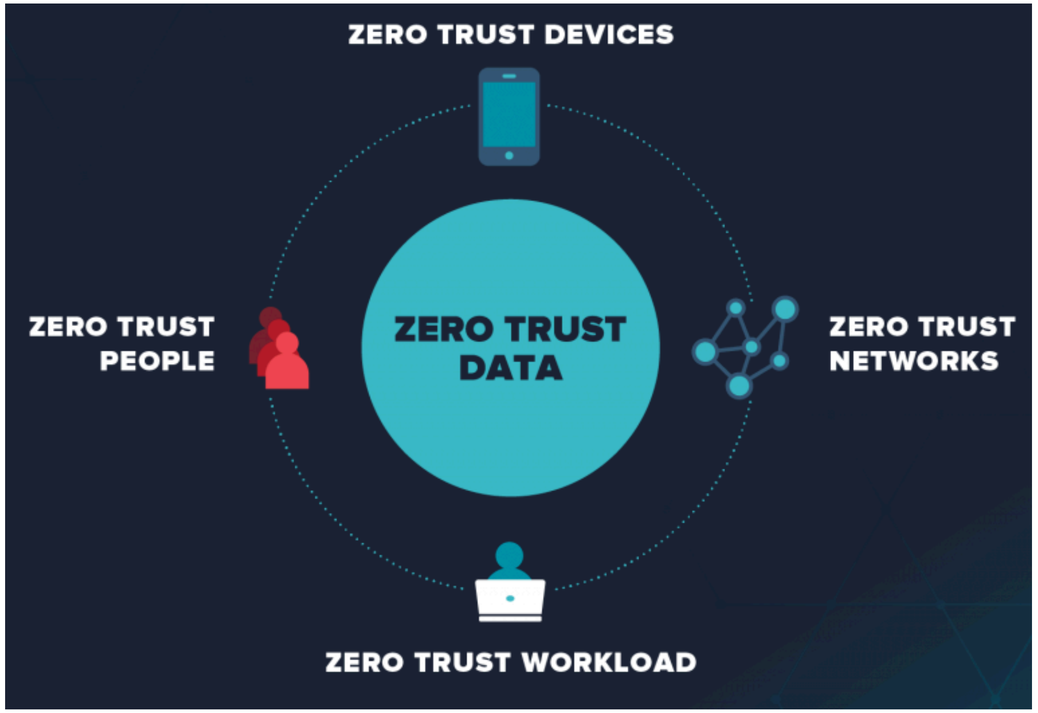
UNIVERSITY OF OSLO

TEK5530 Measurable Security for the Internet of Things

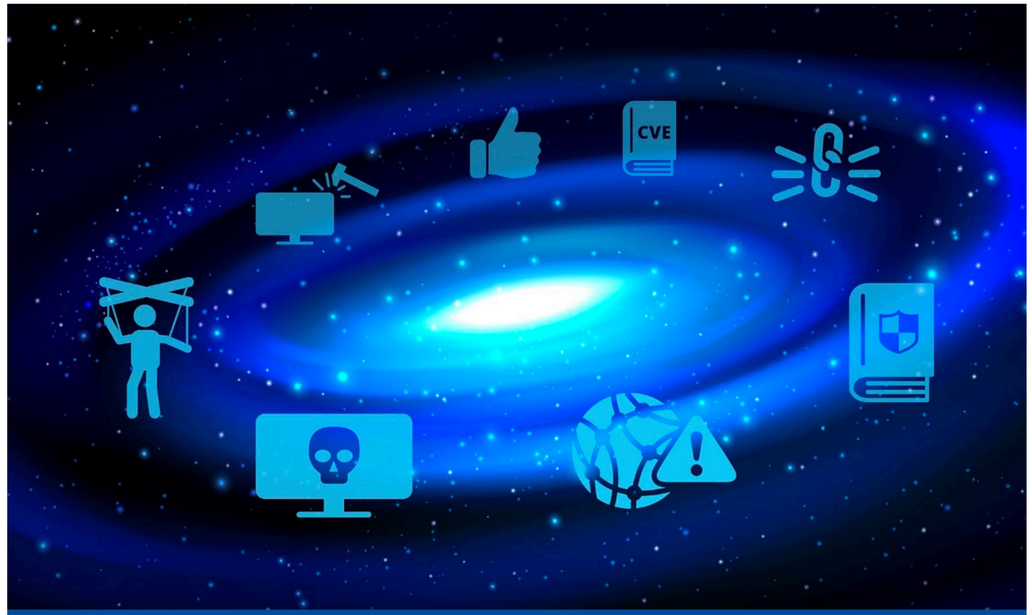
L11 - Zero Trust Architecture



[Source: Varonis - https://dtc1.com/how-to-set-up-a-zero-trust-network/]

Josef Noll
Professor
Department of Technology Systems

UNIVERSITY
OF OSLO

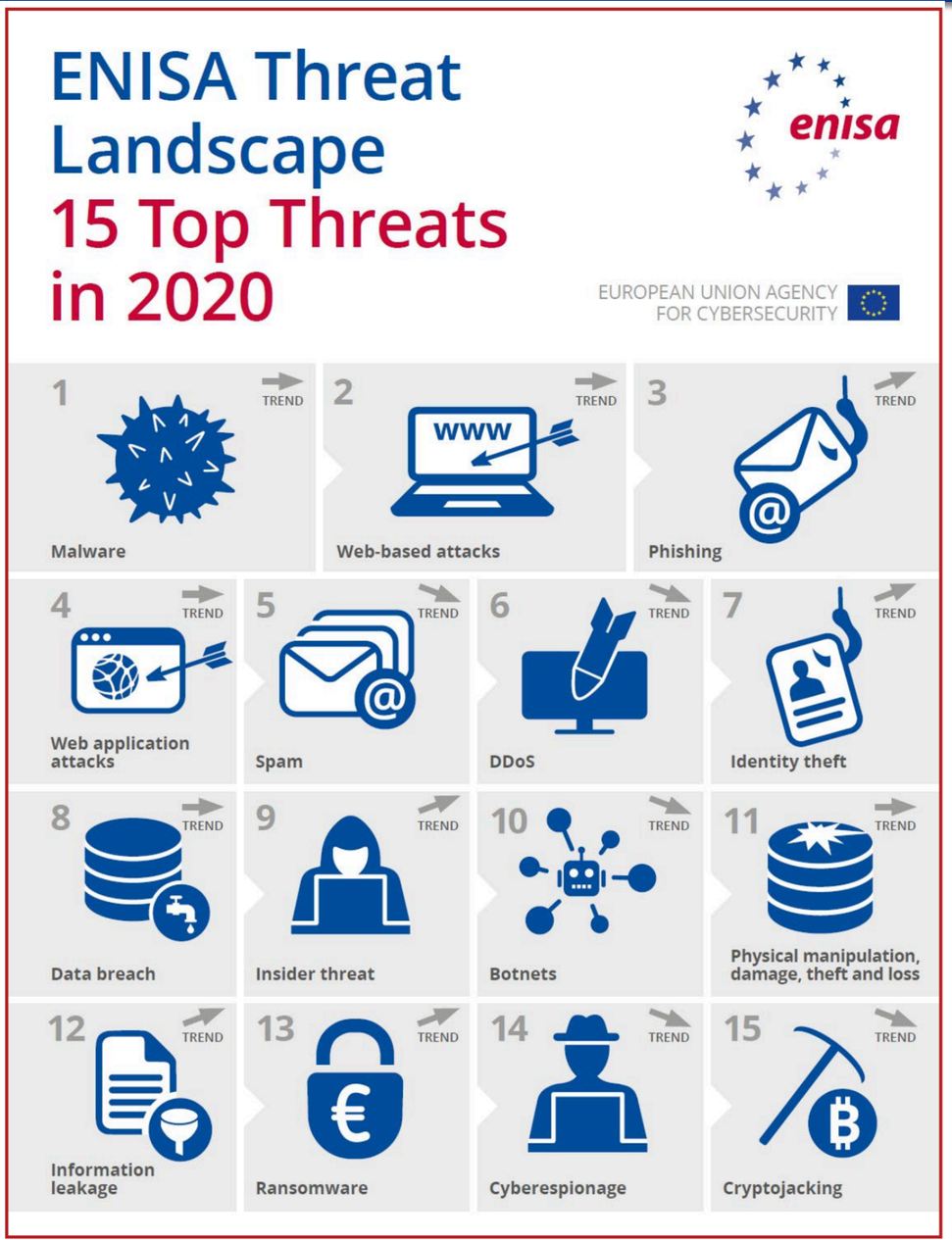


ENISA THREAT LANDSCAPE 2023

July 2022 to June 2023

OCTOBER 2023

EUROPEAN UNION AGENCY FOR CYBERSECURITY



July 2022 - June 2023

1. Ransomware 31.3%
2. DDoS 21.4%
3. Data theft 20.1%
4. Malware 8.24%
5. Social Engineering 7.9%
6. Information Manipulation 4.8%
7. Web threats 3%
8. Supply chain 2.1%
9. zero day 0.05%

Objectives

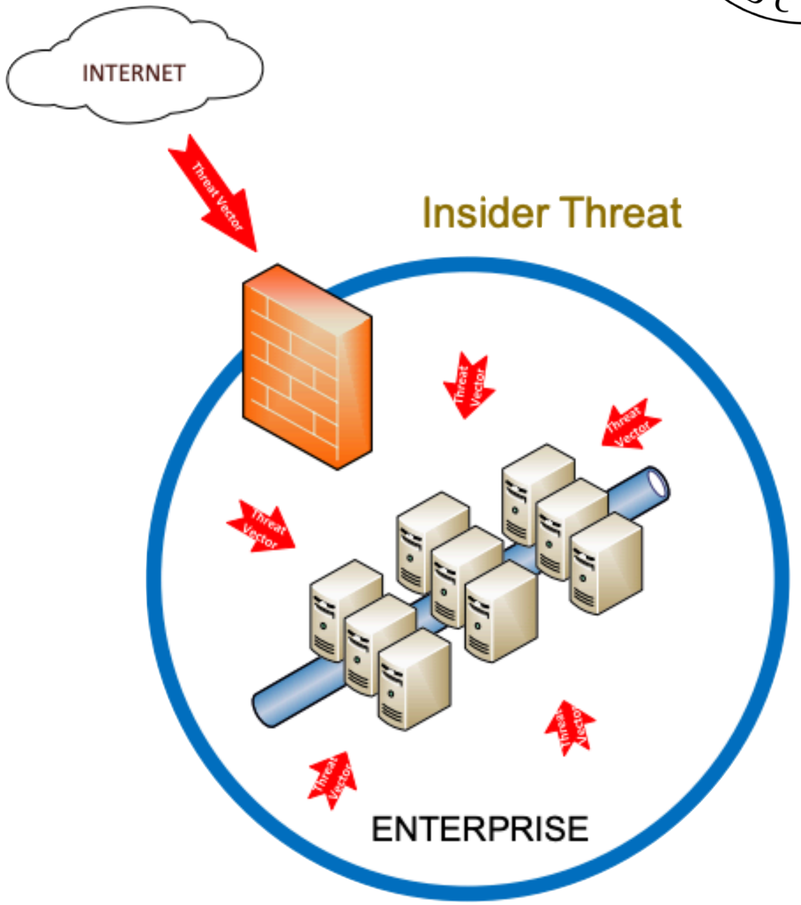
- Explain zero-trust in security
- Why do we talk about “zero trust”?
- Principles
- Domain examples

Consequences/measures for

- roles and responsibilities
- risk analysis
- inventory (rapid assessment of system)
- user training, control, certification
- audits
- monitoring process
- business resumption and continuity plan
- emergency modes
- alert and crisis management
- network segmentation and segregation
- remote diagnosis, maintenance and management
- surveillance and intrusion detection methods
- security approval

Example: Hospital Access

- "hard outside" & "soft inside"
  - once inside, access to everywhere
  - threats: modern cyberattacks, remote access
- No implicit trust
- never trust, always verify



https://csrc.nist.gov/CSRC/media/Presentations/zero-trust-networks-brief/images-media/2-4Kerman%20-%20Zero%20Trust%20Architecture%20-%20NCCoE%20-%202019%20-%20ISPAB.pdf

Zero-trust cloud access

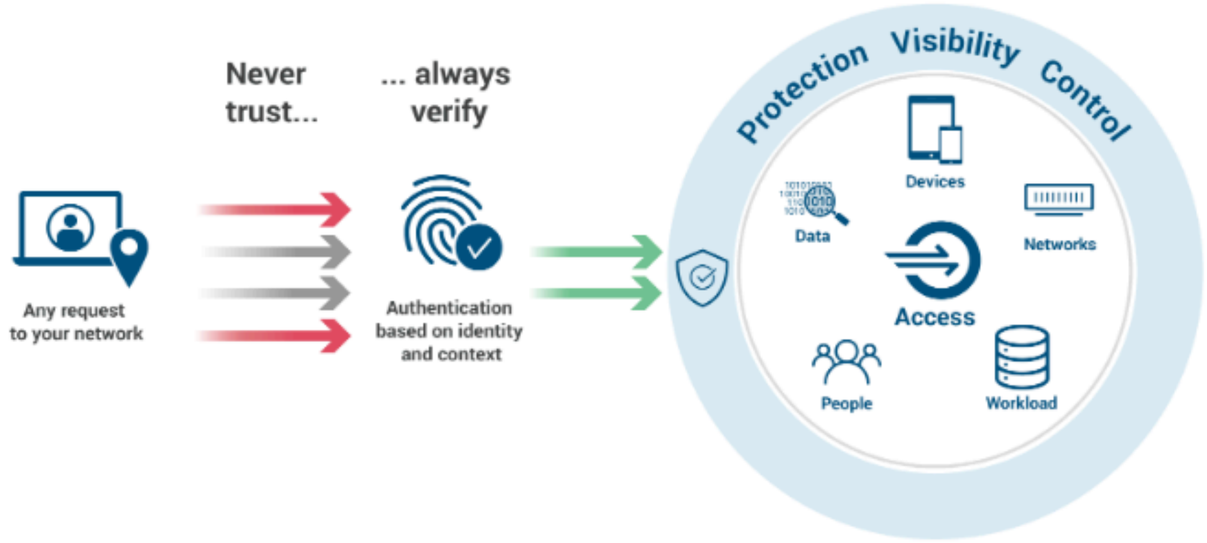
Man steals hundreds of thousands of personal pictures from people's iPhones by pretending to work for Apple

Andrew Griffin • Wednesday 25 August 2021 17:06 BST • Comments

https://www.independent.co.uk/tech/man-steals-hundreds-of-thousands-of-personal-pictures-from-people-s-iphones-by-pretending-to-work-for-apple-b1908693.html

306 victims, 620 k Photos

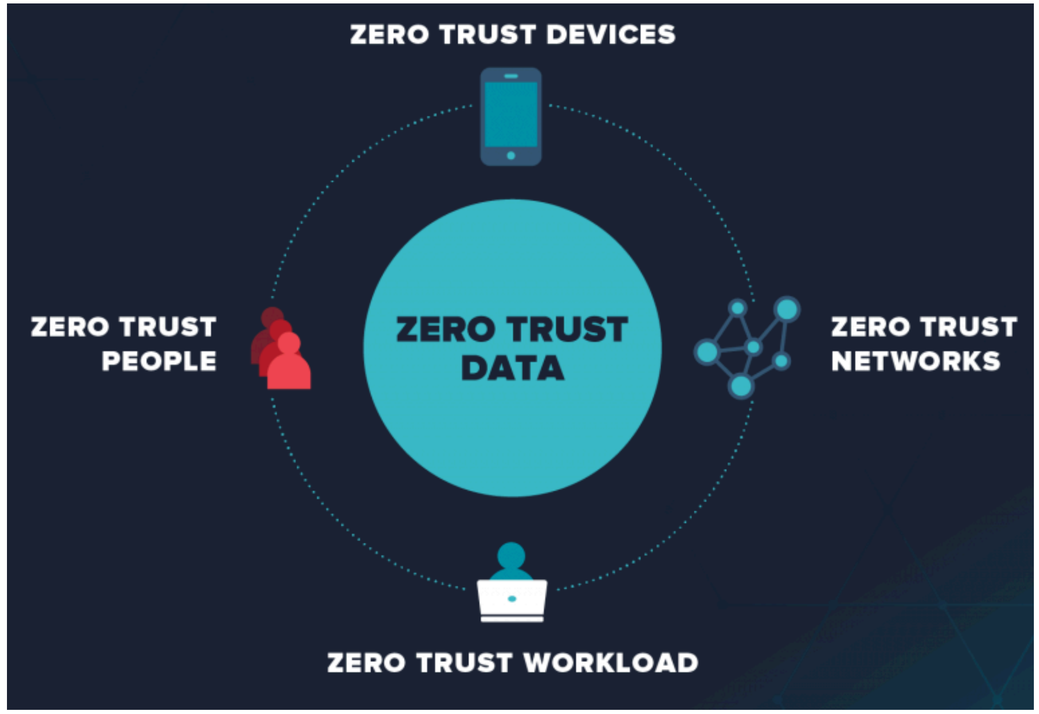
- Cloud sign in
  - always full access



https://dzone.com/articles/implementing-zero-trust-architecture-on-azure-hybr

Principles of Zero Trust

1. All data sources and computing services are considered resources.
2. All communication is secured regardless of network location.
3. Access to individual enterprise resources is granted on a per-connection basis.
4. Access to resources is determined by dynamic policy, including the observable
5. state of user identity and the requesting system, and may include other behavioral attributes.
6. The enterprise ensures all owned and associated systems are in the most
7. secure state possible and monitors systems to ensure that they remain in the most secure state possible.
8. All resource authentication is dynamic and strictly enforced before authorized access is allowed.



NIST Risk Management Framework

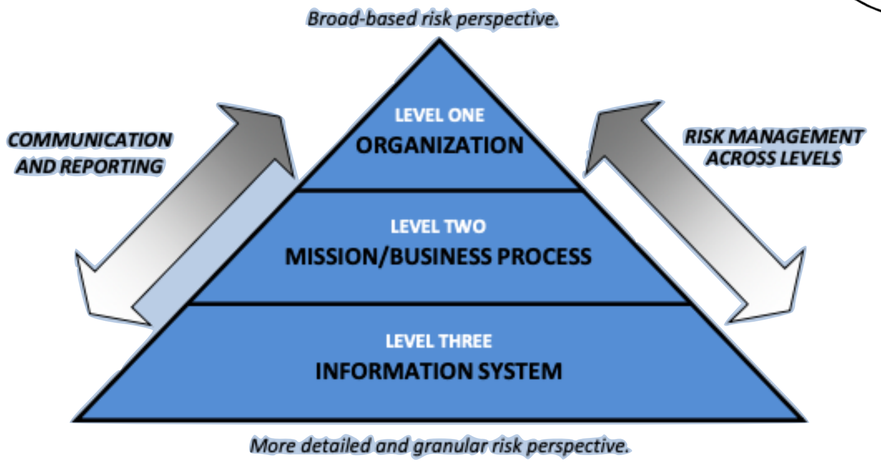
- National Institute of Standards and Technology (NIST)
- Developed by the Computer Security Resource Center (CSRC, USA)
  - https://csrc.nist.gov/projects/risk-management/about-rmf

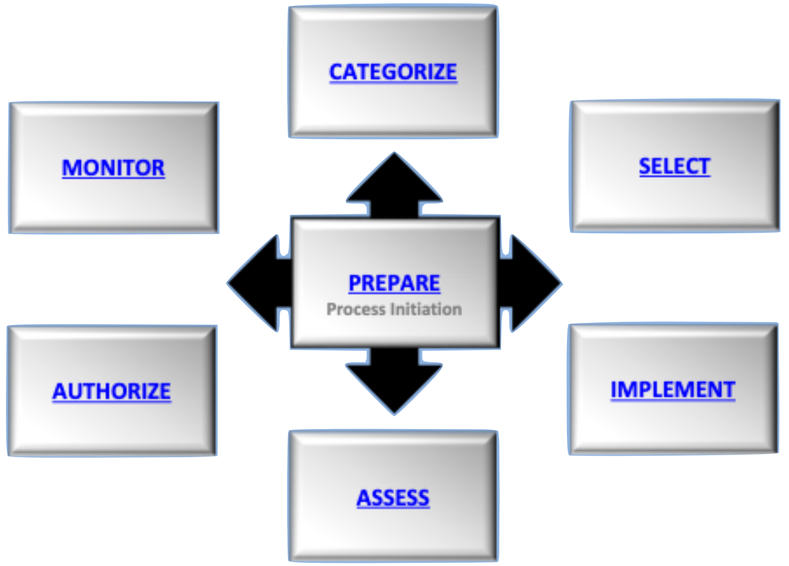
Prepare	Essential activities to **prepare** the organization to manage security and privacy risks
Categorize	**Categorize** the system and information processed, stored, and transmitted based on an impact analysis
Select	**Select** the set of NIST SP 800-53 controls to protect the system based on risk assessment(s)
Implement	**Implement** the controls and document how controls are deployed
Assess	**Assess** to determine if the controls are in place, operating as intended, and producing the desired results
Authorize	Senior official makes a risk-based decision to **authorize** the system (to operate)
Monitor	Continuously **monitor** control implementation and risks to the system

https://csrc.nist.gov/projects/risk-management/about-rmf

Walk-through NIST RMF standard

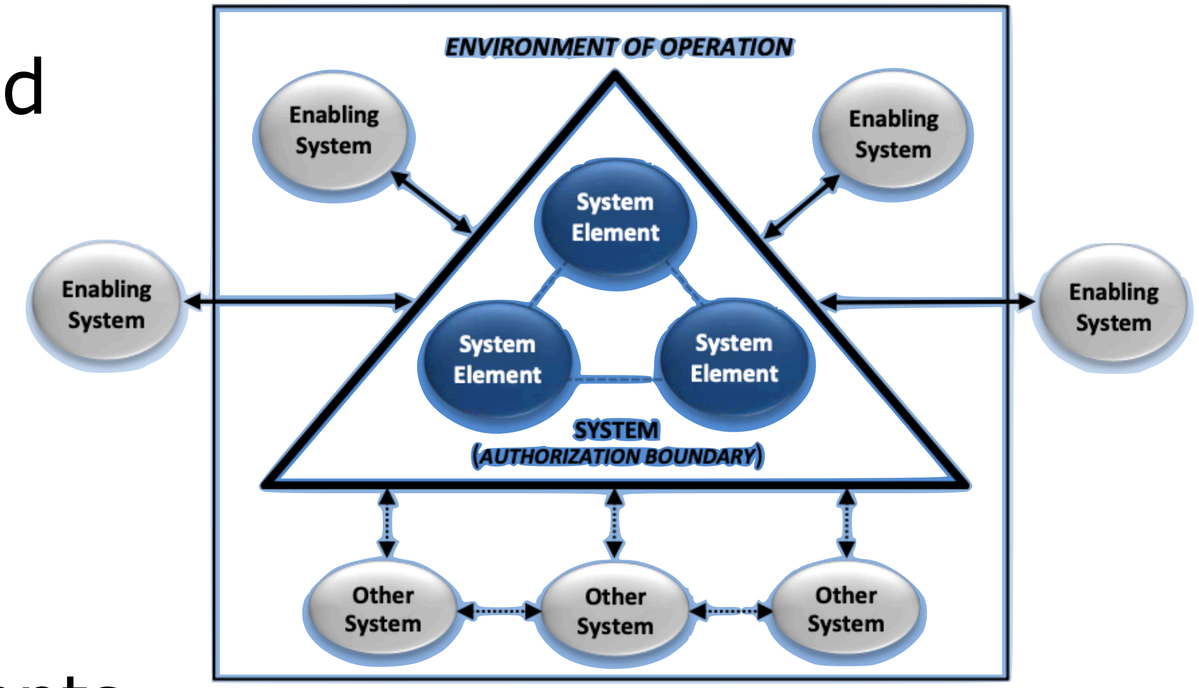
- Publication 800-37v2:
  - https://doi.org/10.6028/NIST.SP.800-37r2
- Relevance for which part of the organisation?
- Prepare (P1-P7):
  - Roles
  - strategy
  - assessment
  - framework (which to follow)
  - control mechanisms
  - impact-level prioritisation
  - continuous monitoring - organisation





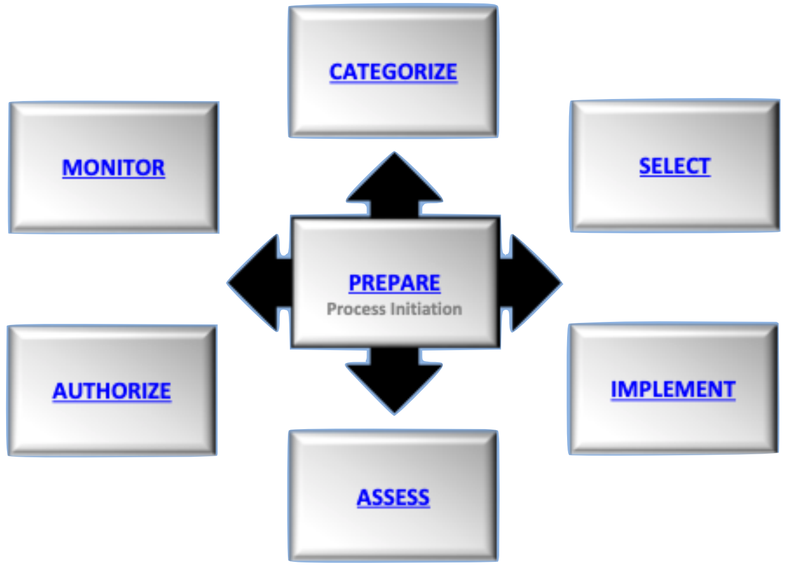
NIST RMF - authorisation boundary

- Modular design of the system and system operation
  - mapping of system
  - “in scope for authorisation”
- Authorisation boundary
  - same business function/mission
  - similar data/information requirements
- Context-dependent



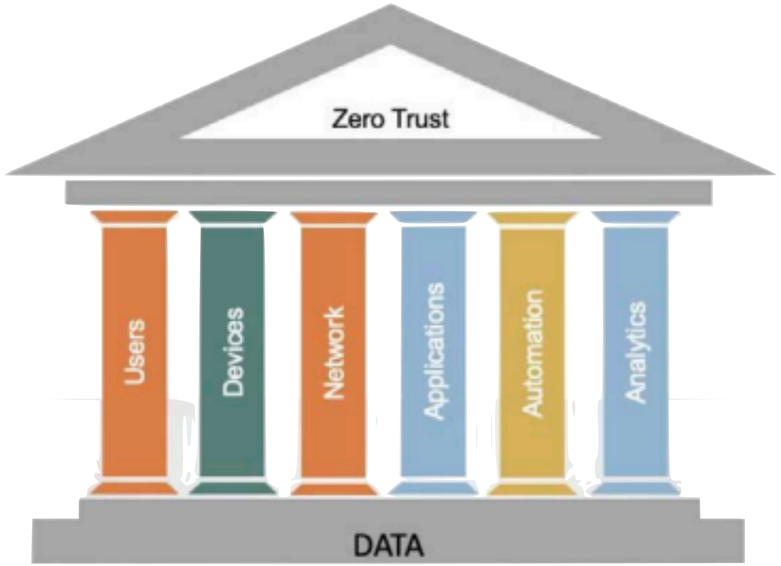
NIST RMF implementation

- Use the tasks and outputs of the Organization-Level and System-Level **Prepare** Step to promote a consistent starting point within organizations to execute the RMF.
- Maximize the use of **common controls** to promote standardized, consistent, and cost-effective security and privacy capability inheritance.
- Maximize the use of **shared** or **cloud-based** systems, services, and applications where applicable, to reduce the number of organizational authorizations.
- Employ **organizationally-tailored control baselines** to increase the speed of security and privacy plan development, promote consistency of security and privacy plan content, and address organization-wide threats.
- Employ **organization-defined controls based** on security and privacy requirements generated from a systems security engineering process.
- Maximize the use of **automated tools** to manage security categorization; control selection, assessment, and monitoring; and the authorization process.
- Decrease the level of effort and resource expenditures for **low-impact systems** if those systems cannot adversely affect higher-impact systems through system connections.
- Maximize the reuse of RMF artifacts (e.g., security and privacy assessment results) for standardized hardware/software deployments, including configuration settings.
- Reduce the **complexity** of the IT/OT infrastructure by eliminating unnecessary systems, system elements, and services — employ least functionality principle.
- Make the transition to **ongoing authorization** and use **continuous monitoring** approaches to reduce the cost and increase the efficiency of security and privacy programs.



NIST RMF system level outcomes (P8-P18)

- Mission or business focus - intended to support
- System stakeholders - identification
- Asset identification - prioritised
- Authorisation boundary - determined
- Information types - identified flows
- Information life cycle - identified and understood
- Risk assessment - completed and updated
- Requirement - security and privacy prioritised
- Enterprise architecture - where is our system?
- Requirement allocation - sec/priv mapping to system
- System registration - registry, management, accountability

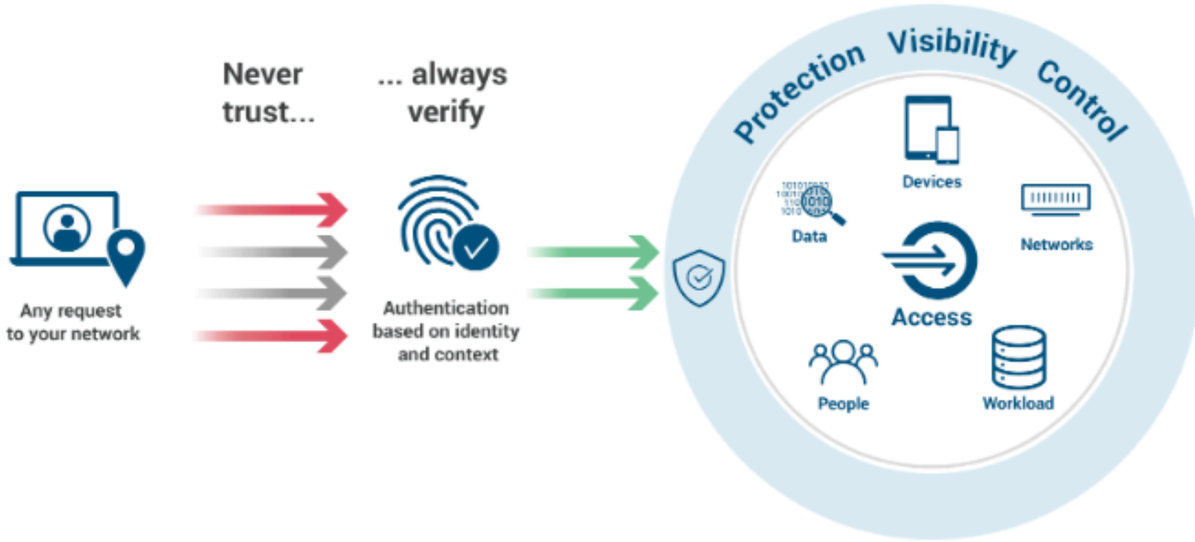


Six Pillars of a Zero Trust Security Model

https://csrc.nist.gov/CSRC/media/Presentations/zero-trust-architecture-101/images-media/Zero%20Trust%20Architecture%20101%20-%20Scott.pdf

Zero-trust cloud access

- Identity & access management
- Access control:
  - Role-Bases Access Control RBAC
  - Attribute-based .. ABAC
  - Semantic Attribute … S-ABAC
- map organisational roles
  - minimum level of access
- build the attribute base



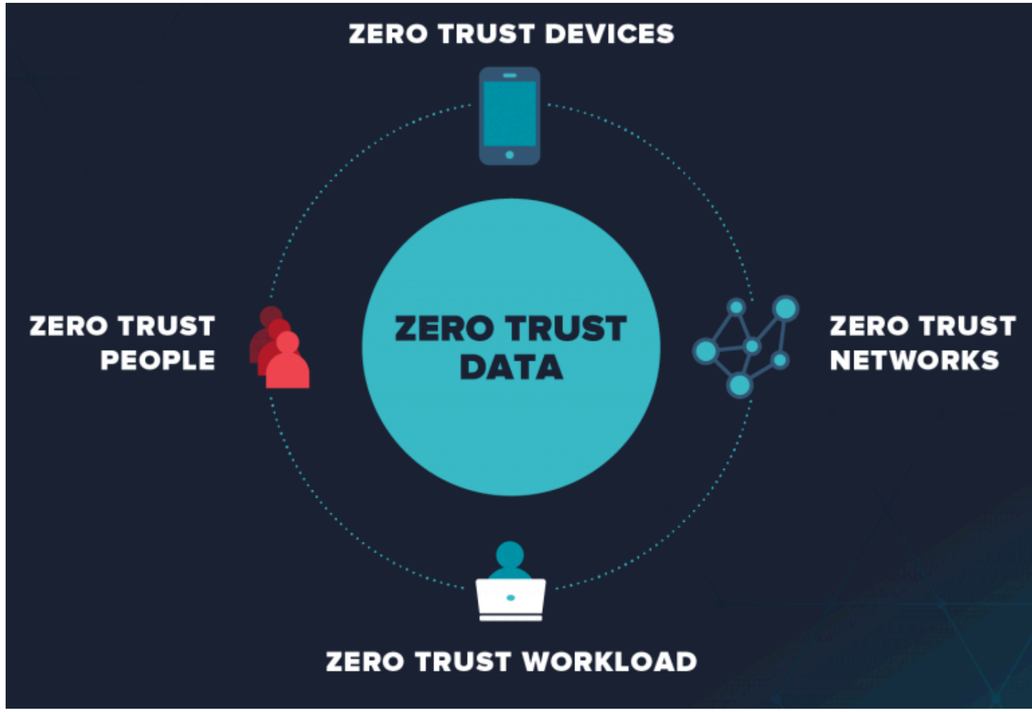
https://dzone.com/articles/implementing-zero-trust-architecture-on-azure-hybr

Zero trust for your Group Work?

- please elaborate

Take away from L11 ZeroTrust Architecture

- Why zero trust
  - "your system is hacked already"
  - "no user or device is trusted until they have proved otherwise"
  - what do you do in case of hacking/ ransomware?
- Domain examples
  - Hospital architecture
  - IT-deployment, docker bases
  - Cloud access



https://dtc1.com/how-to-set-up-a-zero-trust-network/