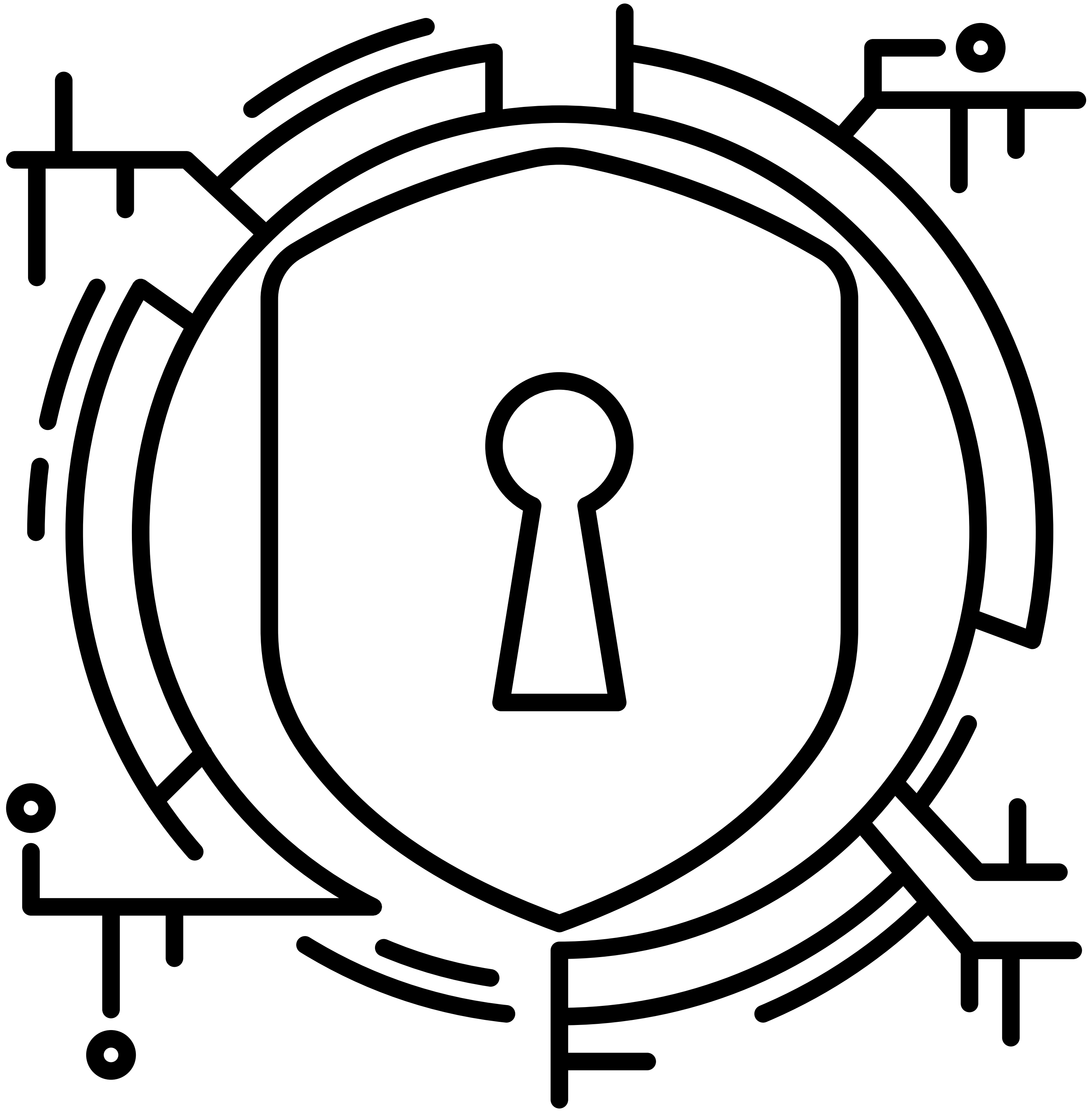
OCTOBER 2023

# SECURITY ARCHITECTURE

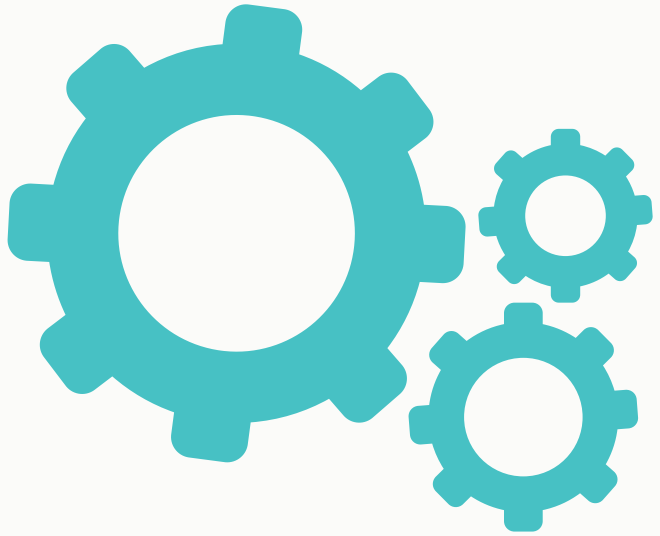
Barbara Krašovec



# TABLE
of contents

# Security Architecture

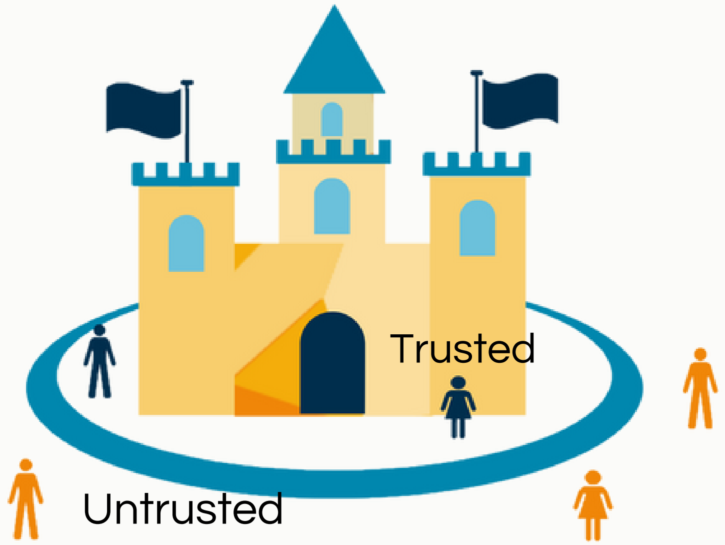
- Security principles, methods and models designed to keep your infrastructure safe,
- security design that addresses potential risks,
- overall system required to protect your infrastructure,
- security controls, policies, procedures, and guidelines.
- building security into system design, implementation and deployment.



# Traditional vs defensible approach

## Traditional security architecture

The focus is on hardening systems against potential risks and on perimeter-based network security. “Castle and moat model*” - the objective is to keep the intruders out, and the supposition that everything inside the network is safe.



*"Castle-and-moat" - network design where the organization's network is seen as a castle and the network perimeter as a moat. Once the drawbridge is lowered and someone crosses it, they have free rein inside the castle grounds.

Image source: https://www.clouddirect.net/a-beginners-guide-to-zero-trust/t

## Defensible security architecture

Ongoing process of adapting security controls and procedures, based on the current risks and threats. It is based on the implementation of fundamental security principles such as zero trust. It is about the design of infrastructure and applications resilient under attack

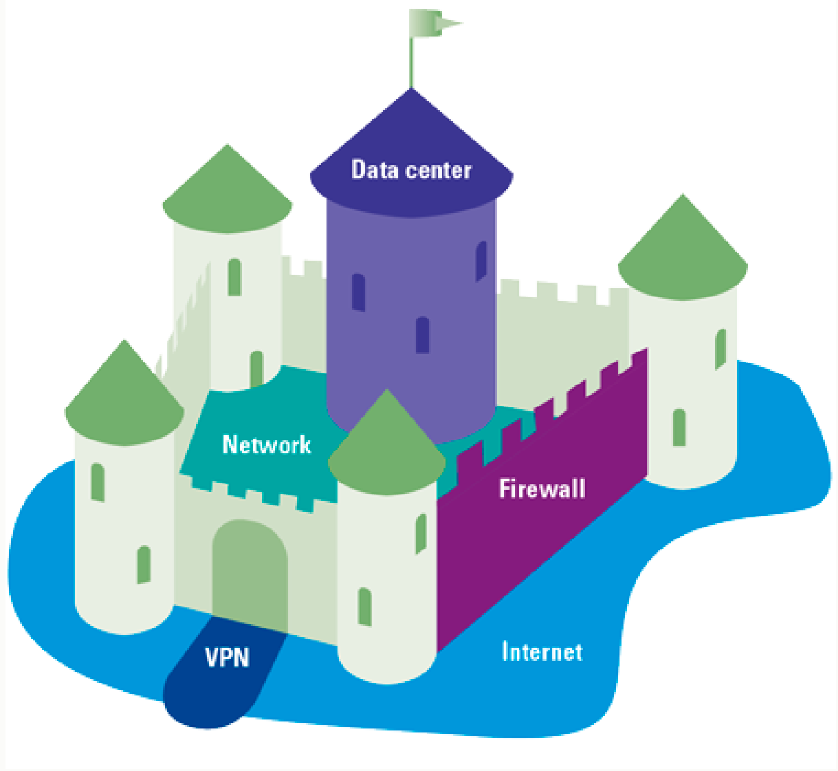
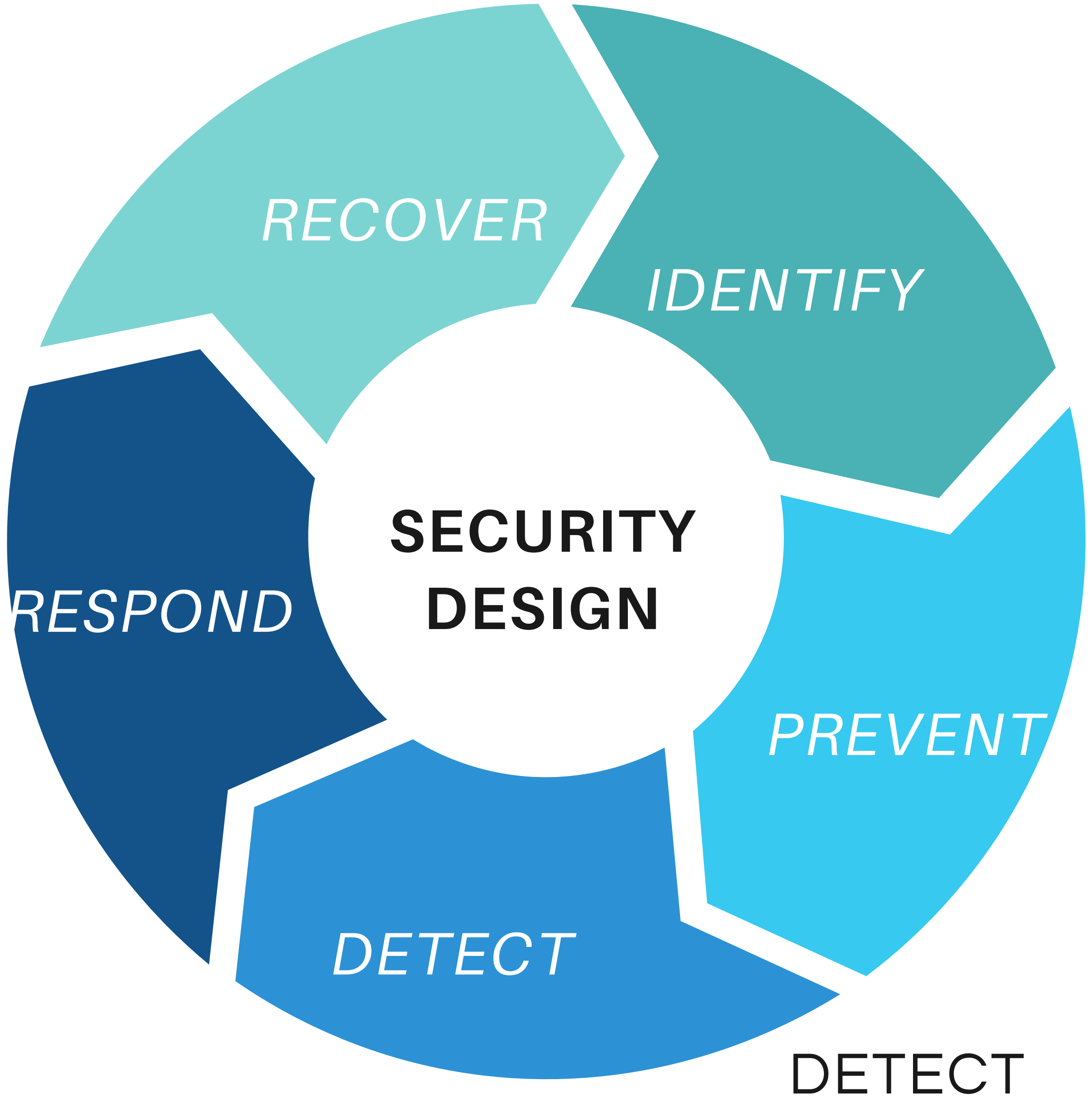


Image source: https://www.compact.nl/articles/zero-trust-beyond-the-hype/

# OBJECTIVES



### IDENTIFY

Understand the system and its operation, the context and potential risks.

### PREVENT

Apply security controls to prevent the risk. Harden and isolate systems.

### DETECT

Provide continuous monitoring and logging to detect anomalies.

### RESPOND

Respond to security incident, investigate system, run analysis, and inform stakeholders.

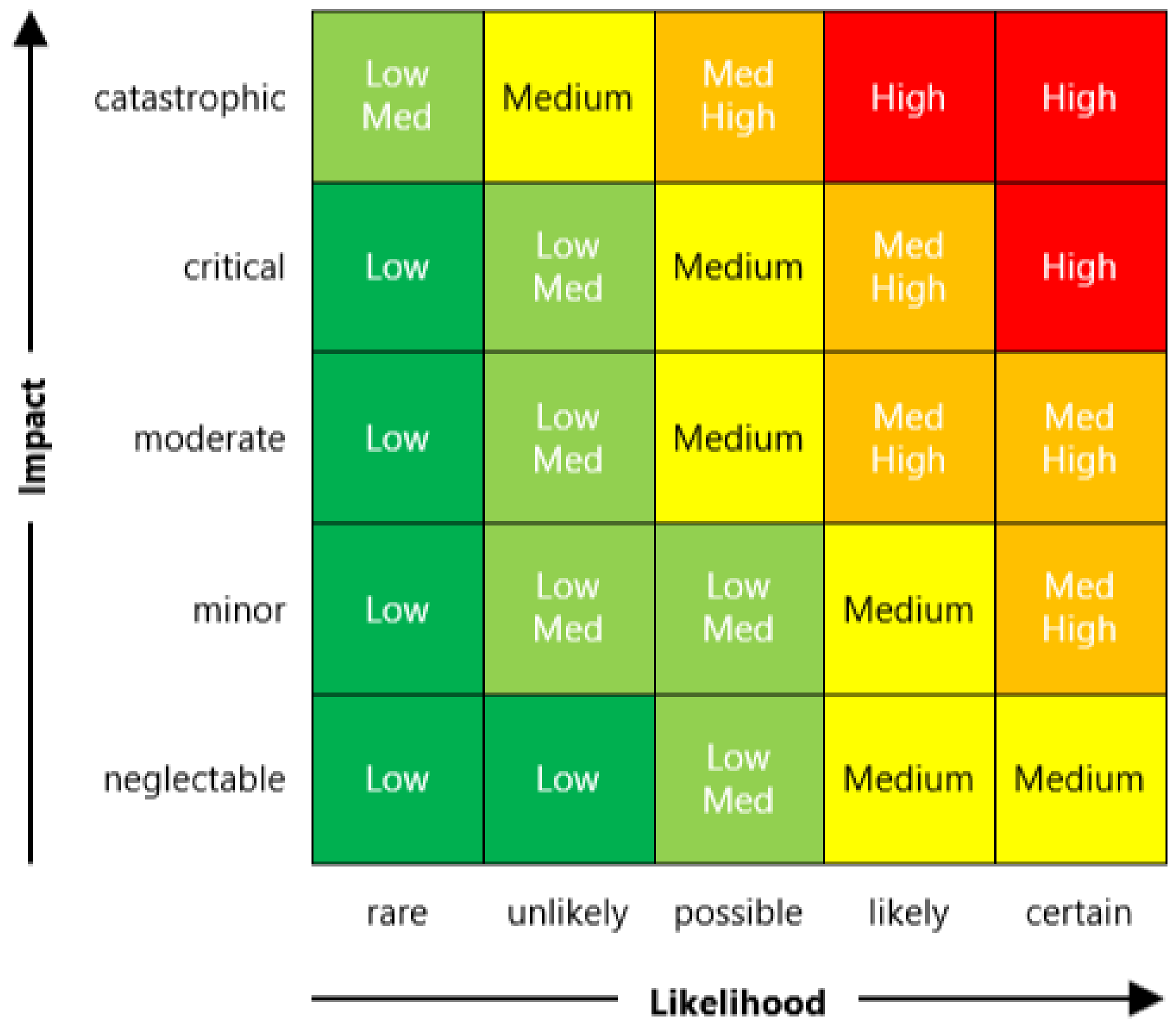
### RECOVER

Update security policies, and procedures, and prepare guidelines, and documentation.

# RISK - Focus of security

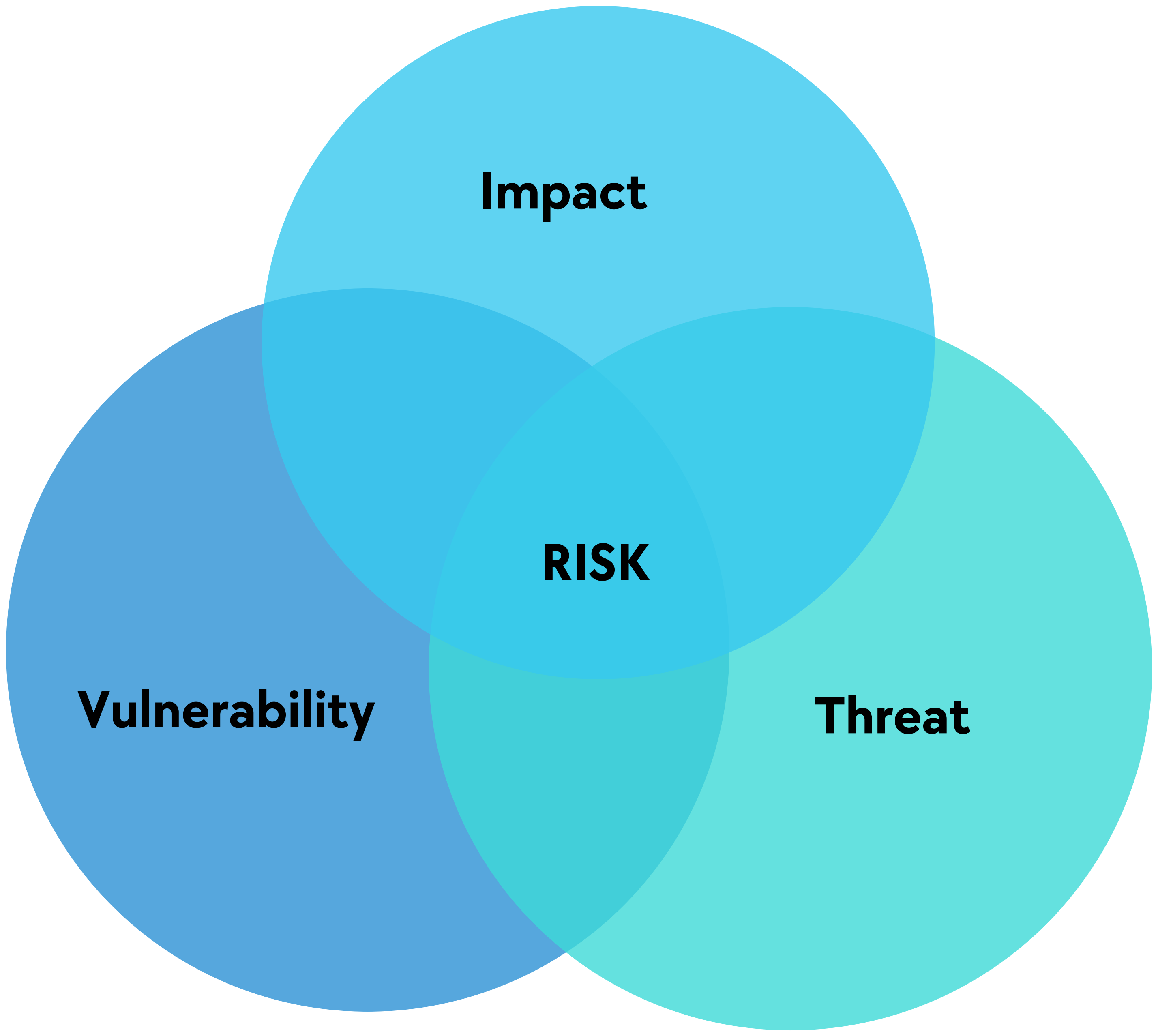
Likelihood = Threat x Vulnerability

**RISK = Likelihood x Impact**



| Impact | rare | unlikely | possible | likely | certain |
|---|---|---|---|---|---|
| catastrophic | Low Med | Medium | Med High | High | High |
| critical | Low | Low Med | Medium | Med High | High |
| moderate | Low | Low Med | Medium | Med High | Med High |
| minor | Low | Low Med | Low Med | Medium | Med High |
| neglectable | Low | Low | Low Med | Medium | Medium |

Likelihood



- Security is about managing risk to the critical assets.
- Risk is the likelihood of a threat touching a vulnerability in the system.
- The key is understanding what is critical and high risk to your organisation and how to reduce it.

# Threats

## Non-actor driven

Usually unintentional, a result of negative outcomes from operations. Caused by:

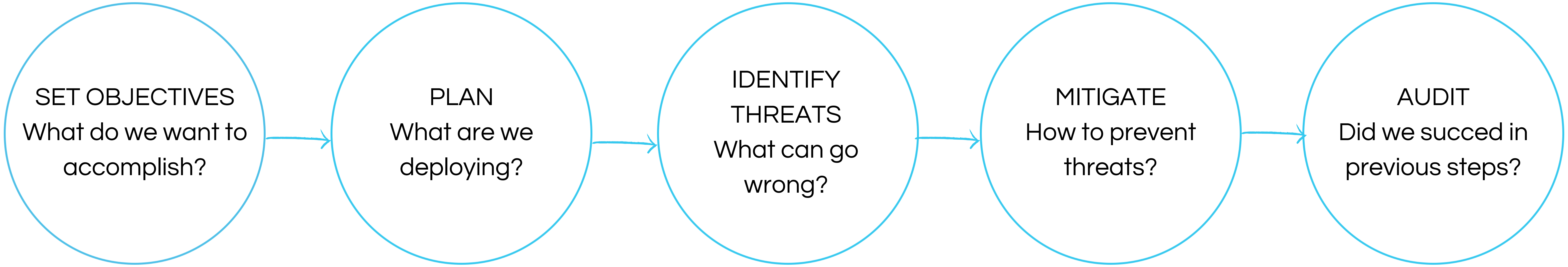
- natural disaster
- errors in systems (bugs)
- human error (accidents, negligence)

## Actor driven

Usually deliberate/intentional, caused by deliberate actions from actors/groups.

# Threat modelling

Strategically thinking about what can go wrong.



SET OBJECTIVES
What do we want to accomplish?

PLAN
What are we deploying?

IDENTIFY THREATS
What can go wrong?

MITIGATE
How to prevent threats?

AUDIT
Did we succed in previous steps?

# FUNDAMENTAL SECURITY PRINCIPLES

### Defence-in-depth

Multiple layers of protection, if a level of protection fails, the subsequent level will prevent an attack.

### Zero trust

No person, device or service can automatically be trusted.

### Least privileges

Only services and people that need permissions, will get them.

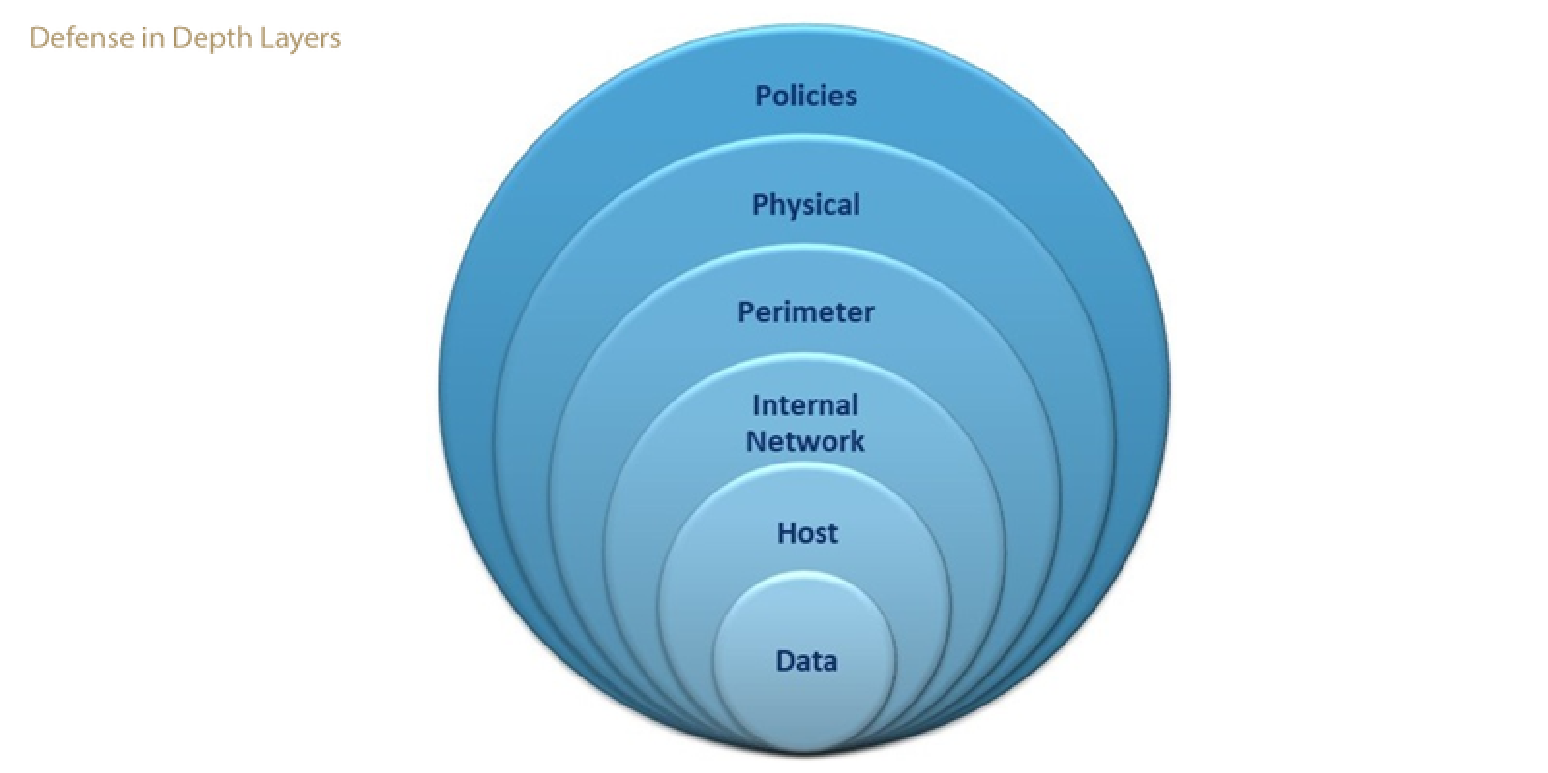
### Separation of duties

SPOC - no single point of control, a single person cannot do a compromise.

### CIA triad

Cybersecurity is the protection of Confidentiality, Integrity and Availability of information in the system.

# Defence-in-depth



- Any layer of protection might fail

- Integration of defence-in-depth means that multiple levels of protection must be deployed and different types of security controls (organisational, technical etc.)
- A single magical solution doesn't exist.
- An example: MFA + patches + firewall + IDS + automatic penetration tests + data encryption

# Zero trust

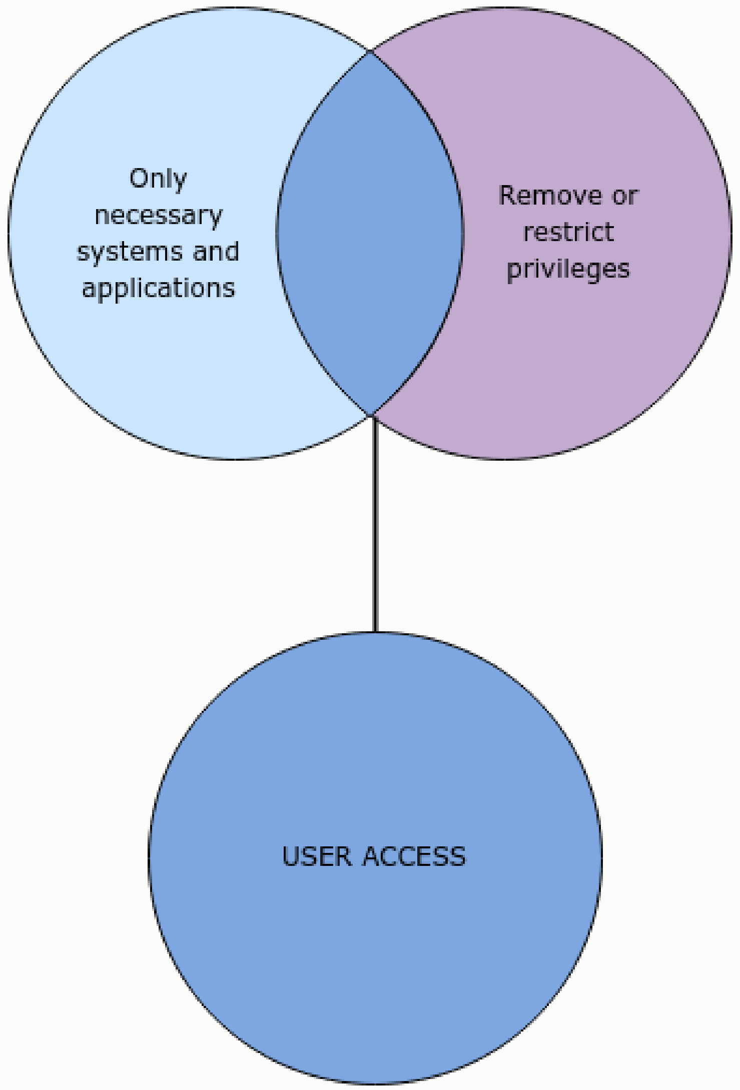
- ***No asset or user is trusted.***

- You don’t automatically believe everything inside your firewall can be trusted.
- All users should be authenticated (in or outside of an organisation network) - MFA if possible.
- Key principles: continuous verification, minimising the impact of a compromise if it occurs, and granting access only if it is really needed.
- The focus is on protecting resources, not network segments
- See NIST SP 800-207: https://csrc.nist.gov/pubs/sp/800/207/final

# Least privilege

- Access rights are not permanent.
- Revise assigned privileges regularly.
- Hardening hosts is part of this approach too: delete default accounts, and uninstall/disable services that are installed by default but not needed.
- Don’t give users privileges on a “just-in-case” you need them basis.

***The principle of least privilege (POLP) access means granting a minimum level of access rights to users and services to perform their jobs.***


Only necessary systems and applications
Remove or restrict privileges
USER ACCESS

# Separation of duties

- ***No single point of control***

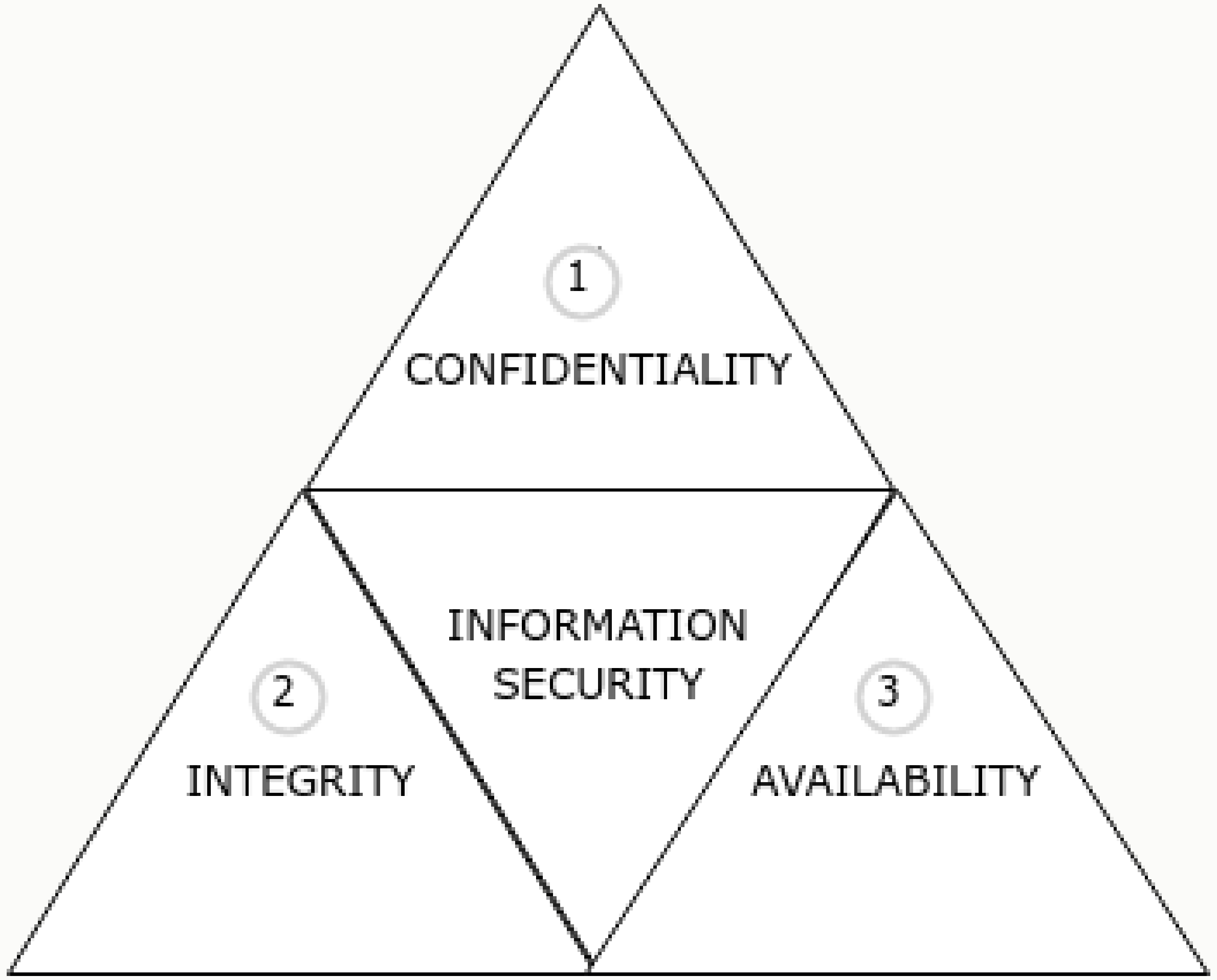
- No user should be given enough privileges to misuse the system.
- Security measures to prevent fraud, misuse of information, and error.
- SOD principle can be implemented by defining roles, by enforcing controls of access, by two-person rule etc.
- Example: two signatures required for a bank transaction, door with two locks and single key for each lock, separate action in separate location...

# CIA triad

- **CONFIDENTIALITY:** Only authorised users should be able to access the information
- **INTEGRITY**: Make sure that data has not been modified, and that it is accurate.
- **AVAILABILITY**: Information should be available when required.

This concept is part of ISO 27001, a global standard for information security.

:



# QUIZ

Is unauthorised access to the information loss of

- integrity
- availability
- confidentiality

Web server is down when trying to access a website. Is this the loss of:

- integrity
- availability
- confidentiality

To access her mailbox, Alice has to use the company’s VPN and log in with her username and password and OTP.  Is this implementation of:

- defence-in-depth principle
- zero trust principle
- separation of duties principle

# Security architect

***Security architect works to design, build, test, and implement security systems withing an organisation.***

1 **Define objectives**

Based on risk assessment, security architect defines the objectives of the information system.

2 **Create architecture plan**

Preparation of reference architecture, definition of the approach and required security controls (topology diagram, definition of processes etc.)

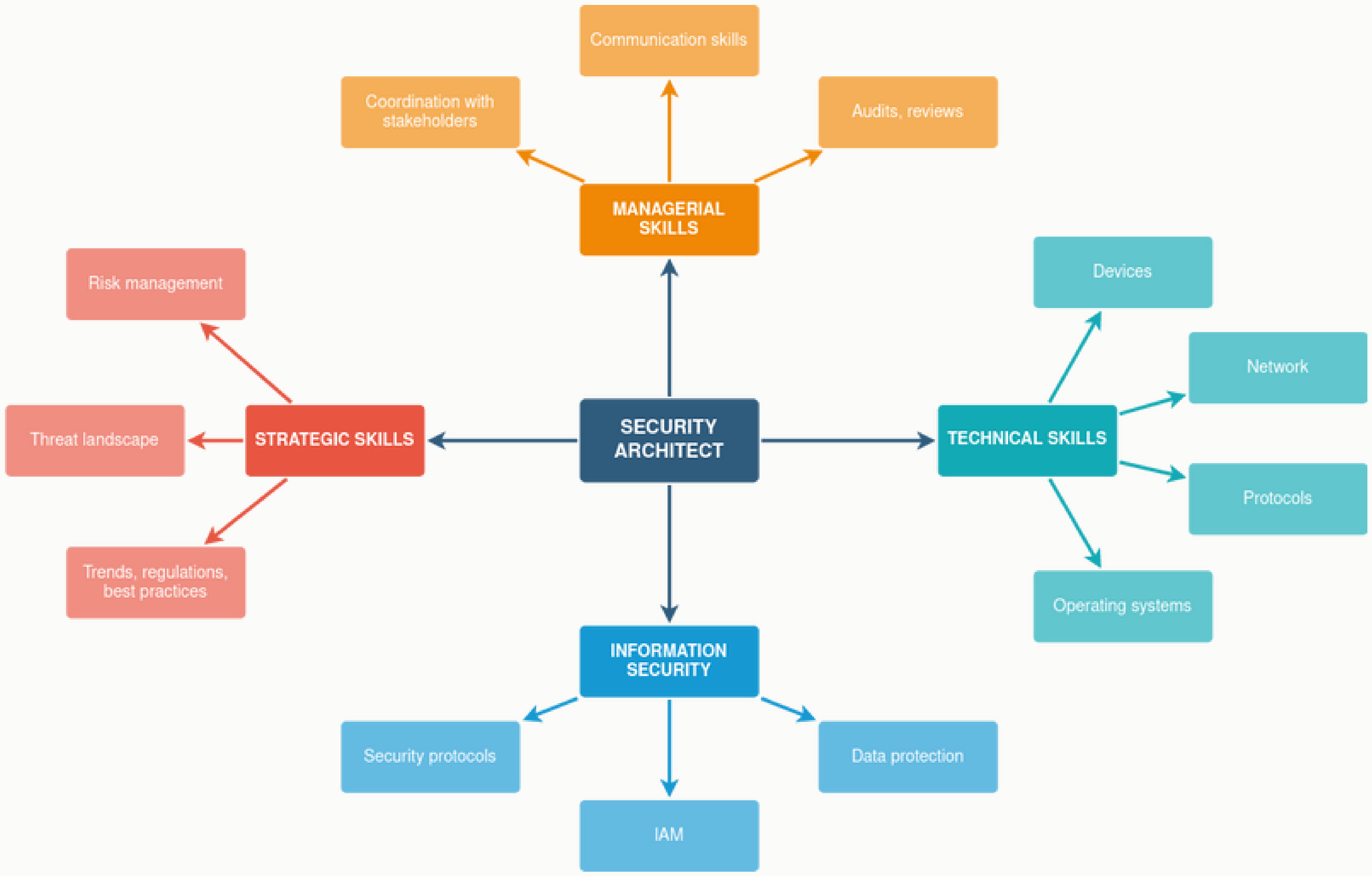
3 **Create security solution architecture**

Development of Security Solution Architecture

4 **Detect anomalies and revise**

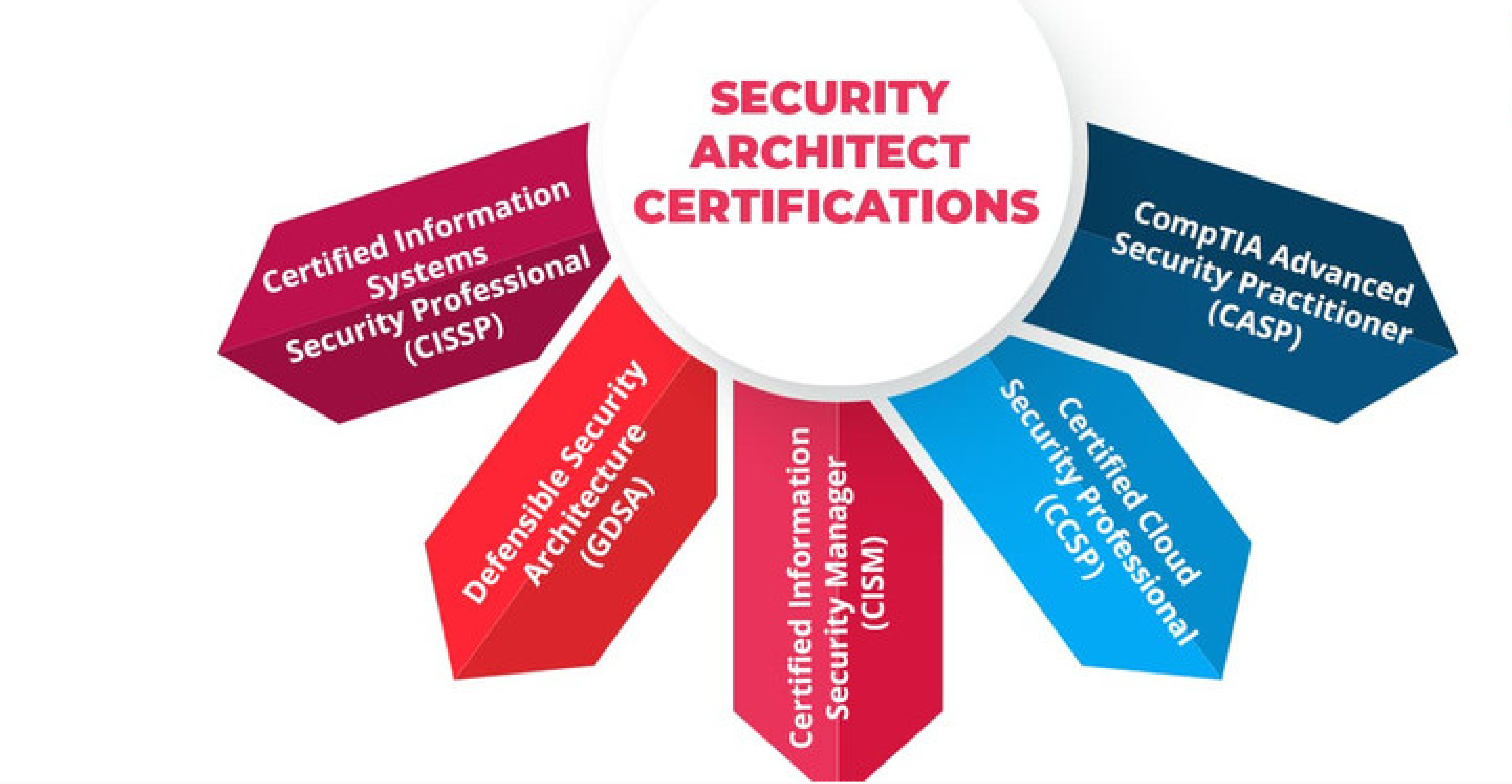
Monitor the system, audit it, and review the procedures, policies, and controls. Based on the results, revise the architecture framework and security controls.

# Role of security architect



## • Core tasks

- Develop security design for systems and networks, taking into account the fundamental security principles and objectives of the organisation.
- Define the scope of the information system, its location, required services and what kind of data will be processed.
- Prepare security policies and procedures.
- Prepare documentation on assets, risk assessment and treatment, vulnerability management etc.
- Run risk assessment to identify critical processes and services and apply security controls that will reduce the risk.
- Implement the information system.
- Perform security reviews and audits.
- Ensure staff training and security awareness.
- Monitor the system and detect anomalies.
- Review and revise.



## SECURITY ARCHITECT CERTIFICATIONS

- Certified Information Systems Security Professional (CISSP)
- Defensible Security Architecture (GDSA)
- Certified Information Security Manager (CISM)
- Certified Cloud Security Professional (CCSP)
- CompTIA Advanced Security Practitioner (CASP)

# How to design security architecture

Security should be included in the process from start to finish, from design to production. You cannot do security when the service is in production, as you cannot build an earthquake proof builing after it is already built.

1. **Use security principles and security frameworks**

   Use visual charts to communicate info more effectively.

2. **Run risk assessment**

   Understand how a system works and how it can fail, what are the critical services, what is the highest risk, what are the threats.

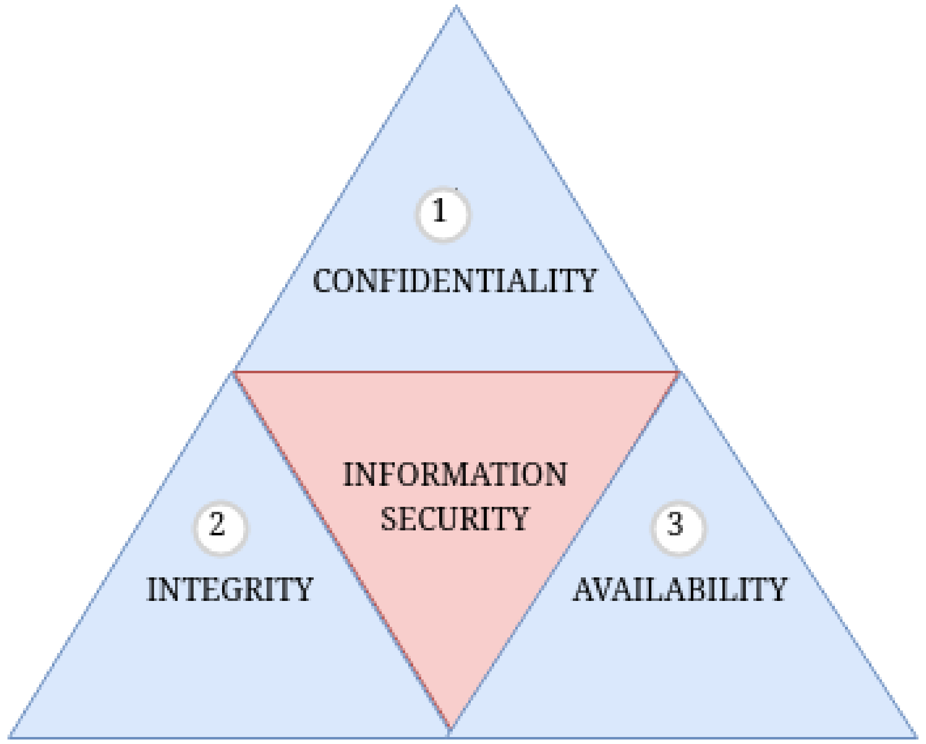
3. **Prepare policies and system design**

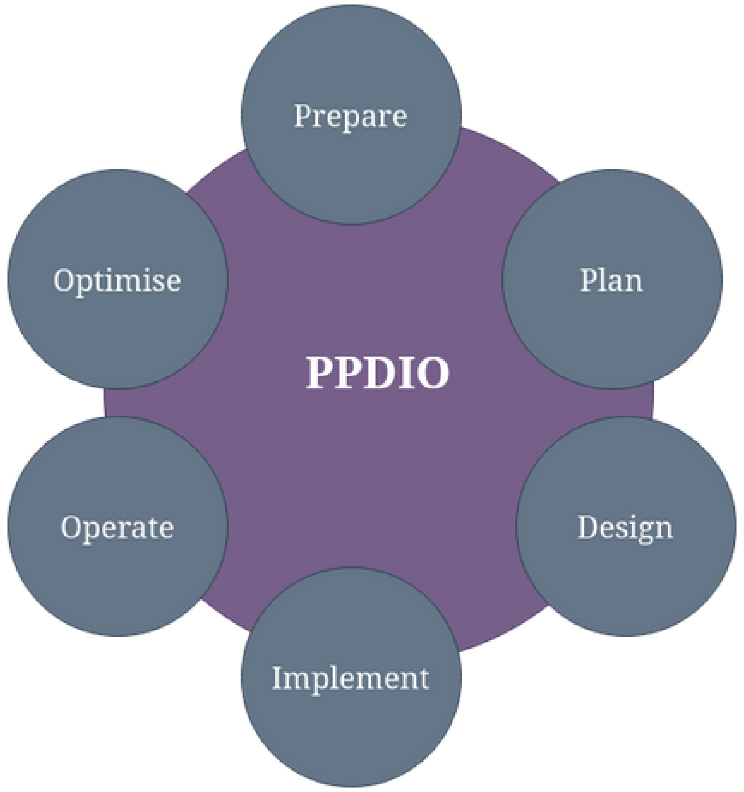
   Based on the risk assessment, prepare security controls, policies, procedures.

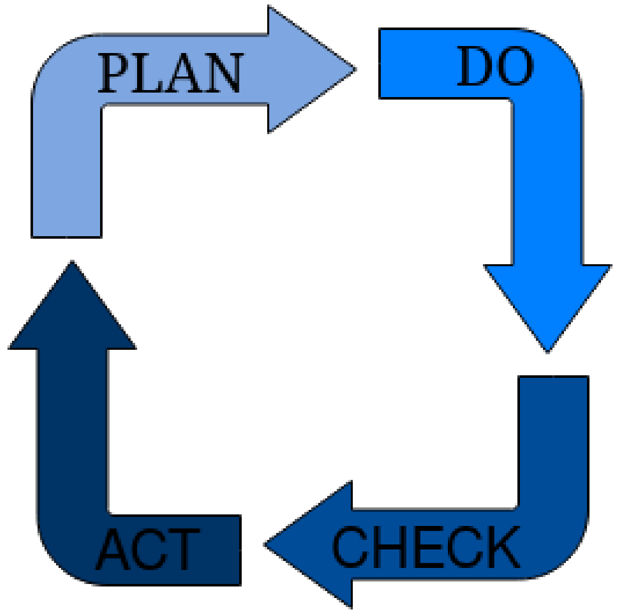
4. **Implement and review**

   Prepare the system, implement it. After the implementation, monitor the system to detect anomalies and prevent cybersecurity attacks. Constantly improve the procedures and controls.

# Security models







## CIA TRIAD

Confidentiality, Integrity and Availability as three crucial components of security

## CISCO PPDIOO

Prepare - Plan - Design - Implement - Operate - Optimise

The basis is lifecycle approach to network design that improves business agility and network availability.

## PDCA

Repetitive four stage model Plan - do - check - act for continuous improvement, considered as the basis for quality control.
Also called Deming wheel or Shewhard cycle.

# Security design priciples

- The **context**: understand the components of your system, and its objectives, address shortcomings, and separate responsibilities, and understand the threat model.
- Assess the **risk** to the organisation.
- Identify the legal, regulatory, and contractual **requirements** your organisation must comply with.
- **Design system**: network segments, services, communication channels, authN and authZ options.
- Identify **critical services** and sensitive data.
- Provide mechanisms for compromise **detection** (collect logs and monitor events).
- Reduce attack surface, and reduce the impact of the compromise and failure.
- Provide **incident response plan.**

# CYBERSECURITY PROGRAMME

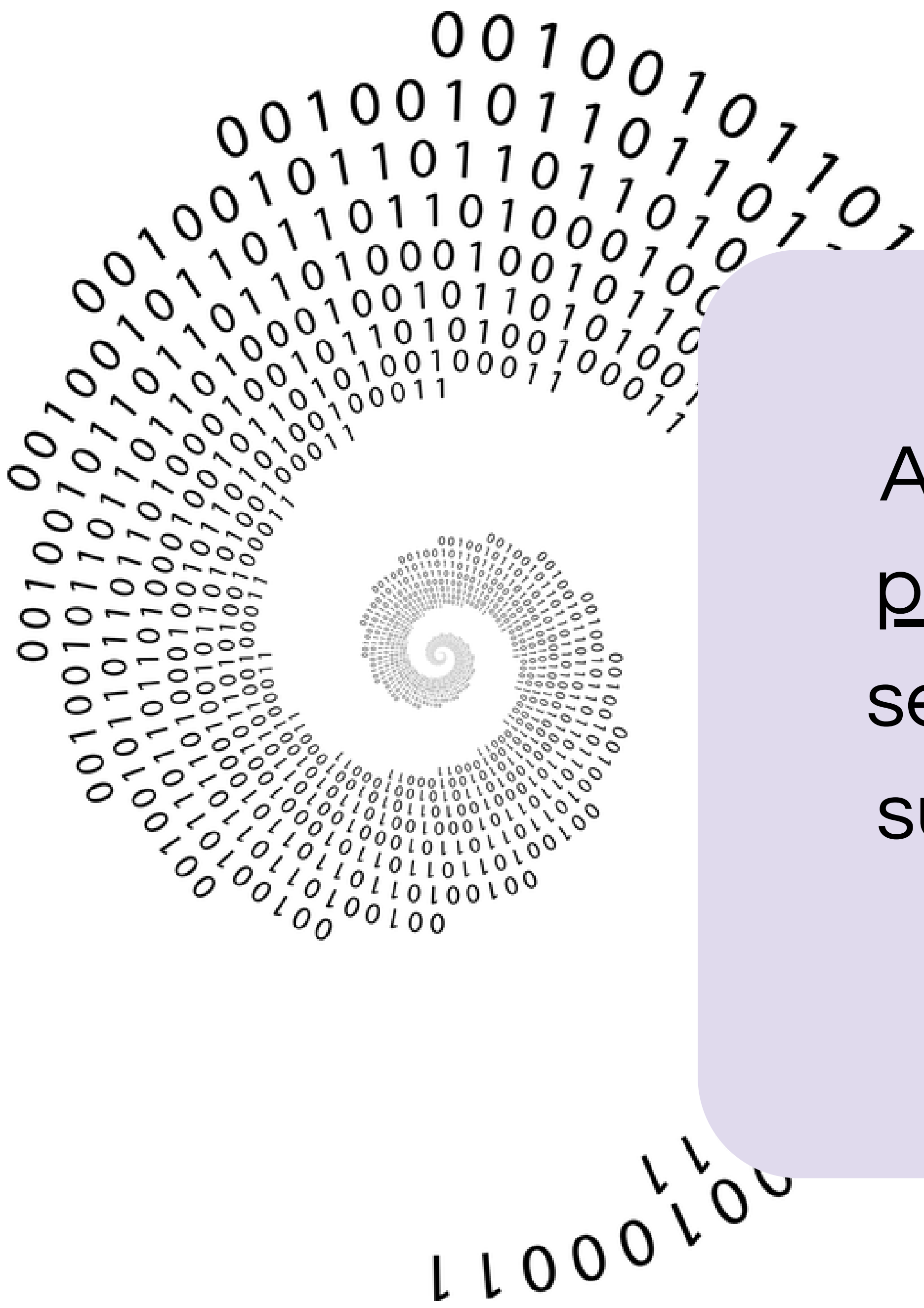
- incorporates **strategy of an organisation**, organisational policies, standards, how-tos, procedures
- based on experience, industry standards, regulations, guidelines
- built with the help of a **security framework**, which is adapted to an organisation
- Following a security framework is not enough, a defensive strategy is needed to implement CSP

A DEFENSIVE STRATEGY is a plan to achieve organisational security objectives, based on risk assessment, identification of cyber threats, organisation’s assets, security controls, detection and incident response procedures etc.

Benefits of CSF:

- Specifically describes current and targeted cybersecurity posture
- identifies security gaps
- identifies how to improve the security
- demonstrates alignment with standards and best practices
- addresses the organisation‘s security risks and their mitigation
- Designs and implements security controls

# Security frameworks



A security framework is a set of policies, guidelines, and best practices designed to manage an organization’s information security risks. As the name suggests, frameworks provide the supporting structure needed to protect internal data against cyber threats and vulnerabilities. (source: OneTrust)

To implement security and develop cybersecurity programme.

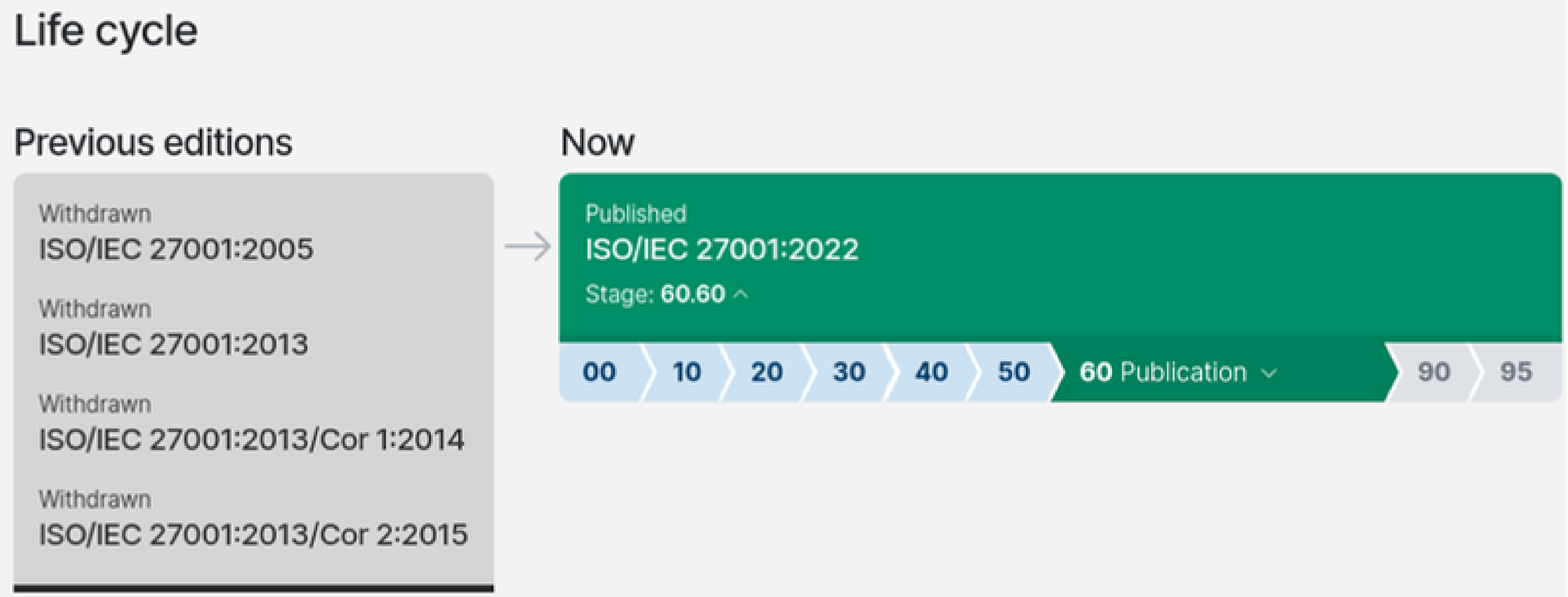
# When should an organisation implement Cybersecurity Programme?

- when you have unclear roles and responsibilities for information systems and data,
- when you lack of work procedures,
- when information is stored all over the organisation,
- when dealing with low security awareness,
- when no incident management procedures are in place
- when there is no risk management defined,
- when you lack formal policies and procedures.

# ISO 27000 series

- also known as the 'ISMS Family of Standards' or 'ISO27K' for short
- international standard for information security, cybersecurity and protection. Updated in 02/2022.
- more than 100k organisation worldwide certified
- organisation has to formalise procedures, security policies, has risk assessment plan

**ISO27001** Specification of Information Security Management System (ISMS)
**ISO27002** Information security controls
**ISO27005** Iso standard for information security risk management



Life cycle

Previous editions

Withdrawn
ISO/IEC 27001:2005

Withdrawn
ISO/IEC 27001:2013

Withdrawn
ISO/IEC 27001:2013/Cor 1:2014

Withdrawn
ISO/IEC 27001:2013/Cor 2:2015

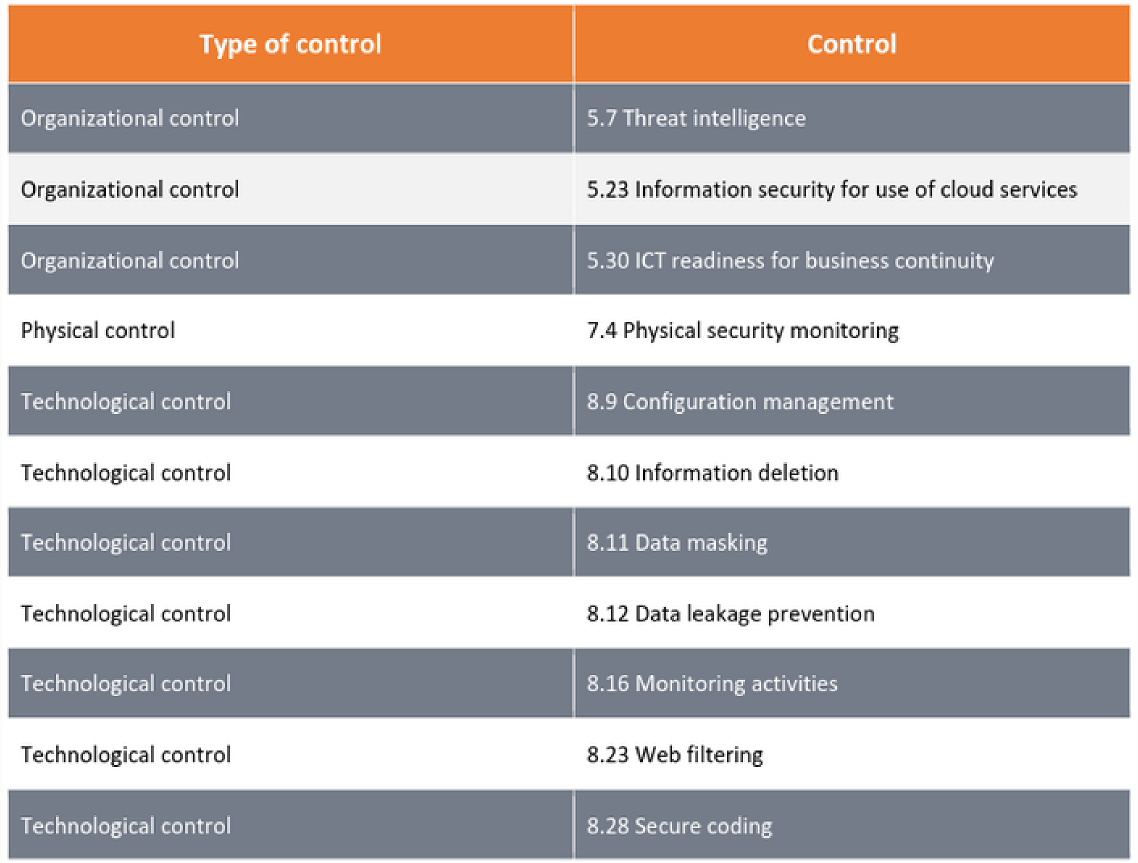
Now

Published
ISO/IEC 27001:2022
Stage: 60.60

https://www.iso.org/standards.html

# ISO 27001

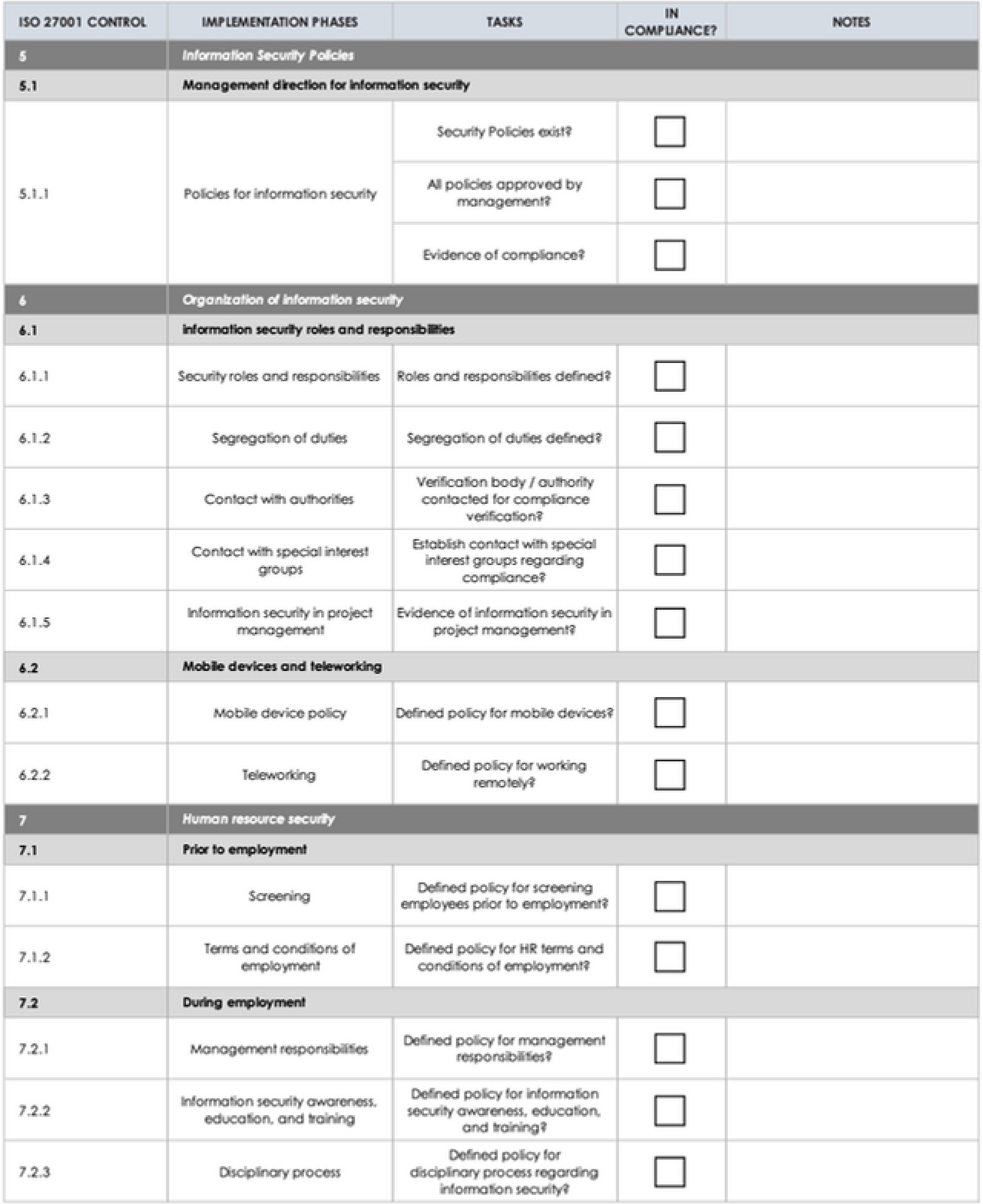
- Specification of Information Security Management System (ISMS)
- Security controls structure: **Organisational, physical, and technological controls**
- Controls' attributes are either **Preventive, Detective or Corrective**.
- The new version released in 2022 - includes **new security controls** (threat intelligence, security for use of cloud services, business continuity, physical security monitoring, data deletion/masking and leaking prevention, web filtering, configuration management and secure coding.
- 93 security controls (before 114), some of them were merged

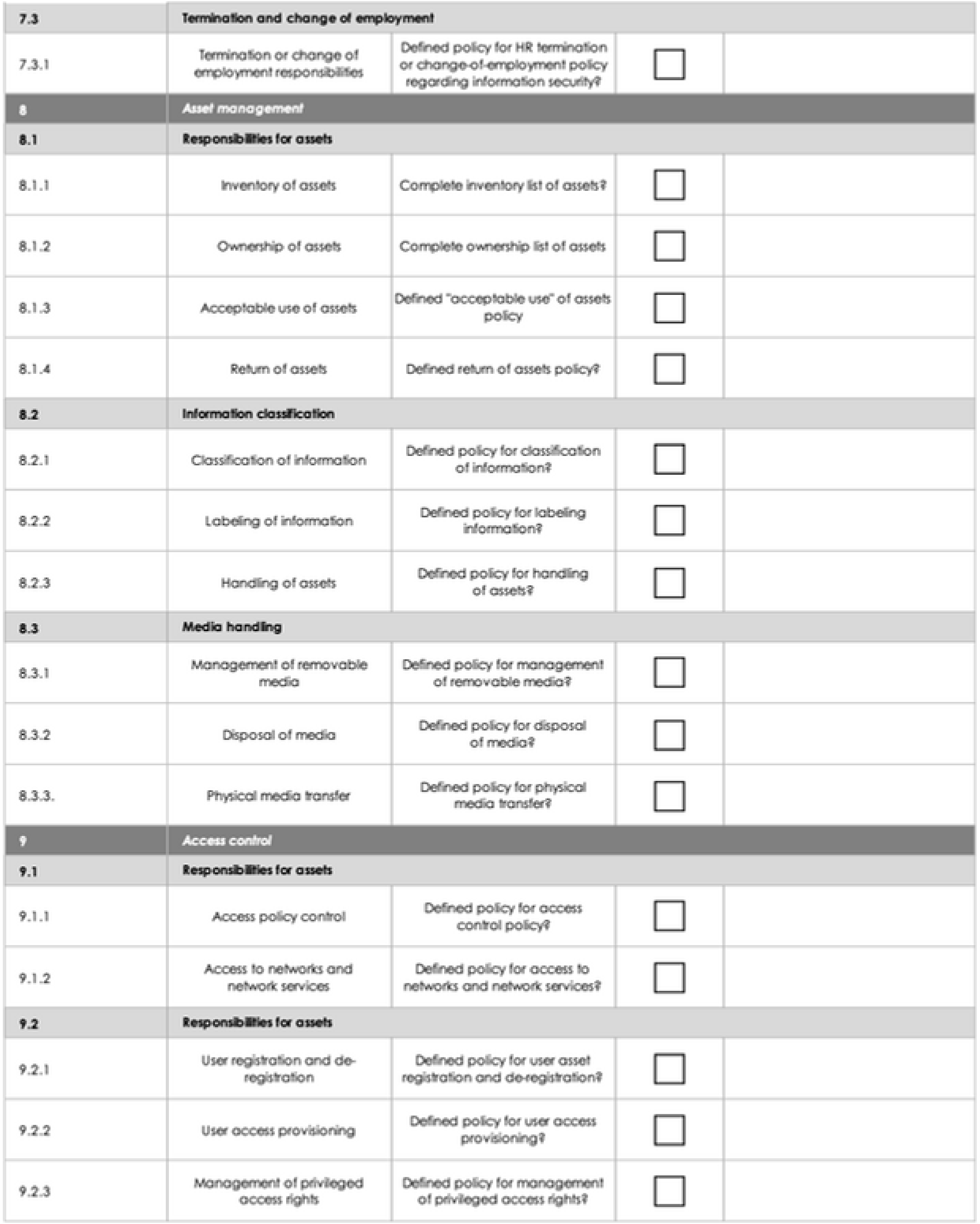


| Type of control | Control |
|---|---|
| Organizational control | 5.7 Threat intelligence |
| Organizational control | 5.23 Information security for use of cloud services |
| Organizational control | 5.30 ICT readiness for business continuity |
| Physical control | 7.4 Physical security monitoring |
| Technological control | 8.9 Configuration management |
| Technological control | 8.10 Information deletion |
| Technological control | 8.11 Data masking |
| Technological control | 8.12 Data leakage prevention |
| Technological control | 8.16 Monitoring activities |
| Technological control | 8.23 Web filtering |
| Technological control | 8.28 Secure coding |

Source: Advisera

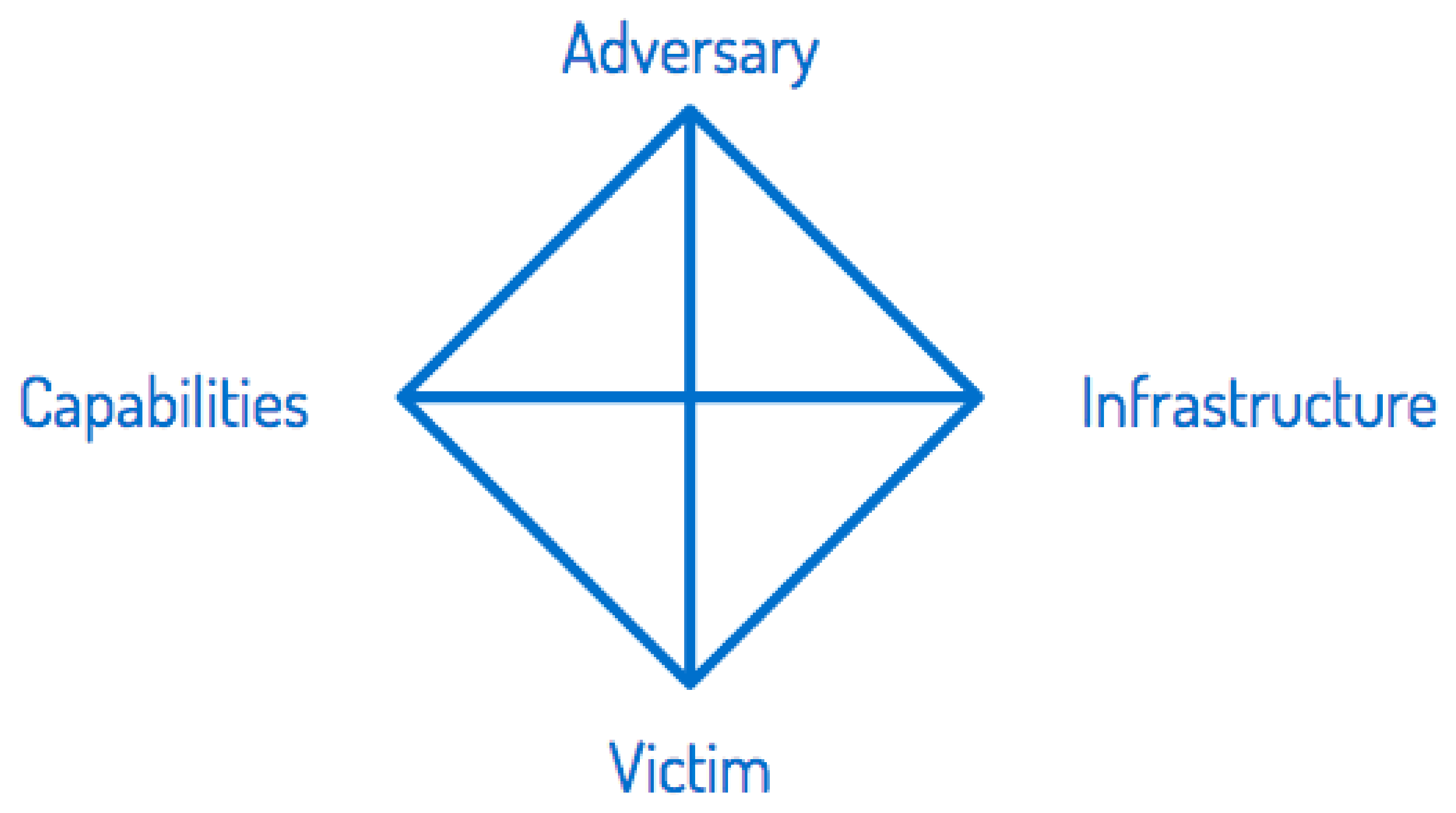
# ISO27k CHECKLIST





| ISO 27001 CONTROL | IMPLEMENTATION PHASES | TASKS | IN COMPLIANCE? | NOTES |
|---|---|---|---|---|
| 5 | *Information Security Policies* | | | |
| 5.1 | **Management direction for information security** | | | |
| 5.1.1 | Policies for information security | Security Policies exist? | □ | |
| | | All policies approved by management? | □ | |
| | | Evidence of compliance? | □ | |
| 6 | *Organization of information security* | | | |
| 6.1 | **information security roles and responsibilities** | | | |
| 6.1.1 | Security roles and responsibilities | Roles and responsibilities defined? | □ | |
| 6.1.2 | Segregation of duties | Segregation of duties defined? | □ | |
| 6.1.3 | Contact with authorities | Verification body / authority contacted for compliance verification? | □ | |
| 6.1.4 | Contact with special interest groups | Establish contact with special interest groups regarding compliance? | □ | |
| 6.1.5 | Information security in project management | Evidence of information security in project management? | □ | |
| 6.2 | **Mobile devices and teleworking** | | | |
| 6.2.1 | Mobile device policy | Defined policy for mobile devices? | □ | |
| 6.2.2 | Teleworking | Defined policy for working remotely? | □ | |
| 7 | *Human resource security* | | | |
| 7.1 | **Prior to employment** | | | |
| 7.1.1 | Screening | Defined policy for screening employees prior to employment? | □ | |
| 7.1.2 | Terms and conditions of employment | Defined policy for HR terms and conditions of employment? | □ | |
| 7.2 | **During employment** | | | |
| 7.2.1 | Management responsibilities | Defined policy for management responsibilities? | □ | |
| 7.2.2 | Information security awareness, education, and training | Defined policy for information security awareness, education, and training? | □ | |
| 7.2.3 | Disciplinary process | Defined policy for disciplinary process regarding information security? | □ | |
| 7.3 | **Termination and change of employment** | | | |
| 7.3.1 | Termination or change of employment responsibilities | Defined policy for HR termination or change-of-employment policy regarding information security? | □ | |
| 8 | *Asset management* | | | |
| 8.1 | **Responsibilities for assets** | | | |
| 8.1.1 | Inventory of assets | Complete inventory list of assets? | □ | |
| 8.1.2 | Ownership of assets | Complete ownership list of assets | □ | |
| 8.1.3 | Acceptable use of assets | Defined "acceptable use" of assets policy | □ | |
| 8.1.4 | Return of assets | Defined return of assets policy? | □ | |
| 8.2 | **Information classification** | | | |
| 8.2.1 | Classification of information | Defined policy for classification of information? | □ | |
| 8.2.2 | Labeling of information | Defined policy for labeling information? | □ | |
| 8.2.3 | Handling of assets | Defined policy for handling of assets? | □ | |
| 8.3 | **Media handling** | | | |
| 8.3.1 | Management of removable media | Defined policy for management of removable media? | □ | |
| 8.3.2 | Disposal of media | Defined policy for disposal of media? | □ | |
| 8.3.3. | Physical media transfer | Defined policy for physical media transfer? | □ | |
| 9 | *Access control* | | | |
| 9.1 | **Responsibilities for assets** | | | |
| 9.1.1 | Access policy control | Defined policy for access control policy? | □ | |
| 9.1.2 | Access to networks and network services | Defined policy for access to networks and network services? | □ | |
| 9.2 | **Responsibilities for assets** | | | |
| 9.2.1 | User registration and de-registration | Defined policy for user asset registration and de-registration? | □ | |
| 9.2.2 | User access provisioning | Defined policy for user access provisioning? | □ | |
| 9.2.3 | Management of privileged access rights | Defined policy for management of privileged access rights? | □ | |

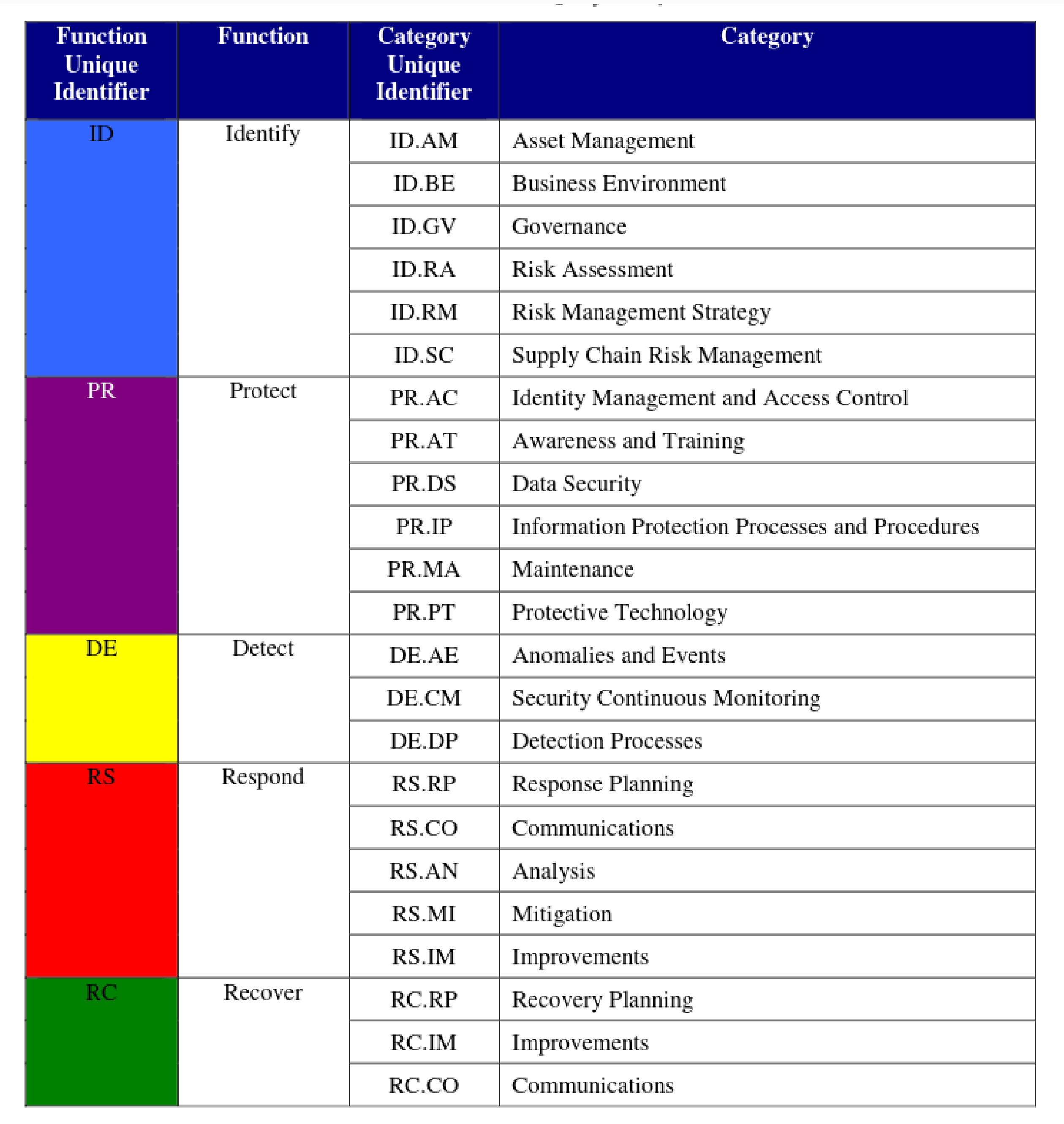
# Diamond model



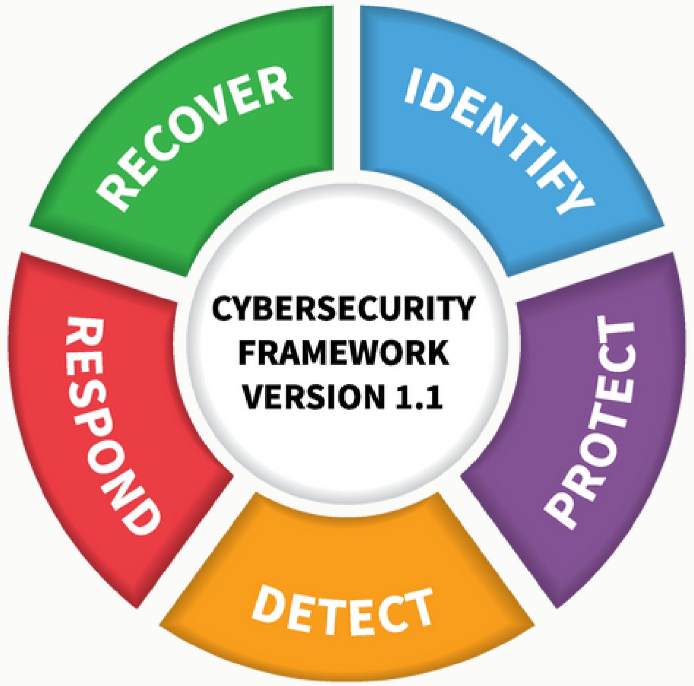
**The Diamond Model of Intrusion Analysis is a framework for investigating and analyzing cybersecurity incidents. Intelligence analysts and computer security researchers developed it to help understand and characterize cyber-attacks. Valuable model for threat intelligence.**

- **adversary** - what is the motive, why did the attack happen?
- **infrastructure**: location of the attacker, the methods used to attack the target system, and the tools and techniques employed.
- **victim** = target of the attack, which was the security gap and what the potential impact of the attack on the organisation.
- **capabilities**: attacker's methods and techniques, which vulnerability he/she exploited, which malware was installed, how sophisticated the attack

# NIST CSF



| Function Unique Identifier | Function | Category Unique Identifier | Category |
|---|---|---|---|
| ID | Identify | ID.AM | Asset Management |
| | | ID.BE | Business Environment |
| | | ID.GV | Governance |
| | | ID.RA | Risk Assessment |
| | | ID.RM | Risk Management Strategy |
| | | ID.SC | Supply Chain Risk Management |
| PR | Protect | PR.AC | Identity Management and Access Control |
| | | PR.AT | Awareness and Training |
| | | PR.DS | Data Security |
| | | PR.IP | Information Protection Processes and Procedures |
| | | PR.MA | Maintenance |
| | | PR.PT | Protective Technology |
| DE | Detect | DE.AE | Anomalies and Events |
| | | DE.CM | Security Continuous Monitoring |
| | | DE.DP | Detection Processes |
| RS | Respond | RS.RP | Response Planning |
| | | RS.CO | Communications |
| | | RS.AN | Analysis |
| | | RS.MI | Mitigation |
| | | RS.IM | Improvements |
| RC | Recover | RC.RP | Recovery Planning |
| | | RC.IM | Improvements |
| | | RC.CO | Communications |



- NIST SP 800 by the National Institute for Standards and Technology
- Currently version 1.1. is in place, but a Draft for CSF 2.0 Core  is available and you can provide comments until Nov 2023
- Based on 5 pillars: identify, protect, detect, respond, recover

https://www.nist.gov/itl/smallbusinesscyber/planning-guides/nist-cybersecurity-framework

# NIST CSF

- NIST helps you answer the following questions:
    - How to categorise and protect your data?
    - How to conduct risk assessments?
    - How to prepare a security plan?
    - How to implement security controls?
    - How to measure performance and efficiency?
    - How to process data?

https://www.nist.gov/cybersecurity

# CIS controls

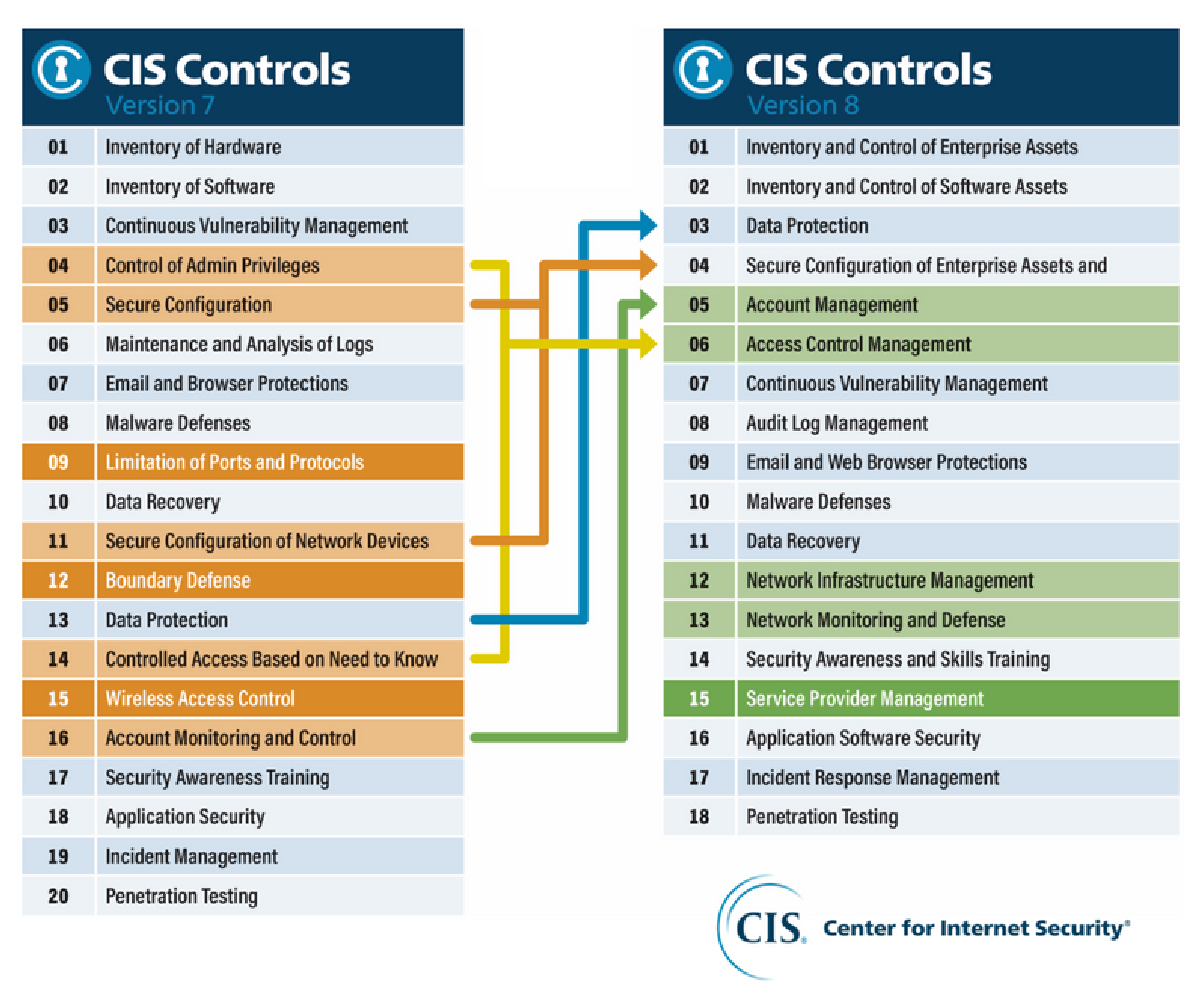
- known also as Critical Security Controls,
- developed by Center for Internet security,
- contain a set of actions for system cyber defense.
- CIS controls are used to identify common exploits,
- they provide recommendations on how to defend (safeguards),
- are measurable,
- each safeguard has a description (for small office, for large organization with IT, for organization with security expert group).

See: https://www.cisecurity.org/

CIS Center for Internet Security®

*Creating Confidence in the Connected World.*™

# CIS controls



## CIS Controls
Version 7

| | |
|---|---|
| 01 | Inventory of Hardware |
| 02 | Inventory of Software |
| 03 | Continuous Vulnerability Management |
| 04 | Control of Admin Privileges |
| 05 | Secure Configuration |
| 06 | Maintenance and Analysis of Logs |
| 07 | Email and Browser Protections |
| 08 | Malware Defenses |
| 09 | Limitation of Ports and Protocols |
| 10 | Data Recovery |
| 11 | Secure Configuration of Network Devices |
| 12 | Boundary Defense |
| 13 | Data Protection |
| 14 | Controlled Access Based on Need to Know |
| 15 | Wireless Access Control |
| 16 | Account Monitoring and Control |
| 17 | Security Awareness Training |
| 18 | Application Security |
| 19 | Incident Management |
| 20 | Penetration Testing |

## CIS Controls
Version 8

| | |
|---|---|
| 01 | Inventory and Control of Enterprise Assets |
| 02 | Inventory and Control of Software Assets |
| 03 | Data Protection |
| 04 | Secure Configuration of Enterprise Assets and |
| 05 | Account Management |
| 06 | Access Control Management |
| 07 | Continuous Vulnerability Management |
| 08 | Audit Log Management |
| 09 | Email and Web Browser Protections |
| 10 | Malware Defenses |
| 11 | Data Recovery |
| 12 | Network Infrastructure Management |
| 13 | Network Monitoring and Defense |
| 14 | Security Awareness and Skills Training |
| 15 | Service Provider Management |
| 16 | Application Software Security |
| 17 | Incident Response Management |
| 18 | Penetration Testing |

CIS. Center for Internet Security®

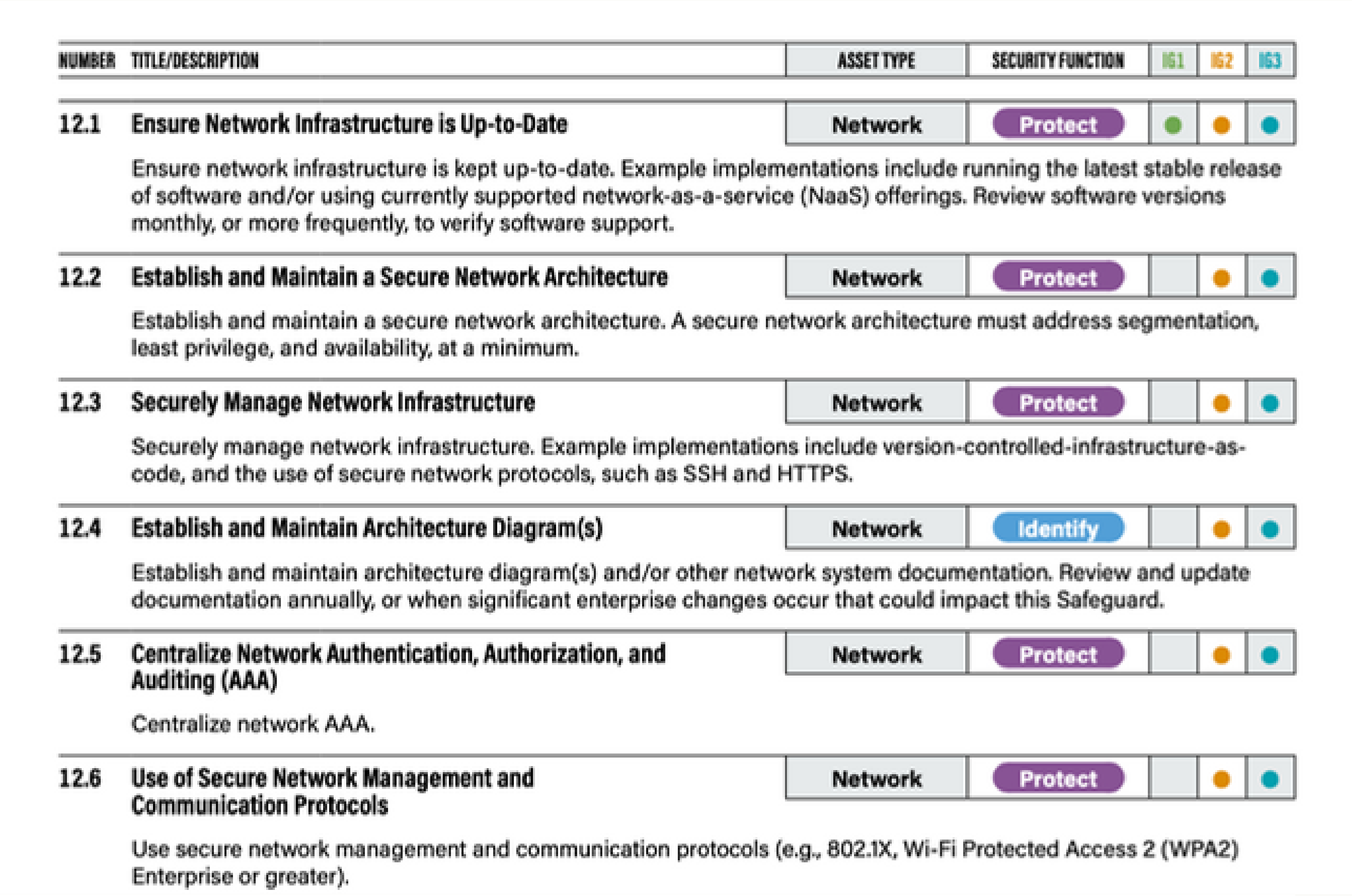
Source: https://www.sans.org/blog/cis-controls-v8

# CIS benchmarks

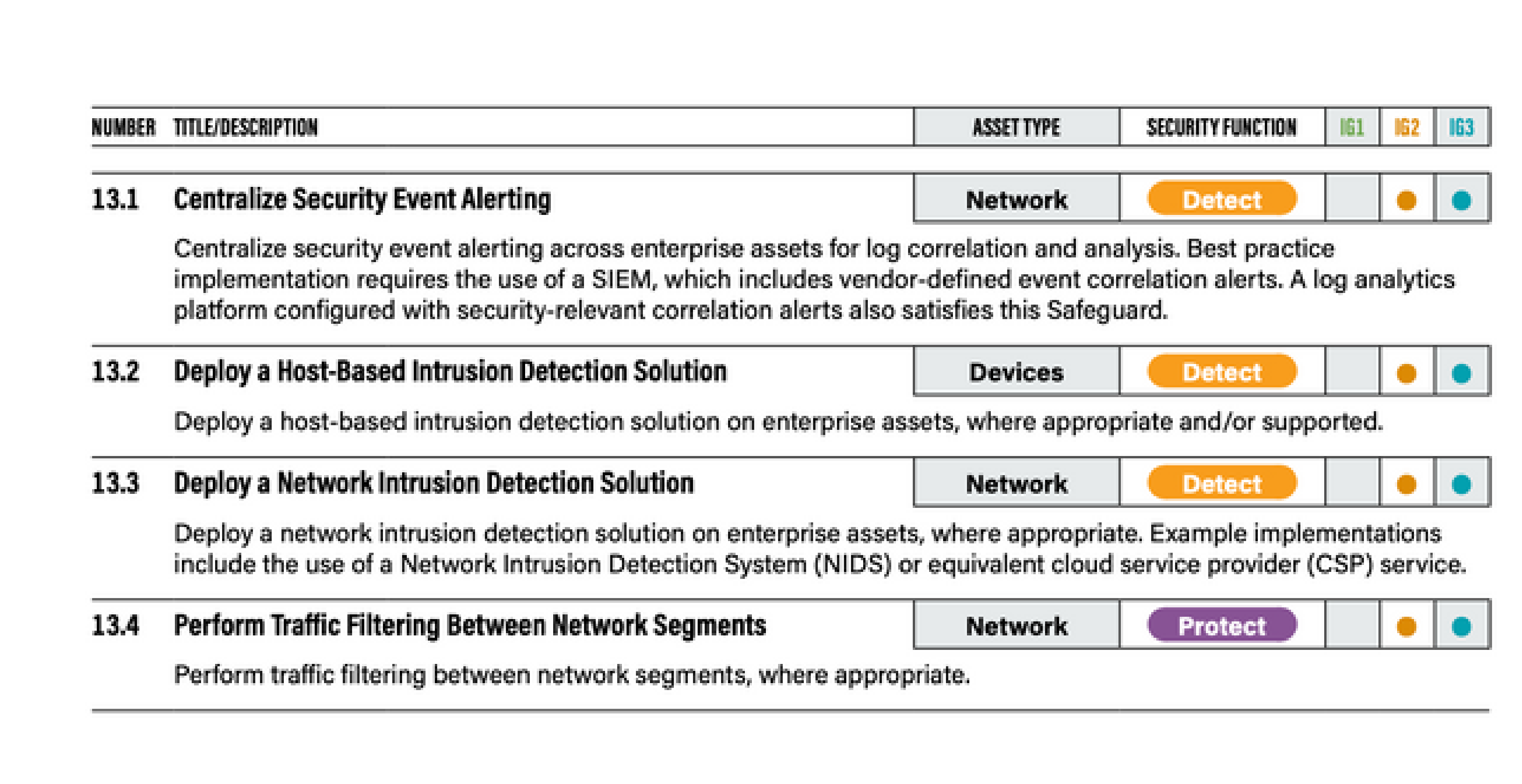
**How to translate a CIS safeguard to action - configuration guidelines**

- more than 100 benchmarks/saveguards available, for network devices, operating systems, software packages, cloud providers etc.
- more than 25 vendor products included, such as Cisco, F5, Juniper.
- many vendors implement CIS benchmarks (such as Nessus, OpenVAS etc.).
- See: https://learn.cisecurity.org/benchmarks

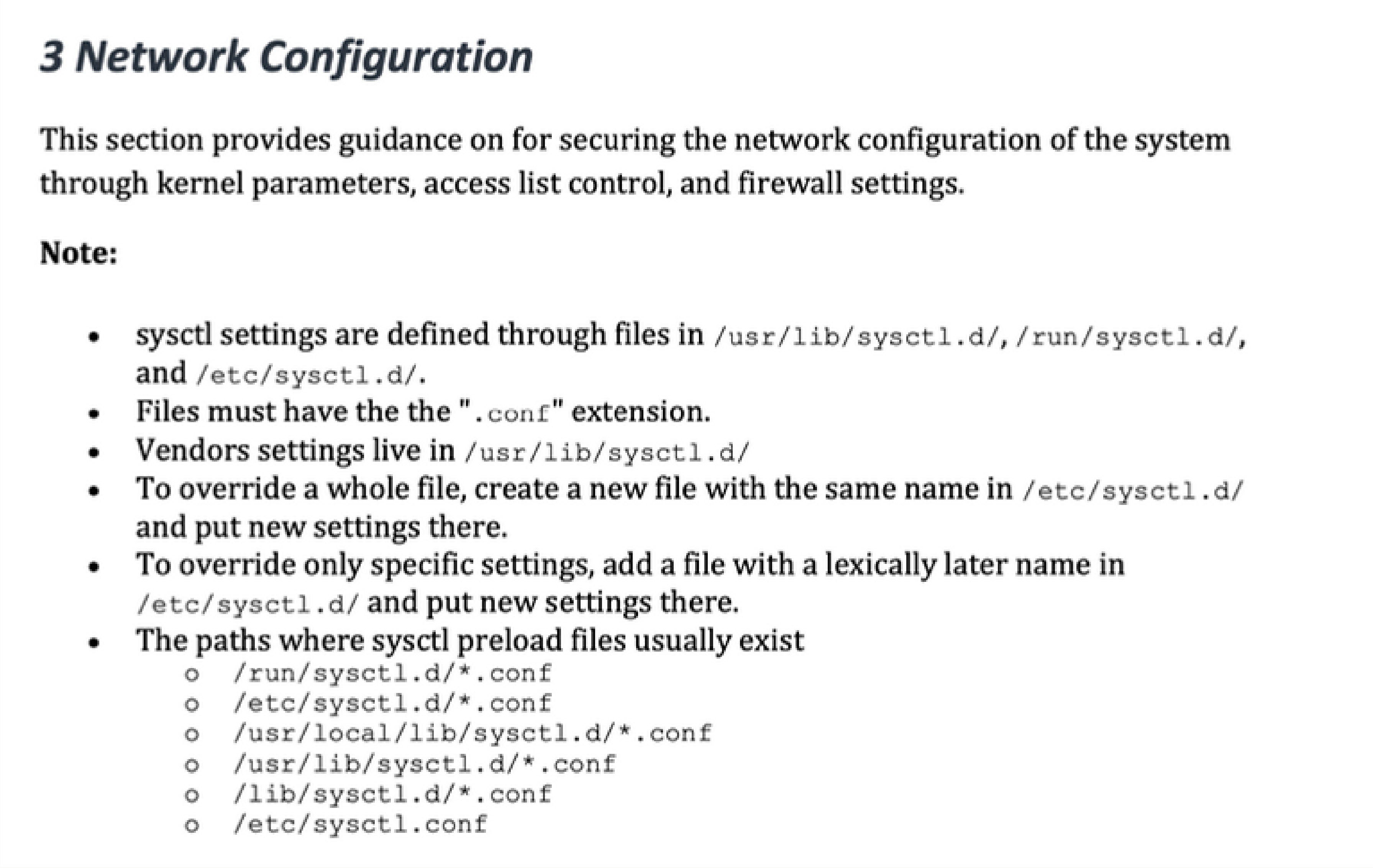
# CIS - network



| NUMBER | TITLE/DESCRIPTION | ASSET TYPE | SECURITY FUNCTION | IG1 | IG2 | IG3 |
|---|---|---|---|---|---|---|
| 12.1 | **Ensure Network Infrastructure is Up-to-Date**<br>Ensure network infrastructure is kept up-to-date. Example implementations include running the latest stable release of software and/or using currently supported network-as-a-service (NaaS) offerings. Review software versions monthly, or more frequently, to verify software support. | Network | Protect | ● | ● | ● |
| 12.2 | **Establish and Maintain a Secure Network Architecture**<br>Establish and maintain a secure network architecture. A secure network architecture must address segmentation, least privilege, and availability, at a minimum. | Network | Protect |  | ● | ● |
| 12.3 | **Securely Manage Network Infrastructure**<br>Securely manage network infrastructure. Example implementations include version-controlled-infrastructure-as-code, and the use of secure network protocols, such as SSH and HTTPS. | Network | Protect |  | ● | ● |
| 12.4 | **Establish and Maintain Architecture Diagram(s)**<br>Establish and maintain architecture diagram(s) and/or other network system documentation. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard. | Network | Identify |  | ● | ● |
| 12.5 | **Centralize Network Authentication, Authorization, and Auditing (AAA)**<br>Centralize network AAA. | Network | Protect |  | ● | ● |
| 12.6 | **Use of Secure Network Management and Communication Protocols**<br>Use secure network management and communication protocols (e.g., 802.1X, Wi-Fi Protected Access 2 (WPA2) Enterprise or greater). | Network | Protect |  | ● | ● |



| NUMBER | TITLE/DESCRIPTION | ASSET TYPE | SECURITY FUNCTION | IG1 | IG2 | IG3 |
|---|---|---|---|---|---|---|
| 13.1 | **Centralize Security Event Alerting**<br>Centralize security event alerting across enterprise assets for log correlation and analysis. Best practice implementation requires the use of a SIEM, which includes vendor-defined event correlation alerts. A log analytics platform configured with security-relevant correlation alerts also satisfies this Safeguard. | Network | Detect |  | ● | ● |
| 13.2 | **Deploy a Host-Based Intrusion Detection Solution**<br>Deploy a host-based intrusion detection solution on enterprise assets, where appropriate and/or supported. | Devices | Detect |  | ● | ● |
| 13.3 | **Deploy a Network Intrusion Detection Solution**<br>Deploy a network intrusion detection solution on enterprise assets, where appropriate. Example implementations include the use of a Network Intrusion Detection System (NIDS) or equivalent cloud service provider (CSP) service. | Network | Detect |  | ● | ● |
| 13.4 | **Perform Traffic Filtering Between Network Segments**<br>Perform traffic filtering between network segments, where appropriate. | Network | Protect |  | ● | ● |



## *3 Network Configuration*

This section provides guidance on for securing the network configuration of the system through kernel parameters, access list control, and firewall settings.

**Note:**

- sysctl settings are defined through files in `/usr/lib/sysctl.d/`, `/run/sysctl.d/`, and `/etc/sysctl.d/`.
- Files must have the the "`.conf`" extension.
- Vendors settings live in `/usr/lib/sysctl.d/`
- To override a whole file, create a new file with the same name in `/etc/sysctl.d/` and put new settings there.
- To override only specific settings, add a file with a lexically later name in `/etc/sysctl.d/` and put new settings there.
- The paths where sysctl preload files usually exist
  - `/run/sysctl.d/*.conf`
  - `/etc/sysctl.d/*.conf`
  - `/usr/local/lib/sysctl.d/*.conf`
  - `/usr/lib/sysctl.d/*.conf`
  - `/lib/sysctl.d/*.conf`
  - `/etc/sysctl.conf`

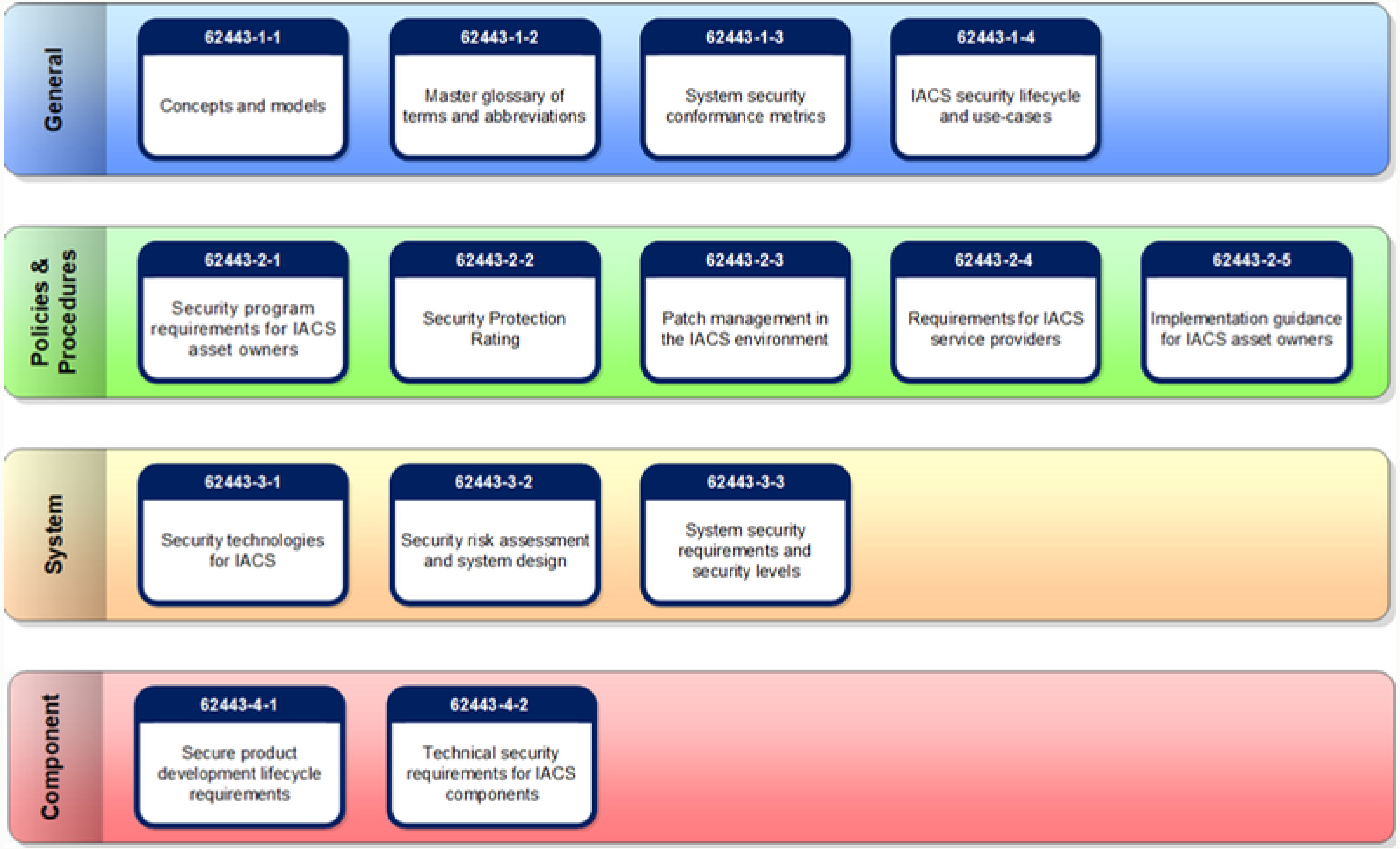
# ISA

ISA International Society of Automation

- Adoption of the NIST standards for the operating technologies (OT)
- the organisation has to formalise procedures and security policies, has a risk assessment plan
- policies and practices that are suitable for industrial automated control systems
- over 150 standards
- ISA standards committees produce two types of related documents:
    a. recommended practices (RP) with suggestions for applying a standard
    b. technical reports (TR) as guidance for understanding a topic/standard.

See: https://www.isa.org/standards-and-publications/isa-standards

# ISA



**General**

- 62443-1-1 Concepts and models
- 62443-1-2 Master glossary of terms and abbreviations
- 62443-1-3 System security conformance metrics
- 62443-1-4 IACS security lifecycle and use-cases

**Policies & Procedures**

- 62443-2-1 Security program requirements for IACS asset owners
- 62443-2-2 Security Protection Rating
- 62443-2-3 Patch management in the IACS environment
- 62443-2-4 Requirements for IACS service providers
- 62443-2-5 Implementation guidance for IACS asset owners

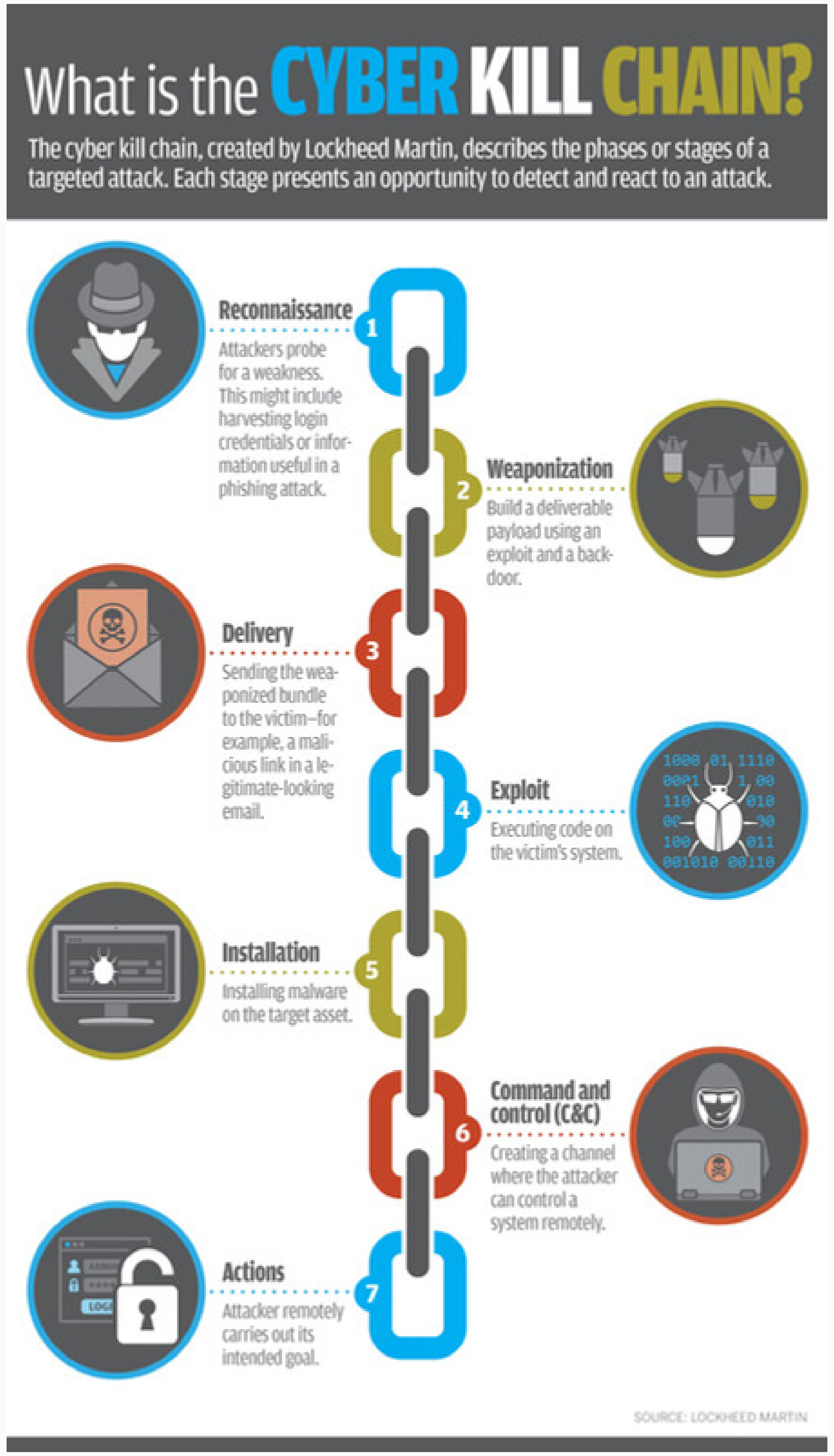
**System**

- 62443-3-1 Security technologies for IACS
- 62443-3-2 Security risk assessment and system design
- 62443-3-3 System security requirements and security levels

**Component**

- 62443-4-1 Secure product development lifecycle requirements
- 62443-4-2 Technical security requirements for IACS components

# Cyber Security Kill Chain



What is the CYBER KILL CHAIN?

The cyber kill chain, created by Lockheed Martin, describes the phases or stages of a targeted attack. Each stage presents an opportunity to detect and react to an attack.

1 **Reconnaissance** Attackers probe for a weakness. This might include harvesting login credentials or information useful in a phishing attack.

2 **Weaponization** Build a deliverable payload using an exploit and a backdoor.

3 **Delivery** Sending the weaponized bundle to the victim—for example, a malicious link in a legitimate-looking email.

4 **Exploit** Executing code on the victim's system.

5 **Installation** Installing malware on the target asset.

6 **Command and control (C&C)** Creating a channel where the attacker can control a system remotely.

7 **Actions** Attacker remotely carries out its intended goal.

SOURCE: LOCKHEED MARTIN

**Cyber Security Kill Chain Intrustion model explains the typical procedure that hackers take when performing a successful cyber attack. Developed by Lockheed Martin and is derived from military attack models**

This model is implemented by Mittre Att&ck and has 7 steps:

1. reconnaissance
2. weaponisation
3. delivery
4. exploit
5. installation
6. C2 (command and control)
7. Actions

Source: www.csoonline.com

# Mittre Att&ck

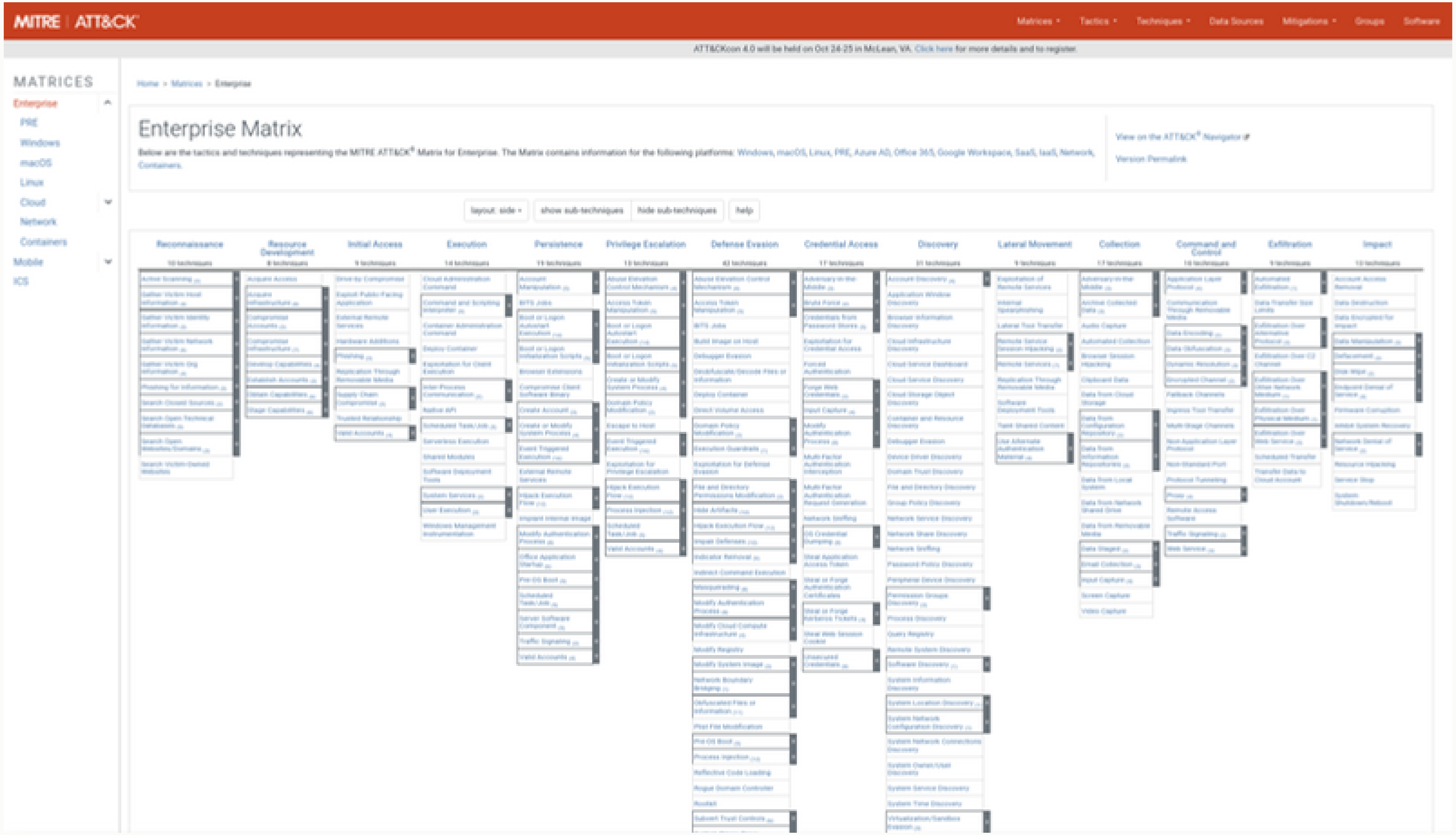
- security framework,
- KB for cyber adversary behaviour based on real-world observations,
- used by cybersecurity professionals to understand, analyze, and defend against cyber threats,
- useful to plan for security improvements,
- useful to understand security risks against known adversary behaviour.

ATT&CK®

**KB organised into a matrix of tactics and techniques (goals and  methodology):**

- **tactics = initial access, execution, persistence, exfiltration**
- **techniques: phishing, scripting, keys, encryption**

# Mittre Att&ck



ATT&CKcon 4.0 will be held on Oct 24-25 in McLean, VA. Click here for more details and to register.

## Enterprise Matrix

Below are the tactics and techniques representing the MITRE ATT&CK® Matrix for Enterprise. The Matrix contains information for the following platforms: Windows, macOS, Linux, PRE, Azure AD, Office 365, Google Workspace, SaaS, IaaS, Network, Containers.

| Reconnaissance | Resource Development | Initial Access | Execution | Persistence | Privilege Escalation | Defense Evasion |
|---|---|---|---|---|---|---|
| 10 techniques | 8 techniques | 9 techniques | 14 techniques | 19 techniques | 13 techniques | 42 techniques |
| Active Scanning | Acquire Access | Drive-by Compromise | Cloud Administration Command | Account Manipulation | Abuse Elevation Control Mechanism | Abuse Elevation Control Mechanism |
| Gather Victim Host Information | Acquire Infrastructure | Exploit Public-Facing Application | Command and Scripting Interpreter | BITS Jobs | Access Token Manipulation | Access Token Manipulation |
| Gather Victim Identity Information | Compromise Accounts | External Remote Services | Container Administration Command | Boot or Logon Autostart Execution | Boot or Logon Autostart Execution | BITS Jobs |
| Gather Victim Network Information | Compromise Infrastructure | Hardware Additions | Deploy Container | Boot or Logon Initialization Scripts | Boot or Logon Initialization Scripts | Build Image on Host |
| Gather Victim Org Information | Develop Capabilities | Phishing | Exploitation for Client Execution | Browser Extensions | Create or Modify System Process | Debugger Evasion |
| Phishing for Information | Establish Accounts | Replication Through Removable Media | Inter-Process Communication | Compromise Client Software Binary | Domain Policy Modification | Deobfuscate/Decode Files or Information |
| Search Closed Sources | Obtain Capabilities | Supply Chain Compromise | Native API | Create Account | Escape to Host | Deploy Container |
| Search Open Technical Databases | Stage Capabilities | Trusted Relationship | Scheduled Task/Job | Create or Modify System Process | Event Triggered Execution | Direct Volume Access |
| Search Open Websites/Domains | | Valid Accounts | Serverless Execution | Event Triggered Execution | Exploitation for Privilege Escalation | Domain Policy Modification |
| Search Victim-Owned Websites | | | Shared Modules | External Remote Services | Hijack Execution Flow | Execution Guardrails |
| | | | Software Deployment Tools | Hijack Execution Flow | Process Injection | Exploitation for Defense Evasion |
| | | | System Services | Implant Internal Image | Scheduled Task/Job | File and Directory Permissions Modification |
| | | | User Execution | Modify Authentication Process | Valid Accounts | Hide Artifacts |
| | | | Windows Management Instrumentation | Office Application Startup | | Hijack Execution Flow |
| | | | | Pre-OS Boot | | Impair Defenses |
| | | | | Scheduled Task/Job | | Indicator Removal |
| | | | | Server Software Component | | Indirect Command Execution |
| | | | | Traffic Signaling | | Masquerading |
| | | | | Valid Accounts | | Modify Authentication Process |
| | | | | | | Modify Cloud Compute Infrastructure |
| | | | | | | Modify Registry |
| | | | | | | Modify System Image |
| | | | | | | Network Boundary Bridging |
| | | | | | | Obfuscated Files or Information |
| | | | | | | Plist File Modification |
| | | | | | | Pre-OS Boot |
| | | | | | | Process Injection |
| | | | | | | Reflective Code Loading |
| | | | | | | Rogue Domain Controller |
| | | | | | | Rootkit |
| | | | | | | Subvert Trust Controls |

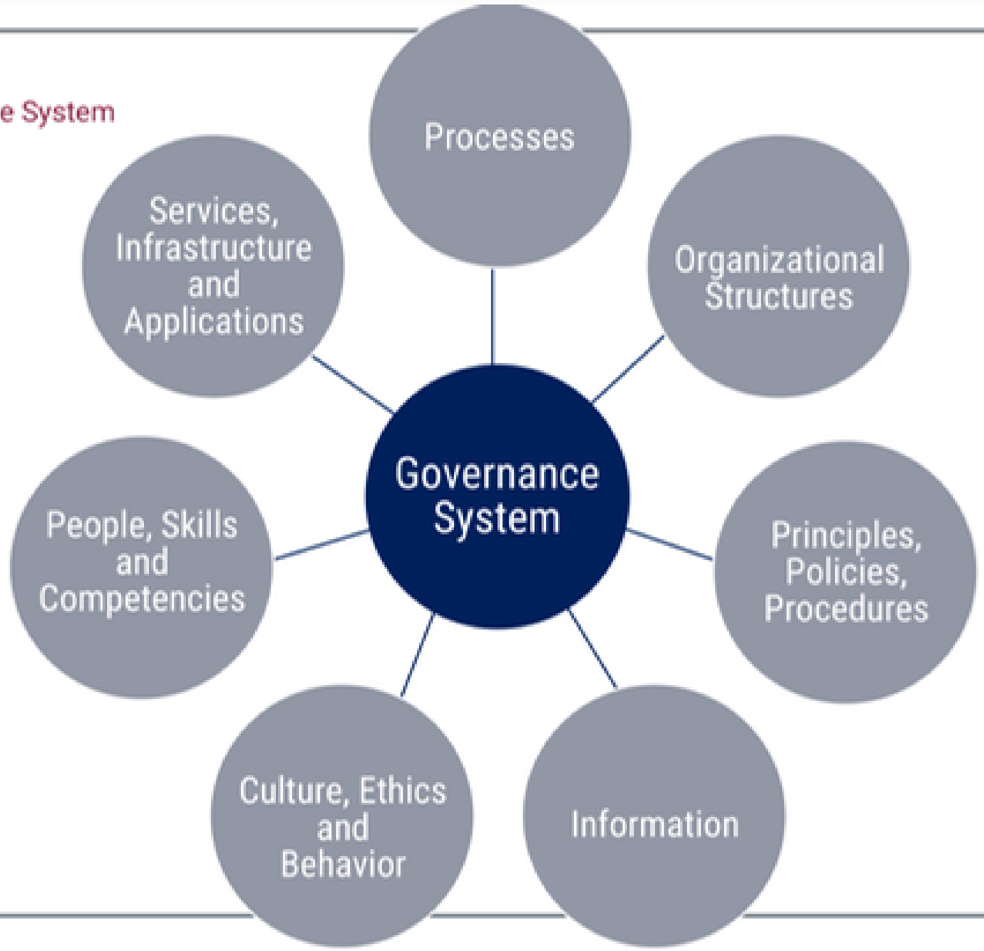
| Credential Access | Discovery | Lateral Movement | Collection | Command and Control | Exfiltration | Impact |
|---|---|---|---|---|---|---|
| 17 techniques | 31 techniques | 9 techniques | 17 techniques | 16 techniques | 9 techniques | 13 techniques |
| Adversary-in-the-Middle | Account Discovery | Exploitation of Remote Services | Adversary-in-the-Middle | Application Layer Protocol | Automated Exfiltration | Account Access Removal |
| Brute Force | Application Window Discovery | Internal Spearphishing | Archive Collected Data | Communication Through Removable Media | Data Transfer Size Limits | Data Destruction |
| Credentials from Password Stores | Browser Information Discovery | Lateral Tool Transfer | Audio Capture | Data Encoding | Exfiltration Over Alternative Protocol | Data Encrypted for Impact |
| Exploitation for Credential Access | Cloud Infrastructure Discovery | Remote Service Session Hijacking | Automated Collection | Data Obfuscation | Exfiltration Over C2 Channel | Data Manipulation |
| Forced Authentication | Cloud Service Dashboard | Remote Services | Browser Session Hijacking | Dynamic Resolution | Exfiltration Over Other Network Medium | Defacement |
| Forge Web Credentials | Cloud Service Discovery | Replication Through Removable Media | Clipboard Data | Encrypted Channel | Exfiltration Over Physical Medium | Disk Wipe |
| Input Capture | Cloud Storage Object Discovery | Software Deployment Tools | Data from Cloud Storage | Fallback Channels | Exfiltration Over Web Service | Endpoint Denial of Service |
| Modify Authentication Process | Container and Resource Discovery | Taint Shared Content | Data from Configuration Repository | Ingress Tool Transfer | Scheduled Transfer | Firmware Corruption |
| Multi-Factor Authentication Interception | Debugger Evasion | Use Alternate Authentication Material | Data from Information Repositories | Multi-Stage Channels | Transfer Data to Cloud Account | Inhibit System Recovery |
| Multi-Factor Authentication Request Generation | Device Driver Discovery | | Data from Local System | Non-Application Layer Protocol | | Network Denial of Service |
| Network Sniffing | Domain Trust Discovery | | Data from Network Shared Drive | Non-Standard Port | | Resource Hijacking |
| OS Credential Dumping | File and Directory Discovery | | Data from Removable Media | Protocol Tunneling | | Service Stop |
| Steal Application Access Token | Group Policy Discovery | | Data Staged | Proxy | | System Shutdown/Reboot |
| Steal or Forge Authentication Certificates | Network Service Discovery | | Email Collection | Remote Access Software | | |
| Steal or Forge Kerberos Tickets | Network Share Discovery | | Input Capture | Traffic Signaling | | |
| Steal Web Session Cookie | Network Sniffing | | Screen Capture | Web Service | | |
| Unsecured Credentials | Password Policy Discovery | | Video Capture | | | |
| | Peripheral Device Discovery | | | | | |
| | Permission Groups Discovery | | | | | |
| | Process Discovery | | | | | |
| | Query Registry | | | | | |
| | Remote System Discovery | | | | | |
| | Software Discovery | | | | | |
| | System Information Discovery | | | | | |
| | System Location Discovery | | | | | |
| | System Network Configuration Discovery | | | | | |
| | System Network Connections Discovery | | | | | |
| | System Owner/User Discovery | | | | | |
| | System Service Discovery | | | | | |
| | System Time Discovery | | | | | |
| | Virtualization/Sandbox Evasion | | | | | |

# COBIT

- Control Objectives for Information and Related Technologies
- good-practice framework made by ISACA
- suitable for enterprises

See: https://www.isaca.org/resources/cobit

**Figure 4.3**
COBIT Components of a Governance System



Governance System

Processes

Organizational Structures

Principles, Policies, Procedures

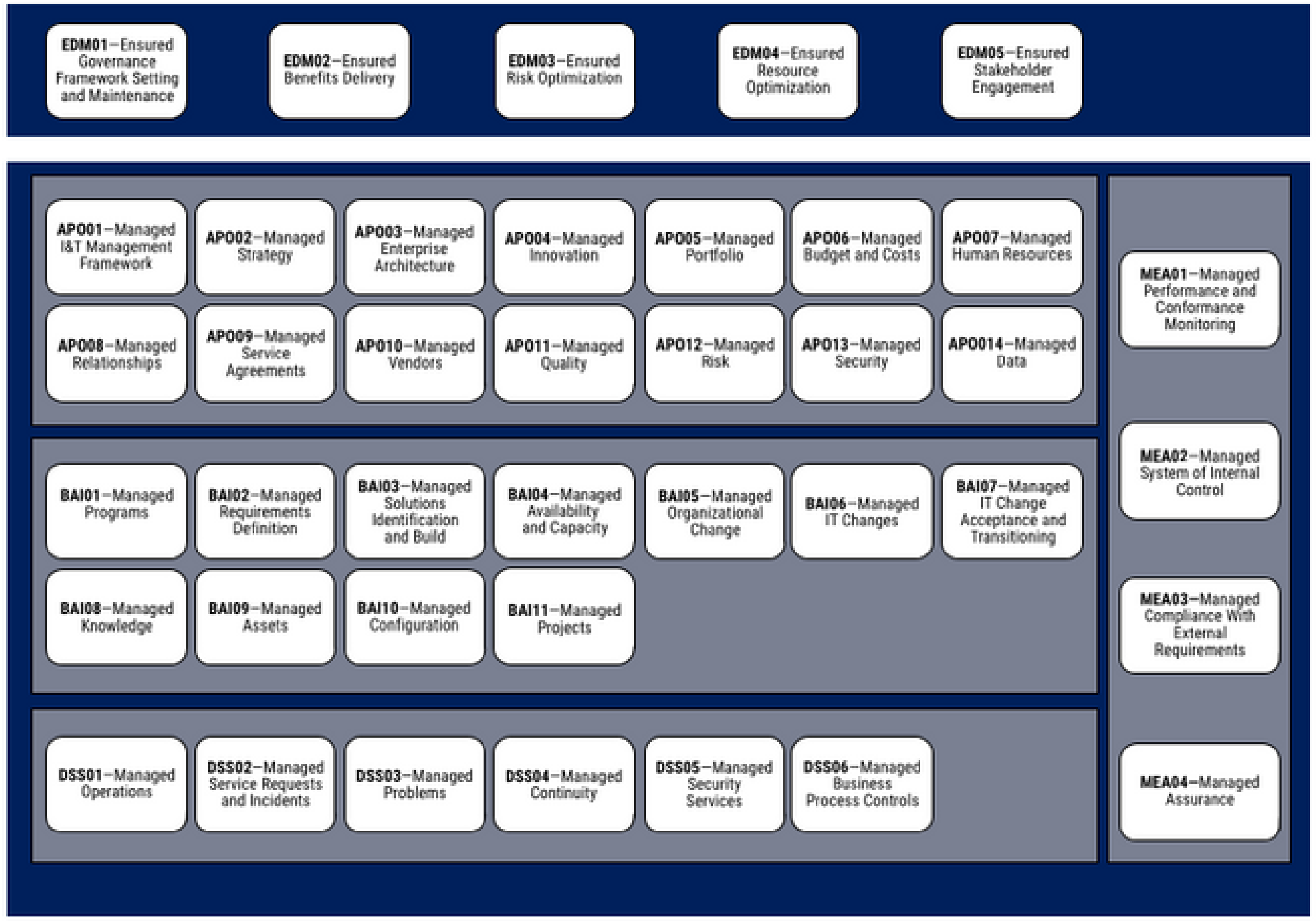
Information

Culture, Ethics and Behavior

People, Skills and Competencies

Services, Infrastructure and Applications

**Figure 4.2**
COBIT Core Model



**EDM01**—Ensured Governance Framework Setting and Maintenance

**EDM02**—Ensured Benefits Delivery

**EDM03**—Ensured Risk Optimization

**EDM04**—Ensured Resource Optimization

**EDM05**—Ensured Stakeholder Engagement

**APO01**—Managed I&T Management Framework

**APO02**—Managed Strategy

**APO03**—Managed Enterprise Architecture

**APO04**—Managed Innovation

**APO05**—Managed Portfolio

**APO06**—Managed Budget and Costs

**APO07**—Managed Human Resources

**APO08**—Managed Relationships

**APO09**—Managed Service Agreements

**APO10**—Managed Vendors

**APO11**—Managed Quality

**APO12**—Managed Risk

**APO13**—Managed Security

**APO014**—Managed Data

**BAI01**—Managed Programs

**BAI02**—Managed Requirements Definition

**BAI03**—Managed Solutions Identification and Build

**BAI04**—Managed Availability and Capacity

**BAI05**—Managed Organizational Change

**BAI06**—Managed IT Changes

**BAI07**—Managed IT Change Acceptance and Transitioning

**BAI08**—Managed Knowledge

**BAI09**—Managed Assets

**BAI10**—Managed Configuration

**BAI11**—Managed Projects

**DSS01**—Managed Operations

**DSS02**—Managed Service Requests and Incidents

**DSS03**—Managed Problems

**DSS04**—Managed Continuity

**DSS05**—Managed Security Services

**DSS06**—Managed Business Process Controls

**MEA01**—Managed Performance and Conformance Monitoring

**MEA02**—Managed System of Internal Control

**MEA03**—Managed Compliance With External Requirements

**MEA04**—Managed Assurance

# Information security related regulations in EU

- The European General Data Protection Regulation (GDPR)
- Digital future strategy
- The Network and Information Systems Directive (NIS Directive)
- Revision of the NIS Directive (New NIS2 Directive)
- The EU Cybersecurity Act
- The EU-Wide Cybersecurity Certification Scheme

A collection of all EC standards can be found here (=! regulation):
https://ec.europa.eu/info/files/security-standards-information-systems_en

# Establish security policies

## How to put policies in place?

- Use the documentation and templates, that are already available:
  - AARC Project: https://aarc-project.eu/policies/policy-development-kit/
  - WISE: https://wise-community.org/published_documents

# QUIZ

- What kind of skills does a security architect need?
  - technical skills
  - management skills
  - risk assessment skills
  - communication skills
  - all above

- Which security framework is most suitable for OT systems?
  - ISA
  - NIST CSF
  - COBIT

- Which of the following security controls are added to the new ISO27001:2022 standard?
  - Configuration management
  - Physical security
  - Human resource security

# Physical security

**Physical security is the protection of personnel, hardware, software, networks and data from physical actions and events that could cause serious loss or damage to an enterprise, agency or institution. This includes protection from fire, flood, natural disasters, burglary, theft, vandalism and terrorism. (definition by Techtarget)**

**ISO27001:2022** includes physical and environmental security controls to safeguard information systems from physical threats. It expands on the control related to safe areas to cloud environments.

- Is important equipment vulnerable?
- Where can the equipment be used?
- Who is responsible for maintenance?
- Are policies in place for using equipment that leaves the premises?

Also EC published its standard on physical and environmental security, with the same focus as ISO27k.  Download here: https://commission.europa.eu/select-language?destination=/media/6775

# Physical security - threats

**What are the threats that physical security controls should tackle:**

- Fire,
- water damage,
- destruction of equipment,
- earthquakes,
- failure of air conditioning,
- loss of power supply,
- remote spying,
- eavesdropping,

- tempering,
- disclosure,
- unauthorised use,
- corruption of stored data
- theft
- etc.

# Physical security by ISO27k

**ISO27001 includes the following categories of physical and environmental security controls:**

- **Secure areas (including virtual/cloud):** walls, card-controlled entry gates, physical security for offices, data centres, protection against flood, fire, and earthquake, access control for secure areas, IAM etc.
- **Physical entry controls**: CCTV surveillance, security guards, protective barriers, locks, perimeter intrusion detection, policy on visitor management process etc.
- **Equipment security:** protected from power failures, unauthorised usage, fire protection, clear policies for removable storage media, and policies on data removal that are saved on the equipment.
- **Reuse of equipment:** clear policy on data erasure and destruction
- **Protection against environmental threats:** controls for monitoring environmental conditions, such as temperature, humidity, air quality

# Hardware Security

**Hardware security includes:**

- secure hardware design,
- access controls,
- secure procurement process,
- secure supply chain (shipping, credentialing of all involved participants etc.),
- maintenance,
- security of hardware off-premises.

**Hardware must be protected from physical and environmental threats and from opportunities for unauthorised access.**

- Place sensitive equipment in a well-protected zone
- Monitor and restrict access to the equipment, both physical access and software-based access.
- Disable unused interfaces (physically, in BIOS, from OS) or configure them in a restrictive manner, e.g. USB device whitelisting.
- Power and communication cables must be protected

# QUIZ

- Which is NOT part of ISO27k on physical security?
  - secure areas
  - physical access controls
  - reuse of equipment
  - fire procedure

- `Is the following true or false?
  - Cloud equipment was only added to ISO27k standard in the 2022 release?
  - EC has no standards or guidelines on physical security?
  - Because of the remote work, organisations had to address the use of equipment off-premises in their policies?

# Network security

Objective of network security is to reduce attack surface and provide isolation.

**Since the network is the attack vector, monitoring is crucial to detect (attempts for) compromises**

**TO GET THE WHOLE PICTURE**

Conceptual network design includes the identification of all core components of the network architecture, to have an overview of what the purpose of the network is.

Understanding the threats to your system is crucial. What are the attack methods? And what are the attacker's objectives? Where is your critical data? Who has access to it?

Main problem:

- many network devices are not kept up to date
- many network devices are accessible from external network
- many network devices are accessible via a password
- network is not segmented, critical services are not isolated.

# Network design

## NETWORK TOPOLOGY

**PHYSICAL:** how the nework is connected, how the data flows
**LOGICAL**: how services communicate, which protocols are used.

Detect what you cannot prevent.

## NETWORK DESIGN CONSIDERATIONS

- Network segmentation
- Secure channels (VPN)
- Network access control
- Security policy enforcement
- Regulatory compliance
- CIA triad

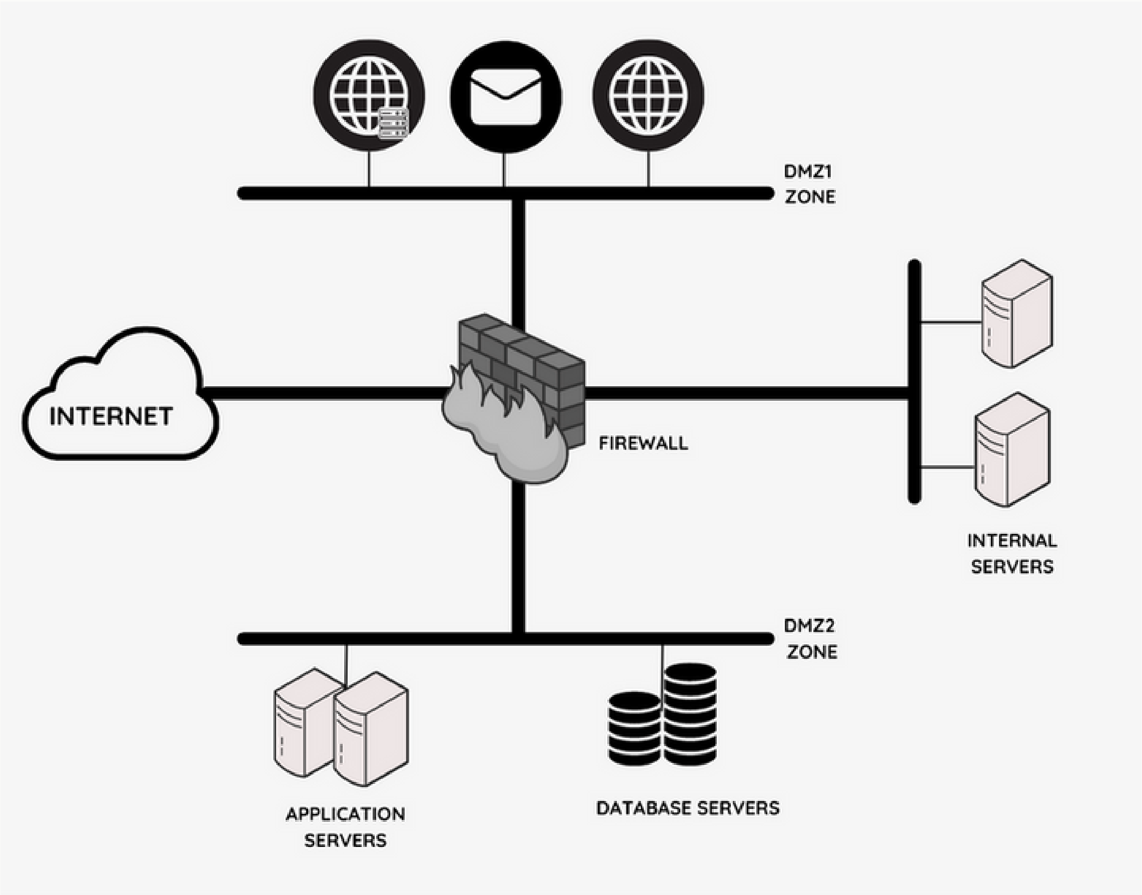
**Network segmentation means that we split the network into multiple segments/sub-networks by using firewalls, VLANs, access controls or SDN.**

### How to segregate?

- follow the least privilege rule and only provide access to the system when it is necessary
- define network segments based on the location of sensitive data and critical services
- KISS principle = keep it simple stupid
- Guests should have access to the Internet, but not to the internal network
- Services and desktop users should be in different subnets

# Why segregate?

- to ensure isolation
- to improve performance (less congestion in network traffic
- to reduce attack surface
- to prevent single point of failure
- to improve network monitoring



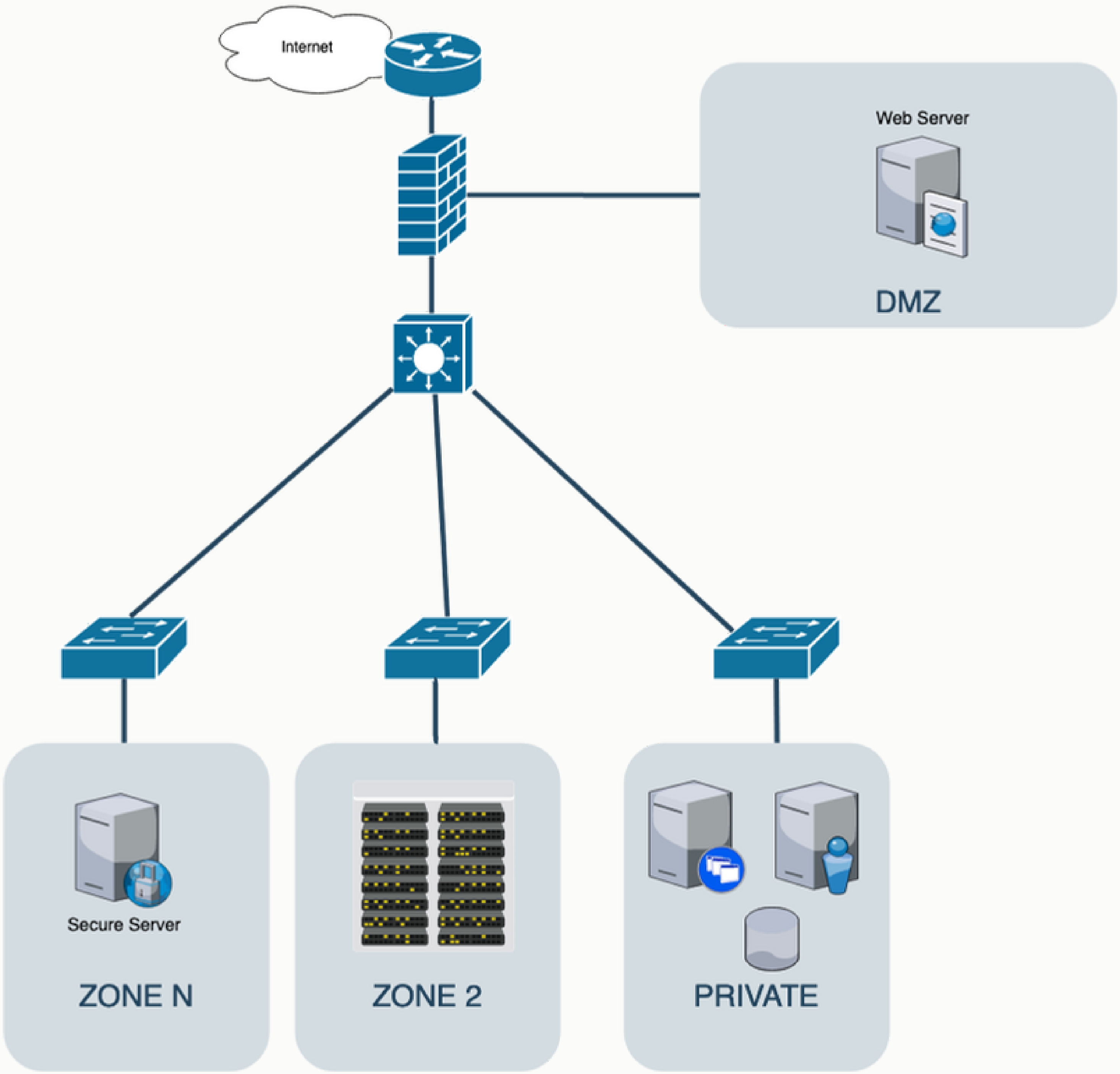
https://www.zenarmor.com/docs/network-basics/network-segmentation

**DO NOT SEGREGATE TOO MUCH**

Multiple segments lead to:

- additional costs
- more chances for misconfigurations
- increased complexity
- multiple access policies to maintain

# Common network segments



**PUBLIC NETWORK** - Internet, not under control of an organisation
**DMZ NETWORK** - semi-public network, services that need access to the internet (web, mail, DNS etc.)
**MIDDLEWARE NETWORK** - used to separate DMZ from private network (filtered access, proxy servers),
**PRIVATE NETWORK** - internal services (sensitive information) - only access from middleware network is possible

Firewall usually placed between public and other networks. Also between DMZ and private network and also between trusted zones.

# Basics for network design

- Allow internal users to access the internet,
- services that require Internet access should be limited,
- access to the internal services should be prohibited from the public networks, it should be restricted to DMZ,
- resources in public networks cannot be trusted,
- a system that is visible from the Internet cannot contain sensitive data, sensitive services need to be in a private network,
- DMZ communicates with private networks via proxy,
- apply zero trust principle in all segments,
- apply defence-in-depth (segmentation + firewall(s) + IDS + attack mitigation software etc.),
- databases and storage systems should not be accessible from the public internet.

# Network attacks against devices

**Attacks against routers:**

- DoS
- DDoS
- packet sniffing
- packet misrouting
- SYN flood
- TCP reset attack
- Insider threat

**Attacks against switches:**

- MAC Flooding
- Brute force Password Attack
- DHCP Spoofing and Starvation
- STP Attacks
- VLAN hopping
- Telnet attack
- CDP Manipulation

**How to defend your network against these attacks?**

- Shut down/disable unused services and ports.
- Use strong passwords and a well-defined password change policy. If possible, disable password login completely.
- Control physical access to devices.
- Use tools for automatic configuration, this ensures a backup of your configuration.
- Patch devices for security issues.
- Implement defense-in-depth approach.
- Perform security auditing.

# How to prevent attacks from network?

- Account lock-out,
- configure rate-limiting,
- use the deny rule by default and only open the ports that are really necessary,
- use packet filtering (looks into packet header and checks source and destination IP and port),
- use stateful packet inspection (open header/envelope to see the context),
- use proxies to ensure another layer of protection (MIM inspection),
- use NAT for internal networks (local IPs that are not routable across the internet),
- enable IP source verification (customer cannot spoof its IP address),
- LPTS = local packet transport service - configure allowed settings (e.g. number of allowed ICMP packets, number of TCP sessions etc.,
- provide continuous monitoring,
- defence-in-depth (multiple layers of security),
- use VPN - it provides a secure channel over an untrusted network, encrypted packets (broad vs. application-specific VPN),
- DDoS protection (such as BGP Flowspec, which blocks ports that are part of a DDoS attack automatically).
- use IDS/IPS.

# Network security devices

PREVENTION

- **Firewall** - as a hardware appliance, as software inserted into a network device for other purposes, or software firewall.
    - hw option is a router with a filtering ruleset, it increases privacy and reduces risks, enforces the organisation's security policy
- **IPS** - Intrusion protection system

DETECTION

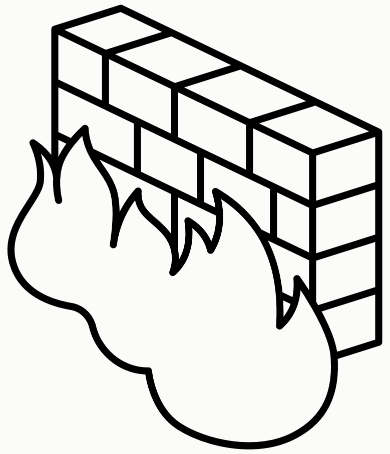
- **IDS -** Intrusion detection system

# Firewall

- ***Benefits***
  - it enforces organisation’s security policy
  - it protects systems from incoming and outgoing attacks
  - ingress and egress traffic filtering
  - filtering communication based on content
  - it encrypts communication
  - in stores logs about successful and blocked traffic
  - in increases privacy

- ***Shortcomings***
  - they cannot prevent attacks on applications
  - encrypted traffic (e.g. VPN) might bypass it
  - organisation sees firewall as sufficient security control
  - if the traditional approach is in use, they represent a single point of failure

**A firewall is just one of the technological security controls. To be secure, an organisation has to apply a defence-in-depth principle, implementing multi-layer security. If one control fails, another one is still in place to prevent a compromise.**



# Intrusion detection system

- ***NIDS = network IDS***

- serves as a detection system, it checks network traffic
- IDS can be seen as an alarm system, not as a firewall
- reports attacks against monitored systems
- the alerts that are sent, are revised by human
- it is deployed as a passive sniffer, captures traffic, detects events of interest and sends alerts
- it is placed in different points in the network

## VARIANTS of DETECTION:

- anomaly detection (relies on AI, it understands what normal traffic is and reports anomalies)
- signature-based detection (detection of bad patterns, malware) - has a db of patterns
- reputation-based detection (reports security events based on a reputation score

IDS process uses 2 methods of packet inspection:

- shallow packet inspection: checks header (is limited)
- deep packet inspection: inspection of all fields, including variable-length

IDS SOFTWARE:

- Suricata
- Snort
- Zeek
- Security Onion
- Sguil

Also HIDS = host intrusion detection system, checks traffic to/from device and local file changes

# Intrusion prevention system

- ***NIPS = network IPS***

- serves as a protection system
- often combined with the NIDS in the same software
- should be used in combination with a firewall and other security controls
- usually deployed right in front or behind the firewall, if behind the firewall, it can also check internal traffic
- rule-based approach
- problem if there are false-positives and stop legitimate traffic

Also HIPS = host intrusion protection system, stops attacks at the OS level

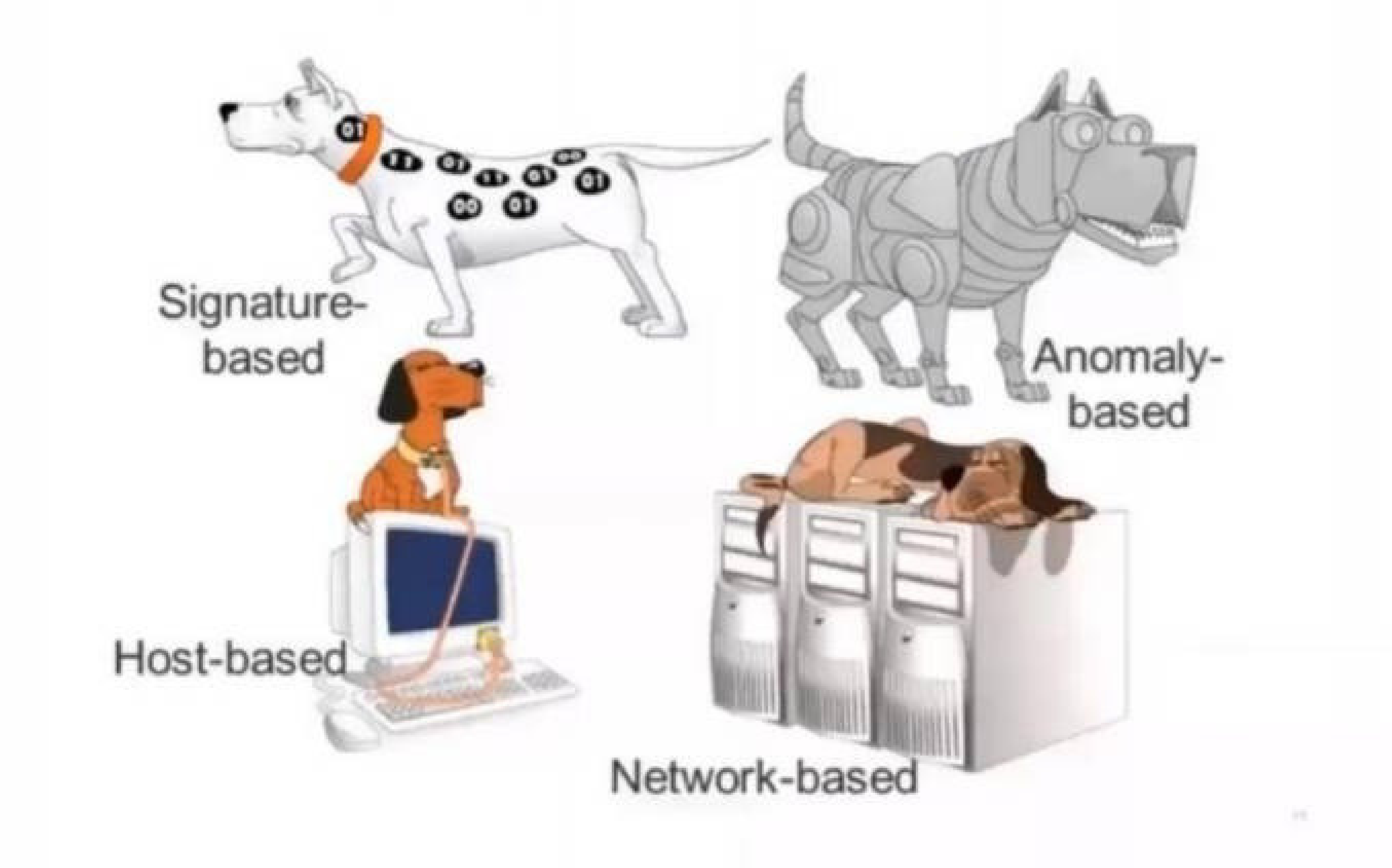
IPS SOFTWARE:

- Cisco IPS
- Snort
- Fail2ban
- Zeek
- SolarWinds

**IPS =! FIREWALL**

A firewall allows or denies traffic based on ports or the source/destination addresses. IPS compares traffic patterns to signatures and allows or drops packets based on any signature matches found.

# How IPS detects threats?

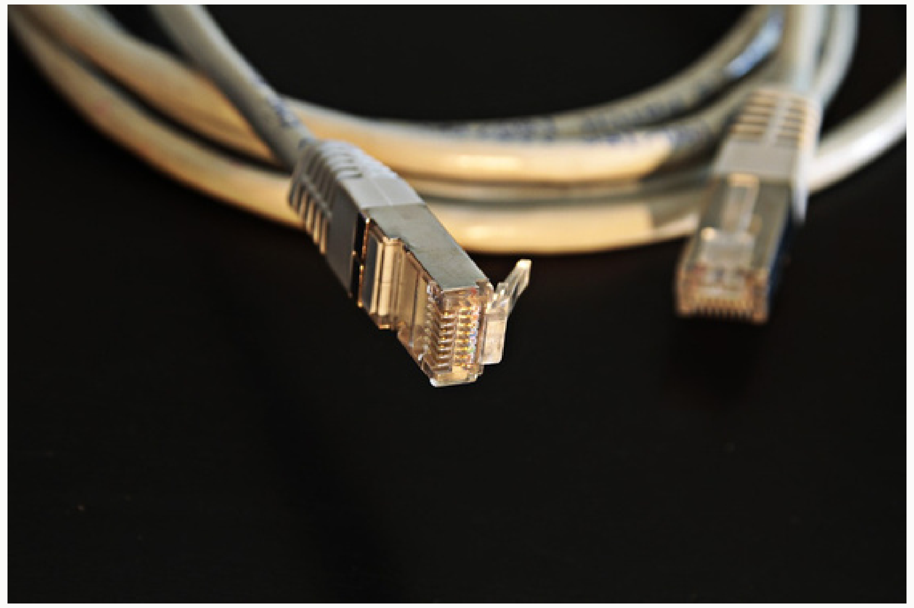


# Network Attack mitigation software

Usually, physical appliances, deployed between router and network firewall, commercial solutions. Prevent DDoS attacks (blackholes, scrubbing), brute force attacks, syn flood attacks etc.

EXAMPLES:

- Arbor Edge Defense (AED) is an inline security appliance deployed at the network perimeter (i.e. between the internet router and network firewall).
- F5 Silverline DDoS prevention
- Radware Defense pro



# NETWORK SECURITY POLICIES

A network security policy (NSP) is a generic document that outlines rules for computer network access, determines how policies are enforced and lays out some of the basic architecture of the company security/ network security environment. (Redhat)

- policies should be defined because they make us aware of how the system normally performs and what is allowed.
- policies can be enforced by firewalls, proxies, IDS/IPS, and ACLs on switches/routers, on the application level.

Useful security policies for your network:

- Account Management
- Password policy
- E-Mail policy
- Security Incident Management
- Log Management
- VPN Acceptable Use
- Server Security
- Bring Your Own Device (BYOD) Agreement
- Patch Management
- Systems Monitoring And Auditing
- Remote work policies
- Vulnerability Management
- Workstation Configuration Security

# IPv6 SECURITY

- Organisations are transitioning to IPv6. Security considerations encompass:
  - issues due to the IPv6 protocol itself,
  - o issues due to transition mechanisms, and
  - o issues due to IPv6 deployment.

See https://datatracker.ietf.org/doc/html/rfc4942

IPv6 uses 128-bit internet addresses, it can support 2^128 internet addresses. The number of IPv6 addresses is 1028 times larger than the number of IPv4 addresses

- Internet Society offers links to useful articles and standards: https://www.internetsociety.org/deploy360/ipv6/security/

# IPv6 SECURITY

IPv6 is not more secure than IPv4 by itself.

- Benefits of IPv6:
  - Auto-configuration of IP-addresses (no more DHCP)
  - Built-in authentication and privacy support (IPsec is part of the protocol suite)
  - No more private address collisions
  - QoS using the Flow Label field of the IPv6 header
  - Simpler header format
  - Better multicast routing
  - Simplified, more efficient routing
  - Flexible options and extensions
  - No more NAT (Network Address Translation)

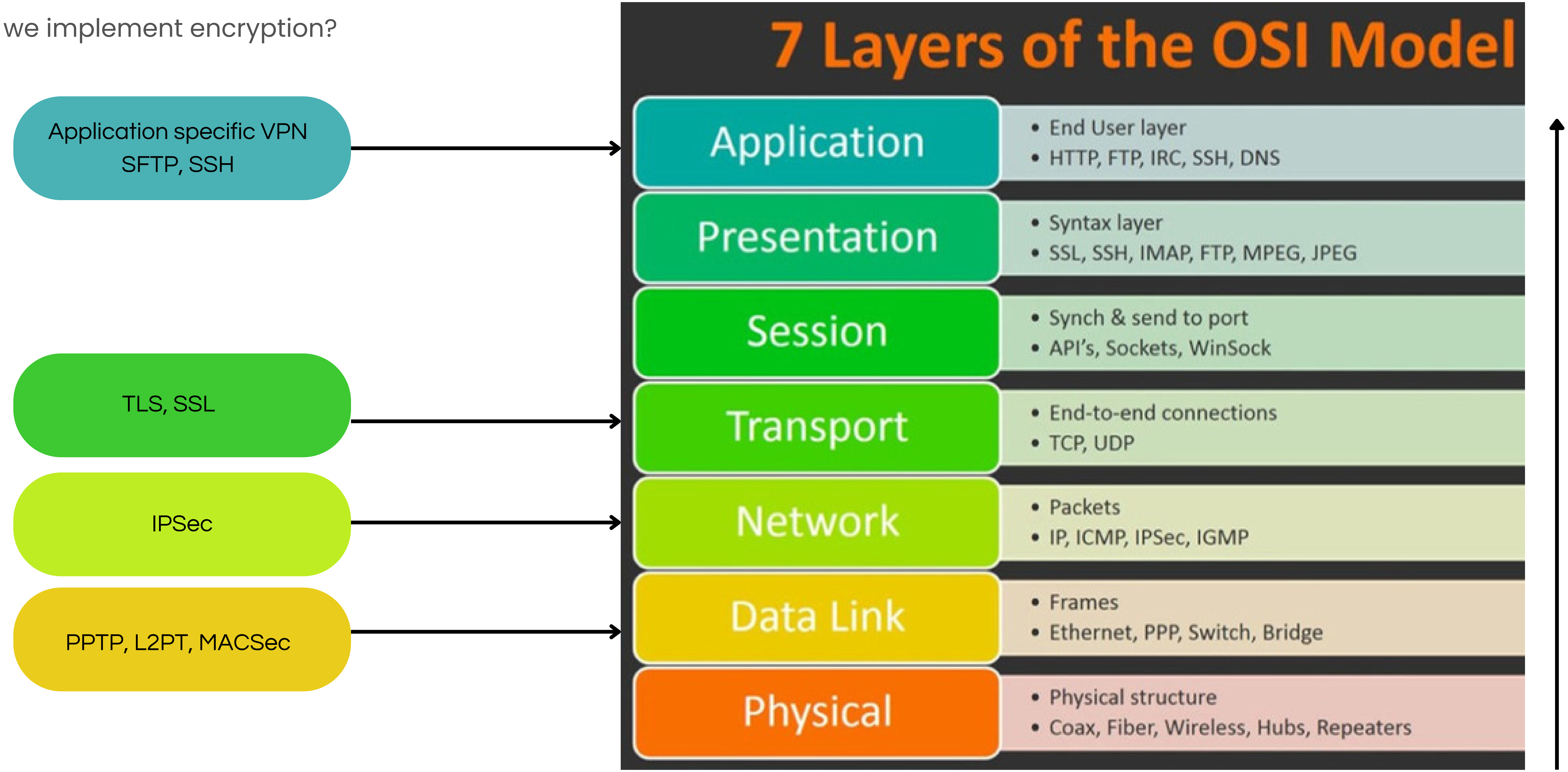
- **Problems:**
  - human error (IPv6 hardening not included by default, only IPv4)
  - Lack of knowledge and experience about IPv6
  - Ineffective Rate Limiting
  - Lack of IPv6 support at ISPs, service providers and vendors
  - a host can have multiple IPv6 addresses simultaneously, which is unusual in an IPv4 -> problem for IDS/IPS
  - IPv6 is often enabled by default, without knowing

# DEFENCE-IN-DEPTH

## Encryption

Where can we implement encryption?

Encryption in one layer means encryption in all upper layers.



Application specific VPN
SFTP, SSH

TLS, SSL

IPSec

PPTP, L2PT, MACSec

## 7 Layers of the OSI Model

| | |
|---|---|
| Application | • End User layer<br>• HTTP, FTP, IRC, SSH, DNS |
| Presentation | • Syntax layer<br>• SSL, SSH, IMAP, FTP, MPEG, JPEG |
| Session | • Synch & send to port<br>• API's, Sockets, WinSock |
| Transport | • End-to-end connections<br>• TCP, UDP |
| Network | • Packets<br>• IP, ICMP, IPSec, IGMP |
| Data Link | • Frames<br>• Ethernet, PPP, Switch, Bridge |
| Physical | • Physical structure<br>• Coax, Fiber, Wireless, Hubs, Repeaters |

# OTHER NETWORK SECURITY CONSIDERATIONS

01.

## Network security policies

Policies are a translation of network requirements into a set of rules. Policies should be defined, they make us aware of how the system normally performs and what is allowed.

02.

## Network access control

Security mechanisms include limiting physical access to devices, security policies, user authentication, device security, firewalls, proxies and others.

03.

## Software defined network

The objective is to make the network as flexible and as agile as a VM. SDN enables micro-segmentation and decreases the exposure to system attacks.

04.

## KISS principle

A too-complex network design will be difficult to manage. Find a compromise between the complexity and usability.

# Network security tools

- **Wireshark + tshark** - network sniffer
- **Metasploit** - scanners for more than 1500 operations
- **Nessus** - identifies and corrects faulty updates
- **OpenVAS** - checks configuration and basic web flaws
- **Argus** - open-source network analysis tool
- **tcpdump** - network sniffer
- **Kali linux** - bootable Linux with multiple security and forensics tools
- **Snort** - network intrusion detection and prevention system (traffic analysis)
- **Suricata** - IPS
- **Netcat** - utility that reads/writes data accross TCP/UDP network connections
- **nmap**

## Traffic sniffers

- Snort
- tcpdump
- Wireshark
- dsniff (for switches)
- Kismet (for wireless)
- nmap

# Logging and monitoring

CENTRAL LOGGING

- Loki
- ELK
- rsyslog
- syslog-ng
- Graylog
- Splunk

WHAT TO LOG?

- network traffic
- syslog from devices
- snmp for network devices
- ntp (sync time across entire network)

- Use central logging
- normalise and visualise logs
- analyse daily operations and look into security events that may be signs of an attack, apply countermeasurements
- collect snmp logs, ntp logs and network traffic logs
- collect syslog from devices

# Network device hardening

- CISCO DEVICES:
- passwords are not encrypted by default
- ssh version 1 by default, change to version 2
- console password is not set, do it
- disable telnet (plain text), only allow ssh acces
- limit access to console

- disable unused ports
- unused ports can be put in a separate VLAN which is not used
- disable unused services (for instance http server is enabled by default on Cisco devices)
- use infrastructure ACLs - disable invalid traffic from external network, eg. only allow web traffic for www, block everything else (filter fragments)
- use port security - port is configured for a specific MAC or only certain range is allowed
- limit remote access to console

# QUIZ

- Are the following statements true or false?
  - The objective of network security is to reduce the attack surface.
  - It is not possible to implement defence-in-depth only on the network layer
  - NAT should be used for internal networks.
  - Security of network devices includes primarily physical security, remote access control and environmental threats.
  - Cisco devices have SHA256 set as default password encryption.
  - Port Security feature can protect the switch from MAC flooding attacks and from DDoS.

- Which access mode should be disabled on network devices, because it sends username and password in plain text?

- `Name at least three measures that apply to network security?

- Explain at least 3 ways for hardening network devices.