

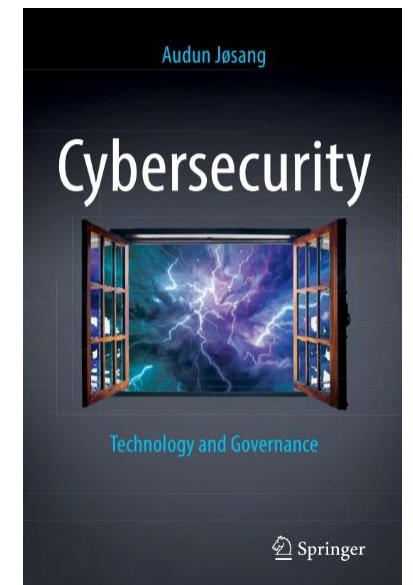
# Chapter 1: Basic Concepts of Cybersecurity

---

## **Cybersecurity: Technology and Governance**

Audun Jøsang,

1st Edition, Springer Nature, 2024.



# What is security?

Security is the protection of assets from harm

Physical  
assets



Life and  
health



Natural  
environment



Law  
and order



Critical  
infrastructure



State  
integrity



Digital  
assets

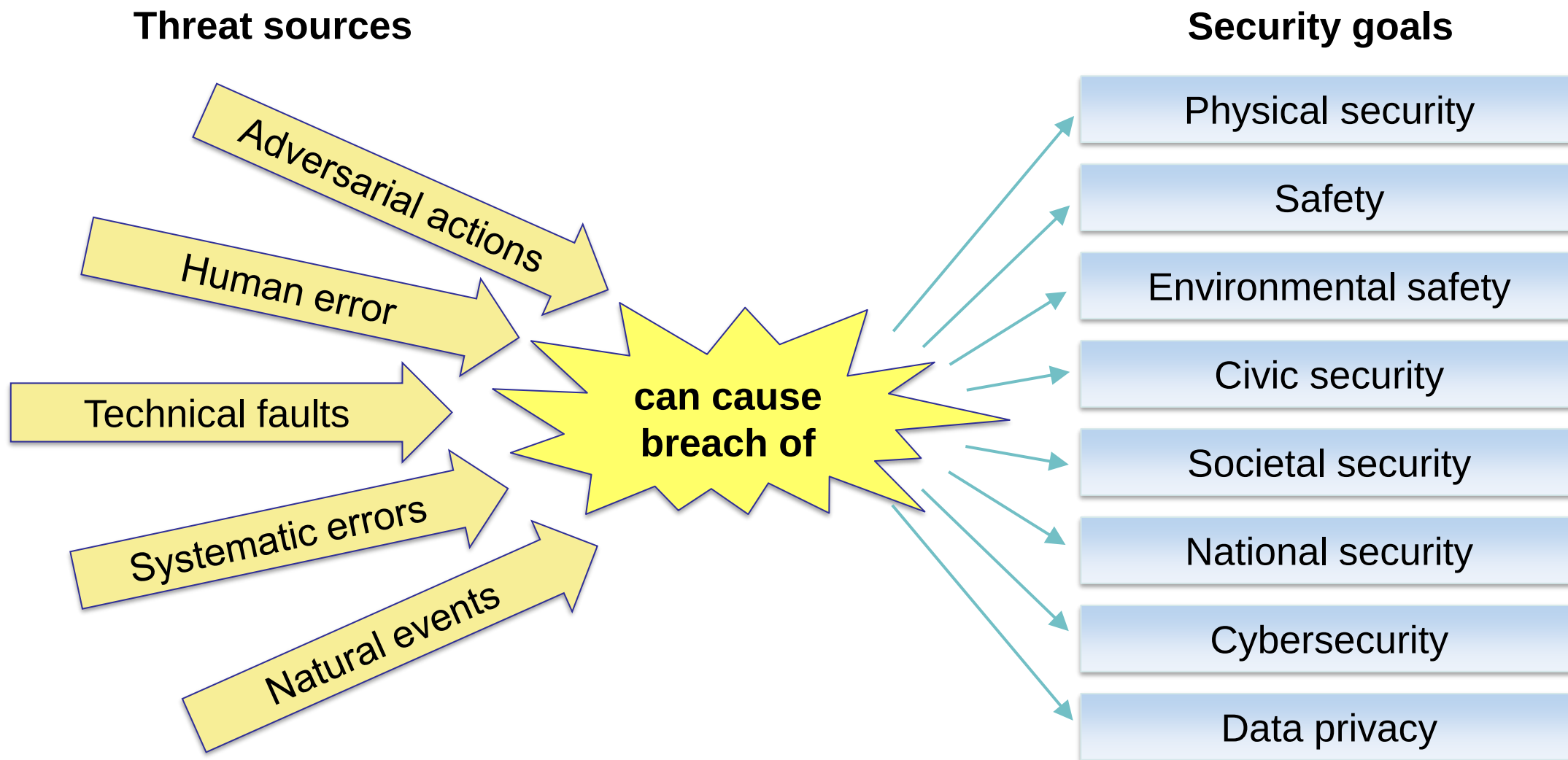


Personal  
data



- **Physical security:** Prevention of break-ins, theft and tampering with facilities equipment
- **Safety:** Protection of life and health
- **Environmental safety:** Preventing pollution and invasion of alien species into nature.
- **Civic security:** Maintaining law and order
- **Societal security:** Protection of critical infrastructures and basic functions in the society
- **National security:** Preservation of national sovereignty, territorial integrity, and government
- **Cybersecurity:** Protection of digital assets
- **Data privacy:** Following legal principles for collecting, storing, processing and sharing personal data

# Various sources of security breaches

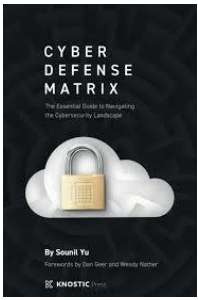


# What is cybersecurity? (1)

- **Cybersecurity is the protection of digital assets from harm.**
- Digital assets are (see Cyber Defense Matrix, ch.18):
  - DEVICES
  - APPS
  - NETWORKS
  - DATA
  - USERS
- How can digital assets be harmed?
  - Breach of one or more of the security goals Confidentiality, Integrity and Availability (CIA)
- Mainly focuses on damage cause by adversarial threats
  - But threats can also be accidents or technical failures
  - Humans can do harm both intentionally and unintentionally



# Asset Types of the Cyber Defense Matrix



- DEVICES are hardware devices and the commodity software that runs on them.
  - Firmware, operating systems and standard applications from vendors belong to this class.
  - Distinguish by who owns device, e.g organization, staff (BYOD), or cloud providers.
  - Networking devices like switches and routers also belong to this class.
- APPS are business applications and processes specially developed by or for the organization itself.
  - APPs are typically producing the services and products which deliver the organization's value and business functions. Hence, the continuity and integrity of APPS are typically critical.
- NETWORKS are communication channels, routings, protocols, and firewall filterings.
  - Configuration of networking devices such as DNS (Domain Name System), AS (Autonomous Systems) and PKI (Public Key Infrastructure), and which provides routing, filtering and VPN
- DATA is all types of business data whether at-rest, in-motion, or in-use by the asset listed above.
- USERS are the people and AI agents using the assets listed above, with their IDs and credentials.
  - An AI agent could perhaps be considered to be a device, but if it carries the characteristics of a user with its own ID, authentication credentials, access authorizations, and intelligent decisions.

# What is cybersecurity? (2)



- More verbosely, cybersecurity is the protection of digital assets from threats that may result in unauthorized disclosure of information, corruption of data, software and hardware, as well as disruption of the services they provide.
- There is no exact consensus of what cybersecurity is, and there are many different definitions proposed by various standards, guidelines, and frameworks.
- Practitioners who know where the shoe pinches typically describe cybersecurity in practical terms such as Rick Howard's first principle of cybersecurity which is *"to reduce the probability of material impact due to a cyber incident over the next three years."*

R. Howard, *Cybersecurity First Principles* (Wiley, 2023)

# What is information security?



- ISO's definition of Information Security:
  - ***The preservation of confidentiality, integrity and availability of information.***  
*In addition, other properties, such as authenticity, accountability, non-repudiation, and reliability can also be involved.*

(ISO/IEC 27000:2025)



Maybe it would have been better to say «preservation of CIA of information assets».

# We have many names for the things we love



- **Cybersecurity:** The protection of digital assets from harm.  
The term has been popular since the 2010s.
- **Information security:** General term, i.e. it also covers the protection of information on paper, popularly from the 1970s. Direct translation of "information security" that is enshrined in several international standards and frameworks.
- **Computer Security:** To be interpreted as the protection of data stored in computer systems, as well as the systems themselves. The term has been popularly since the 1980s.
- **IT and ICT security:** To be interpreted as security in IT/ICT systems. The term has been popular since the 1990s.
- **Digital security:** The protection of anything digital, i.e. that has IT components.

Note that all these terms have more or less the same meaning!

# Sources of requirements for cybersecurity

- **Good practice:** Requirements for adequate security in business processes according to common good practice and management.
    - Good practice sets requirements for e.g. user authentication and access control.
  - **Risk assessment:** Requirements to limit security risks to an acceptable level. Measures are identified through risk assessment and risk management.
    - Risk assessment can, for example, require 2-factor authentication.
  - **Regulations:** Legal, regulatory, industry, and contractual information security requirements, such as:
    - The NIS2 Directive in the EU, mandating organizations to implement security measures.
    - GDPR Article 32 mandates adequate security protection for personal data.
    - PCI DSS (Payment Card Industry Data Security Standard) (Industry norm in finance).
- Note that regulatory and legal requirements for information security often refer to risk assessment as a requirement and a tool for identifying necessary security measures.

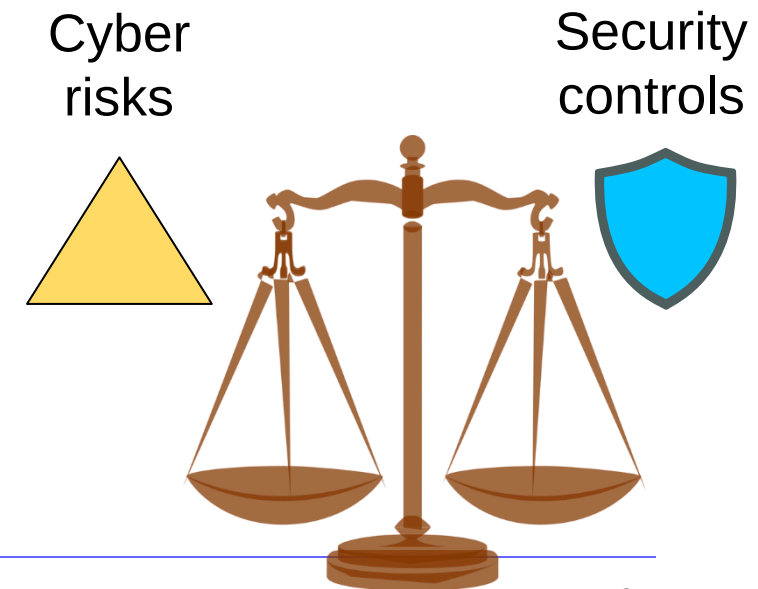


# Goal of cybersecurity governance

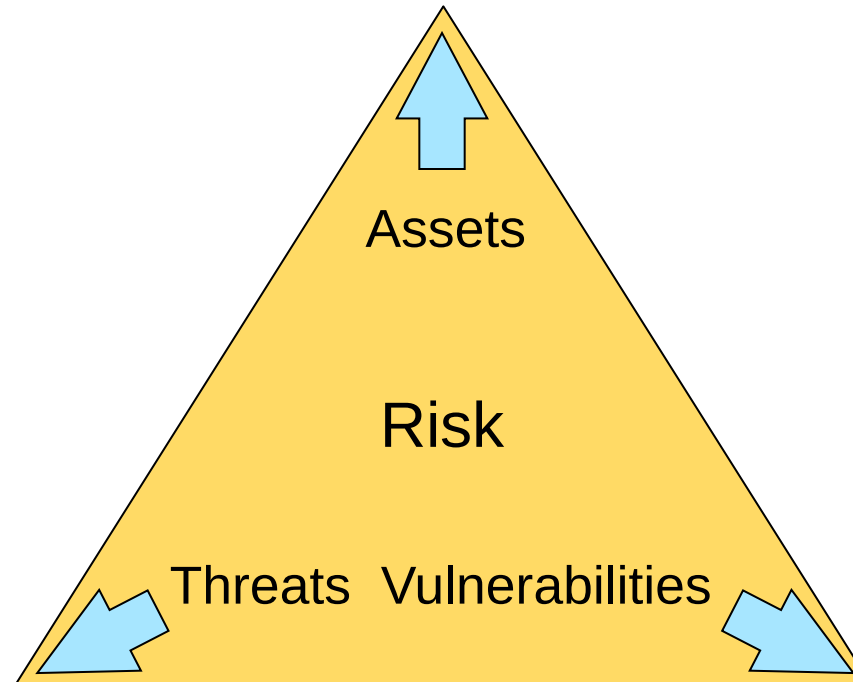
- Would it be possible to solve all security problems?
- No, because:
  - New vulnerabilities are being discovered in legacy systems
  - New services, often with vulnerabilities, are being exposed online
  - Threat actors are good at finding vulnerabilities that can be exploited
  - Increasingly effective attack tools are being developed
  - Increasing number and severity of threats

Conclusion: cybersecurity is a continuous process to remove vulnerabilities and mitigate threats.

- The goal of cybersecurity governance is to get a good balance between security risk and security controls.



# General model for IT security risk

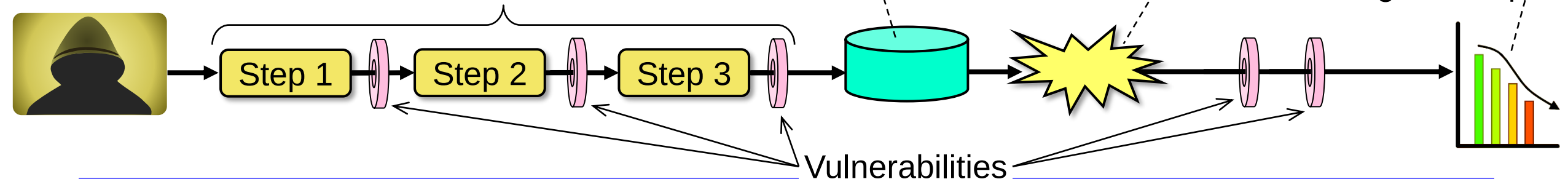


- General risk model:
  - The greater and more assets you have, the stronger and more threats you are faced with, and the more serious vulnerabilities you have, then the greater your risk exposure.

# Assets, Threats, Vulnerabilities and Security Controls

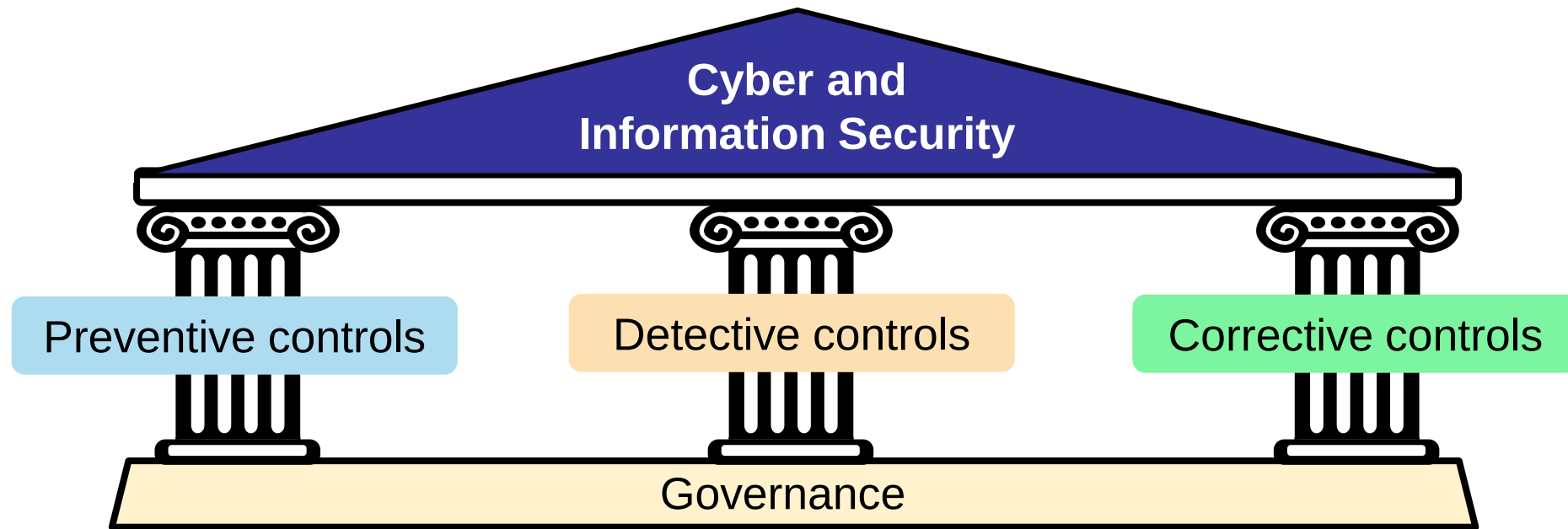
- **Assets:** (Information) resources that are of value to the organization.
  - Data, Systems, Applications, Networks, Devices, IT Services, People (as they interact with IT).  
The goal of cybersecurity is to protect the CIA of assets, depending on the need.
  - Personal data
- **Threat:** A potential attack scenario controlled by a threat actor that could harm your organization's assets.
- **Vulnerability:** Absence of controls against threats and inability to handle incidents.
- **Security Control:** Method to prevent or mitigate threats, or method reduce the impact of incidents.

Threat actor executes ... threat scenario ... which harms assets and causes incident ... with negative impact



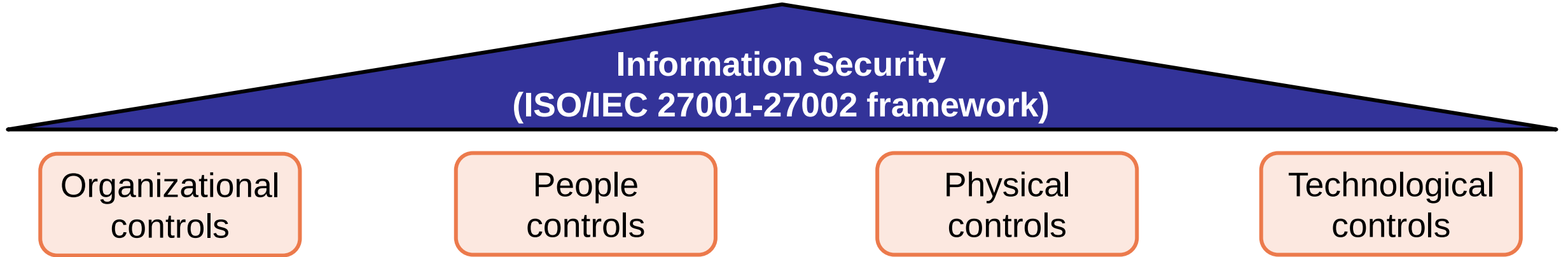
# Information Security Controls

categorized according to cybersecurity functions



# Information Security Controls

categorized in general control domains



## Information Security Management System (ISMS)

|                                                                                                                                                                                                                                            |                                                                                                                                                                                                           |                                                                                                                                                                                                                    |                                                                                                                                                                                                           |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Organizational controls examples:</b> <ul style="list-style-type: none"><li>• Policies/Procedures</li><li>• Roles and responsibilities</li><li>• Information classification</li><li>• Cyber readiness training</li><li>• etc.</li></ul> | <b>People controls examples:</b> <ul style="list-style-type: none"><li>• Staff screening</li><li>• Employment contract</li><li>• Awareness training</li><li>• NDA when resigning</li><li>• etc.</li></ul> | <b>Physical controls examples:</b> <ul style="list-style-type: none"><li>• Camera surveillance</li><li>• Physical access control</li><li>• Shielding of cables</li><li>• Locks and alarms</li><li>• etc.</li></ul> | <b>Technological controls examples:</b> <ul style="list-style-type: none"><li>• User authentication</li><li>• Encryption</li><li>• Network security</li><li>• Incident detection</li><li>• etc.</li></ul> |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|

# The four P's

- The four P's correspond roughly to the traditional “People + Process + Technology” (PPT) aspects of cyber governance described e.g. by NIST CSF, but with the “Partner” aspect added.



- People:** Staff must have necessary skills training for operating and managing cybersecurity, which includes a good security culture in the organization.
- Product (Technology):** Organizations must carefully consider which products/technology that in the most optimal way can support the goal of reducing risk to an acceptable level.
- Partner:** Organizations need to engage with partners when acquiring products and services from 3rd parties. It can be a waste of money to buy an expensive security product if the vendor is not able to provide adequate support for operating the product.
- Process:** All use of technology (Product) consists of processes, so when an organization acquires or implements security technology, they must ensure that there is an adequate process for operating the technology. If the process is ineffective or inefficient, the technology has little value.

# General Security Goals: CIA + P

- Information security is traditionally defined as the preservation of CIA:

- 
- Confidentiality
- Integrity
- Availability:
- 



- Data privacy (data protection) has an additional set of goals that includes, among other things, CIA. The GDPR (General Data Protection Regulation) defines data protection requirements.

**Privacy**

# Security goals and controls

- Security goals
  - independent of specific implementation
  - Can be implemented with different controls
- Security controls
  - Based on specific implementation, often tied to specific products

Security goals:

**Confidentiality – Integrity – Availability**

Support

Security controls:

e.g. policies – staff screening – locks – encryption



Analogy for civic security

# Confidentiality

- Property that information is not made available or disclosed to unauthorized individuals, entities, or processes.  
(ISO/IEC 27000)
- Threats:
  - Data theft (external threat)
  - Data leakage (internal threat)
- Security controls examples:
  - Encryption
  - Cryptographic communication protocols, e.g. TLS
  - Authentication and access control,
  - Anonymization, e.g. through a pseudonym or VPN
  - Layered protection
  - Security culture, awareness...



# Integrity

- **Data integrity:** The property that data has not been altered or destroyed in an unauthorized manner. (X.800)
- **Integrity (of information assets in general):** The property of accuracy and completeness. (ISO/IEC 27000)
- Threats: Corrupted data and misconfigured systems
- Security control examples:
  - Hashing, MAC, digital signature, encryption
  - Configuration management
  - Change management
  - Authentication
  - Access control
  - Security culture, awareness...

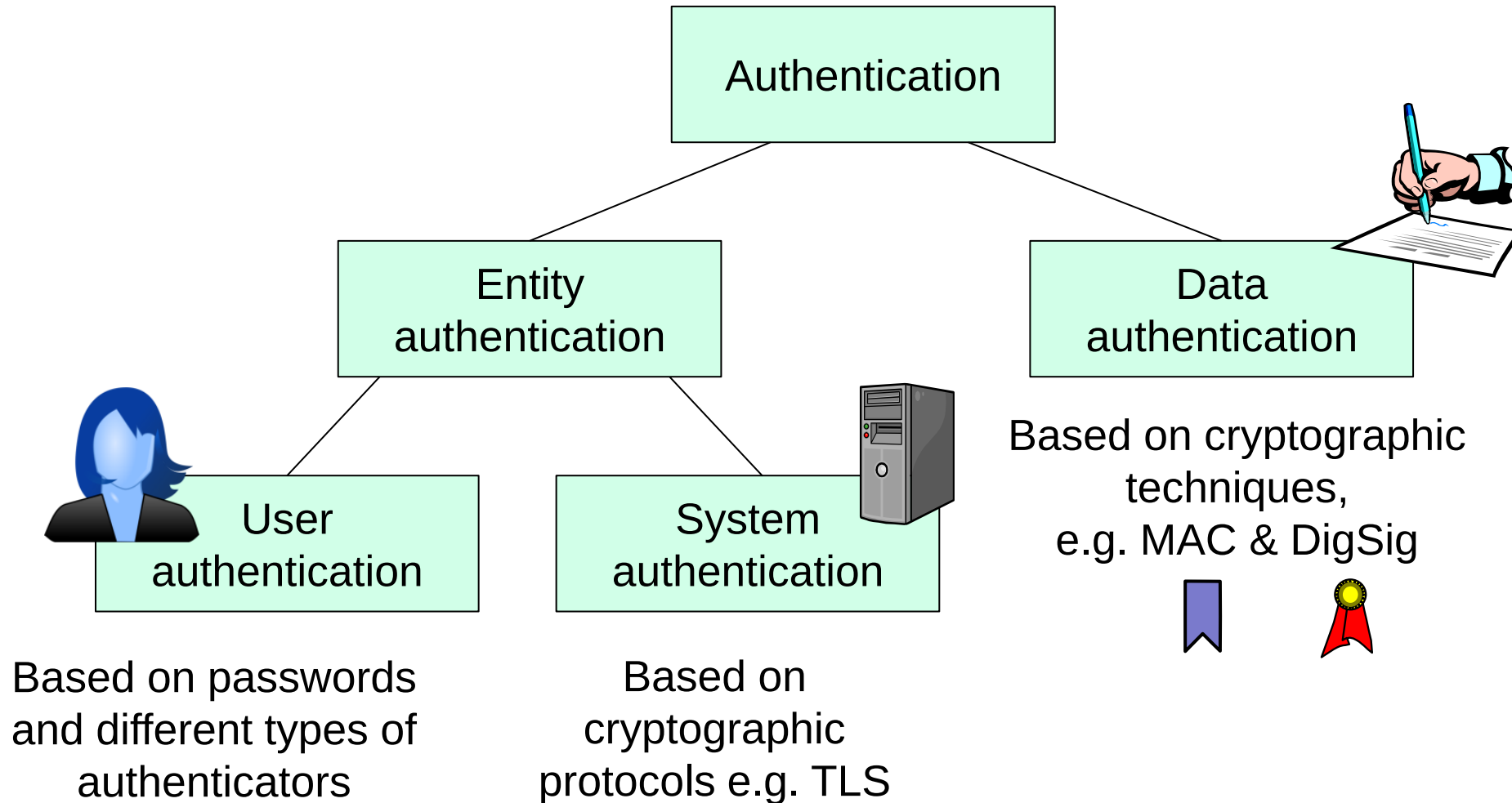


# Availability

- The property of being accessible and usable on demand by an authorized entity. (ISO/IEC 27000)
- Threats:
  - Denial of service, denial-of-service (DoS/DDoS) attacks
  - Ransomware
  - Delay of time-critical functions.
- Security control examples:
  - Redundancy of resources,
  - Failover configuration
  - Firewalls
  - Backup
  - Incident response and preparedness



# Types of authentication

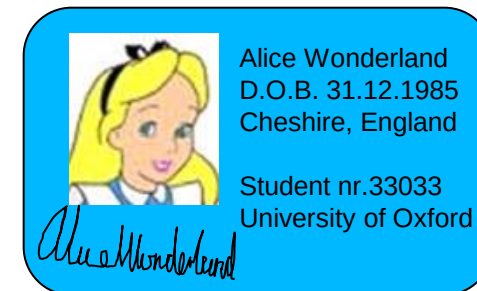


# User authentication

- Present user ID (self-identification)
  - User states (claims to have) a specific identity
- Authentication with Authenticator(s)
  - Prove that you have the identity you claim to have
  - Present authenticator(s)
- Threat: Identity theft, fake login
- Security controls: Authenticators, e.g.:
  - Password
  - Authentication app,
  - Authentication device, OTP generator
  - ID card
  - Biometrics
  - Secondary channels
  - 2FA, multi-factor authentication

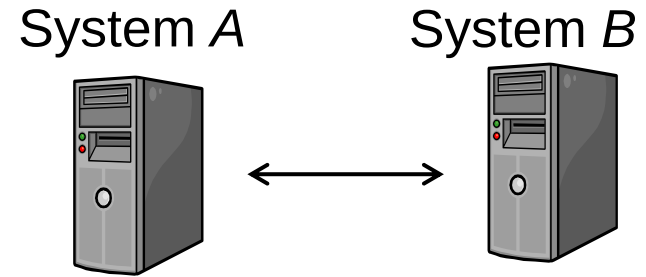


Present user ID



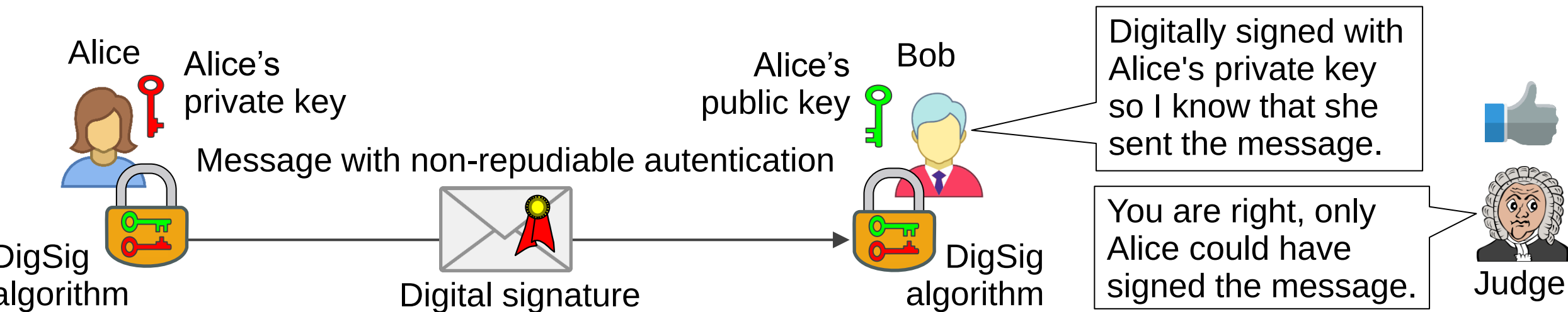
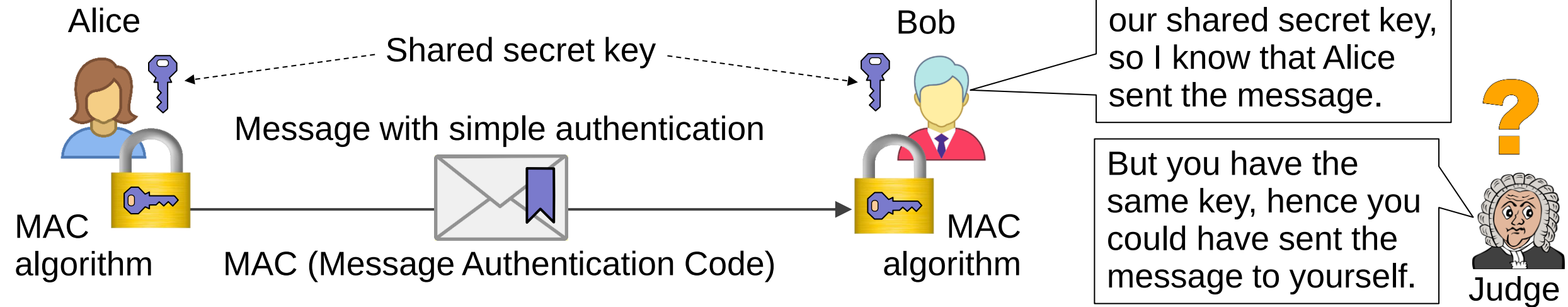
Present authenticator

# System Authentication



- Purpose
  - Correct identification of systems through networks
- Threats:
  - Fake systems
  - Fraudulent transactions
  - Man-in-the-middle attack
  - Network intrusion
- Security controls:
  - Cryptographic protocols for authentication and integrity
  - For example: TLS, IPSEC

# Simple or non-repudiable data authentication



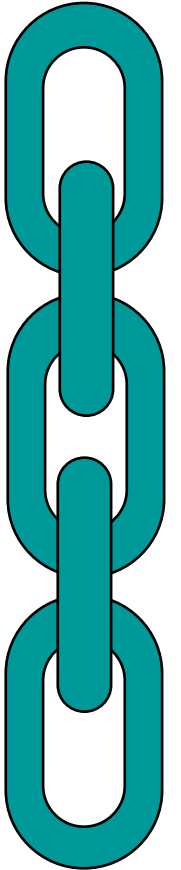
# Accountability

- Purpose: To be able to track events and actions of specific users and entities, so that they must be accountable for their actions.
  - *Systems that are used to process or handle classified or other sensitive information must assure individual accountability.* (TCSEC/Orange Book)
- Threats:
  - Not being able to identify who was behind an action
  - Lacking sufficient evidence to be able to make a report
- Security controls:
  - Authentication of all users
  - Logging of system events
  - Electronic evidence
  - Non-repudiation with digital signatures
  - Digital forensics



# Reliability

- The property that systems do not contain (many) errors or weaknesses. If failures do occur, reliability also means that the systems can tolerate certain failures without (all) functionality dropping out.
- Focuses mostly on preventing non-intended incidents, but is also important for preventing or reducing the consequences of intended adversarial events.
- Threats:
  - Low quality in the development, configuration, error correction and operation of systems and especially a lack of attention to secure system development.
- Controls:
  - Good (or best) practices for the secure development and operation of systems, also known as "built-in information security"



# Access Authorization



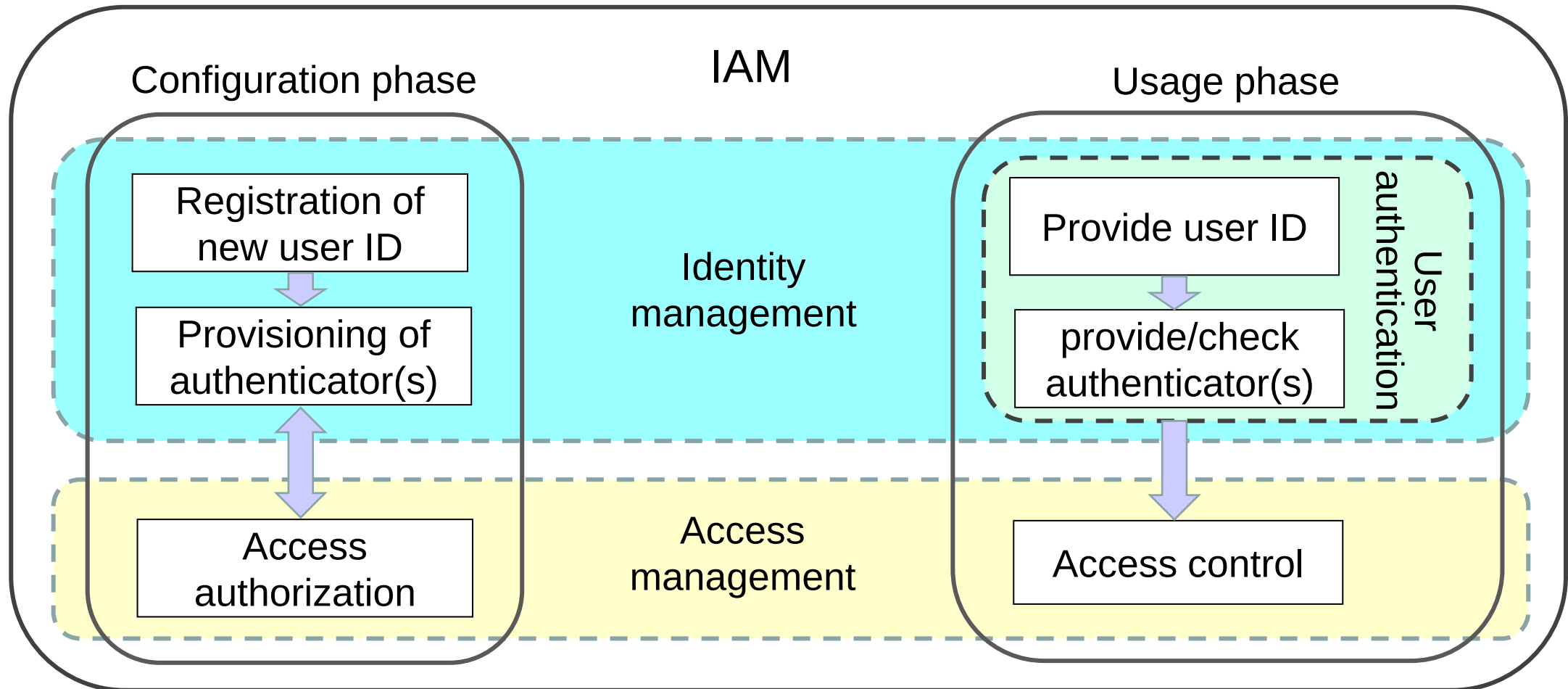
- Access authorization is to specify access rights for entities, i.e., for users, roles, and processes
  - Specifies who should have access to what
  - The authorization policy is usually defined by humans
  - The authorization policy is formalized as rules and configurations for access control in systems.
- Authorization can be delegated
  - Manager → Sys.Admin → User
- Be aware of confusion in literature and many textbooks (but not this textbook):
  - In some text sources, access authorization is defined as equivalent to access control. This is completely wrong, because it makes the definition of confidentiality meaningless, in the sense that it would not be a breach of confidentiality if a hacker accesses an account with a cracked password and steals data.
  - It would make the US CFAA (Computer Fraud and Abuse Act) meaningless (see Sect. 17.3.1).

# Access control



- Access control takes place after the user is authenticated.
- The user/entity must be authenticated for the system to know who is trying to perform an action or requesting access.
- Access Control uses authorization policies/rules to decide whether or not to grant the user access to resources.
- Access authorization policies/rules are defined during the configuration phase so that access control can be performed during the usage phase.
- Many different ways to define access control rules, e.g.
  - Identity-based (DAC)
  - Brand-based (MAC)
  - Role-based (RBAC)
  - Attribute-based (ABAC) (generalization of all the above ways)

# IAM (Identity and Access Management)



End of presentation

