA(S) is old-school but still used in information security



CIA(S) is old-school but still used in information security

Confidentiality is improved by:

- 1) **Determine** how public the information is.
- 2) **Apply** access restrictions.
E.g. Key & Lock
- 3) **Apply** read restrictions.
E.g. apply encryption
- 4) **Re-design** so that information has a lower confidentiality rating -> this is a win!



CIA(S) is old-school but still used in information security

Confidentiality is improved by:

Start with using an Authenticator App and unique passwords via a password manager.



CIA(S) is old-school but still used in information security

Integrity is improved by:

- 1) **Determine** the impact of bad (data) quality.
- 2) **Apply** fingerprinting to detect (data) manipulation.
- 3) **Apply** access restrictions. E.g. Key & Lock
- 4) **Re-design** so that bad quality does not impact the function of the system. -> this is a win!



CIA(S) is old-school but still used in information security

Integrity is improved by:

Start with using by using
a login before all
information



CIA(S) is old-school but still used in information security



Availability is improved by:

- 1) **Determine** the impact of stuff (information) not available.
- 2) **Apply** redundant systems to become resilient.
- 3) **Apply** redundant processes to have options.
- 4) **Re-design** so that unavailability does not impact the function of the system. -> this is a win!



CIA(S) is old-school but still used in information security

Availability is improved by:

**One source is no source.
Two sources is a start.
Always have options.**



CIA(S) is old-school but still used in information security

Safety is about reducing risks of assets being in wrong hands.

- 1.) **Design** a threat-model on your manufacturing assets including your supply chain.
- 2.) **Select** trusted suppliers.
- 3.) **Re-design** your maintenance process.
- 4.) **Re-design** your manufacturing process to minimize impact.



CIA(S) is old-school but still used in information security

Safety is about reducing risks of assets being in wrong hands.

Assume you are already breached. This is known as zero-trust.



CIA(S) is old-school but still used in information security

Summary:

It is about trust!

Who do you trust?



How to improve your personal security fitting to you own CIA(S)

Watch Your Hack



Are you worried your ex might have invaded your Facebook account? That your computer is being held hostage by ransomware? Or that hackers are pillaging your bank account?

contents: [what are hackers](#) . [the basics](#) . [computers](#) . [phones & tablets](#) . [social media](#) . [chatting & phone calls](#) . [advanced](#) . [closing notes](#)



Xebia



ROSI = RETURN ON SECURITY INVESTMENT

The ROSI assessment defines in a quantitative way³ how much loss you avoid thanks to your investment, considering several components of risk.

$$\text{ROSI (\%)} = \frac{\text{ALE} * \text{Mitigation Ratio} - \text{Cost of Solution}}{\text{Cost of Solution}}$$

Quantitative Risk Assessment Formula

Figure 2.3 ROSI Formula [13]

Where:

- **Risk Exposure** = Annual Loss Exposure (**ALE**)
- **ALE** = Single Loss Exposure (**SLE**) * Annual Rate of Occurrence (**ARO**)
- **SLE** = Estimated cost of a negative security event
- **ARO** = Estimated probability of the negative security event occurring in a year



ROSI = RETURN ON SECURITY INVESTMENT

Example 1:

The Acme Corp. is considering investing in an anti-virus solution. Each year, Acme suffers 5 virus attacks (ARO=5). The CSO estimates that each attacks cost approximately 15.000 € in loss of data and productivity (SLE=15.000). The anti-virus solution is expected to block 80% of the attacks (Mitigation ratio=80%) and costs 25.000€ per year (License fees 15.000€ + 10.000€ for trainings, installation, maintenance etc.).

The Return on security investment for this solution is then calculated as follow:

$$ROSI = \frac{(5 * 15000) * 0.8 - 25000}{25000} = 140\%$$

According to this ROSI calculation, this anti-virus solution is a cost-effective solution.



EU LAW vs US LAW KILLED THE (US) CLOUD



BE CAREFUL WITH YOUR INVESTMENT



Public DPIA (NL) on Teams, Sharepoint, Azure AD, Zoom, etc



SURF

Table 4: Overview of US law that can be used to obtain personal data from EU Customers

US law enforcement and court orders	Type of authority, type of data	US secret services surveillance	Type of authority, type of data
Non-Disclosure orders can be issued up to one year ¹²³ and have become 'commonplace'. ¹²⁴ No principled restrictions on transparency reporting		Non-disclosure orders or general secrecy requirements. Transparency reporting is only permitted in ranges. ¹²⁵	
US Stored Communications Act, also allows for preservation orders for specific records/evidence ¹²⁶	Content Data: warrant signed by a judge. Requires <i>probable cause</i> .	Executive Order of the President (E.O.) 12333 as amended (limited) by Presidential Policy Directive (PPD) 28. ¹²⁷ Since January 2021	Does not give direct authority to NSA to order cloud providers to hand-over data, but allows for bulk
	Non-Content Account Data (for example names and IP-addresses) ¹²⁹		



Xebia



US Laws and EU Laws



Patriot Act 1

Patriot Act 2

Cloud Act



GDPR

Data Act

Data Governance Act

Wikileaks

Safe Harbor agr.

Privacy Shield agr.

<http://arno.uvt.nl/show.cgi?fid=155021>
<https://privacyplan.net/privacy-datasets/privacy-legislation-grid>
<https://www.ionos.co.uk/digitalguide/server/know-how/what-is-gaia-x>
<https://thelawreviews.co.uk/title/the-privacy-data-protection-and-cybersecurity-law-review/usa>
https://www.stiftung-nv.de/sites/default/files/snv_solving_the_transatlantic_data_dilemma.pdf
<https://policyreview.info/articles/analysis/mitigating-risk-us-surveillance-public-sector-services-cloud>
<https://tweakers.net/reviews/9990/privacy-shield-20-en-datatransfers-beschermt-dit-wel-tegen-surveillance.html>



Xebia



Wikileaks & der Spiegel showed that the US act (2013/2014)

Appelbaum: "Snowden proved us right"

Internet activist Jacob Appelbaum is clear: our democracy is endangered because organizations like the NSA have unlimited access to our personal digital data. Many of those present in the Blauwe Zaal agreed with his claim, witness the spontaneous bouts of applause for the final speaker of the symposium Security in Times of Surveillance'.

BY TOM JELTES



Privacy advocate exposes NSA spy gear at gathering

BY RAPHAEL SATTER | Lubbock Avalanche-Journal

LONDON - A well-known privacy advocate has given the public an unusually explicit peek into the intelligence world's tool box, pulling back the curtain on the National Security Agency's arsenal of high-tech spy gear.

Independent journalist and security expert Jacob Appelbaum on Monday told a hacker conference in Germany that the NSA could turn iPhones into eavesdropping tools and use radar wave devices to harvest electronic information from computers, even if they weren't online.

Appelbaum told hundreds of computer experts gathered at Hamburg's Chaos Communications Conference that his revelations about the NSA's capabilities "are even worse than your worst nightmares."

"What I am going to show you today is wrist-slittingly depressing," he said.

Even though in the past six months there has been an unprecedented level of public scrutiny of the NSA and its methods, Appelbaum's claims - supported by what appeared to be internal NSA slideshows - still caused a stir.

https://www.youtube.com/watch?v=QNsePZj_Yks
https://en.wikipedia.org/wiki/Jacob_Appelbaum
<https://www.cursor.tue.nl/en/news/2014/april/appelbaum-snowden-proved-us-right>
https://media.ccc.de/v/31c3_-6258_-_en_-_saal_1_-_201412282030_-_reconstructing_narratives_-_jacob_-_laura_poitras#t=38
https://media.ccc.de/v/30C3_-5713_-_en_-_saal_2_-_201312301130_-_to_protect_and_infect_part_2_-_jacob#t=779
<https://eu.lubbockonline.com/story/news/nation-world/2013/12/31/privacy-advocate-exposes-nsa-spy-gear-gathering/15060892007>



Xebia



Schrems court case proved that US Law and EU law are no friends



“Maximilian Schrems (born 1987) is an Austrian activist, lawyer, and author who became known for campaigns [starting as a student] against Facebook for its privacy violations, including violations of European privacy laws and the alleged transfer of personal data to the US National Security Agency (NSA) as part of the NSA's PRISM program.” - Wikipedia

https://en.wikipedia.org/wiki/Max_Schrems
<https://www.gdprsummary.com/schrems-ii>
https://en.wikipedia.org/wiki/EU%E2%80%93US_Privacy_Shield
https://en.wikipedia.org/wiki/General_Data_Protection_Regulation
<https://projectmoore.com/schrems-ii-implications-for-your-organisation>
<https://iapp.org/news/a/why-this-french-court-decision-has-far-reaching-consequences-for-many-businesses>
<https://www.schoenherr.eu/content/landmark-decision-in-austria-use-of-google-analytics-found-to-breach-gdp>



Xebia



EU LAW VS US LAW

KILLED THE (US) CLOUD

→ BE CAREFUL WITH YOUR INVESTMENT



Xebia



Witch, Please

Book 6, Ep. 5 | Security Theatre



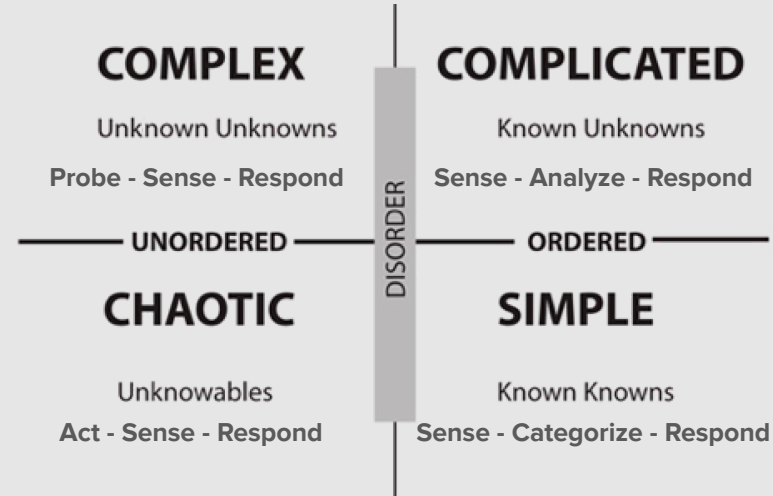
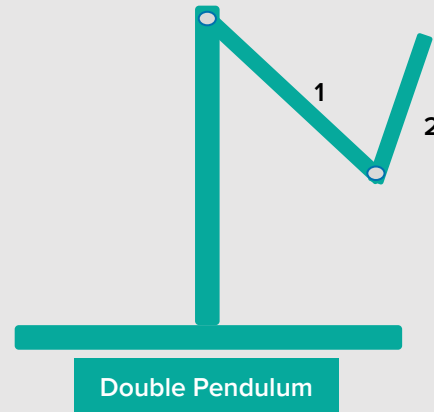
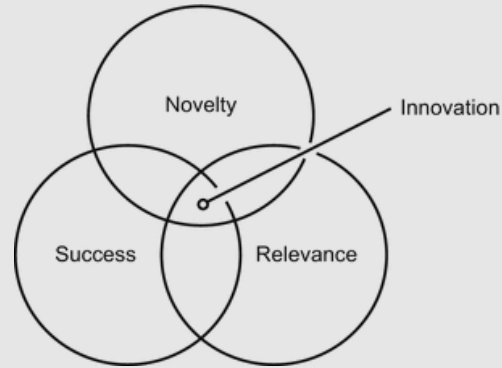
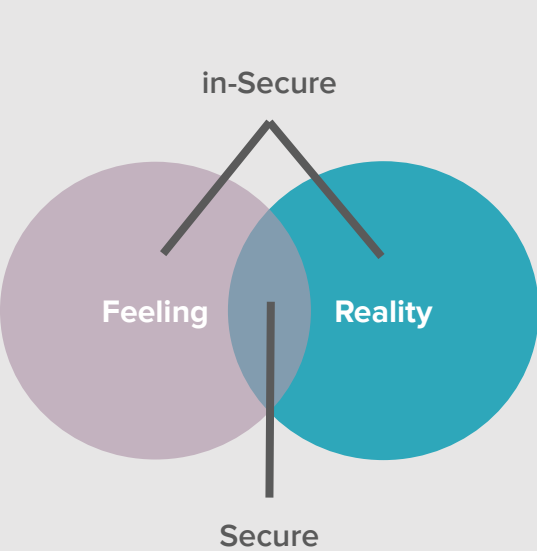
<https://www.ohwitchplease.ca>
<https://play.acast.com/s/oh-witch-please/book-6-ep-6-security-theatre>
<https://open.spotify.com/episode/7GTb7PHP8NXlw7eg067Y2F?si=r9iHlapyQT6JCJ9v71TBWw&nd=1>



Xebia



To become more secure, make sense of your context and respond



<https://zenodo.org/record/3719389>
<https://www.researchgate.net/publication/327700356>
https://en.wikipedia.org/wiki/Double_pendulum
<https://doi.org/10.1108/08944310510556955>
<https://www.researchgate.net/publication/330500755>
<https://ieeexplore.ieee.org/abstract/document/5386804>
<https://thecynefin.co/library/cynefin-weaving-sense-making-into-the-fabric-of-our-world>
https://www.systemswisdom.com/sites/default/files/Snowdon-and-Boone-A-Leader's-Framework-for-Decision-Making_0.pdf



Xebia



emBRACE CHAOS

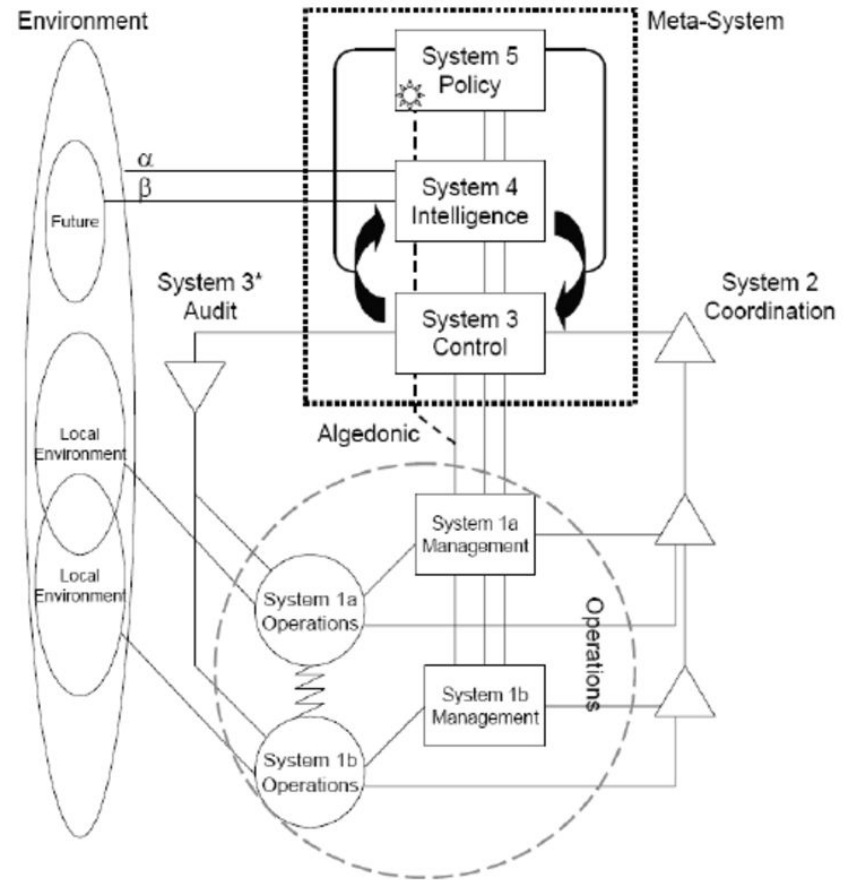
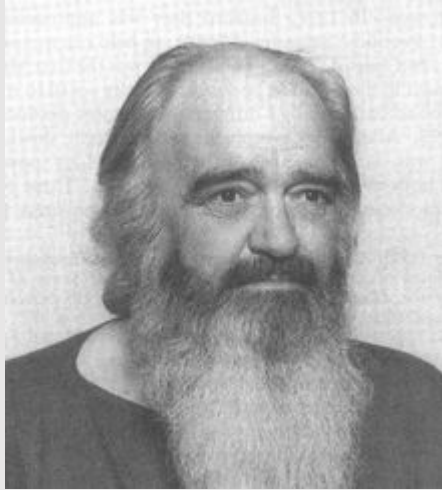
BONUS SLIDES



Xebia

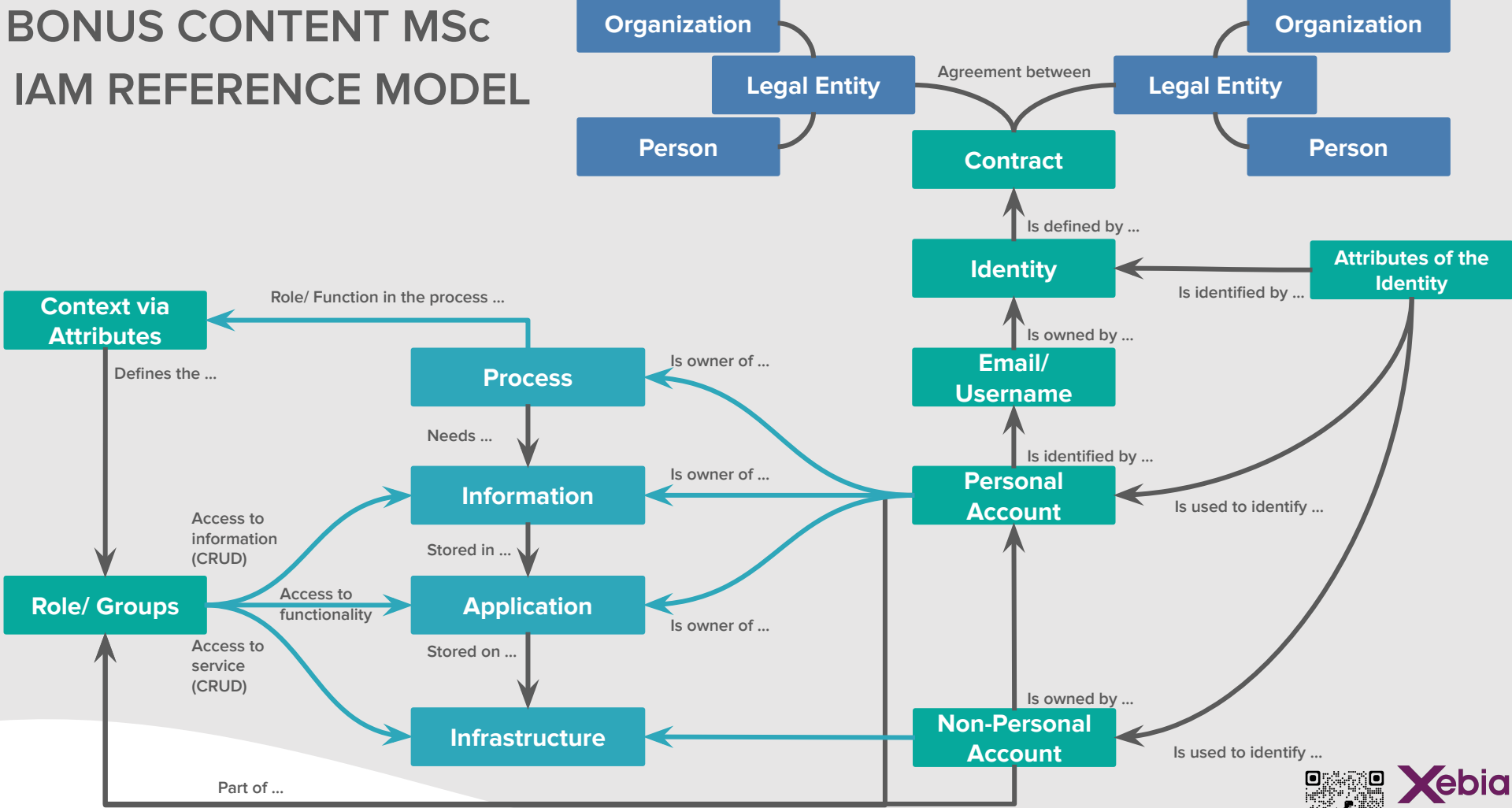


Stafford Beer - Viable Systems Model

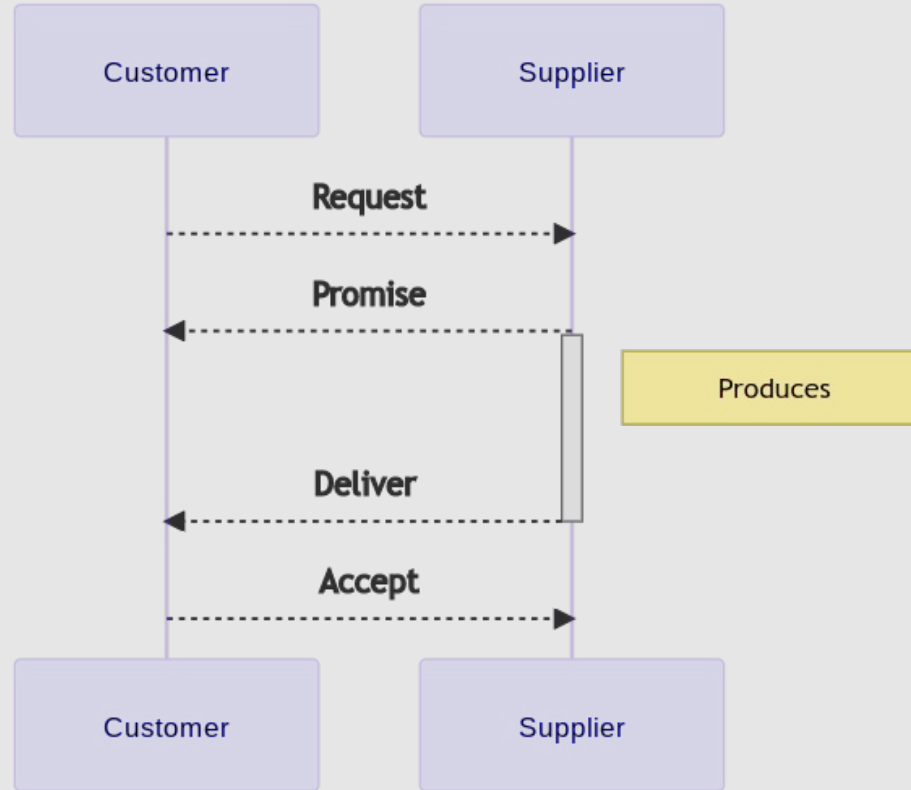


BONUS CONTENT MSc

IAM REFERENCE MODEL



TRANSACTION AS FABRIC OF OUR REALITY



BONUS CONTENT MSc



Xebia



View on reality determines your scientific approach

Tips, for who is going to do their master,
regarding viewpoint on reality:

- (1) Read-up on post-modernism and the alternatives to it, and
- (2) plato.stanford.edu is a great resource.



Affordance is the new way to look at Business & IT

Jan Recker wrote a great book on
MSc research
& is responsible for a great overview
on research methodologies:
<https://aisnet.org/page/ISResearch>



A screenshot of a podcast player interface. On the left is a blue square icon with a black headset and the text "this IS research". To the right, the title "Affordances is the new TAM" is displayed. Below the title, it says "Update: 2021-10-13" followed by a heart icon and the number "1". At the bottom, there are two orange-outlined buttons: a circular play button with two vertical bars (currently showing a pause symbol) and a rectangular "Share" button with a red arrow icon.

