

APRIL 2025

# FUNDAMENTALS OF SECURITY ARCHITECTURE

Barbara Krašovec



# **TABLE** of contents

**1. What is security architecture?**

**2. Fundamental security principles**

**3. How to design security infrastructure?**

**4. Security Culture**

**5. Security frameworks**

**6. Security policies**

**7. Identity and Access Management**

**8. Network security**

# 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.



**Strategy for designing a security infrastructure of your organisation.**

**Security elements to ensure data confidentiality, integrity and availability.**

# Security Principles

# 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

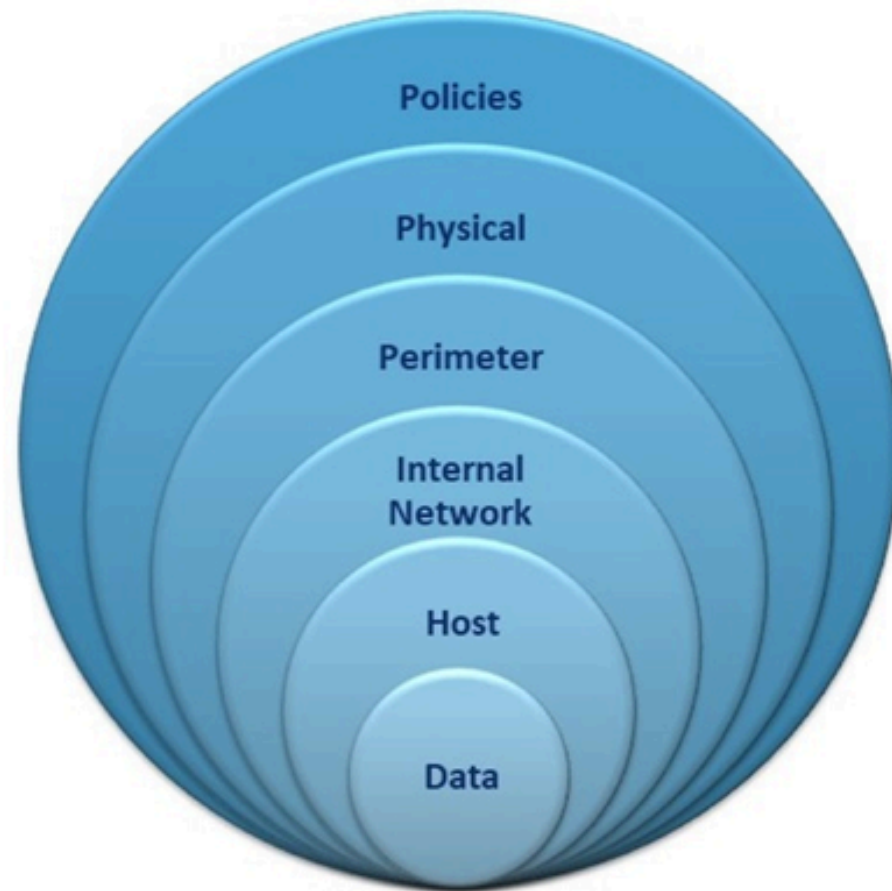
Cybersecurity is the protection of Confidentiality, Integrity and Availability of information in the system.

# Defence-in-depth

- Any layer of protection might fail  
→ **Multilayered defence**

- 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

Defence in Depth Layers

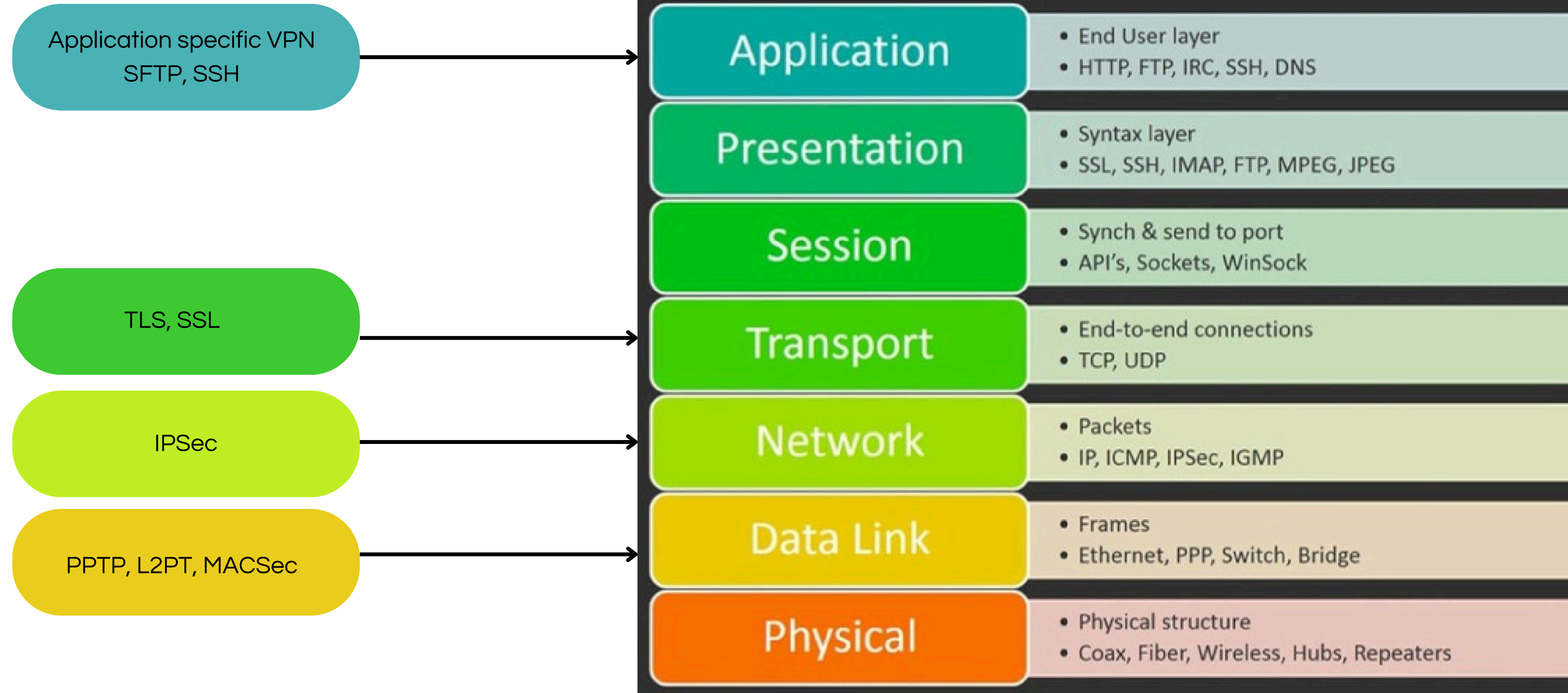


# DEFENCE-IN-DEPTH

## Encryption

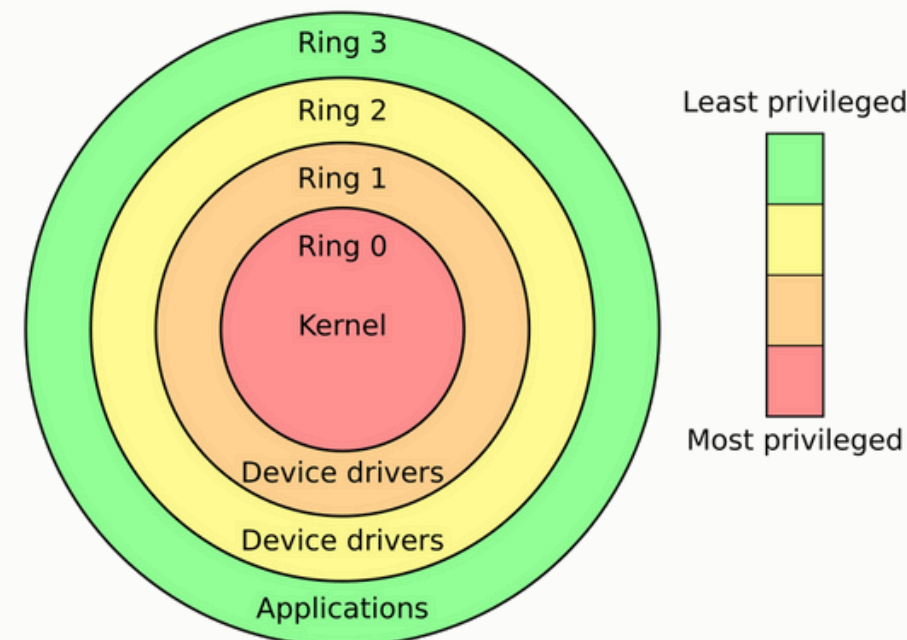
Where can we implement encryption?

Encryption in one layer means encryption in all upper layers.

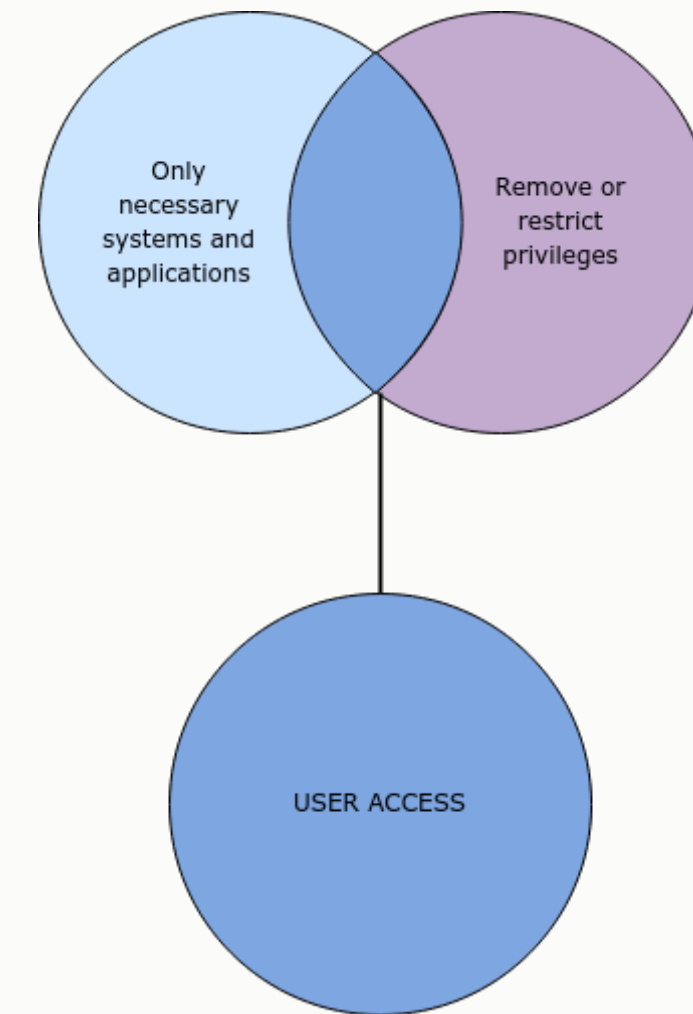


# Least privilege

- Access is restricted.
- Access rights are not permanent, revise assigned privileges regularly.
- 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.***





# Zero trust

***No asset, service or user is trusted.***

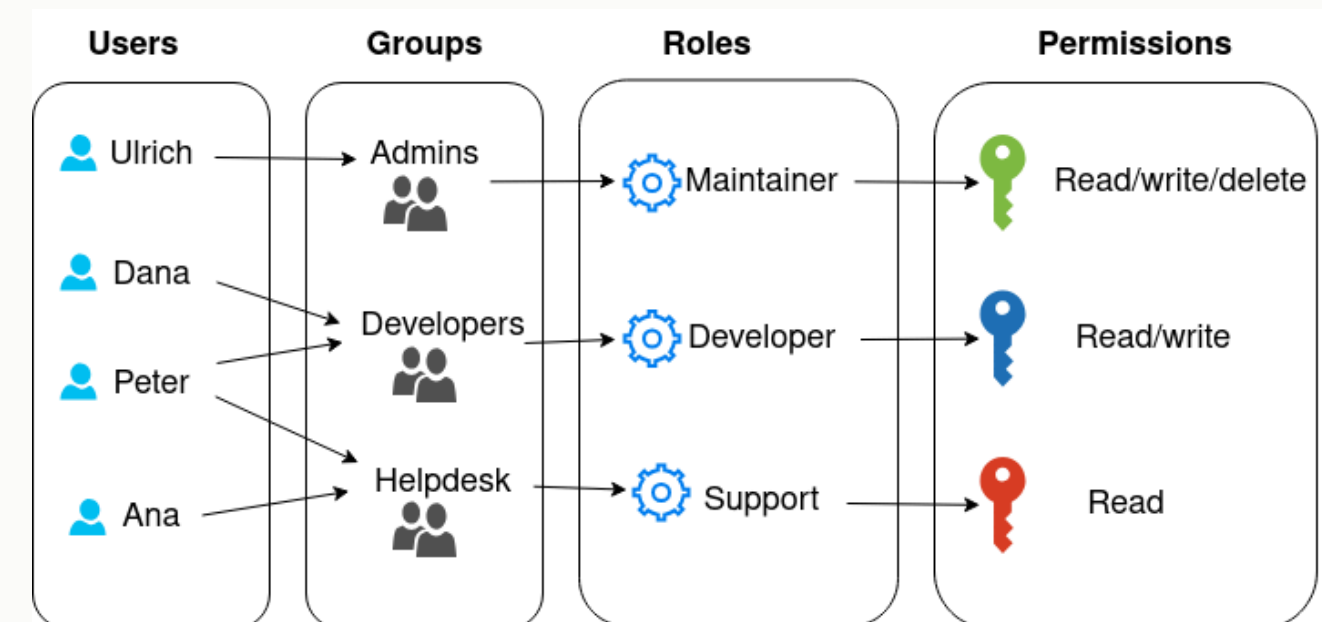
- Trust no one.
- Use least-privilege access.
- All users should be authenticated (in or outside of an organisation network) - MFA if possible.
- Key principles: continuous verification, minimising the impact of a compromise if it occurs, and granting access only if it is really needed.
- The focus is on protecting resources, not network segments
- See NIST SP 800-207: <https://csrc.nist.gov/pubs/sp/800/207/final>



# Separation of duties

- 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 (RBAC), by enforcing controls of access (ACLs), 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...*

## ***No single point of control***



# CIA triad

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



# 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

**How to design security architecture?**



# 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 building after it is already built.

1

## Use security principles and security frameworks

Use visual charts to communicate info more effectively.

## 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.

2

## Prepare policies and system design

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

3

## 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.

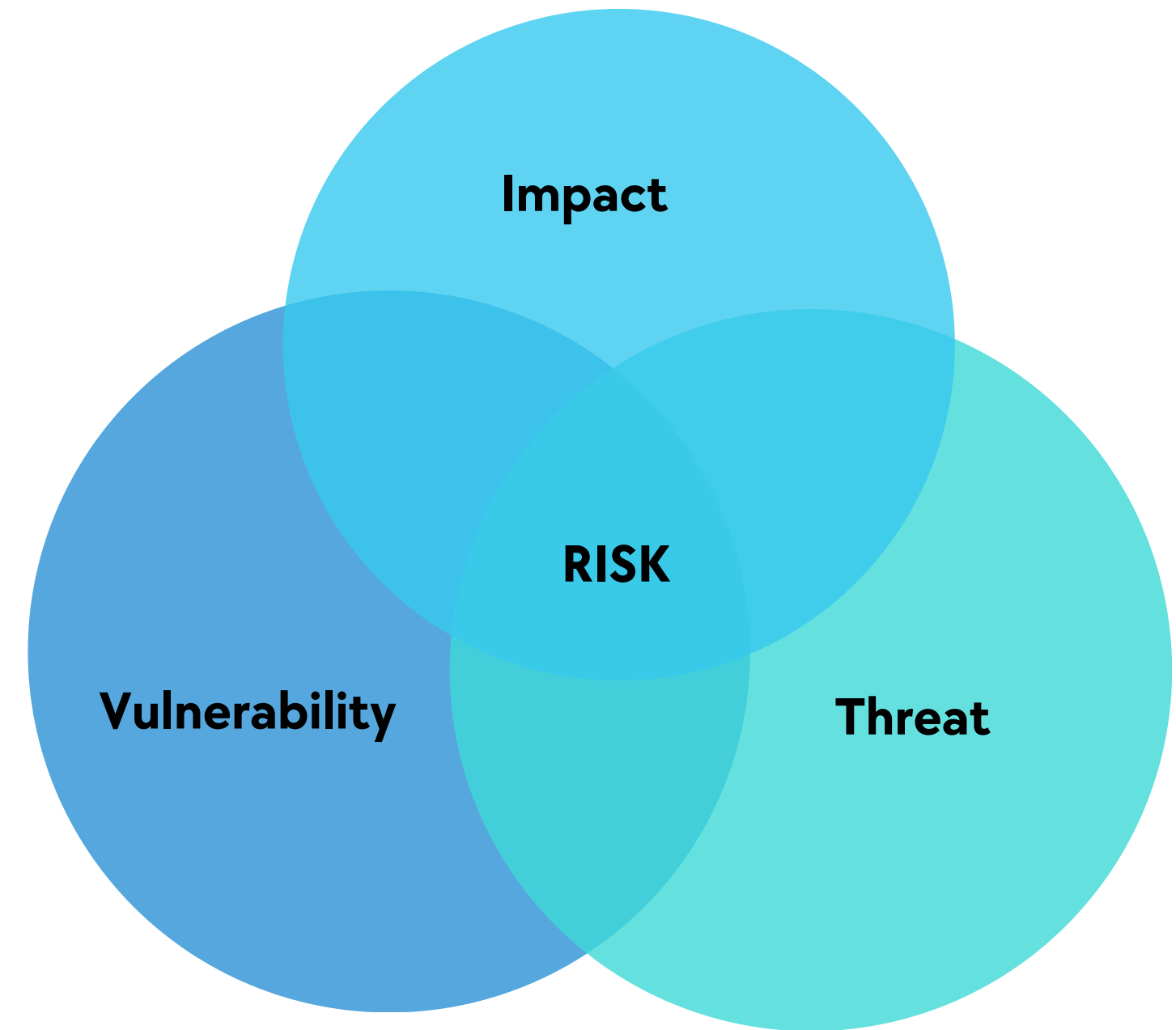
4

# Risk management

Likelihood = Threat x Vulnerability

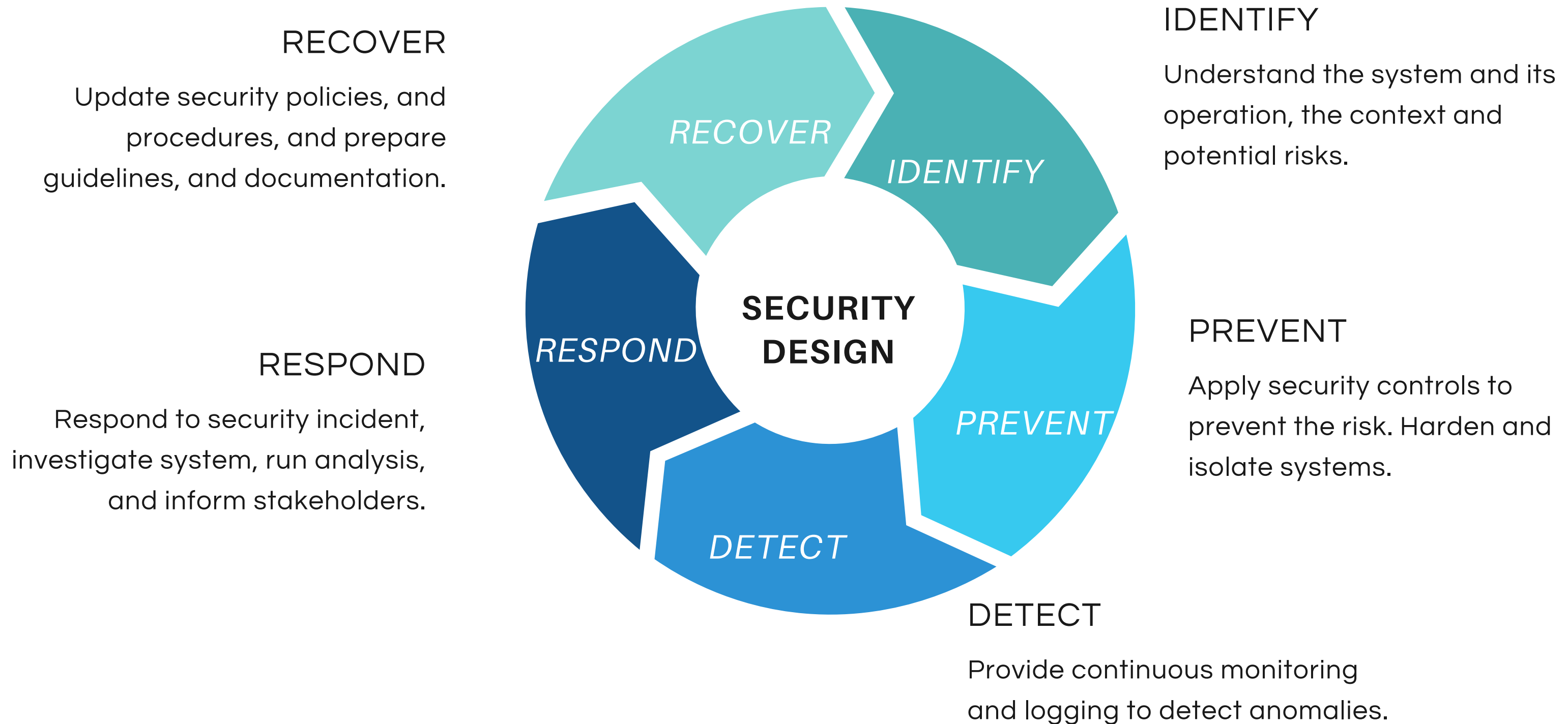
**RISK = Likelihood x Impact**

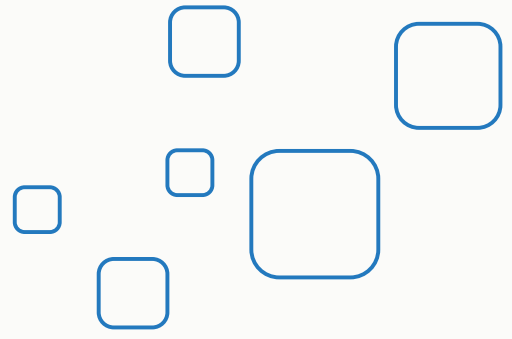
|          |              |              |          |          |          |          |
|----------|--------------|--------------|----------|----------|----------|----------|
| Impact ↑ | catastrophic | Low Med      | Medium   | Med High | High     | High     |
|          | critical     | Low          | 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   |
|          |              | rare         | unlikely | possible | likely   | certain  |
|          |              | 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.

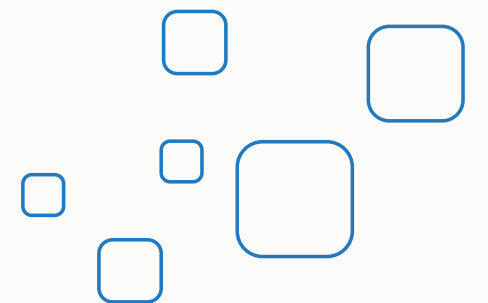
# OBJECTIVES





# Security design principles

- **IDENTIFY:** set the **context**, understand the components of your system, and its objectives, address shortcomings, and separate responsibilities, and understand the threat model. Identify **critical services and sensitive data**. Identify the legal, regulatory, and contractual requirements your organisation must comply with. Assess the **risks**.
- **PREVENT: Design system, define security controls** to mitigate the risks: network segments, services, communication channels, authN and authZ options. Reduce attack surface, and reduce the impact of the compromise and failure.
- **DETECT:** Provide mechanisms for compromise **detection** (collect logs and monitor events).
- **RESPOND:** Provide **incident response plan**.
- **RECOVER:** Update policies and security controls to prevent the same incident from happening again.



# Building blocks for security architecture

- Identity and access management,
- network security,
- endpoint security,
- application security,
- data security,
- cloud security
- etc.

## It ensures:

- **Sensitive data protection**
- **Regulatory compliance**
- **Risk mitigation**
- **Business continuity**
- **Supporting digital transformation**

# Security Governance

- Aligning security with business goals.
- Risk management.
- Ensuring regulatory compliance.
- Ensuring budget to finance security.
- Establish security policies and procedures.
- Assigning Roles, Responsibilities, and Accountability
- Security Awareness and Training
- Developing audit programme, reporting, measuring security performance.

**Organisation's  
approach to security**

**Security culture**

# Security culture

**No security controls will be effective without a strong security culture**

- Clear policies and procedures.
- Employee training and awareness.
- Leadership Commitment.
- Incident reporting.
- Continuous improvement.

Security is a matter of all employees in an organisation.

# Security culture



**Figure 15.1** A structure pyramid, showing how to build an effective security culture.

# Cybersecurity program

- **SECURITY FRAMEWORK:** guidelines, best practices, standards to develop security architecture

- **SECURITY ARCHITECTURE:** ensures implementation of security guidelines and standards

- **CYBERSECURITY PROGRAM:** activities organisation undertakes to manage risks. It is operational in nature. It operationalise security architecture and ensures compliance with the framework.

# CYBERSECURITY PROGRAMME

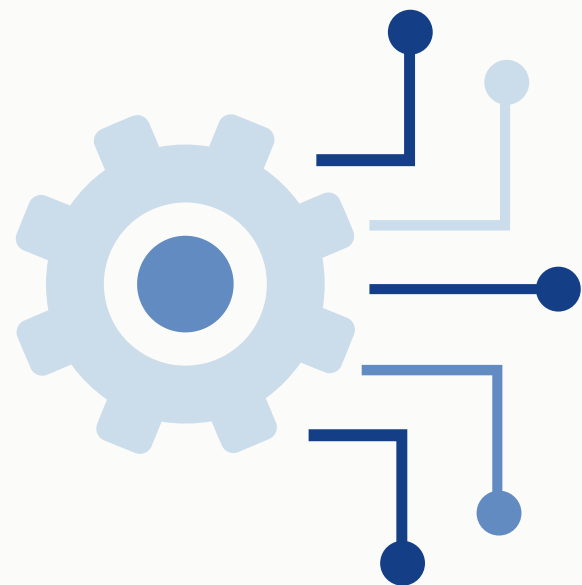
- incorporates **strategy of an organisation**, organisational policies, standards, how-tos, procedures
- based on experience, industry standards, regulations, guidelines
- built with the help of a **security framework**, which is adapted to an organisation
- Following a security framework is not enough,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


# When should an organisation implement Cybersecurity Program



- at the beginning of operations
- when handling sensitive data
- when regulatory compliance is required
- when going through digital transformation
- when roles and responsibilities are unclear
- when lacking 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.

# **Security architecture frameworks**

# 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.

# Why are frameworks useful?

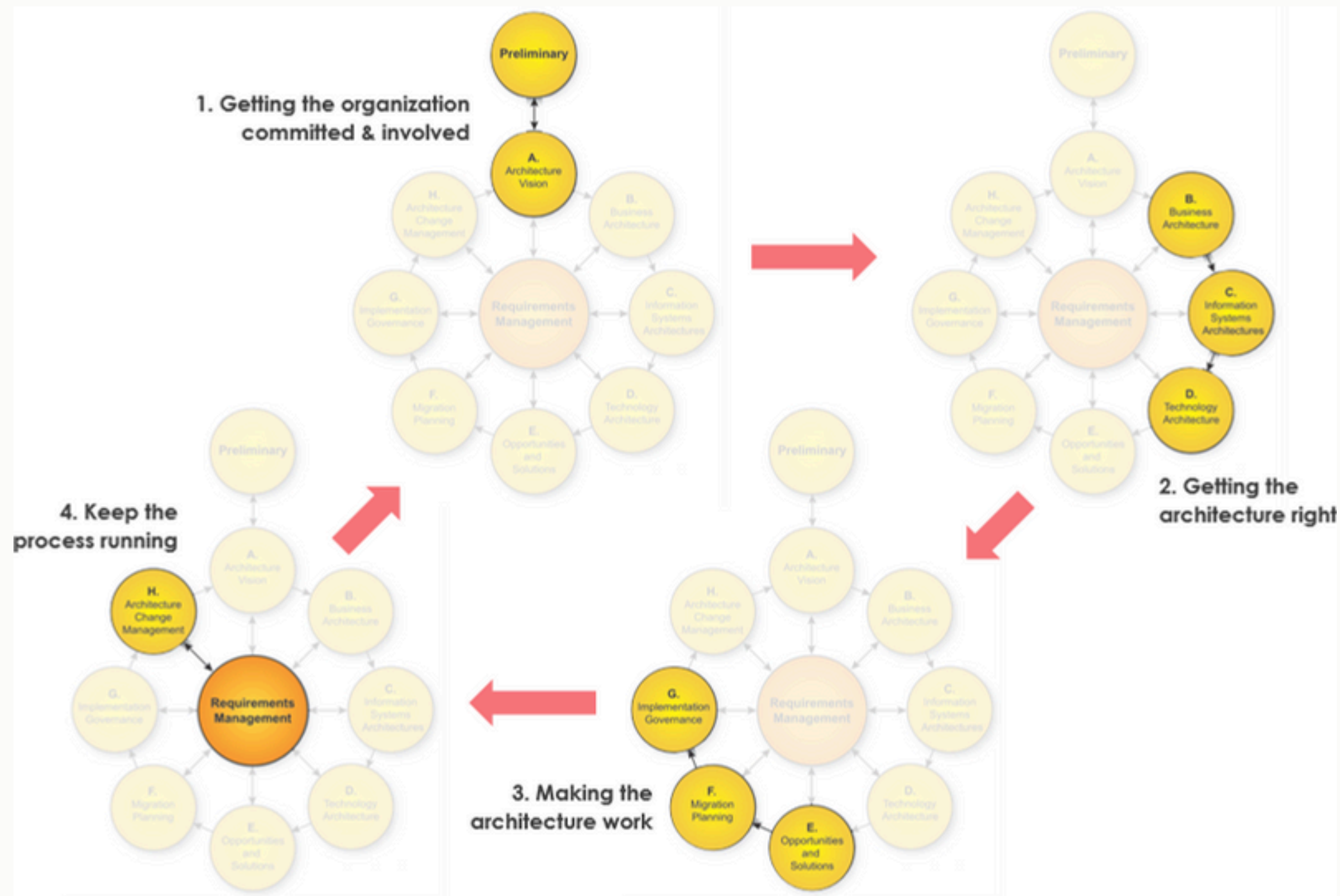
## Structured approach to for managing security

- Set of guidelines, standards, best practices to manage security risks.
- They provide consistency, scalability, compliance, risk management and improve communication between technical and non-technical staff (they provide common language).
- Security should not be an afterthought, it must be integrated into all business processes and IT systems from the outset.
- Collaboration between IT, security teams, and business units is essential for effective security architecture.

Finding the right one for your organisation is challenging. There are many available.

# TOGAF

- Open Group Architecture Framework.
- Enterprise architecture standard.
- Not solely security architecture.
- Used to design large business system architecture. Very complex.
- **Core component: ADM - Architecture Development Method**
- Security is part of every phase of ADM, but not the framework is not security focused



# SABSA

- Sherwood Applied Business Security Architecture
- Security focused framework + risk-driven approach
- **Core component: SABSA matrix**
- also very complex, overkill for smaller enterprises
- can be combined with other architecture modelling frameworks, like TOGAF, Archimate etc.

**SABSA SERVICE MANAGEMENT MATRIX (Aligned with ITIL v3)**

|                         | ASSETS (What)   | MOTIVATION (Why)   | PROCESS (How)  | PEOPLE (Who)  | LOCATION (Where)   | TIME (When)  |
|-------------------------|---|--|--|---|--|--|
|                         | Service Delivery Management   | Operational Risk Management                                    | Process Delivery Management  | Personnel Management  | Management of Environment  | Time & Performance Management                                      |
|                         | The row above is a repeat of Layer 6 of the main SABSA Matrix.<br>The five rows below are an exploded overlay of how this Layer 6 relates to each of these other Layers |  |  |   |  |  |
| CONTEXTUAL ARCHITECTURE | Business Driver Development   | Business Risk Assessment                                       | Service Management   | Relationship Management   | Point-of-Supply Management   | Performance Management   |
|                         | Business Benchmarking & Identification of Business Drivers  | Analysis of Internal & External Risk Factors                   | Managing Service Capabilities for Providing Value to Customers                   | Managing Service Providers & Service Customers; Contract Man'ment         | Demand Man'ment; Service Supply, Deployment & Consumption                  | Defining Business-Driven Performance Targets                       |
| CONCEPTUAL ARCHITECTURE | Proxy Asset Development   | Developing ORM Objectives                                      | Service Delivery Planning  | Service Management Roles  | Service Portfolio  | Service Level Definition   |
|                         | Defining Business Attributes Profile with Performance Criteria, KPIs & KRIs   | Risk Analysis on Business Attributes Proxy Assets              | SLA Planning; BCP; Financial Planning & ROI; Transition Planning                 | Defining Roles, Responsibilities, Liabilities & Cultural Values           | Planning & Maintaining the Service Catalogue                               | Managing Service Performance Criteria and Targets                  |
| LOGICAL ARCHITECTURE    | Asset Management  | Policy Management  | Service Delivery Management  | Service Customer Support  | Service Catalogue Management   | Evaluation Management  |
|                         | Knowledge Management; Release & Deployment Management; Test & Validation Management   | Policy Development; Policy Compliance Auditing                 | SLA Management; Supplier Management; BCM; Cost Management; Transition Management | Access Management; User Privileges, Account Administration & Provisioning | Configuration Management; Capacity Planning; Availability Management       | Monitoring & Reporting Performance against KPIs and KRIs           |
| PHYSICAL ARCHITECTURE   | Asset Security & Protection   | Operational Risk Data Collection                               | Operations Management  | User Support  | Service Resources Protection   | Service Performance Data Collection                                |
|                         | Change Management; Software & Data Integrity Protection   | Operational Risk Management Architecture                       | Job Scheduling; Incident & Event Management; Disaster Recovery                   | Service Desk; Problem Man'ment; Request Man'ment                          | Physical & Environmental Security Management                               | Systems and Service Monitoring Architecture                        |
| COMPONENT ARCHITECTURE  | Tool Protection   | ORM Tools  | Tool Deployment  | Personnel Deployment  | Security Management Tools  | Service Monitoring Tools   |
|                         | Product & Tool Security & Integrity; Product & Tool Maintenance   | ORM Analysis, Monitoring and Reporting Tools & Display Systems | Product & Tool Selection and Procurement; Project Management                     | Recruitment Process Disciplinary Process Training & Awareness Tools       | Products & Tools for Managing Physical & Logical Security of Installations | Service Analysis, Monitoring and Reporting Tools & Display Systems |

# ISO 27001

- Specification of Information Security Management System (ISMS framework)
- 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).
- internationally recognised, comprehensive, compliant with regulations

| 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 |
|-------------------|---|---|--------------------------|-------|
| <b>5</b>          | <b>Information Security Policies</b>                    |   |                          |       |
| <b>5.1</b>        | <b>Management direction for information security</b>    |   |                          |       |
| 5.1.1             | Policies for information security                       | Security Policies exist?  | <input type="checkbox"/> |       |
|                   |   | All policies approved by management?  | <input type="checkbox"/> |       |
|                   |   | Evidence of compliance?   | <input type="checkbox"/> |       |
| <b>6</b>          | <b>Organization of information security</b>             |   |                          |       |
| <b>6.1</b>        | <b>Information security roles and responsibilities</b>  |   |                          |       |
| 6.1.1             | Security roles and responsibilities                     | Roles and responsibilities defined?   | <input type="checkbox"/> |       |
| 6.1.2             | Segregation of duties                                   | Segregation of duties defined?  | <input type="checkbox"/> |       |
| 6.1.3             | Contact with authorities                                | Verification body / authority contacted for compliance verification?        | <input type="checkbox"/> |       |
| 6.1.4             | Contact with special interest groups                    | Establish contact with special interest groups regarding compliance?        | <input type="checkbox"/> |       |
| 6.1.5             | Information security in project management              | Evidence of information security in project management?                     | <input type="checkbox"/> |       |
| <b>6.2</b>        | <b>Mobile devices and teleworking</b>                   |   |                          |       |
| 6.2.1             | Mobile device policy                                    | Defined policy for mobile devices?  | <input type="checkbox"/> |       |
| 6.2.2             | Teleworking   | Defined policy for working remotely?  | <input type="checkbox"/> |       |
| <b>7</b>          | <b>Human resource security</b>                          |   |                          |       |
| <b>7.1</b>        | <b>Prior to employment</b>                              |   |                          |       |
| 7.1.1             | Screening   | Defined policy for screening employees prior to employment?                 | <input type="checkbox"/> |       |
| 7.1.2             | Terms and conditions of employment                      | Defined policy for HR terms and conditions of employment?                   | <input type="checkbox"/> |       |
| <b>7.2</b>        | <b>During employment</b>                                |   |                          |       |
| 7.2.1             | Management responsibilities                             | Defined policy for management responsibilities?                             | <input type="checkbox"/> |       |
| 7.2.2             | Information security awareness, education, and training | Defined policy for information security awareness, education, and training? | <input type="checkbox"/> |       |
| 7.2.3             | Disciplinary process                                    | Defined policy for disciplinary process regarding information security?     | <input type="checkbox"/> |       |

|            |  |  |                          |  |
|------------|--|--|--------------------------|--|
| <b>7.3</b> | <b>Termination and change of employment</b>          |  |                          |  |
| 7.3.1      | Termination or change of employment responsibilities | Defined policy for HR termination or change-of-employment policy regarding information security? | <input type="checkbox"/> |  |
| <b>8</b>   | <b>Asset management</b>                              |  |                          |  |
| <b>8.1</b> | <b>Responsibilities for assets</b>                   |  |                          |  |
| 8.1.1      | Inventory of assets                                  | Complete inventory list of assets?   | <input type="checkbox"/> |  |
| 8.1.2      | Ownership of assets                                  | Complete ownership list of assets  | <input type="checkbox"/> |  |
| 8.1.3      | Acceptable use of assets                             | Defined "acceptable use" of assets policy  | <input type="checkbox"/> |  |
| 8.1.4      | Return of assets                                     | Defined return of assets policy?   | <input type="checkbox"/> |  |
| <b>8.2</b> | <b>Information classification</b>                    |  |                          |  |
| 8.2.1      | Classification of information                        | Defined policy for classification of information?  | <input type="checkbox"/> |  |
| 8.2.2      | Labeling of information                              | Defined policy for labeling information?   | <input type="checkbox"/> |  |
| 8.2.3      | Handling of assets                                   | Defined policy for handling of assets?   | <input type="checkbox"/> |  |
| <b>8.3</b> | <b>Media handling</b>                                |  |                          |  |
| 8.3.1      | Management of removable media                        | Defined policy for management of removable media?  | <input type="checkbox"/> |  |
| 8.3.2      | Disposal of media                                    | Defined policy for disposal of media?  | <input type="checkbox"/> |  |
| 8.3.3      | Physical media transfer                              | Defined policy for physical media transfer?  | <input type="checkbox"/> |  |
| <b>9</b>   | <b>Access control</b>                                |  |                          |  |
| <b>9.1</b> | <b>Responsibilities for assets</b>                   |  |                          |  |
| 9.1.1      | Access policy control                                | Defined policy for access control policy?  | <input type="checkbox"/> |  |
| 9.1.2      | Access to networks and network services              | Defined policy for access to networks and network services?                                      | <input type="checkbox"/> |  |
| <b>9.2</b> | <b>Responsibilities for assets</b>                   |  |                          |  |
| 9.2.1      | User registration and de-registration                | Defined policy for user asset registration and de-registration?                                  | <input type="checkbox"/> |  |
| 9.2.2      | User access provisioning                             | Defined policy for user access provisioning?   | <input type="checkbox"/> |  |
| 9.2.3      | Management of privileged access rights               | Defined policy for management of privileged access rights?                                       | <input type="checkbox"/> |  |

# NIST Cybersecurity Framework



- NIST SP 800 by the National Institute for Standards and Technology
- Widely used in the US, in industries
- Currently version 2.0
- **Core are 6 pillars, functions: govern, identify, protect, detect, respond, recover** (6th pillar, govern, added in the latest release)
- Profiles for different types of organisations
- Broad scope, flexible, but challenging to focus on specific area without additional guidance

# 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?

| Function ID | Function | Category ID | Category  | # of Subcategories |
|-------------|----------|-------------|---|--------------------|
| GV          | Govern   | GV.OC       | Organizational Context                                | 5                  |
|             |          | GV.RM       | Risk Management Strategy                              | 7                  |
|             |          | GV.RR       | Roles, Responsibilities, and Authorities              | 4                  |
|             |          | GV.PO       | Policy  | 2                  |
|             |          | GV.OV       | Oversight   | 3                  |
|             |          | GV.SC       | Cybersecurity Supply Chain Risk Management            | 10                 |
| ID          | Identify | ID.AM       | Asset Management                                      | 7                  |
|             |          | ID.RA       | Risk Assessment                                       | 10                 |
|             |          | ID.IM       | Improvement   | 4                  |
| PR          | Protect  | PR.AA       | Identity Management, Authentication, & Access Control | 6                  |
|             |          | PR.AT       | Awareness and Training                                | 2                  |
|             |          | PR.DS       | Data Security   | 4                  |
|             |          | PR.PS       | Platform Security                                     | 6                  |
|             |          | PR.IR       | Technology Infrastructure Resilience                  | 4                  |
| DE          | Detect   | DE.CM       | Continuous Monitoring                                 | 5                  |
|             |          | DE.AE       | Adverse Event Analysis                                | 6                  |
| RS          | Respond  | RS.MA       | Incident Management                                   | 5                  |
|             |          | RS.AN       | Incident Analysis                                     | 4                  |
|             |          | RS.CO       | Incident Response Reporting and Communication         | 2                  |
|             |          | RS.MI       | Incident Mitigation                                   | 2                  |
| RC          | Recover  | RC.RP       | Incident Recovery Plan Execution                      | 6                  |
|             |          | RC.CO       | Incident Recovery Communication                       | 2                  |

# CIS controls

- known also as Critical Security Controls,
- developed by Center for Internet security,
- set of actions for system cyber defense.
- CIS safeguards as guidelines how to defend
- more than 25 vendor products included, such as Cisco, F5, Juniper
- basis for multiple vendor products: Nessus, OpenVAS etc.

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

| CIS Controls<br>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<br>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 - network

| NUMBER | TITLE/DESCRIPTION   | ASSET TYPE | SECURITY FUNCTION | IG1 | IG2 | IG3 |
|--------|---|------------|-------------------|-----|-----|-----|
| 12.1   | <b>Ensure Network Infrastructure is Up-to-Date</b><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   | <b>Establish and Maintain a Secure Network Architecture</b><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   | <b>Securely Manage Network Infrastructure</b><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   | <b>Establish and Maintain Architecture Diagram(s)</b><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   | <b>Centralize Network Authentication, Authorization, and Auditing (AAA)</b><br>Centralize network AAA.  | Network    | Protect           |     | ●   | ●   |
| 12.6   | <b>Use of Secure Network Management and Communication Protocols</b><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   | <b>Centralize Security Event Alerting</b><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   | <b>Deploy a Host-Based Intrusion Detection Solution</b><br>Deploy a host-based intrusion detection solution on enterprise assets, where appropriate and/or supported.  | Devices    | Detect            |     | ●   | ●   |
| 13.3   | <b>Deploy a Network Intrusion Detection Solution</b><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   | <b>Perform Traffic Filtering Between Network Segments</b><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`

# Mitre 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<sup>®</sup>**

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

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



# Comparison

- Many other available: ISA (for OT sector), COBIT (for industrial/business)

| <b>Framework</b> | <b>Features</b>                          | <b>Best use case</b>            | <b>Strengths</b>                    | <b>Weaknesses</b>             |
|------------------|--|---------------------------------|-------------------------------------|-------------------------------|
| <b>TOGAF</b>     | Comprehensive enterprise architecture    | Enterprise-wide architecture    | Aligns IT with business goals       | Complexity                    |
| <b>SABSA</b>     | Security-focused enterprise architecture | Security and risk management    | Aligns security with business needs | Specialised and complex       |
| <b>NIST</b>      | Cybersecurity risk management            | Cybersecurity across industries | Flexible and comprehensive          | Broad, can be too general     |
| <b>ISO 27001</b> | Information security management          | Compliance and ISMS             | Globally recognised                 | Lengthy certification process |
| <b>COBIT</b>     | IT governance                            | IT and security governance      | Aligns IT with business goals       | Complexity                    |

Comparison of Security Architectural Frameworks (source: Enterprise Fortress, The Ultimate Handbook for Enterprise Security Architecture)

**Policies, procedures,  
regulations**

# Information security related regulations in EU

- 2018, The European General Data Protection Regulation (**GDPR**)
- 2018, The Network and Information Systems Directive (**NIS Directive**)
- 2022, Revision of the NIS Directive (New **NIS2 Directive**)
- 2019, The **EU Cybersecurity Act** (Role of ENISA, certification of security services)
- 2002, **ePrivacy directive**, privacy and electronic communications (being revised)
- 2022, **Data Governance Act** (availability of public data, by ensuring privacy/protection)
- Proposed, **DORA** (Digital Operational Resilience Act - to enhance digital operational resilience of financial institutions in EU)

**EU Cybersecurity Strategy for Digital Decade:** EU's approach to cybersecurity in the next years

A collection of all EC standards (=! regulation):

[https://ec.europa.eu/info/files/security-standards-information-systems\\_en](https://ec.europa.eu/info/files/security-standards-information-systems_en)

# How to establish security policies

- Define security objectives
- Follow the standards and regulations
- Align the policies with business objectives
- Use the documentation and templates, that are already available:
  - **AARC Project**: <https://aarc-project.eu/policies/policy-development-kit/>



Common mistake: formalistic approach, policies are not used in practice because they are not aligned with the business process and objectives.

## QUIZ

- **Which one of the following is not a security framework?**
  - a. NIST CSF
  - b. TOGAF
  - c. WAZUH
  - d. SABSA
  
- **What is the objective of a security framework?**
  - a. To provide guidance and best practices for managing cybersecurity risks
  - b. To create a detailed technical specification of security tools.
  - c. To define the roles and responsibilities of IT staff.
  
- **Which of the following is NOT part of cybersecurity program?**
  - a. Incident response
  - b. Hardware procurement
  - c. Employee security training

**Components of security architecture:**

**IAM**

# Access and Identity Management

User identification

User authentication

MFA

User authorization

RBAC

Access monitoring

## KEY CONCEPTS OF IAM

- Identity management
- Authentication
- Authorization
- User Provisioning/Deprovisioning
- Privileged access
- Single Sign-On
- Federated access
- Access management
- Auditing and monitoring

### Best practices:

- Zero trust approach
- Least privilege principle adoption
- MFA
- Strong password policies.
- RBAC
- Auditing and monitoring of the access.

**Components of security architecture:**

**Network security**

# Network security

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

## 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?***

***What are the attacker's objectives?***

***Where is your critical data? Who has access to it?***

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

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 security mindset

- not if, but when
- never stop learning
- defence-in-depth
- proactiveness (don't wait for an attack to take actions)
- risk awareness: follow changes in threat landscape
- plan incident response
- continuous monitoring

# Network Security Architectures

## PERIMETER-BASED ARCHITECTURE

- focus on protecting the network boundaries
- threats outside of the network
- security measures focus on defending the perimeter: IDS, IPS, Firewall, ACLs
- Access control at the perimeter (often based on IP or network segment)
- simplicity, often legacy systems
- monitoring limited to perimeter

## ZERO TRUST ARCHITECTURE

- principle “never trust, always verify”
- threats outside and inside of the network
- no devices trusted by default
- access restricted, “need to know” basis, granular control
- much more complex
- authentication and authorization controls on all services
- constant verification and active monitoring

# 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

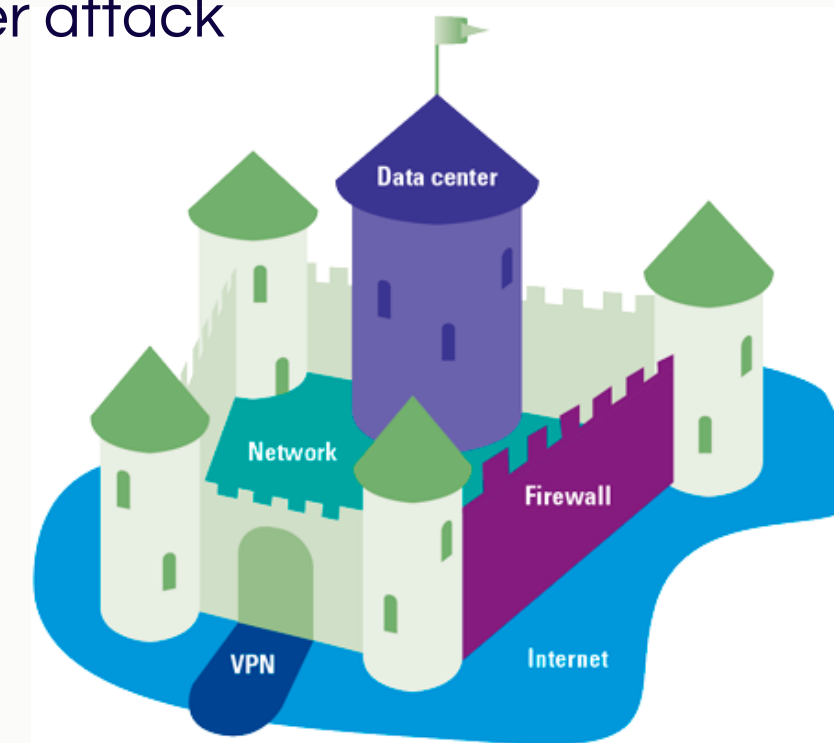


Image source: <https://www.compact.nl/articles/zero-trust-beyond-the-hype/>

# Network design

## NETWORK TOPOLOGY

**PHYSICAL:** how the network 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

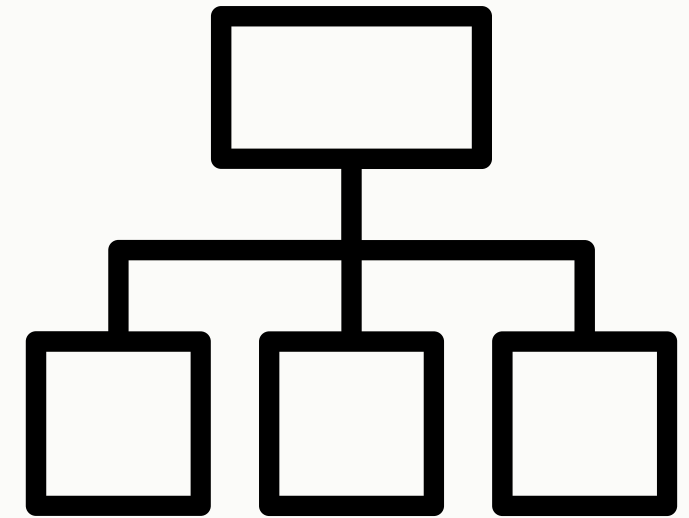
## NETWORK DEVICES:

- switches
- routers
- modems
- network cards

# Network segmentation

## How to segregate?

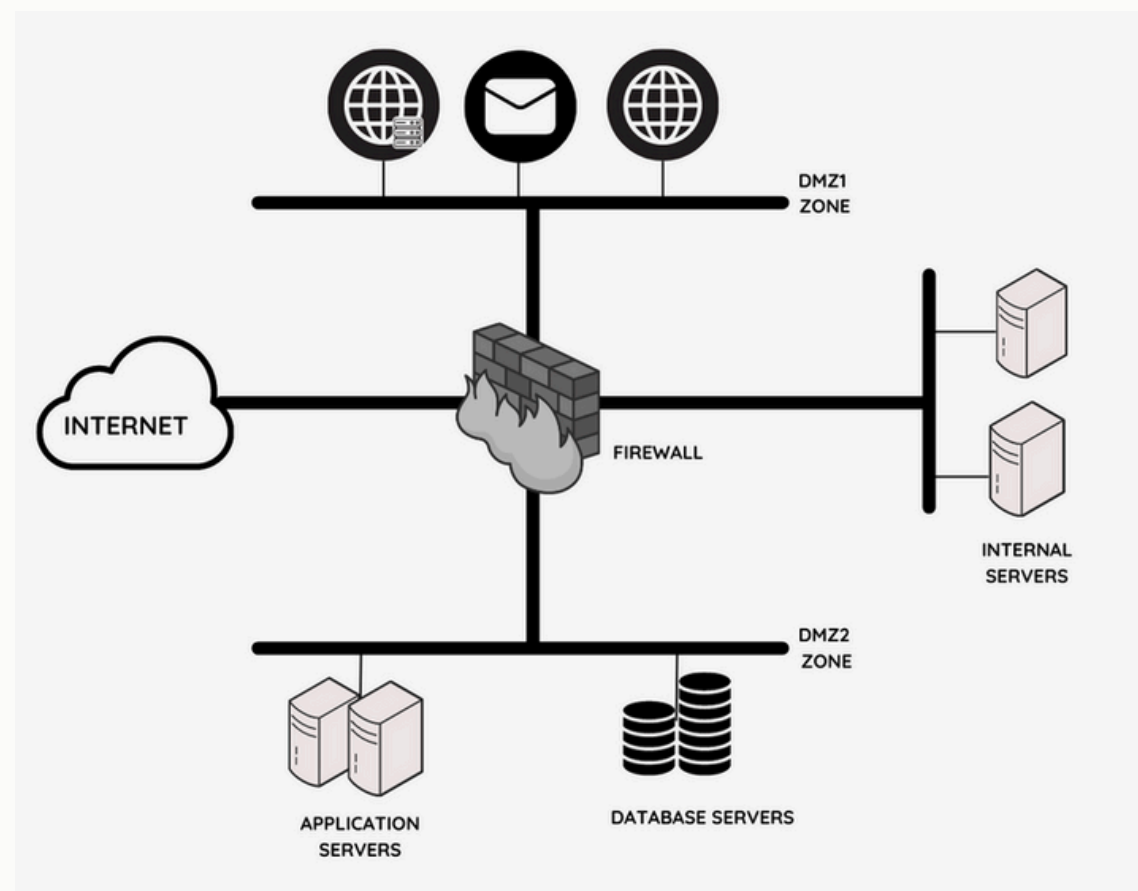
- follow the least privilege rule and only provide access to the system when it is necessary
- define network segments based on the location of sensitive data and critical services
- KISS principle = keep it simple stupid
- Guests should have access to the Internet, but not to the internal network
-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



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

# 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



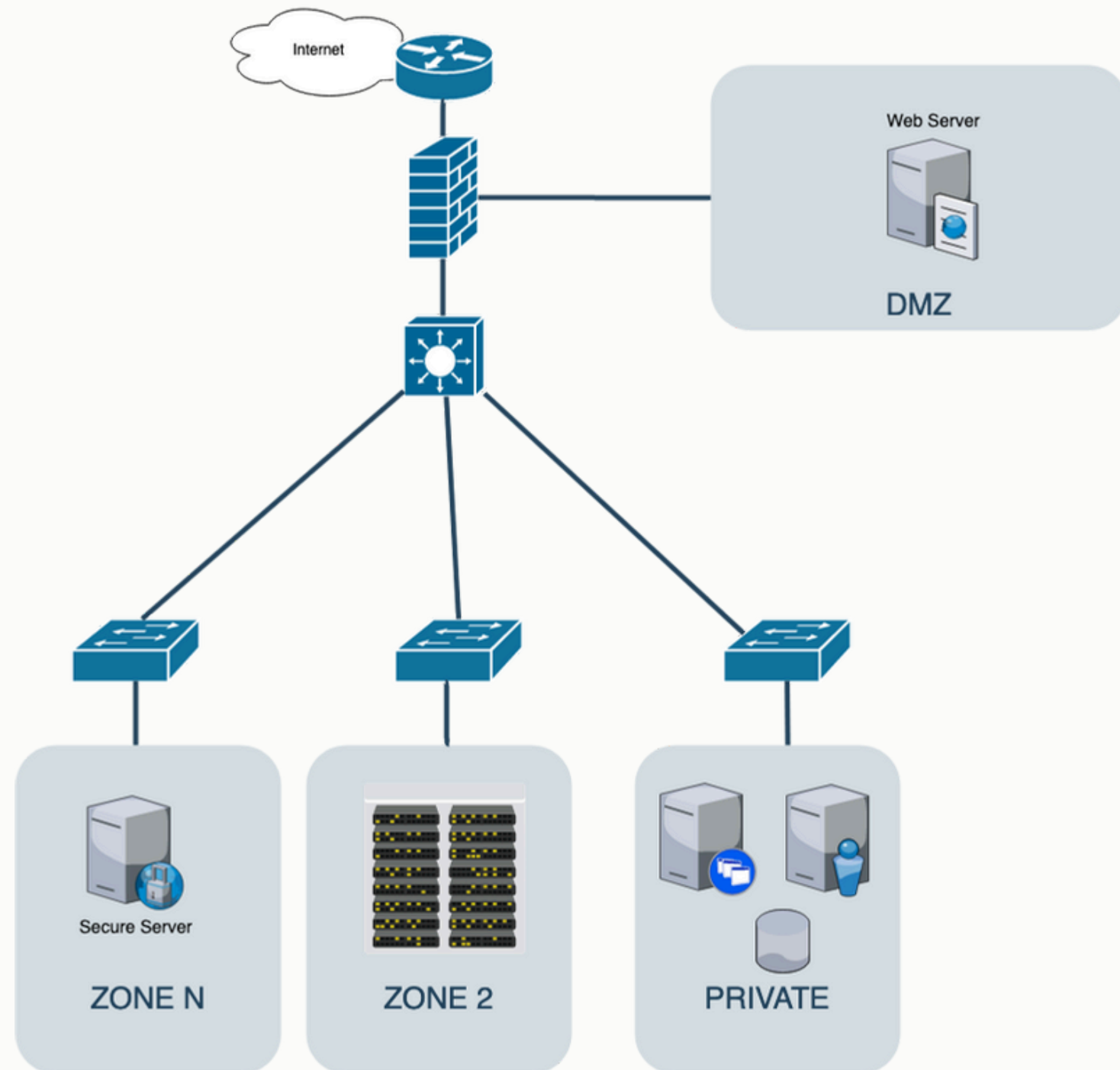
<https://www.zenarmor.com/docs/network-basics/network-segmentation>

## 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
- zero day vulnerabilities
- supply chain attacks

## Attacks against switches:

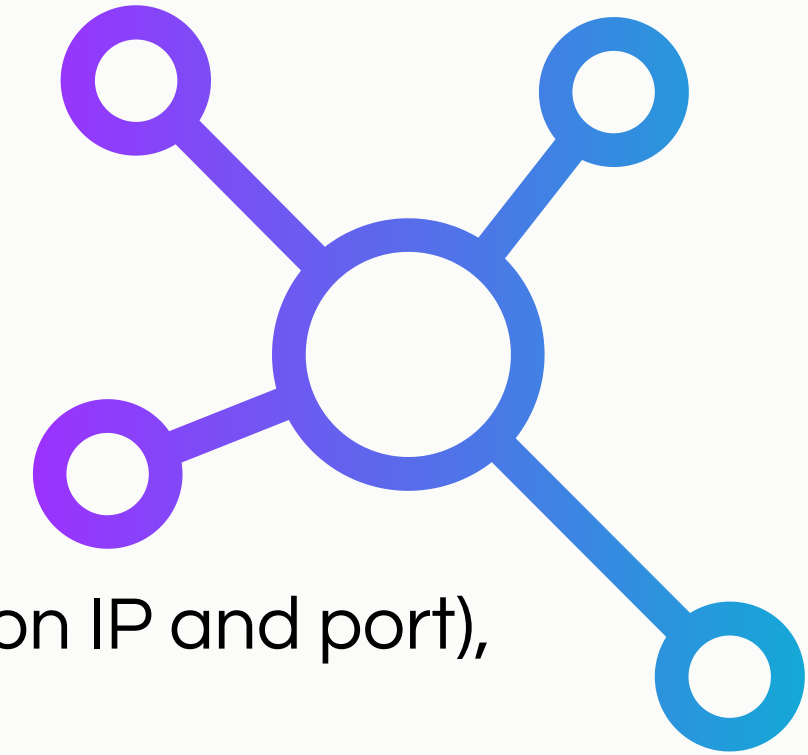
- MAC Flooding
- Brute force Password Attack
- DHCP Spoofing and Starvation
- STP Attacks
- VLAN hopping
- Telnet attack
- CDP Manipulation

## 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.

# Network security controls

- 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 (MITM 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, also netflow monitoring for traffic analysis,
- 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.



# Wireless security

- Choose routers that support latest security protocols (WPA3)
- change default router password,
- enable network encryption,
- create strong network password
- disable remote management,
- setup a guest network (for guests)
- turn off SSID broadcasting
- turn on built-in network firewall
- turn off WPS
- patch the OS/drivers regularly,
- monitor connected devices.

## Wireless hacking tools:

Kismet  
Airsnort  
Aircrack-ng  
Airdump-ng



# 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

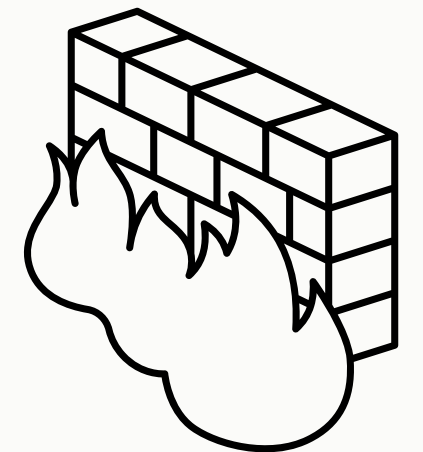
- **Benefits**

- 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
- it stores logs about successful and blocked traffic
- it 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

**FIREWALL LOGS:** log denied traffic, identify connections from one to multiple IPs, or from multiple locations to the same destination IP.



# Types of firewalls

- **PACKET-FILTERING:** most basic, check data packets against a set of filters (IP address, port)
- **STATEFUL INSPECTION:** packet filtering and track ongoing connections, if they deviate from the expected sequence, they can be blocked
- **PROXY FIREWALL:** they act as middlemen, they accept traffic, inspect it and pass it to the destination server
- **NEXT-GENERATION FIREWALL:** advanced options, like encrypted traffic inspection, IDS etc.
- **WEB APPLICATION FIREWALL:** protects web servers from attacks

# VPN

## **Virtual Private Network provides a secure, private tunnel for your data**

- they hide your IP, encrypt your data, prevent eavesdropping
- recommended to access your network from outside
- recommended if you use public wifi networks
- hand in hand with firewall
  
- Some countries have strict regulations on VPN usage, they may block or restrict access to VPN services, because they want to control the traffic.
- In some organisations VPNs are prohibited, because they want to control the flow of the sensitive data.
- VPN logs: audit servers that cannot be reached through VPN, log failed attempts
  
- **Some solutions:** Cisco Anyconnect, OpenVPN, WireGuard, ExpressVPN, Palo Alto GlobalProtect etc.

# 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

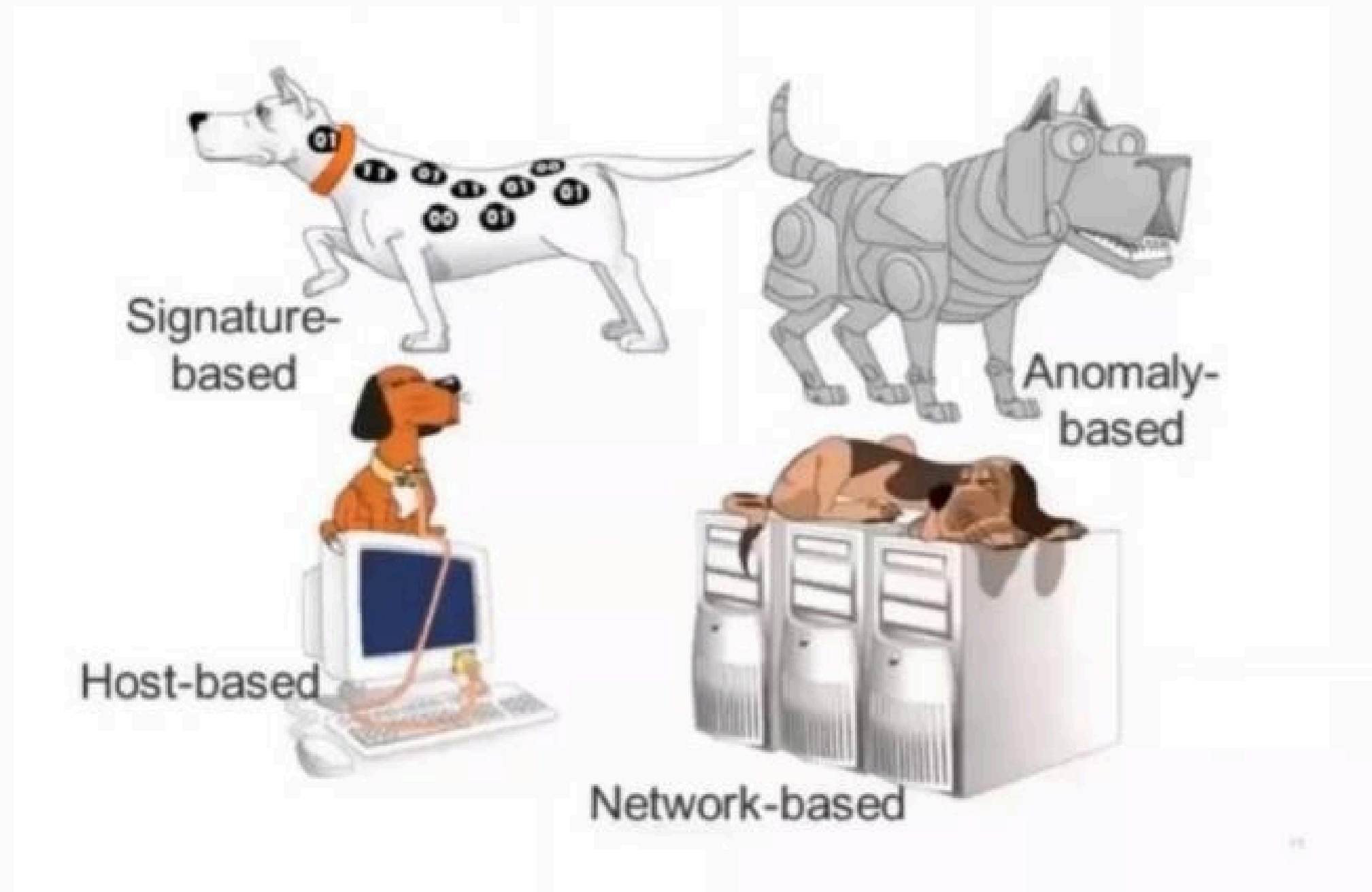
## IPS SOFTWARE:

- 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?



## 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 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.

# NETWORK SECURITY POLICIES

RULES OF  
THE GAME

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 include AUP, access controls, firewalls, proxies, IDS/IPS, and ACLs on switches/routers, on the application level and even incident response procedures.

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

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

- **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
- IPsec enabled by default
- QoS using the Flow Label field of the IPv6 header
- Simpler header format, improved performance
- Better multicast routing
- Simplified, more efficient routing
- Vast address space, no more NAT (Network Address Translation) - easier to implement security policies

IPv6 is not more secure than IPv4 by itself.

- **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

# 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

---

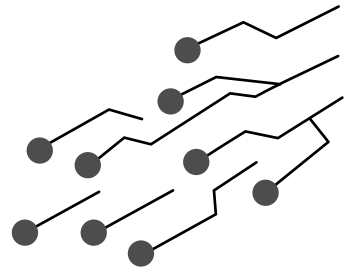
- **Wireshark + tshark** - network sniffer
- **Metasploit** - scanners for more than 1500 operations
- **Nessus** - identifies and corrects faulty updates
- **OpenVAS** - checks configuration and basic web flaws
- **Argus** - open-source network analysis tool
- **tcpdump** - network sniffer
- **Kali 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

## Network forensics

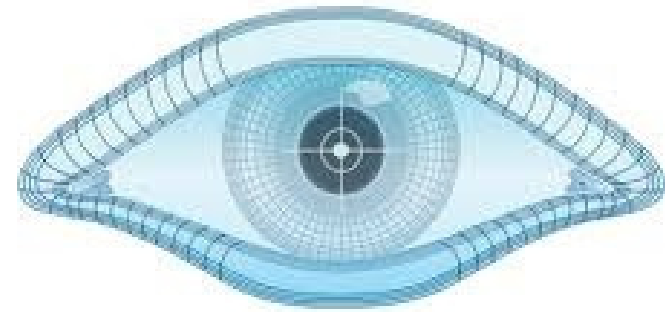
- Wireshark
- Network Miner
- Tcpdump
- Tcpxtract
- Argus
- YARA



# Network discovery

## Some useful commands

- ifconfig
- netstat
- route
- iptables
- tcpdump
- ethtool
- arp
- ip
- nmap
- lsof



## Traffic sniffers

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

## Nmap is a powerful tool!

```
nmap -n -T1 -A 192.168.1.103
```

-n - disable DNS queries

-sV - service detection and versions

-T1 - 15s interval (usually avoids IDS)

```
nmap --top-ports 20 192.168.1.103
```

```
nmap -v -sn 192.168.0.0/16 10.0.0.0/
```

-sn ping scan

```
nmap -O 192.168.1.103
```

-O detects OS

NMAP using Nmap Scripting Engine to detect vulnerabilities:

```
#to update vulnerabilities db
```

```
Nmap --script-updatedb
```

```
#check vuln. with CVSS score 7.5 and above
```

```
nmap --script vuln --script-args=mincvss=7.5
```

Check also: <https://github.com/scipag/vulscan>

## CENTRAL LOGGING

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

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

# Network logging and monitoring

- **What is normal behaviour?**
- **Which events to log?**
- **What is the retention policy?**

## WHAT TO LOG?

- network traffic
- successful/failed logins
- account lockouts
- access control events
- DHCP events
- DNS queries
- firewall logs
- configuration changes on devices
- syslog from devices
- snmp for network devices
- ntp (sync time across entire network)

# 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 access
- 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.
  - DDoS attacks can be completely prevented with the right security measures.
  - Network segmentation can help limit the spread of malware within a network.
  - 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.
  - VPNs provide complete anonymity for users on the Internet.
  - IDS can only detect an attack, but cannot prevent it?
- **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.**

Questions?