Aalto-yliopisto
Aalto-universitetet
Aalto University

Cybersecurity Management

Managing and developing cyber capabilities

Lecture 1: Frameworks Overview for Cybersecurity Management

Part-III

ISO/IEC 27001, CIS security & Other Frameworks

Euroopan unionin rahoittama – NextGenerationEU

Rahoittaja
Jatkuvan oppimisen ja työllisyyden palvelukeskus

Outline: Lecture 1

- Lecture 1 is divided in three parts:
  - Part I: Introduction to Cybersecurity Management Frameworks
  - Part II: NIST Cybersecurity Framework
  - **Part III: ISO/IEC 27001, CIS security & Other Frameworks**
  - **ISO/IEC-20071**
    - **Overview**
    - **Clauses:** *PLAN, DO, CHECK, & ACT*
    - **Security controls**
    - **Benefits**
  - **CIS security controls**
    - **Overview**
    - **Benefits**
  - **COBIT & PCI-DSS: Overview**
  - **Selecting a cybersecurity framework**

ISO/IEC 27001

Introduction

ISO/IEC 20071: Introduction

- Belongs to the family of ISO 27000 series (Information security management).
- Among widely used security practices/standards for information security management systems (ISMS).
- A systematic framework for establishing, implementing, maintaining, and continually improving an organization's ISMS.
- ISO/IEC 27001 helps organizations built an adaptable information security management system and risk management process tailored to their size and needs.
- Help organization preserve the confidentiality, integrity, and availability of information.
- ISO/IEC 27001 helps organizations become risk-aware and proactively identify and address cybersecurity related weaknesses.

A!

Source: https://www.iso.org/standard/27001
Source: https://27001store.com/iso-iec-27001-2022-requirements/

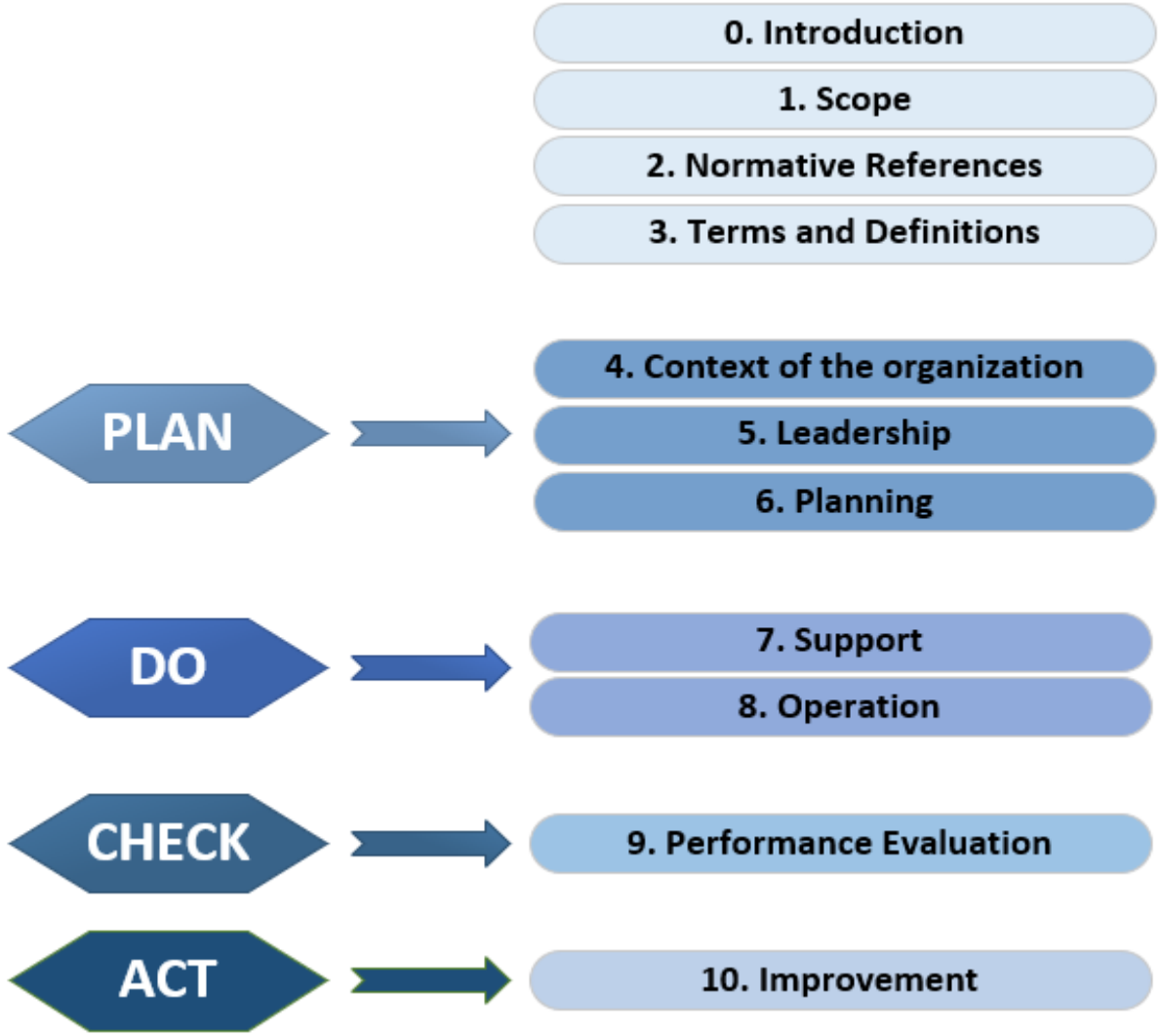
ISO/IEC 27001

Clauses

ISO/IEC 27001: Clauses

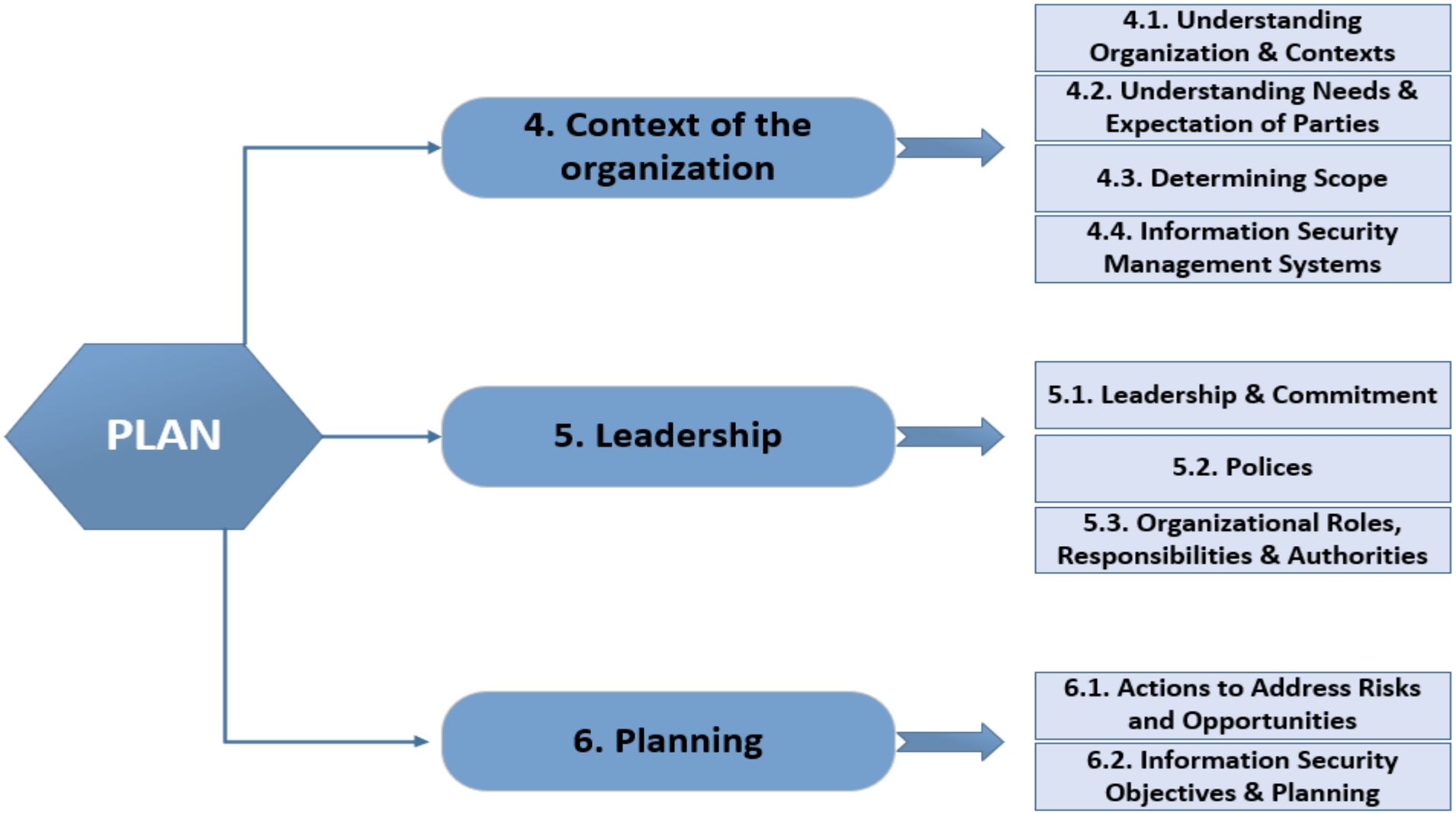
ISO 27001 Standard contains 11 clauses numbered 0-10 and security controls (Annex A)

Clauses 4-10 are the compulsory requirements that organizations are unable to avoid.



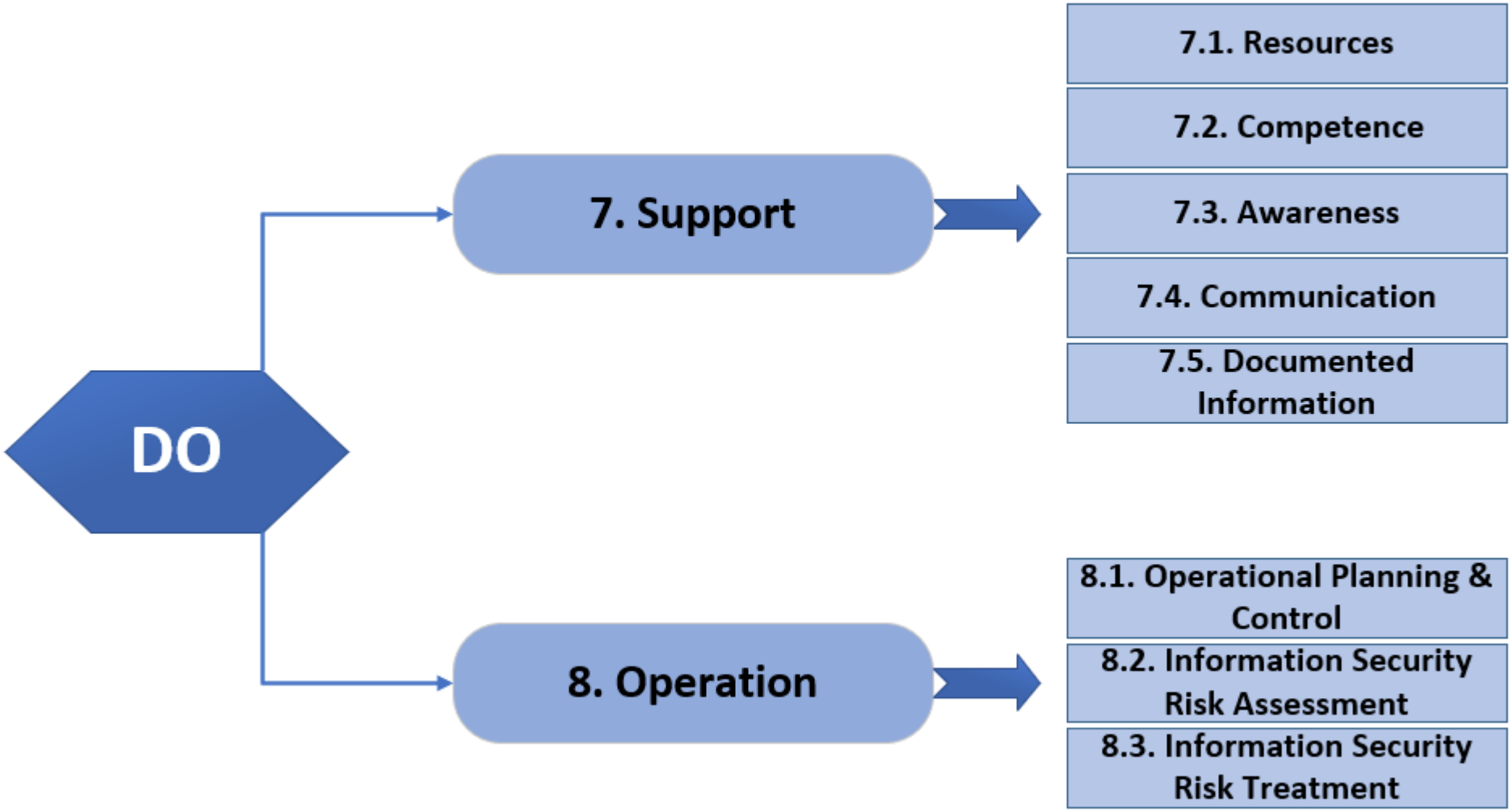
Source: https://www.iso.org/standard/27001
Source: https://27001store.com/iso-iec-27001-2022-requirements/
Source: https://www.iso27001security.com/html/27001.html

ISO/IEC 27001: Clauses: *PLAN*



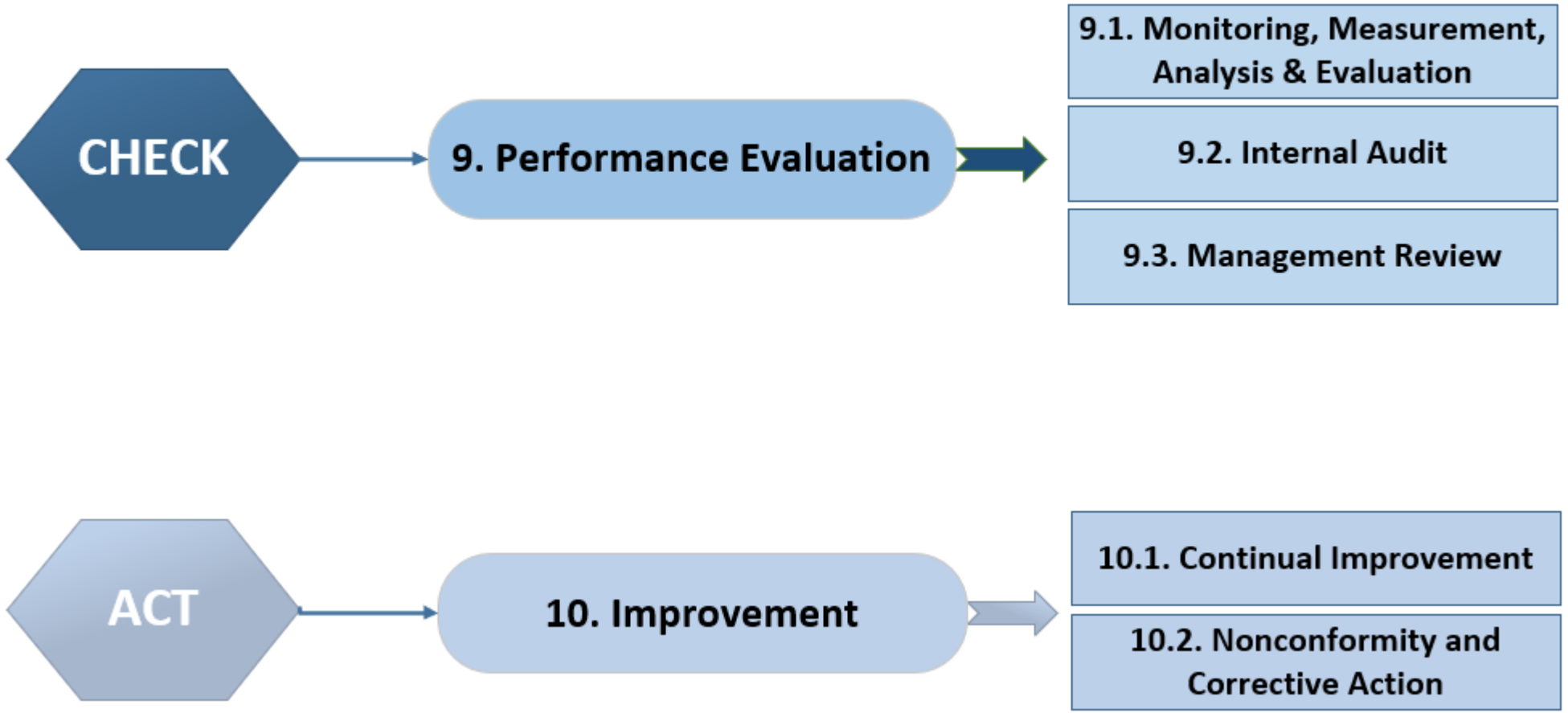
Source: https://www.iso.org/standard/27001
Source: https://27001store.com/iso-iec-27001-2022-requirements/

ISO/IEC 27001: Clauses: *DO*



Source: https://www.iso.org/standard/27001
Source: https://27001store.com/iso-iec-27001-2022-requirements/

ISO/IEC 27001: Clauses: *CHECK & ACT*



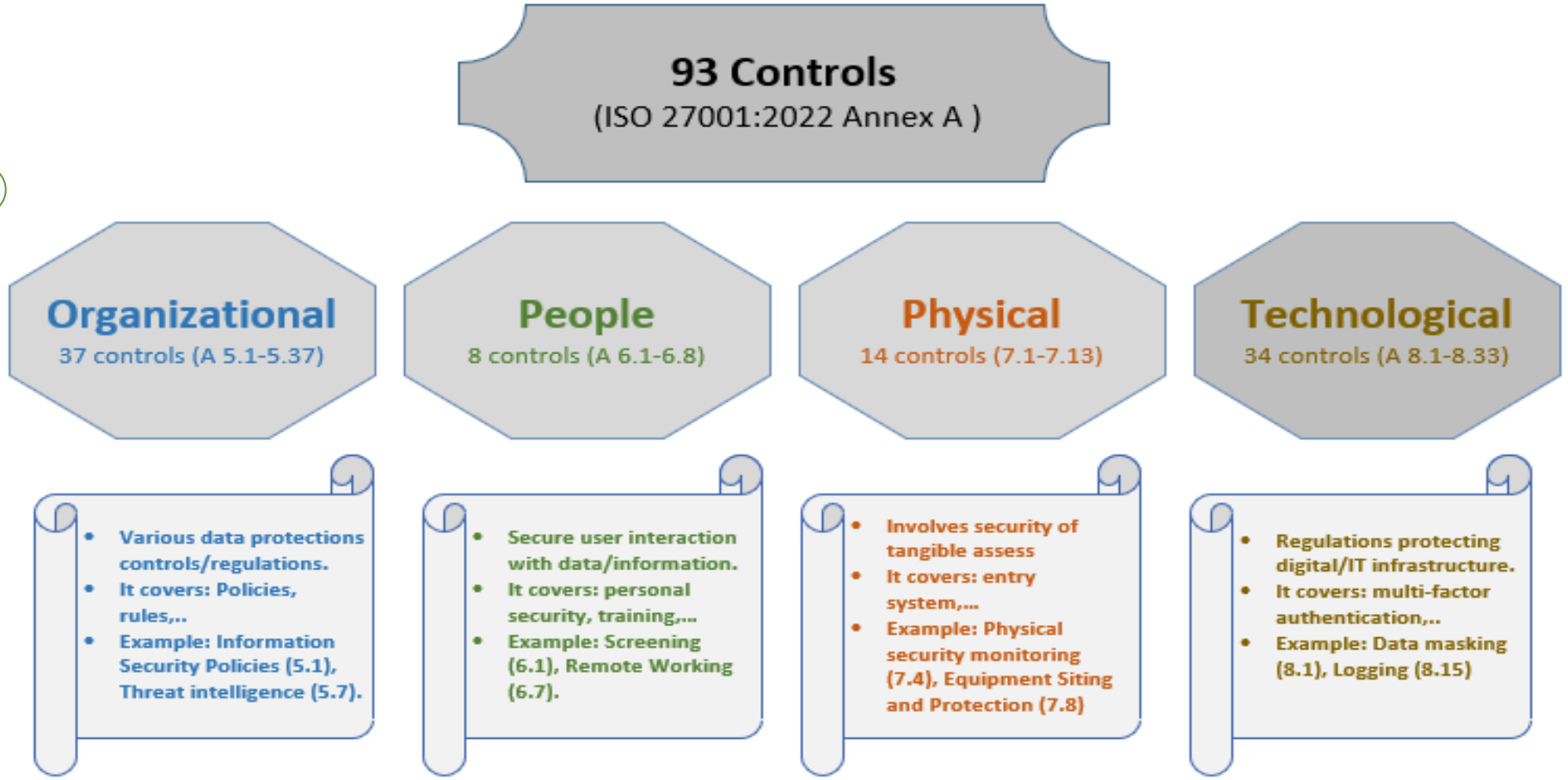
Source: https://www.iso.org/standard/27001
Source: https://27001store.com/iso-iec-27001-2022-requirements/

ISO/IEC 27001

Security Controls (Annex A)

ISO/IEC 27001: Security Controls

Information security controls in Annex A are the procedures and policies implemented to reduce risk.



Source: https://www.douglasthornton.co.uk/wp-content/uploads/2019/11/DTC_Iso-27001-Controls-list-.pdf

ISO/IEC 27001

Benefits

ISO/IEC 27001: Benefits

- Resilience to cyber-attacks.
- Ensure CIA.
- Risk management/mitigation
- Regulatory Compliance
- Preparedness for emerging cybersecurity threats.
- Avoid financial loss and reputation damage
- Increased customer trust
- Overall reduce costs

Source: https://www.iso.org/standard/27001

CIS Security Controls

Introduction

CIS Security Controls: Introduction

- Recently, Center for Internet Security (CIS) published 8th version (v8.1) of their 18 key Critical Security Controls (CSC).
- Main objective is to help organizations to build cybersecurity measures using the best practices and can efficiently utilize the resources to the most critical activities.
- The CIS Controls consist of a list of the prioritized security measures where organization can counter various cyber-attacks on systems and networks.
- These controls are well-aligned/mapped with the industry regulations and other standardization (NIST, HIPAA, PCI DSS)

  These controls are also drafted based on real-life cybersecurity incidents and with the discussion/consensus of experts.

Source: https://www.cisecurity.org/controls

CIS Security Controls

Overview

CIS Security Controls: Overview

Source: https://www.cisecurity.org/controls/cis-controls-list
Source: https://www.impactmybiz.com/blog/cisv8-critical-security-controls/

CIS Security Controls

Benefits

CIS Security Controls: Benefits

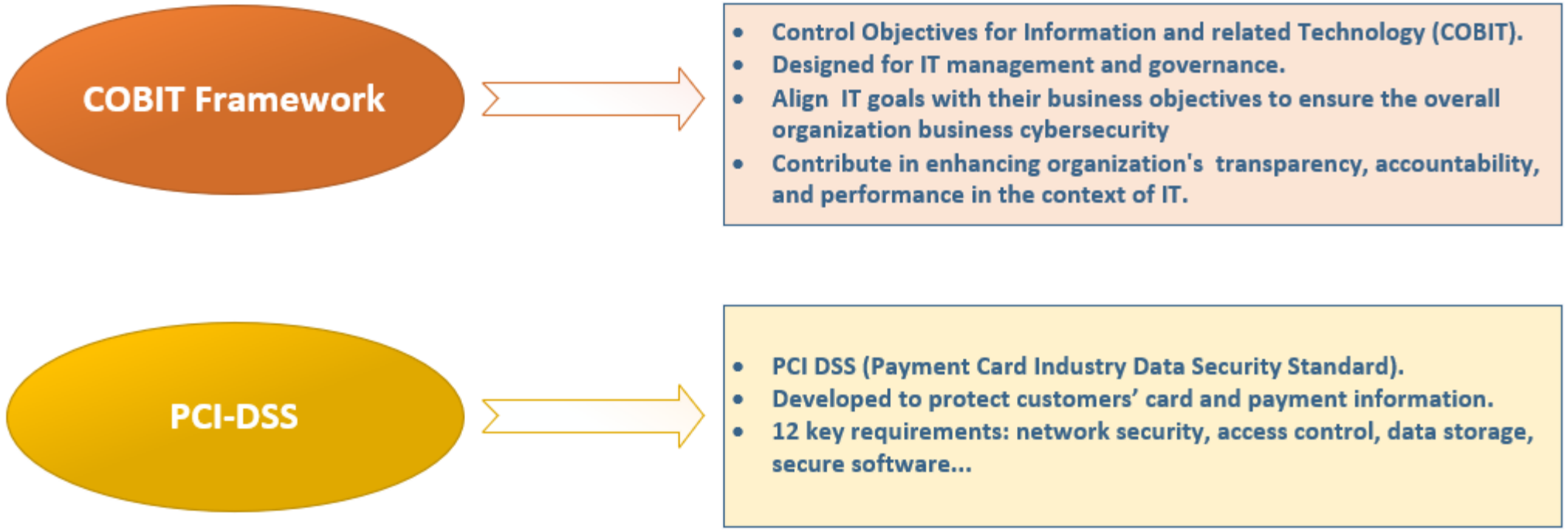
- Prioritized security measures
- Optimization of resources.
- Scalability
- Compliance with security standards and regulations.
- Comprehensive coverage
- Increased customer trust and reputation.

Source: https://www.cisecurity.org/controls

COBIT & PCI DSS

Overview

Further few Frameworks.. COBIT & PCI-DSS: Overview



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

Source: https://listings.pcisecuritystandards.org/documents/PCI_DSS-QRG-v3_2_1.pdf

Selecting a Cybersecurity Framework

Selecting a Cybersecurity Framework

- Choosing a cybersecurity framework is ***not a one-size-fits-all solution***.
- Many **factors** need to consider:
  - Industry or regulatory requirements
  - Alignment with specific security needs/scope of the organization.
  - Flexibility, customization, and maturity of the framework
  - Scalability
  - Support and community
  - Resources and skills
  - Cost and Sustainability

Kiitos
aalto.fi