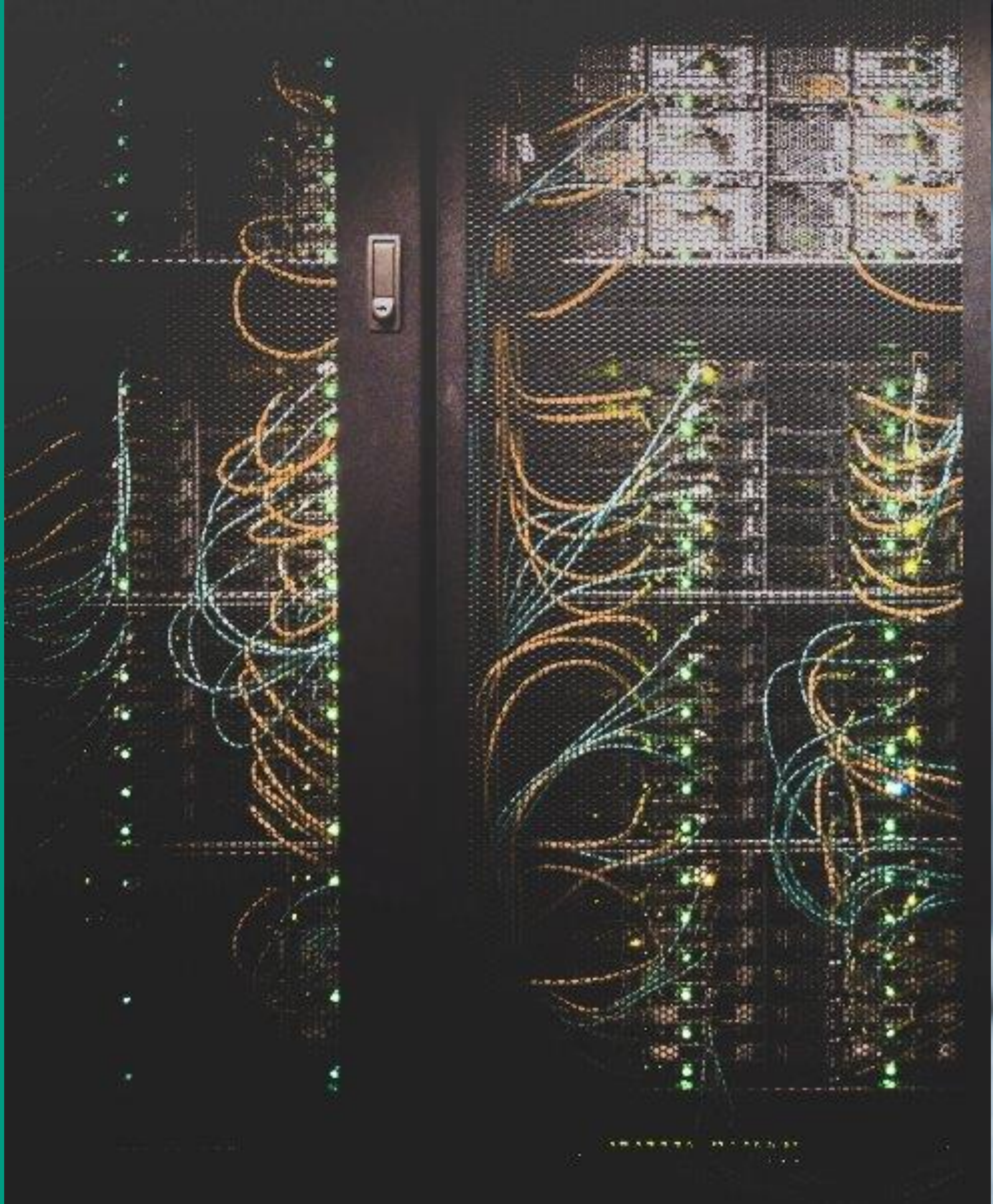
Week 5

Backups & Security

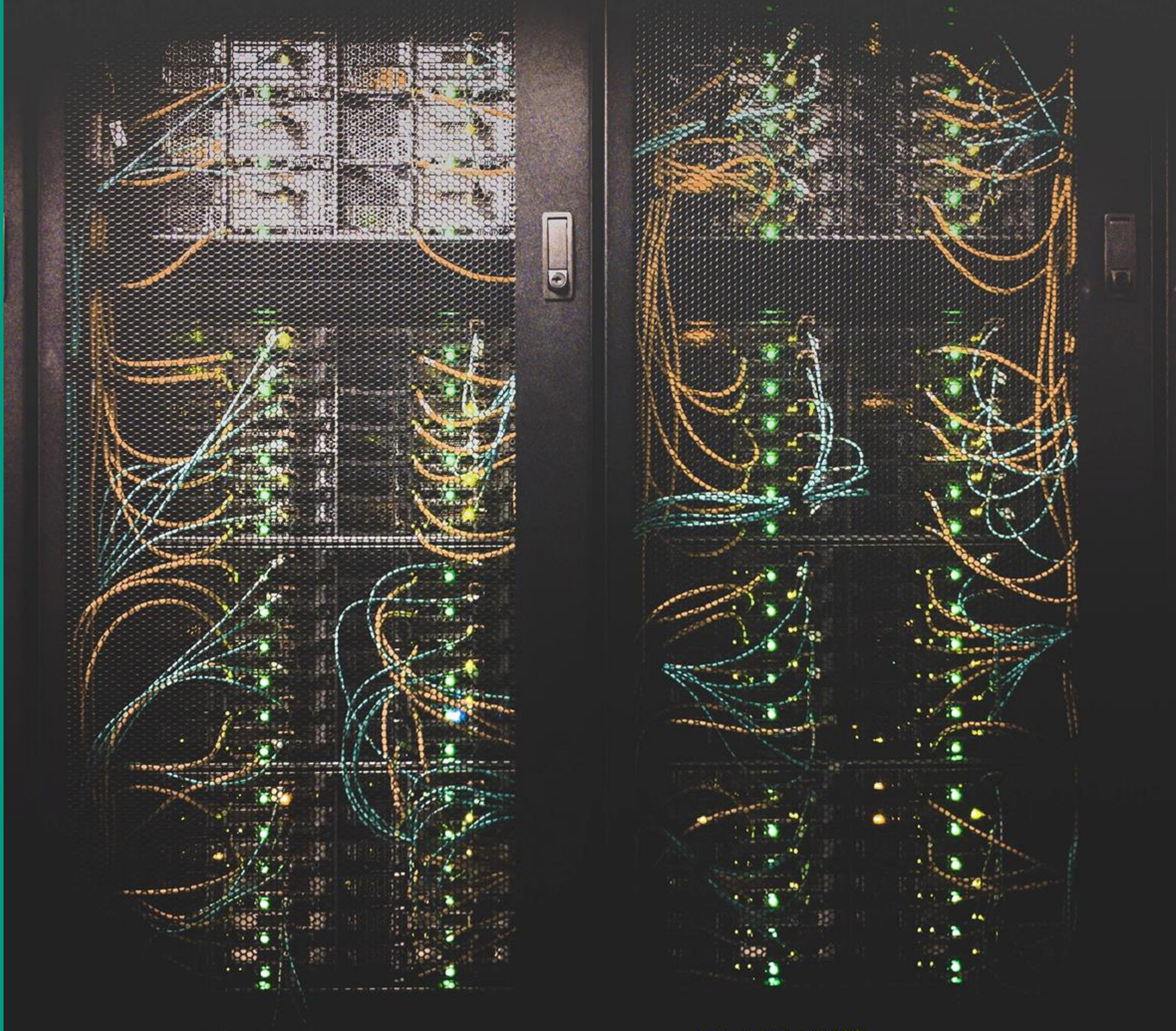
SAXION UNIVERSITY OF APPLIED SCIENCES



Agenda

- What is storage?
- Designing storage architecture
- ICT Security
- ISO 27001/ 27002
- NIST Cybersecurity Framework

What is storage and what types are there?



What is storage?

- A **device** or **medium** in which data can be stored

Various media:

- Hard disk (rotating disks)
- SSD or Flash (on chip; no moving parts)
- Cd-rom or magnetic tape

Types of storage:

- Storage in own data centre (DAS, NAS, SAN)
- Cloud storage
- Hybrid storage: both local and cloud storage (multi storage)

SAXION UNIVERSITY OF APPLIED SCIENCES

The type of data storage needed depends on many factors. **Performance**, **security** and the **amount of** it all play a role.

Storage hierarchy

CPU Clock speed max +/- 4 GHz

Registers and L1, L2, L3 Cache: ~MB
Super fast. Instruction takes **4 ns**

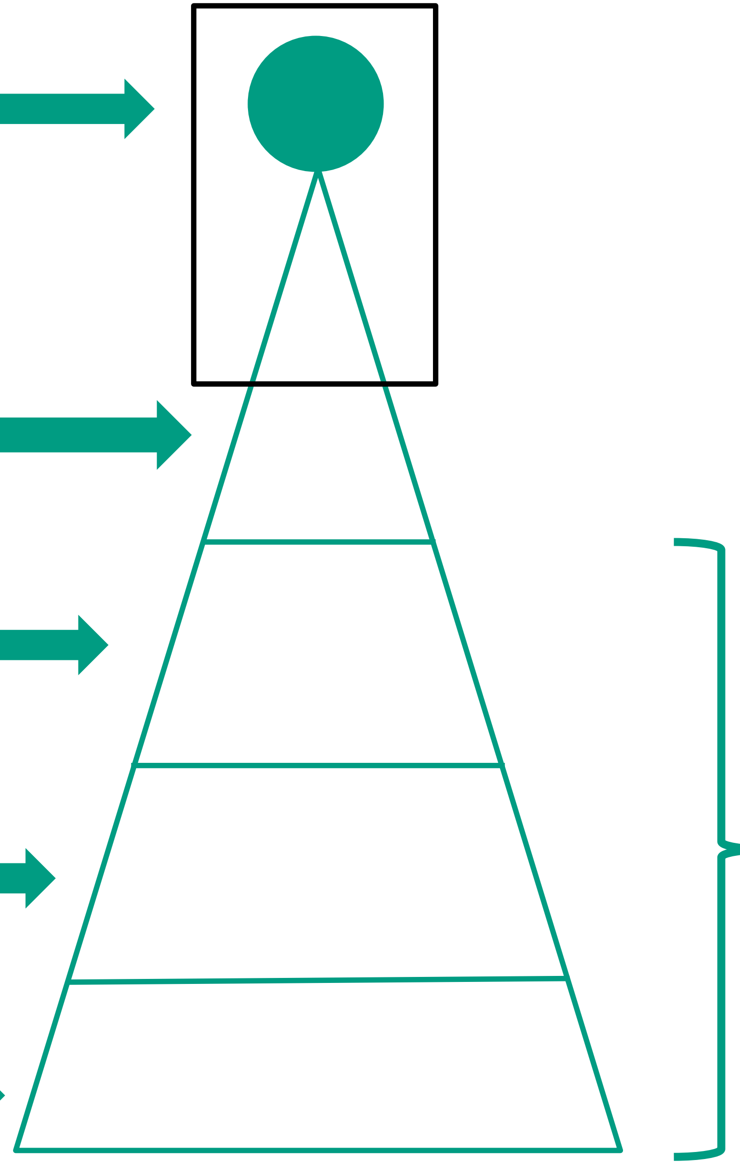
Primary storage (not persistent)

Main memory: ~GB
Very fast. Access time **nanoseconds**

SSD or Flash: ~GB
Fast. Access time **microseconds**

HDD: ~TB
Less fast. Access time **milliseconds**

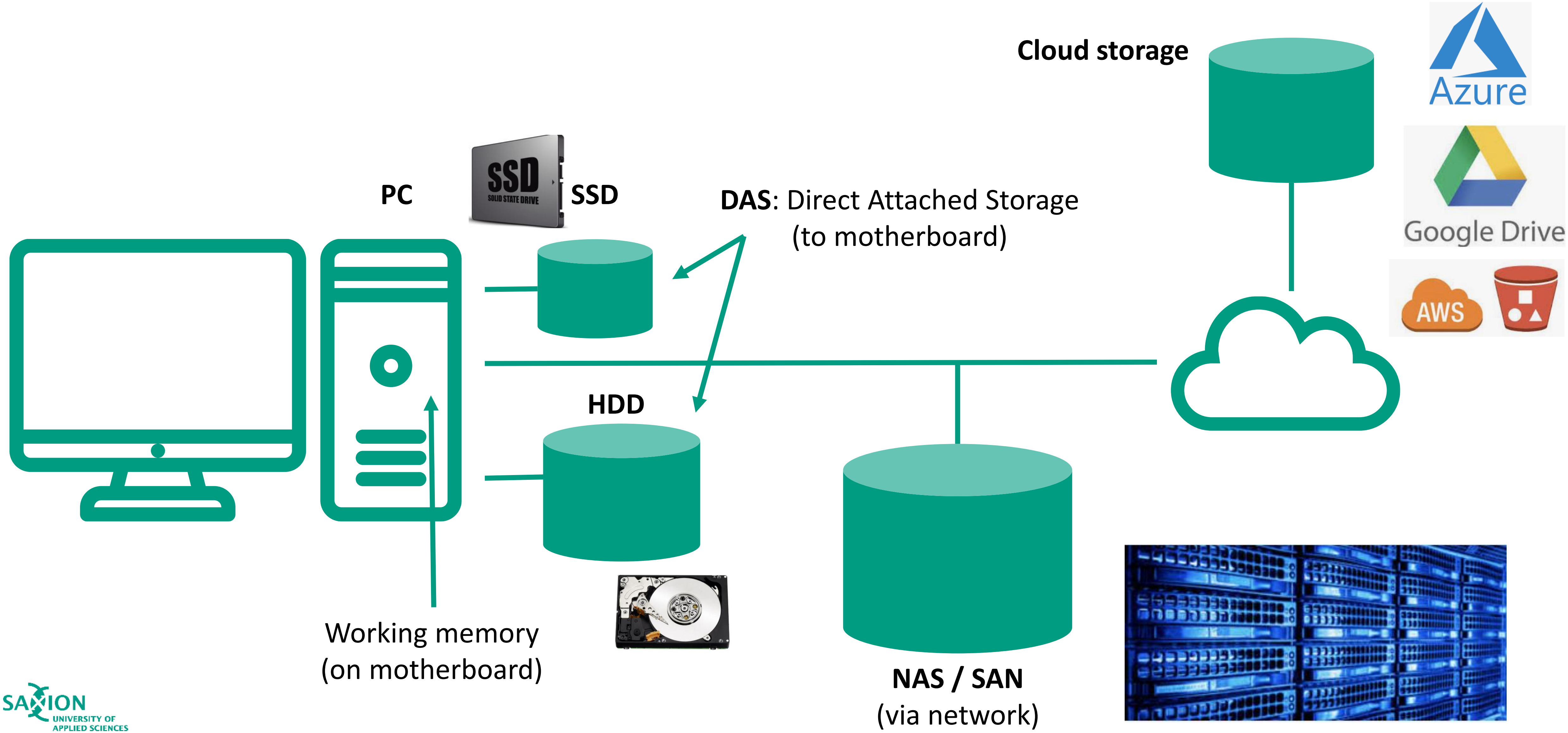
Network storage: ~TB
Less fast. Access time **milliseconds**



This lesson is about Persistent storage!

Secondary storage (persistent)

Storage hierarchy: where is what?



Cloud storage

PC

SSD

DAS: Direct Attached Storage
(to motherboard)

HDD

Working memory
(on motherboard)

NAS / SAN
(via network)

Types of storage

- **HDD (Hard Disk Drive):** Commonly used for personal computers, servers and storage systems. Rotating hard disk (speed up to 15000 Revolutions Per Minute).

- **SSD (Solid State Drive):** Store data in non-volatile flash memory chips. No rotating parts.

- **Flash memory cards:** Used in digital cameras and mobile devices, such as smartphones, tablets, sound recorders, and media players. USB memory sticks are also a form of solid state storage.

- **CD-ROM (Optical Data Storage):** Used for example for computer games and movie storage.

- **Magnetic tapes:** Used for backups.

Storage size

A single binary value (1 or 0) is one bit, eight bits make up one byte

- 8 bits (b) = 1 byte (B)
- 1 kilobyte (KB) = 1024 bytes
- 1 megabyte (MB) = 1,024 KB
- 1 Gigabyte (GB) = 1,024 MB Storage **PC** 100 to 1000 GB
- 1 Terabyte (TB) = 1,024 GB Storage on **storage devices**
- 1 Petabyte (PB) = 1.024 TB as a SAN: often 100 TB - 1 PB.
- 1 Exabyte (EB) = 1.024 PB

Petabyte SAN

Storage Management

Important duties of the Storage Administrator:

- Sufficient storage with the right performance
- Only authorised people can access certain data
- Encryption (if required)
- Backups
- Continuous availability
- Archiving and later cleaning up when data is no longer needed.

What is important for designing storage architecture?

Principles of storage architecture

Functionality:

- Required performance?
- Required availability (24/7)?
- Size (GB, TB or ..)?

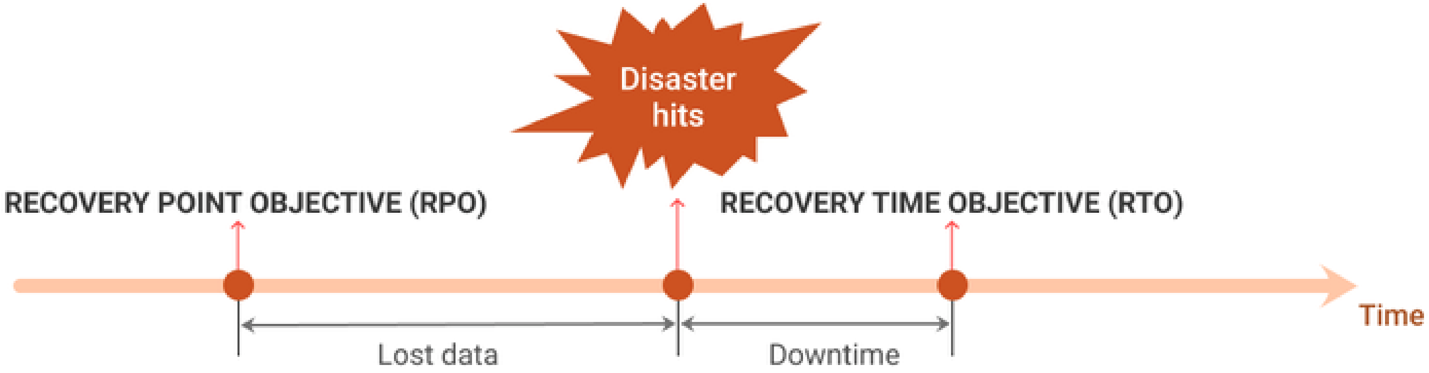
Calamity

Key parameters for establishing business continuity and disaster recovery plans are:

The **RTO** (Recovery Time Objective) and **RPO** (Recovery Point Objective)

Both help with:

- The recovery process
- Determining the recovery time limits
- The frequency of backups
- The recovery procedures



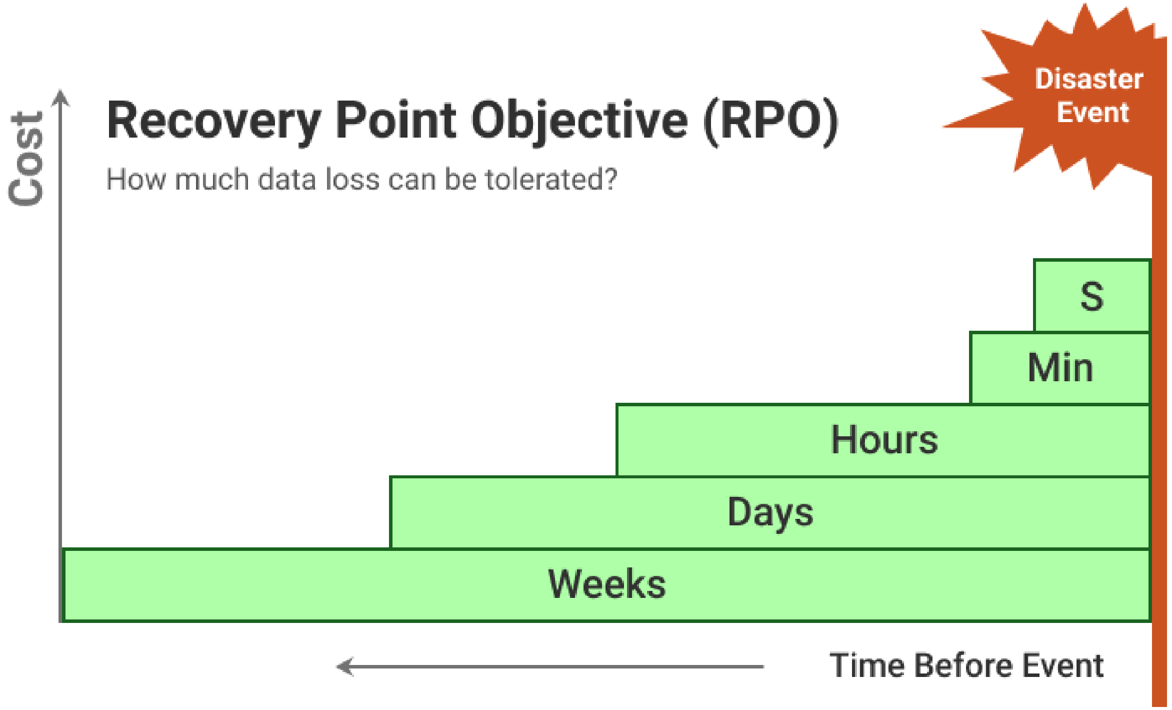
RPO

- **RPO**, or 'Recovery Point Objective' = Measure of the maximum acceptable amount of data a company can afford to lose during a disaster.

- RPO is useful for determining how often data backups should be performed.

Factors for determining your RPO:

- The maximum acceptable amount of data loss that the organization can tolerate.
- The cost of lost data.
- Available budget and resources.

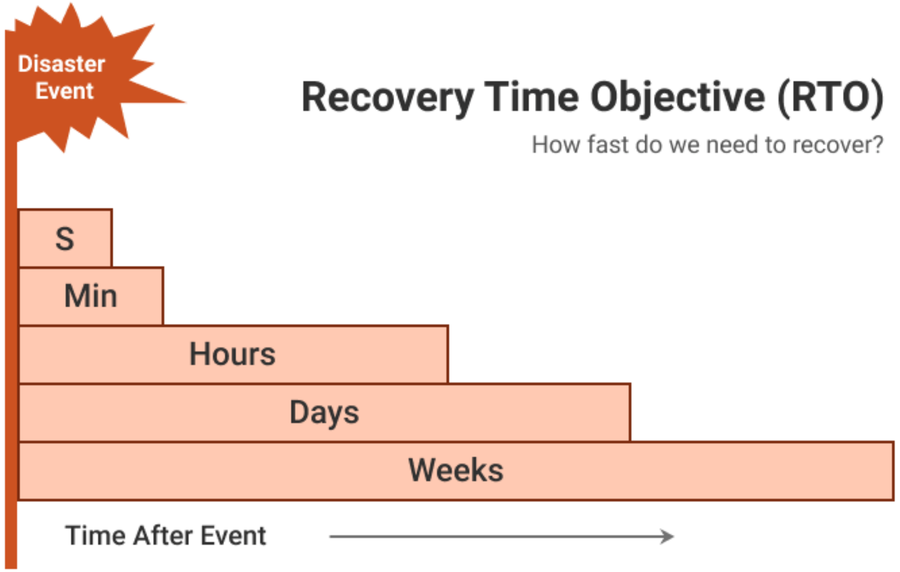

Recovery Point Objective (RPO)
How much data loss can be tolerated?
Cost
Disaster Event
S
Min
Hours
Days
Weeks
Time Before Event

RTO

RTO (Recovery Time Objective) = Measure of how long it takes for IT infrastructure and services to recover from a disaster.

To calculate RTO, consider these factors:

- Time it takes to restore the data *(copying Terabytes takes time).*
- Importance & priority of individual systems.
- Steps required to recover from a disaster (including individual components and processes).
- Available budget and resources


Disaster Event
Recovery Time Objective (RTO)
How fast do we need to recover?
S
Min
Hours
Days
Weeks
Time After Event

Situation 1: Home computer

Where do you store data (e.g. photos)?

1) Local disk (or SSD) of the computer.

Feature:

- Access via this PC only
  If drive crashes = All gone.

Solution:

- Make regular backups. Save them on another disk.
  How often: depends on your RPO. (May the last saved pictures be lost?)

Protect against the risk of disk failure: RAID

Situation 1: Home computer

2) On a disk or storage device in the network
(NAS, Network Attached Storage)

Feature:

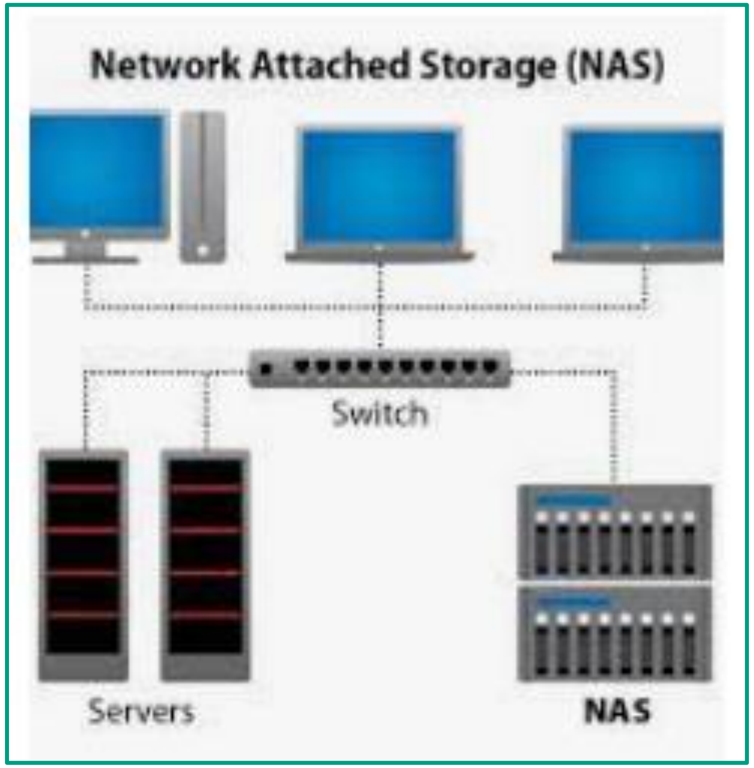
- Access possible from multiple devices
  If NAS crashes = everything gone

Solution:

- Make regular backups. Store them on another device or in the cloud (Dropbox).
  How often: depends on your RPO. (Are the last saved photos allowed to be lost?)

Protect against the risk of disk failure: RAID

3) What is the estimated RTO at home if a disk fails?



Assignment: determine storage architecture at home

Requirements:

- Suppose there are 4 users at home with their own laptops.
- Each user has photos and important files (new ones are added every day) on their own laptop. Backups are made to the NAS (also at home).
- Per day, 0.25 GB of photos or new files are created per user.
- One never wants to lose more than 1 week of data (photos and files).
- They want to be able to store the data for the next 5 years.

Design the storage architecture and specify:

- A schematic drawing of the design
- How much storage each PC should have
- How big the NAS should be.
- How often to backup from the PC to the NAS.

- Would you recommend making an additional backup of the NAS to the cloud? If yes why?

What is a RAID system?

- **RAID** (Redundant Array of Disks) Hard drives configured to work together.

- **Array of disks =** Combination of several disks.
  Each array is seen by the PC as a single disk.
  - In reality, an array consists of several hard drives.
    Goal = Increase the speed or reduce the chance of data loss *(error correction)* or both.

- RAID configurations all have advantages and disadvantages. The choice depends on the goals you want to achieve. So is the importance of: speed, storage space, error correction or cost?

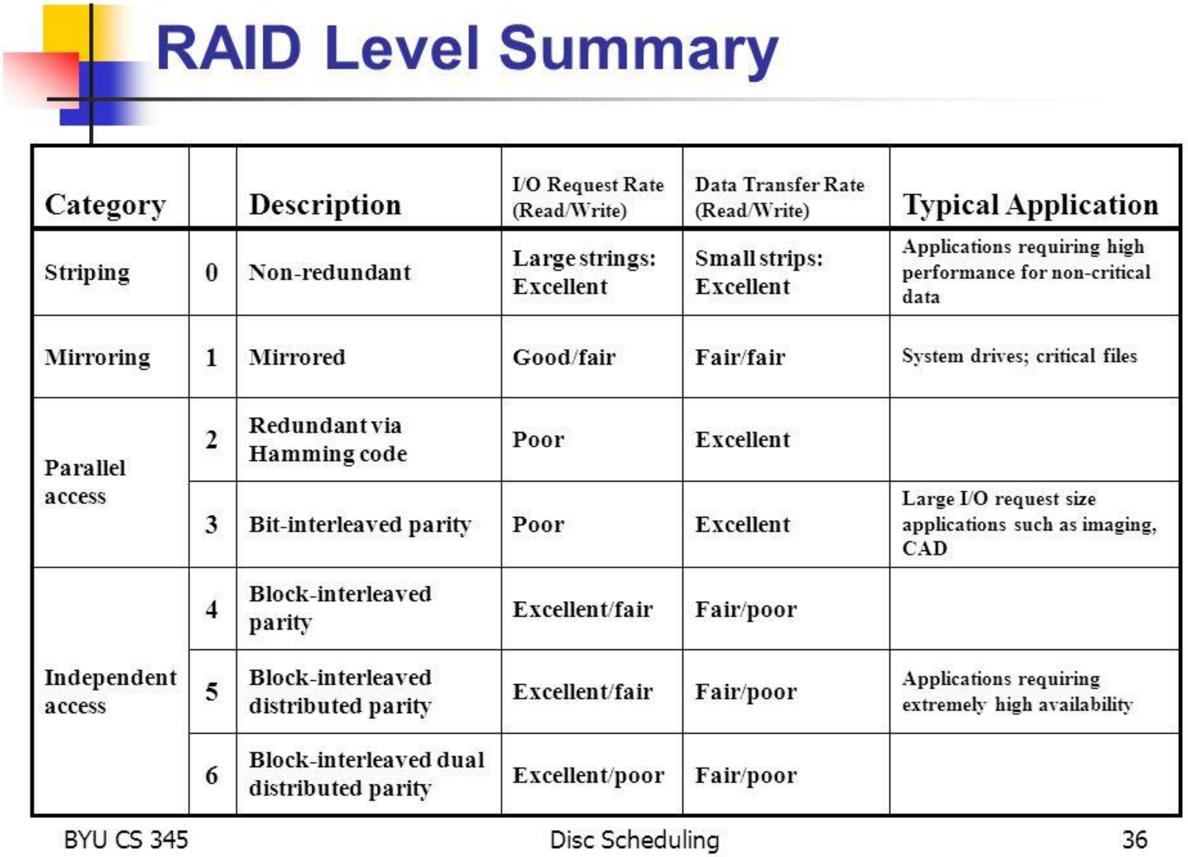
- These different RAID configurations are referred to by various numbers. For example: RAID 0, RAID 1, RAID 5 etc.

?

Important question:
If you use RAID, do you no longer need to make backups?

Important question:
If you use RAID, does that also protect against user errors (e.g. picture accidentally deleted)?

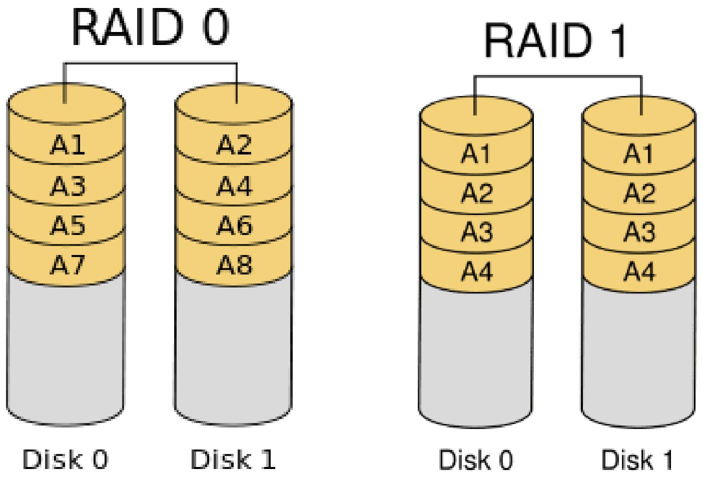
What is a RAID system?

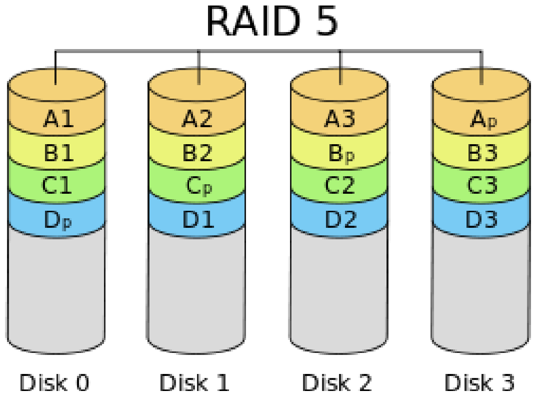


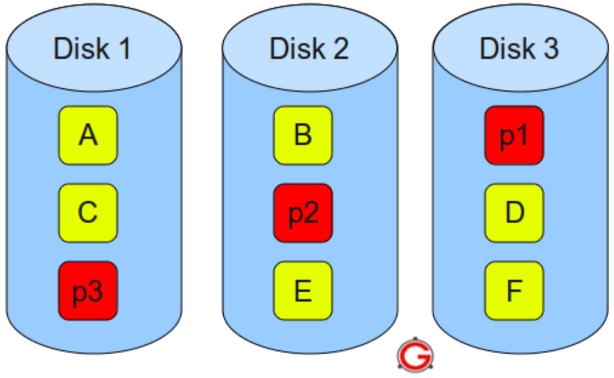
RAID Level Summary

Category		Description	I/O Request Rate (Read/Write)	Data Transfer Rate (Read/Write)	Typical Application
Striping	0	Non-redundant	Large strings: Excellent	Small strips: Excellent	Applications requiring high performance for non-critical data
Mirroring	1	Mirrored	Good/fair	Fair/fair	System drives; critical files
Parallel access	2	Redundant via Hamming code	Poor	Excellent	
	3	Bit-interleaved parity	Poor	Excellent	Large I/O request size applications such as imaging, CAD
Independent access	4	Block-interleaved parity	Excellent/fair	Fair/poor	
	5	Block-interleaved distributed parity	Excellent/fair	Fair/poor	Applications requiring extremely high availability
	6	Block-interleaved dual distributed parity	Excellent/poor	Fair/poor	

BYU CS 345 Disc Scheduling 36







RAID 5 – Blocks Striped. Distributed Parity.

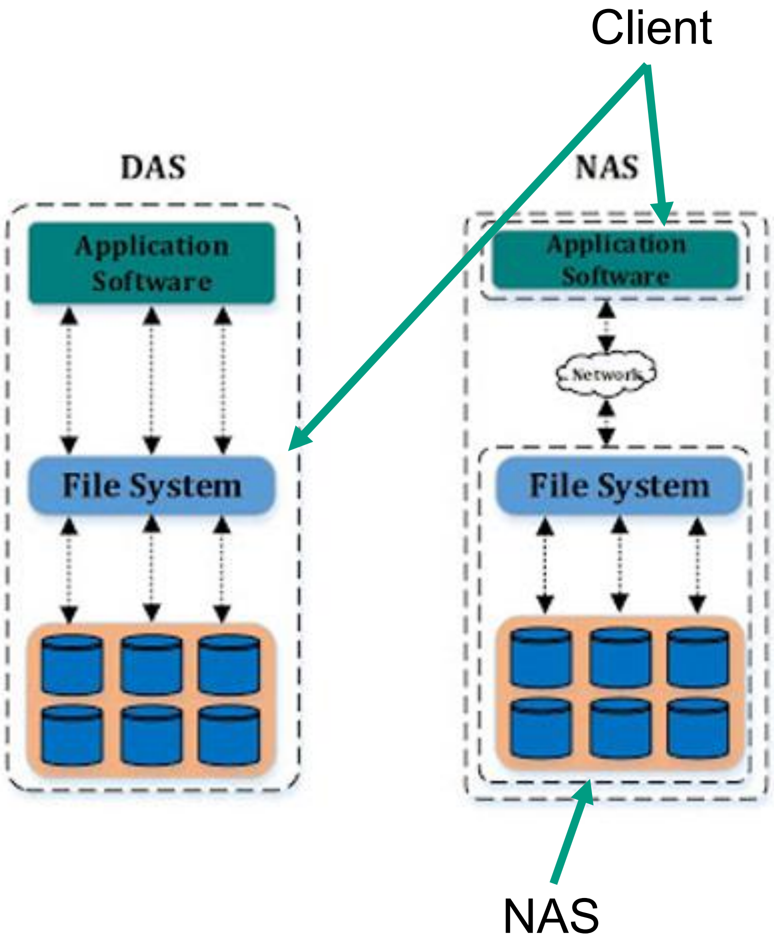
DAS and NAS

1. **DAS Direct Attached Storage**

- File system created by host (e.g. NTFS)
- Directly linked to machine

2. **NAS Network Attached Storage**

- Filesystem created by NAS (e.g. BTRFS)
- Linked to the network
- Fileshare
- Connection: filesharing protocol (cifs or nfs)



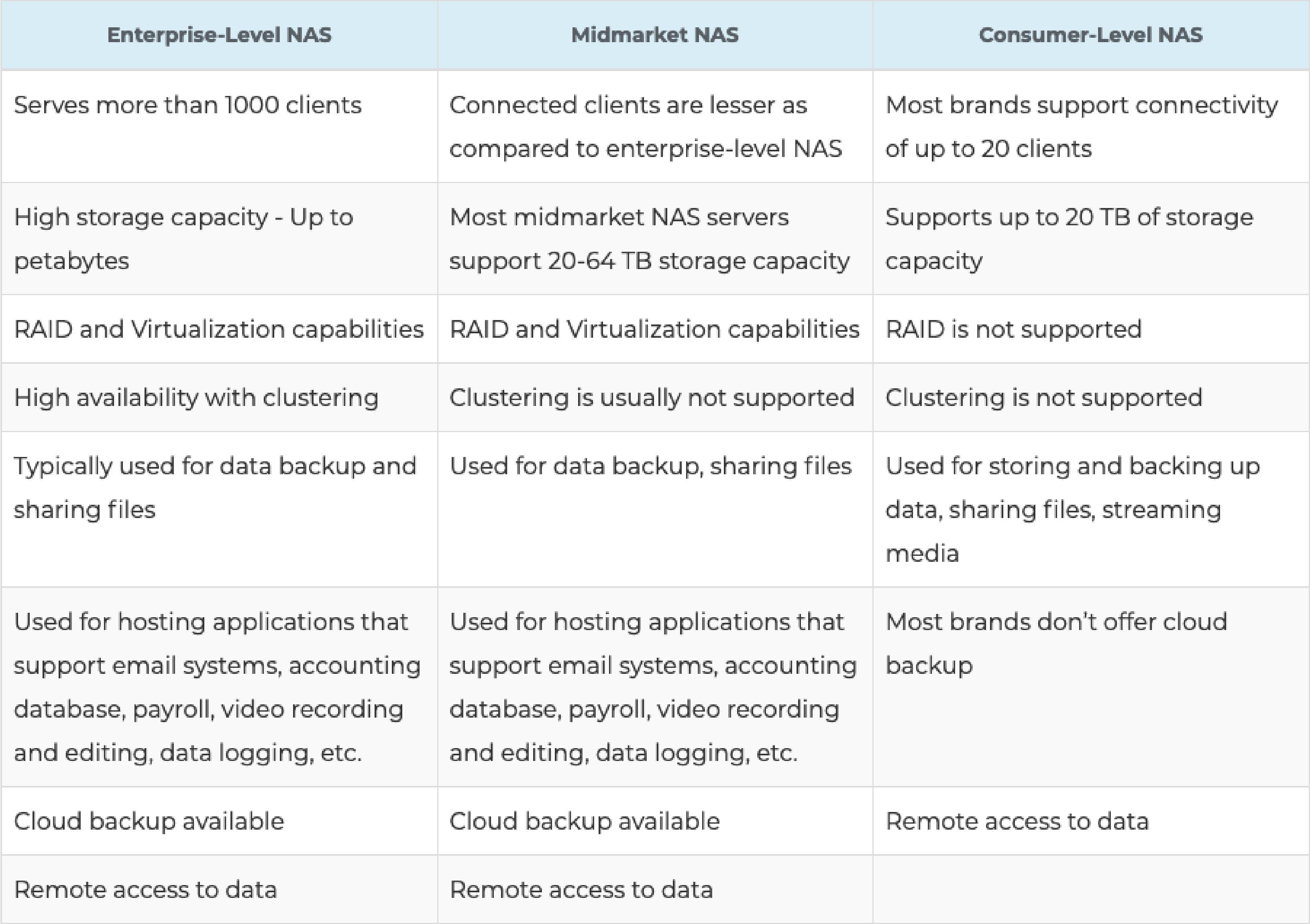
Different types of NAS systems

Enterprise

Midmarket

Consumer

Different types of NAS systems



Enterprise-Level NAS	Midmarket NAS	Consumer-Level NAS
Serves more than 1000 clients	Connected clients are lesser as compared to enterprise-level NAS	Most brands support connectivity of up to 20 clients
High storage capacity - Up to petabytes	Most midmarket NAS servers support 20-64 TB storage capacity	Supports up to 20 TB of storage capacity
RAID and Virtualization capabilities	RAID and Virtualization capabilities	RAID is not supported
High availability with clustering	Clustering is usually not supported	Clustering is not supported
Typically used for data backup and sharing files	Used for data backup, sharing files	Used for storing and backing up data, sharing files, streaming media
Used for hosting applications that support email systems, accounting database, payroll, video recording and editing, data logging, etc.	Used for hosting applications that support email systems, accounting database, payroll, video recording and editing, data logging, etc.	Most brands don't offer cloud backup
Cloud backup available	Cloud backup available	Remote access to data
Remote access to data	Remote access to data	

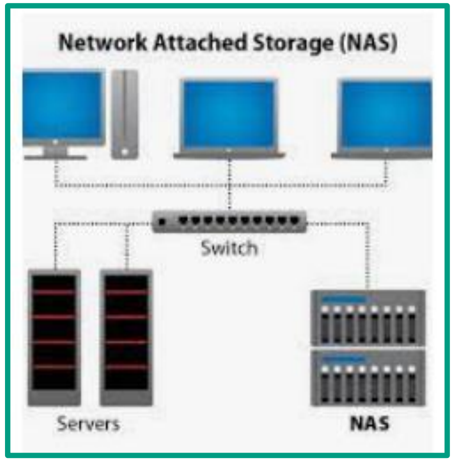
Situation 2: company (e.g. Saxion)

Where does Saxion store all data?

1) Local disk (or SSD) of the computer.

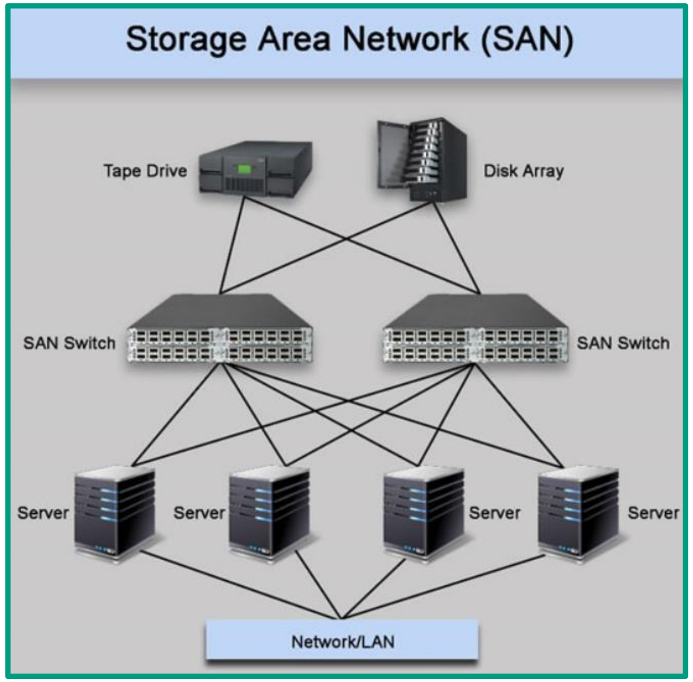
- No; too fragile, too small

Are backups needed here and how often?



2) On a disk or storage device in the network (NAS, Network Attached Storage)
Possibly suitable as a fileshare (e.g. for teachers).

3) **On a SAN (Storage Area Network)**: separate storage network in which
Single Points of Failures (SPOFs) are prevented
Used for storage of virtual machines (good performance needed)

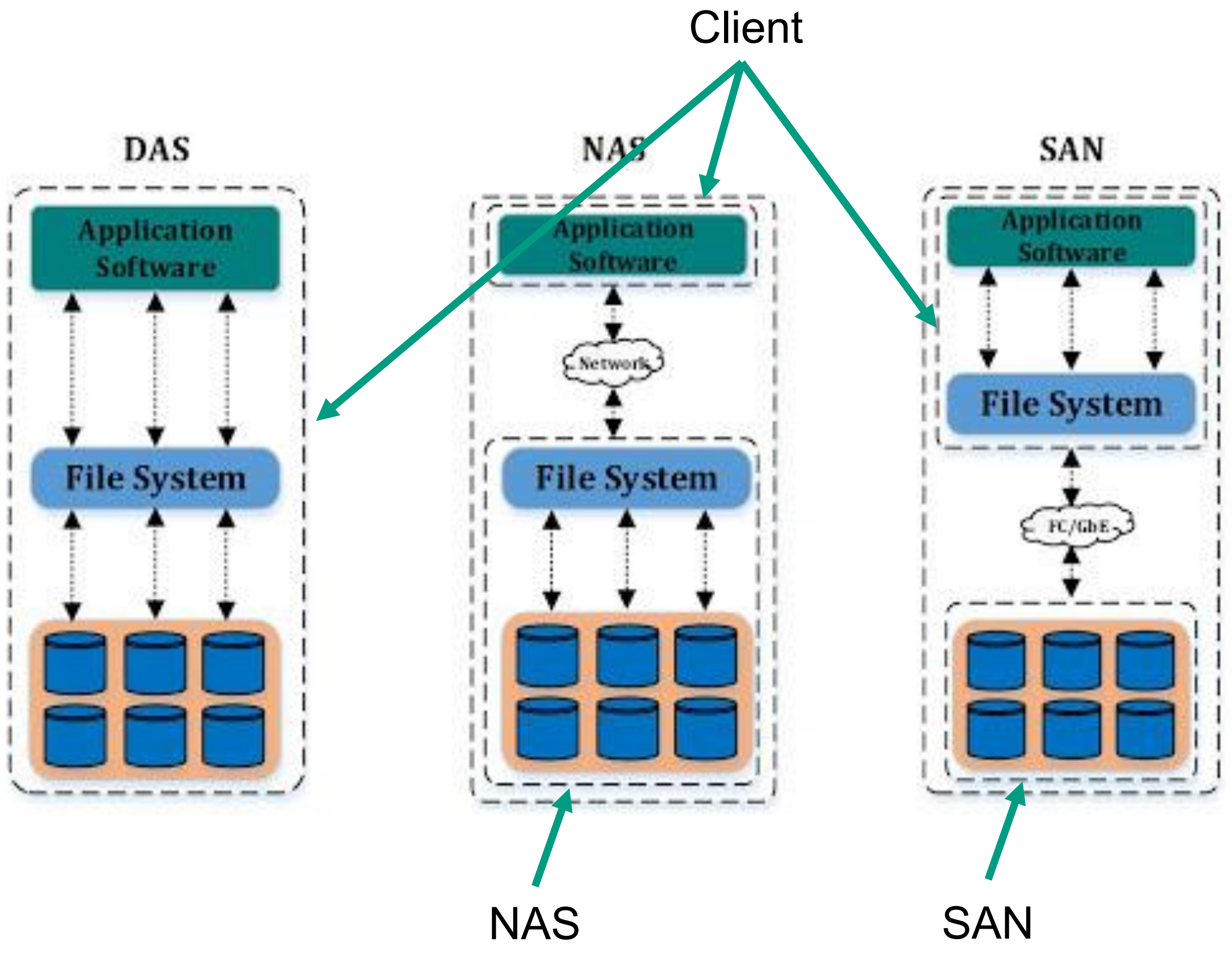


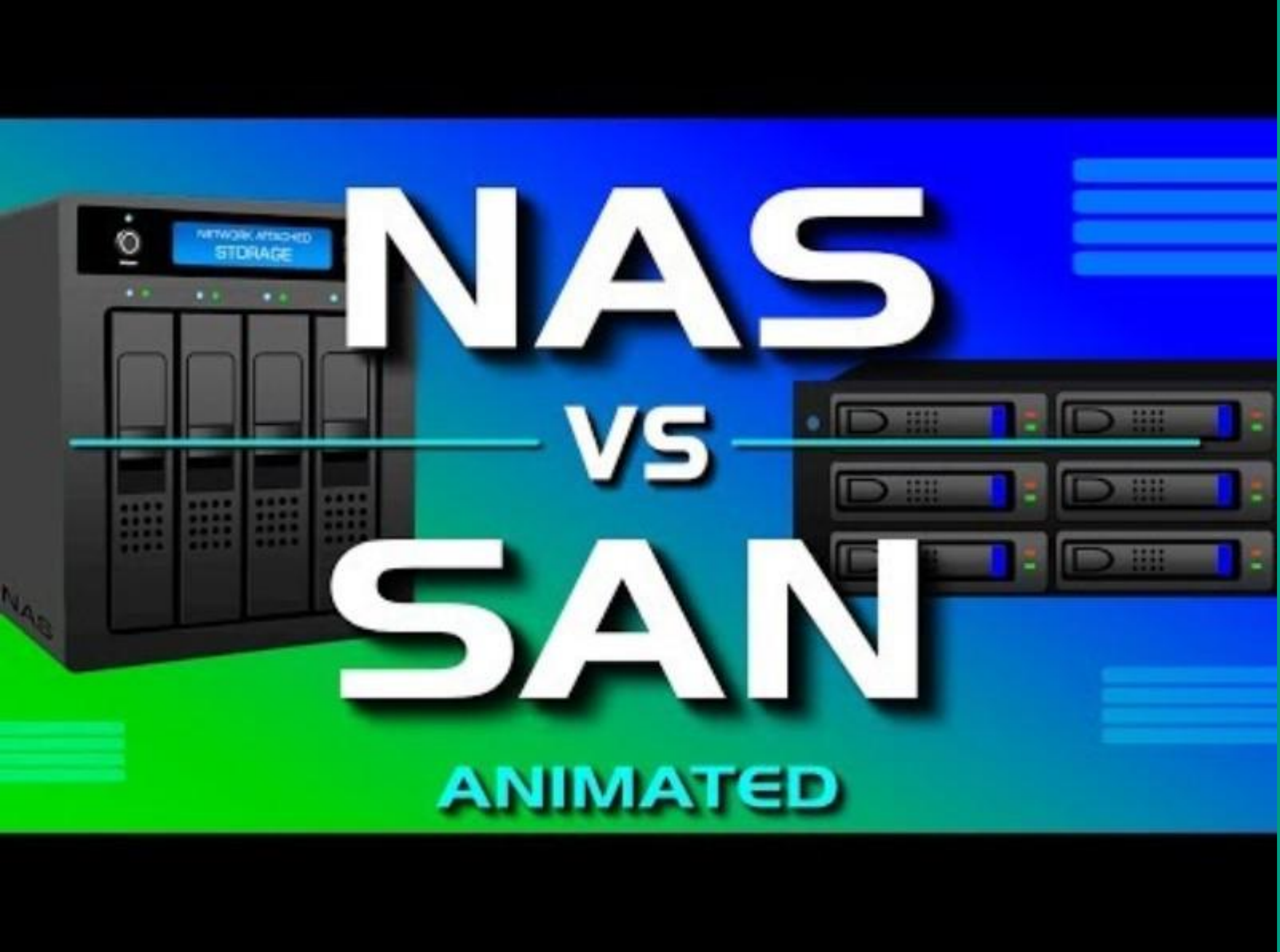
SAN versus NAS

SAN

1. **SAN** (Storage Area Network)

- All components are double ended
- Filesystem created by client
- Connection: fibrechannel or iSCSI
- Installing hypervisors or databases (or virtual NAS)
- Linked to the network
- Can store large amounts of data





Activity

- Watch the following video to learn the difference between NAS and SAN:

https://youtu.be/3yZDDr0JKVc

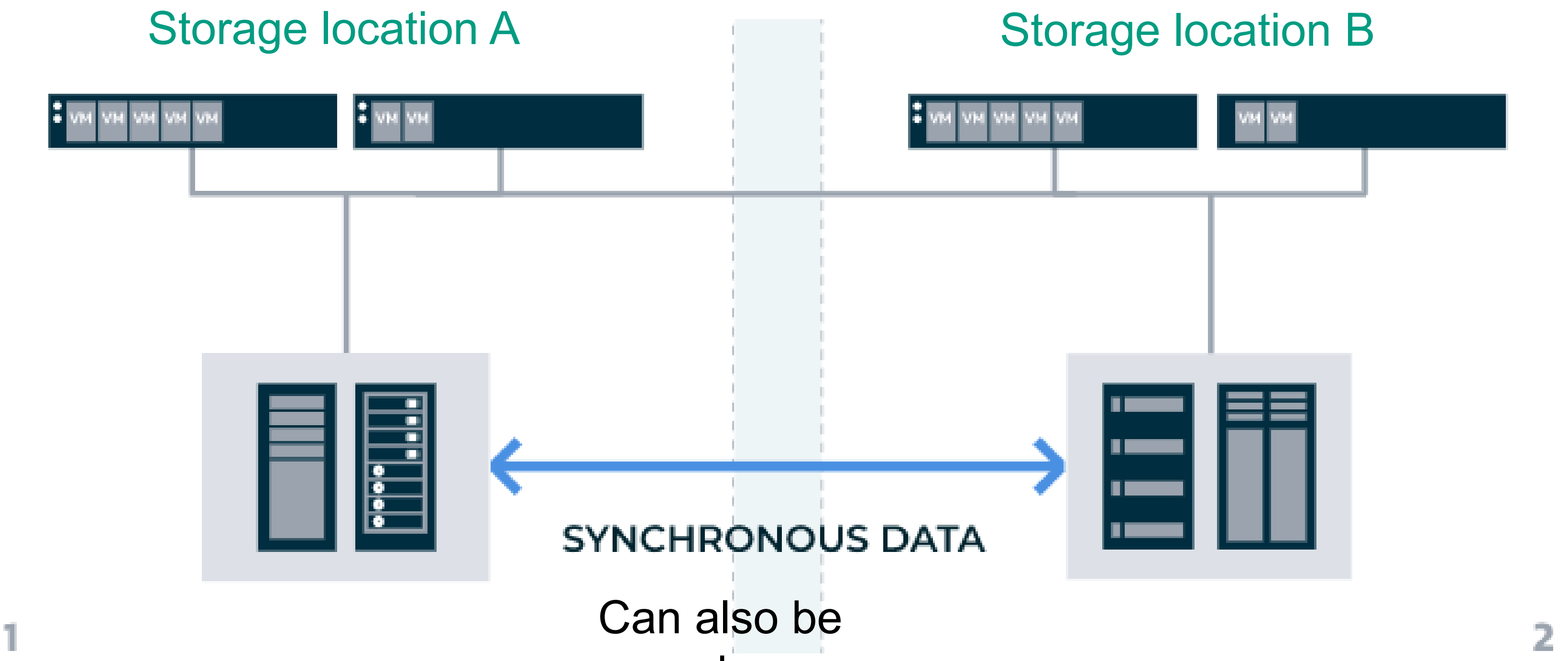
NAS vs SAN

NAS	SAN
Appears as a share folder in the computer network.	Appears as an additional disk in the user's computer network.
The user cannot format it or change it to any file type.	Can format to any file type.
You can only put files on it and share them	On a SAN, VMs but also a NAS can be installed.
Directly connected to switch or router and directly accessible via network	Supports large data storage with high-speed network connection
Usually used in small businesses or homes.	Is fault tolerant and data is spread across multiple disks of different servers
Cheaper than SAN	High scalability and redundancy
	SAN forms in principle an own network and is not directly part of a LAN => less sensitive to disturbances.
	More expensive than NAS and usually applied to large companies.

Clustering

Protect data more effectively: Store data in multiple locations

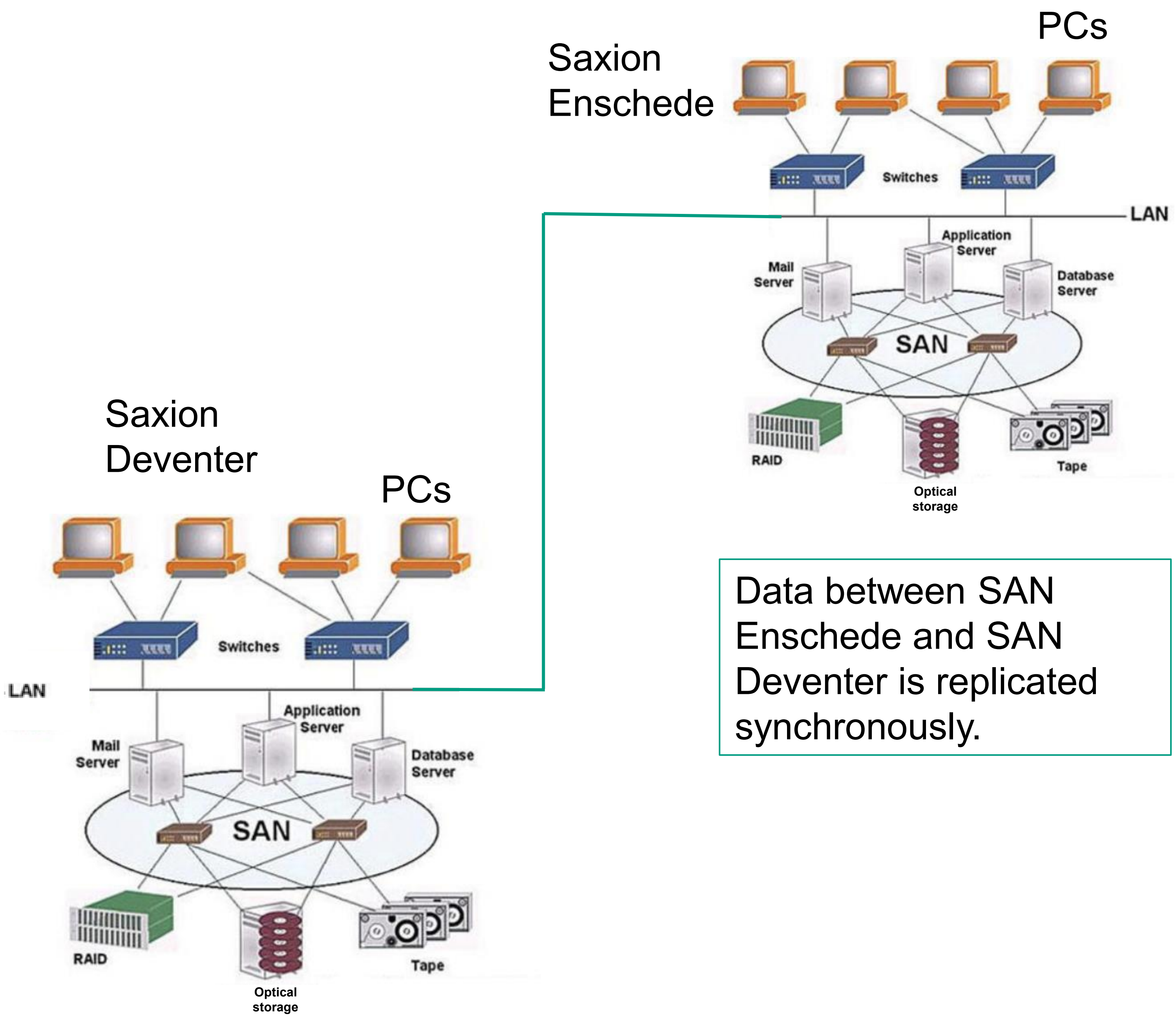
- NAS or SAN e.g. duplicate
- Copying data between both sites



Can also be asynchronous.

Synchronous:
Data on both locations exactly the same

Asynchronous:
Data is always copied after a fixed time interval. E.g. every hour.



Data between SAN Enschede and SAN Deventer is replicated synchronously.

Activity

Storage Saxion

Assume Saxion Storage Architecture is as shown on the left.

- Which Single Points of Failure (SPOFs) may have been resolved and which may remain?
- Do backups still need to be made or are they redundant?

ICT Security

What is security?

- **Keeping** objects **safe**
- Objects of value

- **Examples**:
- **Car**: secured by means of a lock and alarm
- **House**: secured by a fence, lock and alarm

- Security is therefore **by definition preventive**!

After all, a painting that has already been stolen can no longer be secured.

Security in ICT

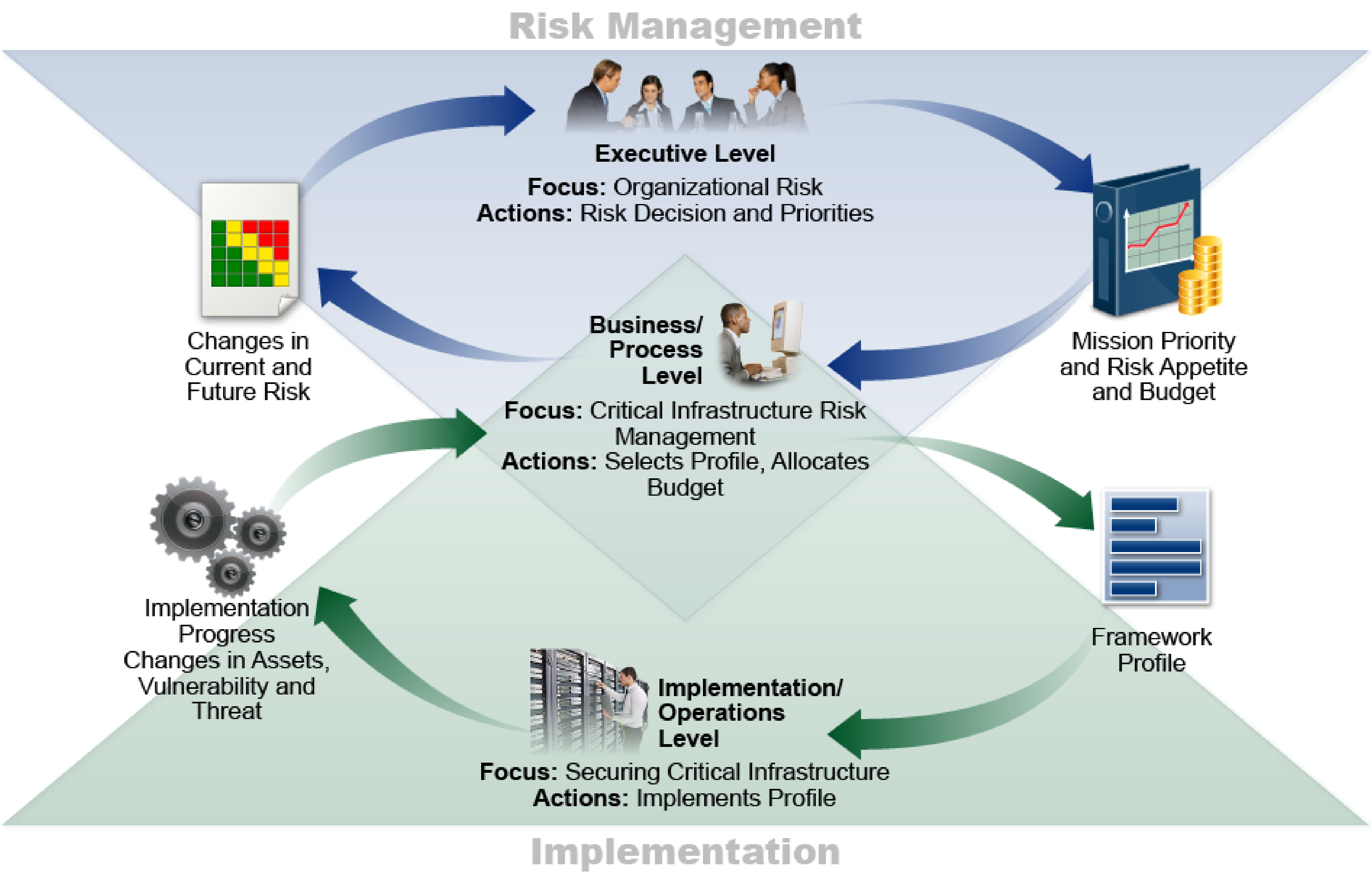
- What is the most valuable thing to be secured in ICT ?

INFORMATION / DATA !

- **Knowledge = power**

- Think about ICT security for example:
  - AVG legislation (GDPR)
  - Operating systems
  - File Systems
  - Networks
  - Data carriers
  - Encryption of the above

A good security approach involves the entire organisation!



Risk Management

Executive Level

Focus: Organizational Risk
Actions: Risk Decision and Priorities

Mission Priority and Risk Appetite and Budget

Business/ Process Level

Focus: Critical Infrastructure Risk Management
Actions: Selects Profile, Allocates Budget

Changes in Current and Future Risk

Framework Profile

Implementation/ Operations Level

Focus: Securing Critical Infrastructure
Actions: Implements Profile

Implementation Progress Changes in Assets, Vulnerability and Threat

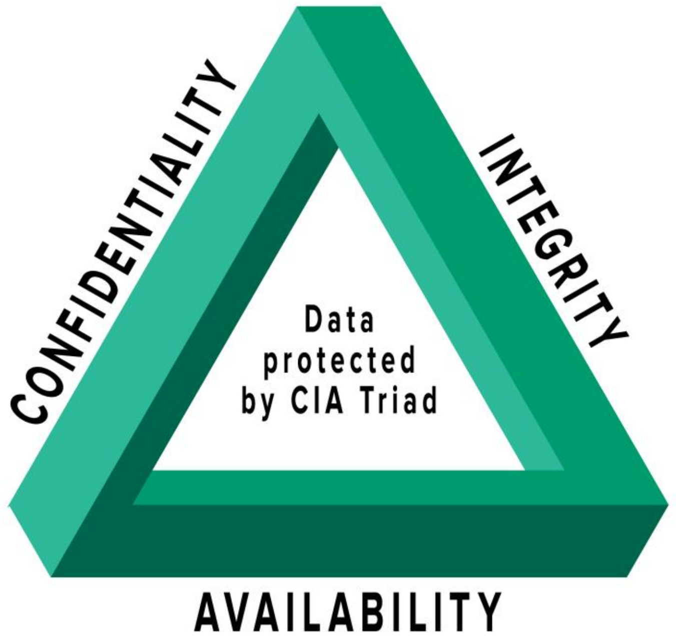
Implementation

CIA triad

CIA

Basic concept: the CIA triad

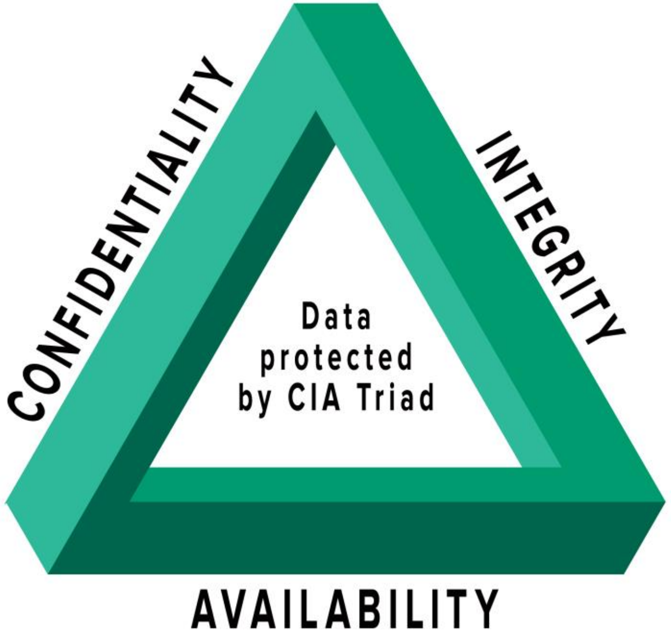
- In protecting information, we must apply the CIA triad.



- Confidentiality:
  - Who can access what? (No more rights than necessary).
- Integrity:
  - Is the information correct and complete?
- Availability:
  - Information must be available at the moment it is needed, think for example of a contingency plan in case of a ransomware attack

Basic concept: the CIA triad

- In order to set up good information security with the aid of the CIA triad, we can elaborate this further via two frameworks:
  - **ISO 27001/ 27002**
  - **NIST security framework**



- Thanks to these frameworks you can set up a structured security plan/system **without forgetting anything!**

ISO 27001/ 27002

ISO 27001

- **ISO 27001** is an ISO standard for information security.
- Established in the Netherlands as the NEN standard **NEN-ISO/IEC 27001**.
- International standard, can apply to all types of organizations.
- **Benefits**:
  - Specifies requirements for determination
  - Implement
  - Execute
  - Check
  - Assess
  - Maintain
  - Improve a Security Management System for information security.
- **Cons**
  - Theoretically set up, which makes it a bit harder to implement in practice.
  - Especially suitable for companies who want to be ISO certified.

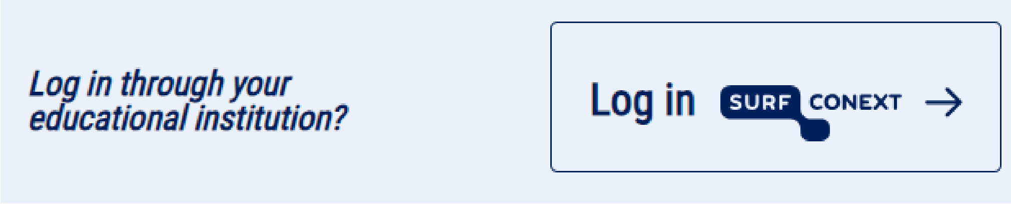
ISO 27002

- **ISO 27002 is a concretization of ISO 27001** and provides more practical guidelines on how security should be applied.

- Consists of a list of measures that an organization can take to reduce security risks.

- Is **more detailed** than ISO 27001

- **Download ISO 27002: Access to the NEN info system: https://connect.nen.nl/**
  - **Click on Log in**



Log in through your educational institution?

Activity

- Examine the ISO 27002 section on *‘enterprise requirements for access security’.*
- Name 3 measures to limit access to information!

Download ISO 27002 : Access to the NEN info system:

https://connect.nen.nl/

Log in through your educational institution?

Log in SURF CONEXT →

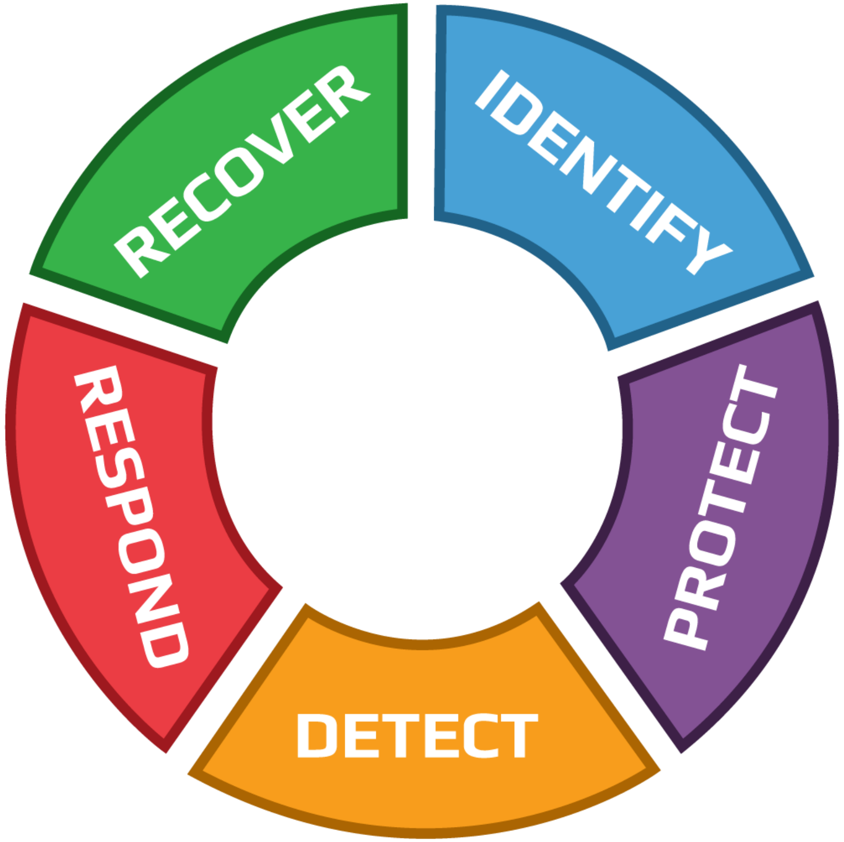
NIST Cybersecurity Framework

NIST Cybersecurity Framework

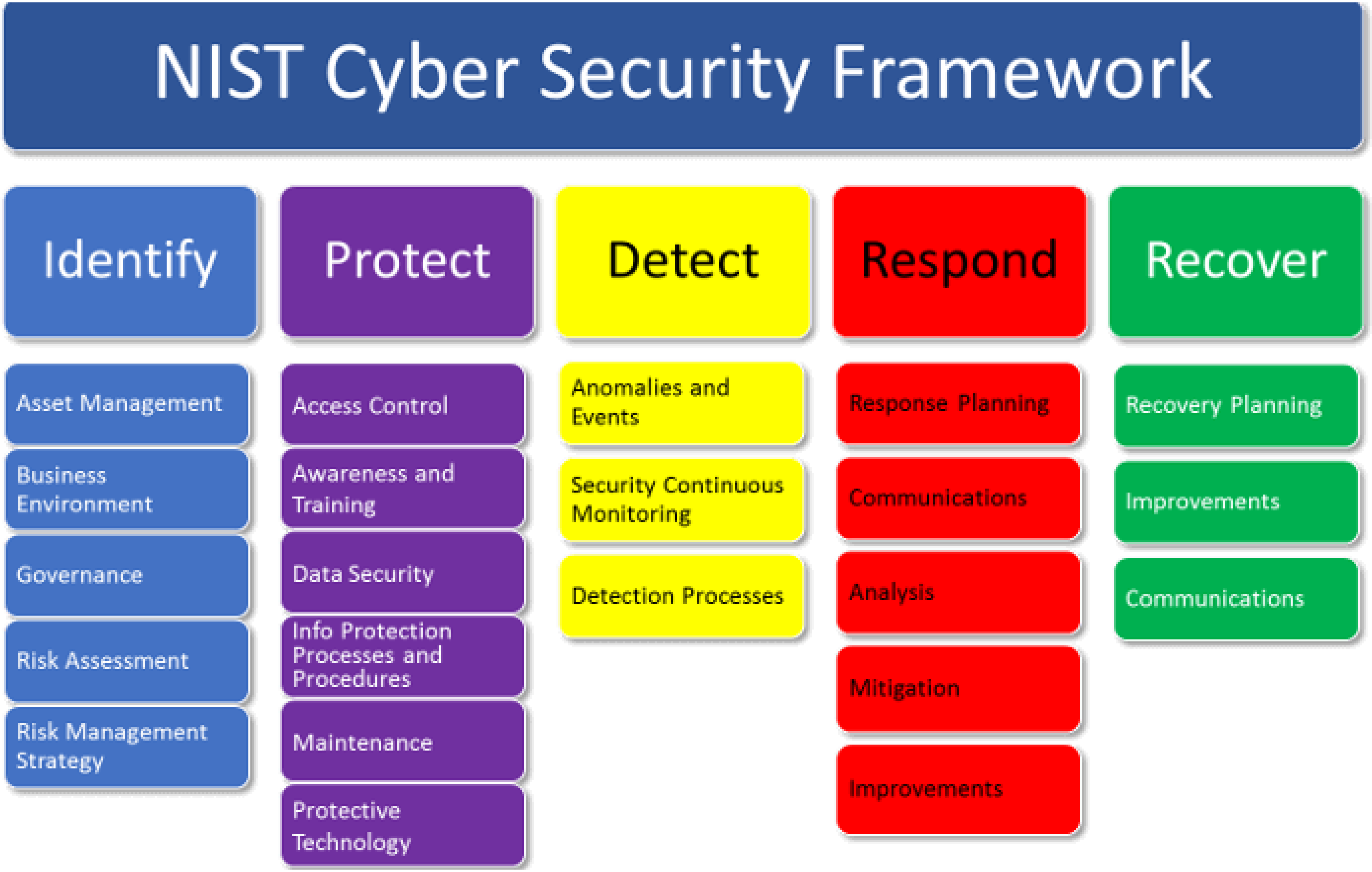
- **International** security framework developed by US National Institute of Standards and Technology.
- More technically detailed, making it easier to implement.
- Subdivides into 5 categories

Can also be applied in the 'real world, such as securing a building:

- **Identify**: First map the building (location, size)
- **Protect**: Place a fence and video cameras
- **Detect**: Provide motion detection on the cameras
- **Respond**: Call in a security company to check out the situation on site
- **Recover**: Repair the fence if it has been broken during the burglary



NIST security framework (ICT)



NIST Cyber Security Framework

Identify	Protect	Detect	Respond	Recover
Asset Management	Access Control	Anomalies and Events	Response Planning	Recovery Planning
Business Environment	Awareness and Training	Security Continuous Monitoring	Communications	Improvements
Governance	Data Security	Detection Processes	Analysis	Communications
Risk Assessment	Info Protection Processes and Procedures		Mitigation	
Risk Management Strategy	Maintenance		Improvements	
	Protective Technology			

IDENTIFY

"Develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities."

- **Think for example of:**
  - The business context, the resources used for critical functionality and the cybersecurity risks involved.
  - Summarized: map the organization

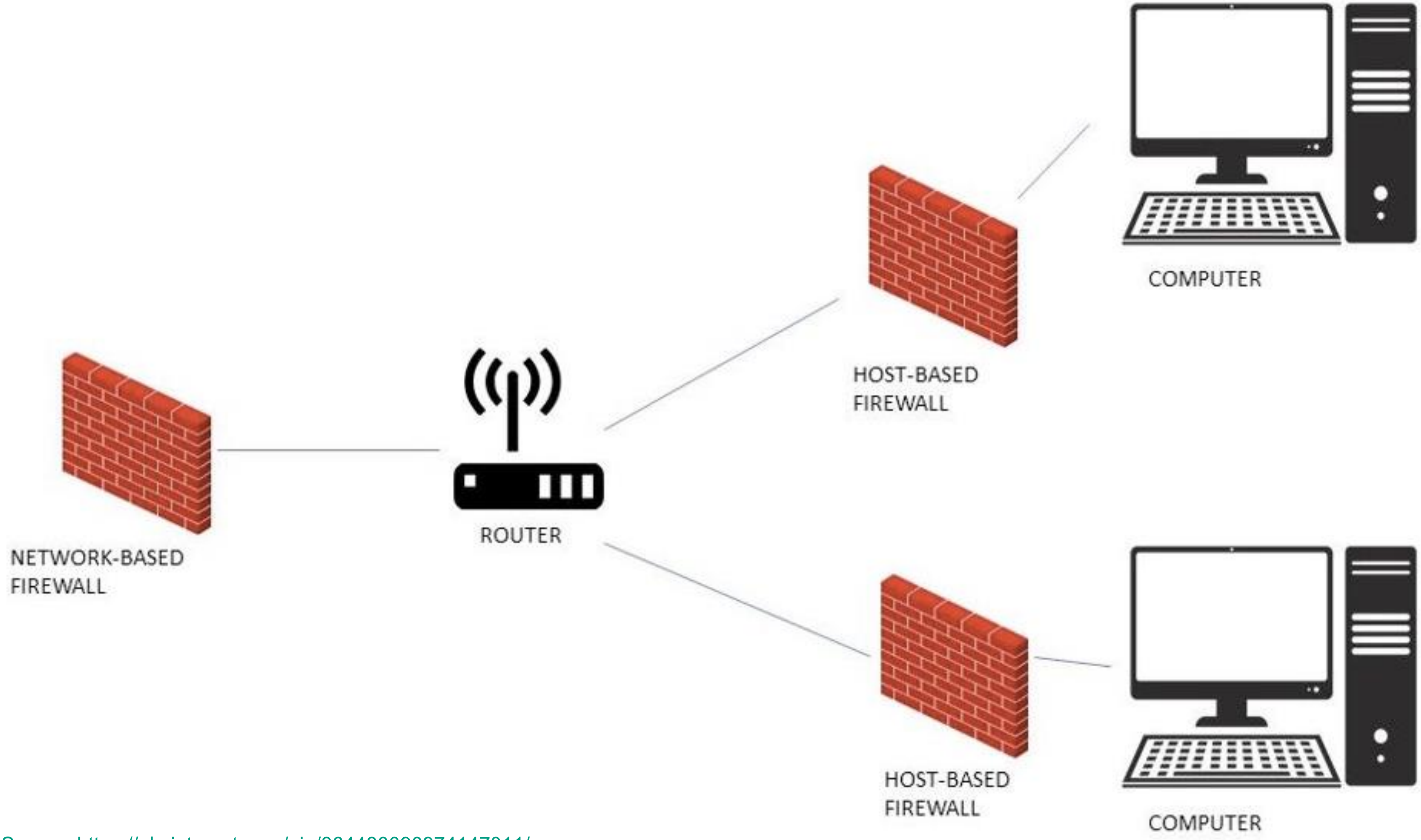
- **Deliverables in this category:**
  - Asset management (e.g. in Topdesk)
  - Business Environment (e.g. BPMN, Archimate)
  - Governance (Policy)
  - Risk assessment
  - Risk Management Strategy

Protect

"Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services."

- **First line of defence**, for example:
    - Authentication, authorization and accounting, AAA (password policy, account lockout, Role-based access control, file system rights, etc.)
    - Firewalls (infra and host)
    - Physical access to server room
    - Physical access to switch ports in the building (NAC)
    - WiFi
    - Encryption
    - User awareness! (phishing, ransomware)

Protect: using firewalls



Source: https://nl.pinterest.com/pin/864480090974147011/

Detect

"Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event".

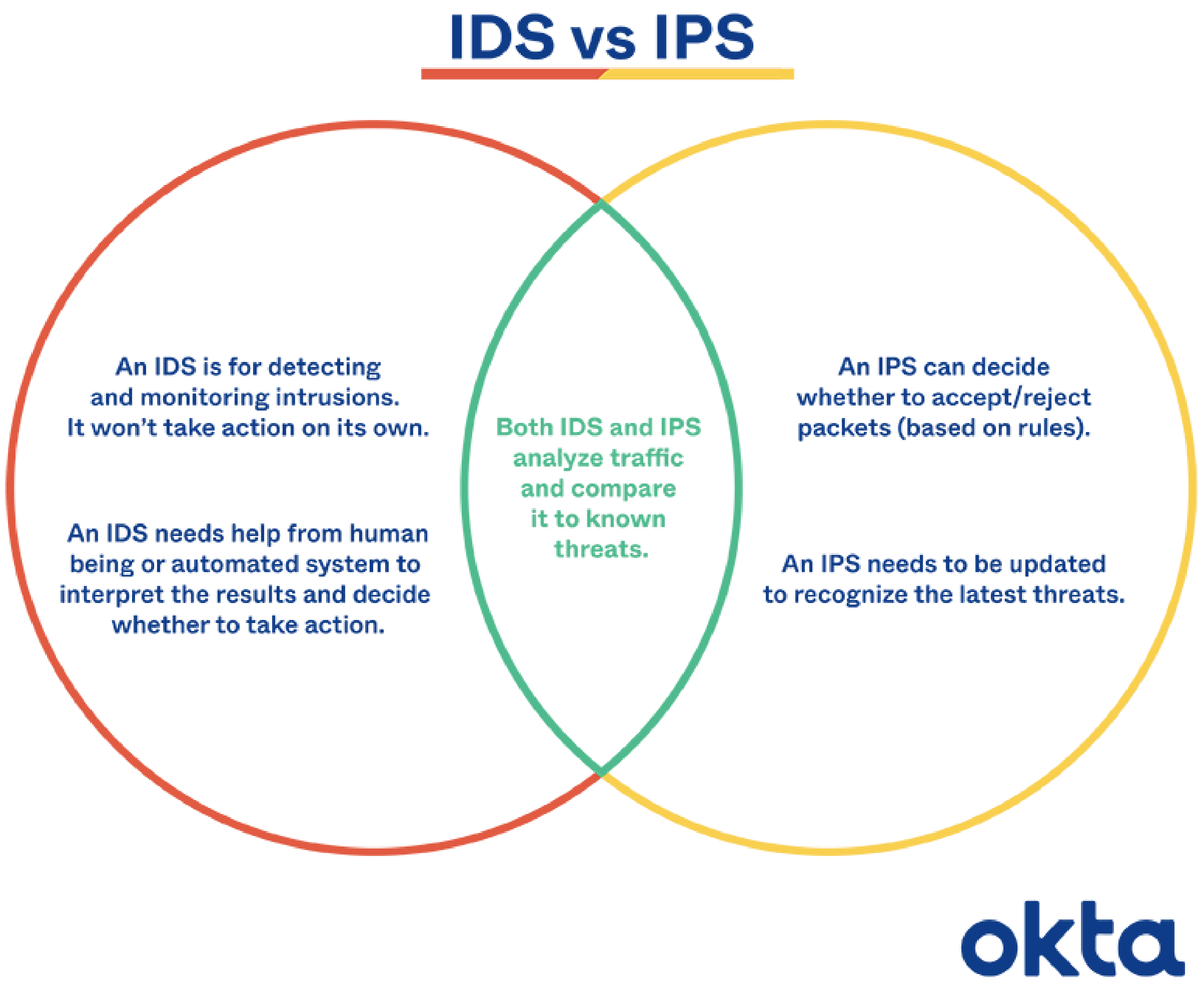
Detecting intrusions and attacks on the infra, think about setting up:

- AntiVirus Scanner: Centrally manageable, heuristic etc.
- Intrusion Detection System (IDS)
- Intrusion Prevention System (IPS)
- Security information and event management (SIEM)
- Honeypot
- User awareness (suspicious activities)

Deliverables in this category:

- Anomalies and Events
- Security Continuous monitoring
- Detection Processes

Detect: IDS vs IPS



IDS vs IPS

An IDS is for detecting and monitoring intrusions. It won't take action on its own.

An IDS needs help from human being or automated system to interpret the results and decide whether to take action.

Both IDS and IPS analyze traffic and compare it to known threats.

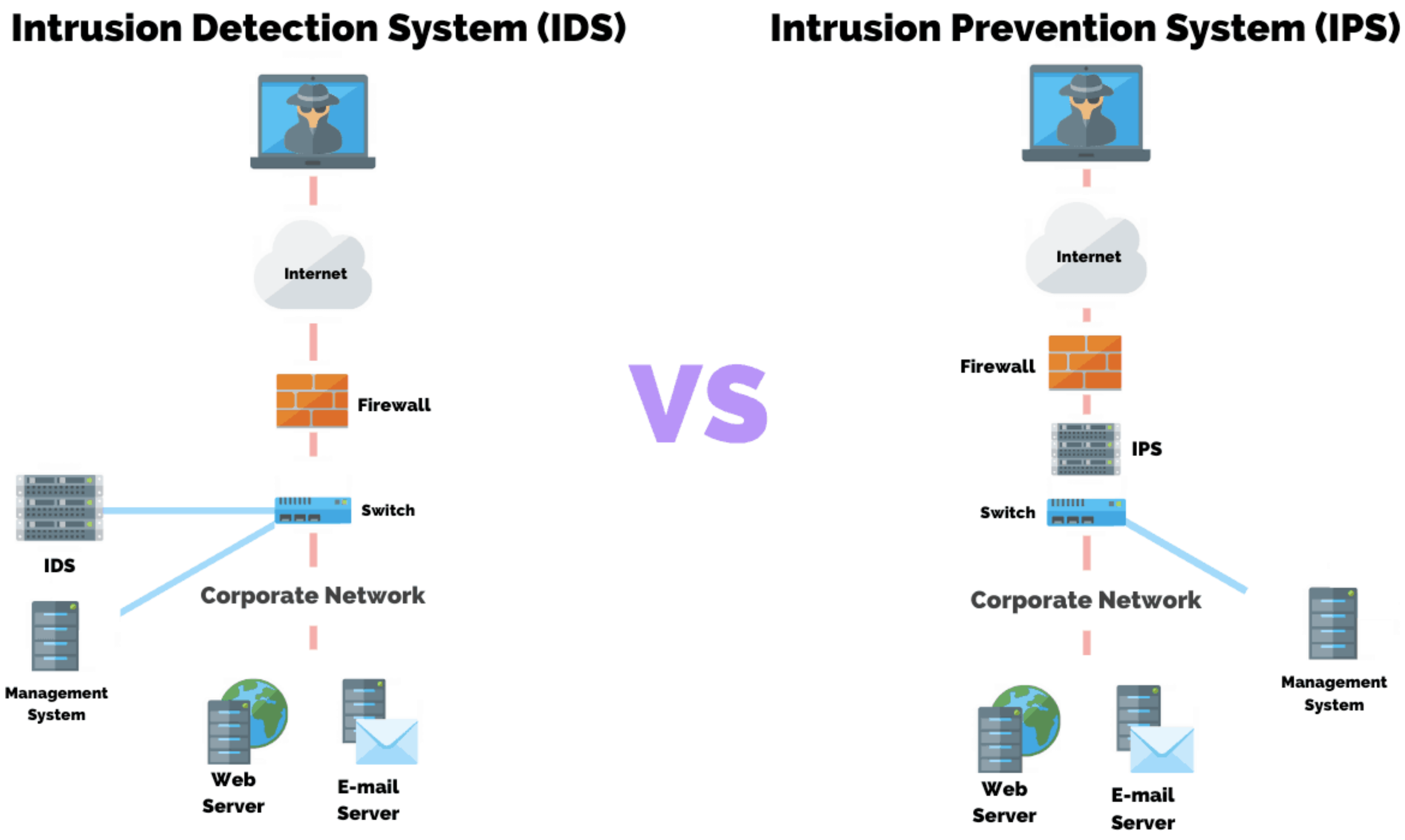
An IPS can decide whether to accept/reject packets (based on rules).

An IPS needs to be updated to recognize the latest threats.

okta

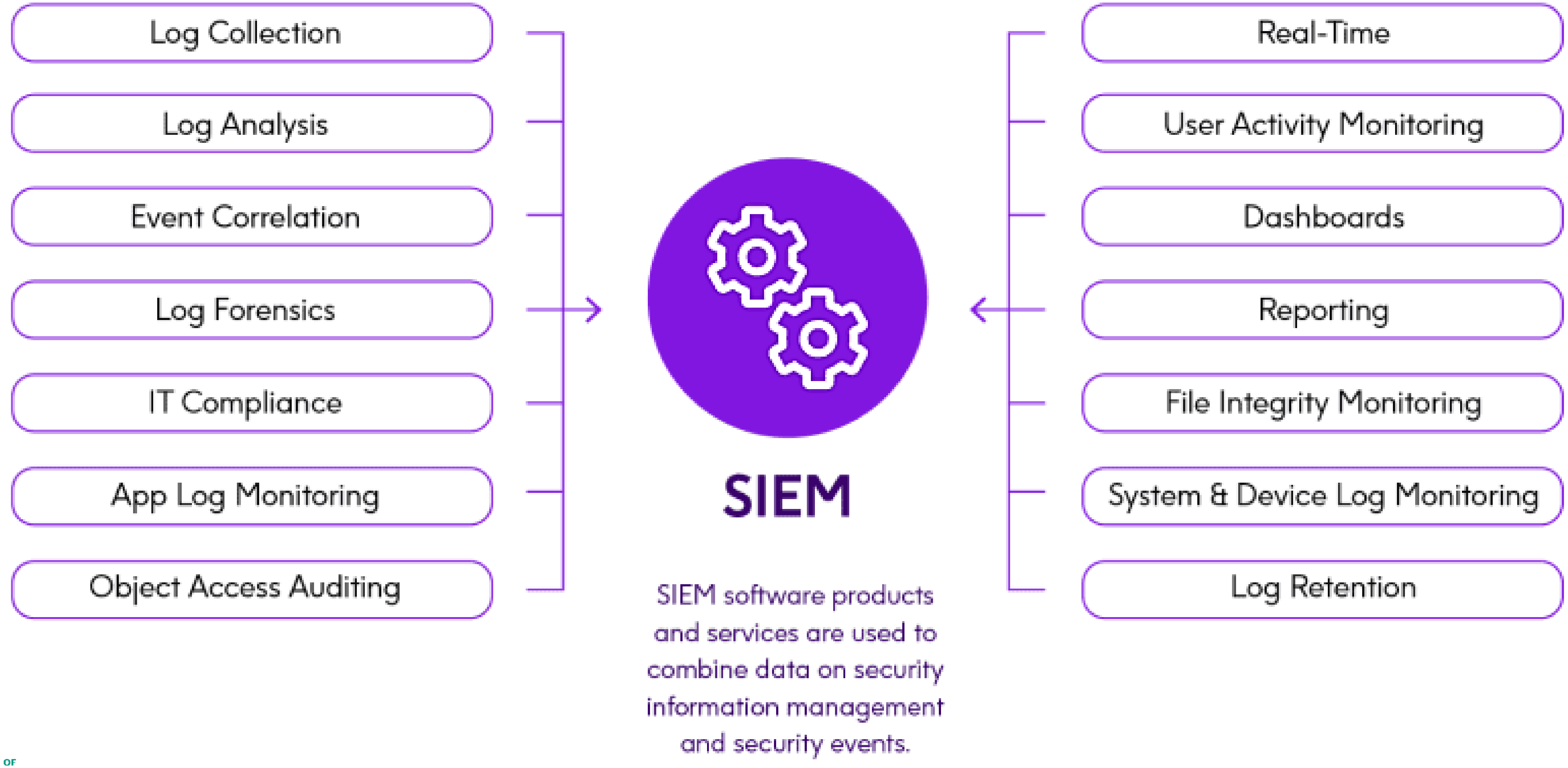
Source : https://www.okta.com/identity-101/ids-vs-ips/

IDS only monitoring, IPS can intervene in network traffic



Source : https://purplesec.us/intrusion-detection-vs-intrusion-prevention-systems/

IPS, IDS also known as SIEM



Log Collection

Log Analysis

Event Correlation

Log Forensics

IT Compliance

App Log Monitoring

Object Access Auditing

Real-Time

User Activity Monitoring

Dashboards

Reporting

File Integrity Monitoring

System & Device Log Monitoring

Log Retention

SIEM

SIEM software products and services are used to combine data on security information management and security events.

Source : https://brasiline.com.br/blog/edr-vs-xdr-vs-siem/

Respond

"Develop and implement the appropriate activities to take action regarding a detected cybersecurity event"

Try to limit the impact of security issues as much as possible:

- Temporarily disable firewalls, servers and possibly other infrastructure components
- Implementation of temporary measures (mitigation)
- Communicate as much as possible with security stakeholders (set up war room)
- Monitor the activities

Deliverables in this category:

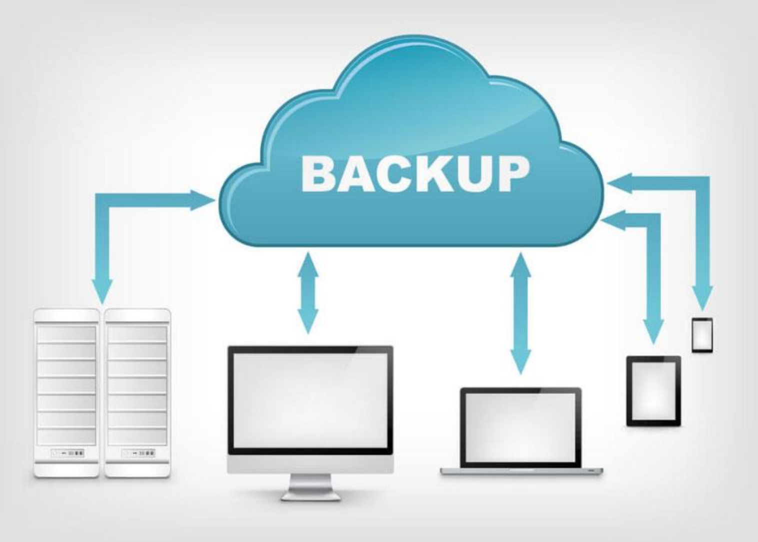
- Response planning (roadmaps)
- Communications
- Analysis
- Mitigation and impovements

Recover

"Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event."

The damage caused must be repaired. (Think about erased or encrypted data.)
Paying for un-encrypting is always discouraged!

- Backup system is the most important here (RPO, RTO, offsite, on other infrastructure, encrypted)
- Disaster Recovery
- Communicate the above with the organization



Deliverables in this category:

- Recovery planning
- Improvements
- Communications

Activity

In January 2025, the systems at the Eindhoven University of Technology were hacked.

- Read the article and management report on the hack. **Click here**.
- **What cause** or **causes** do you find in the document that caused the hack?
- **What measures** could/should the University have taken to prevent this?

Working on the case

Case

- Do the assignments of week 5

Please consult the assignments document and the template report for more details.

Any questions?