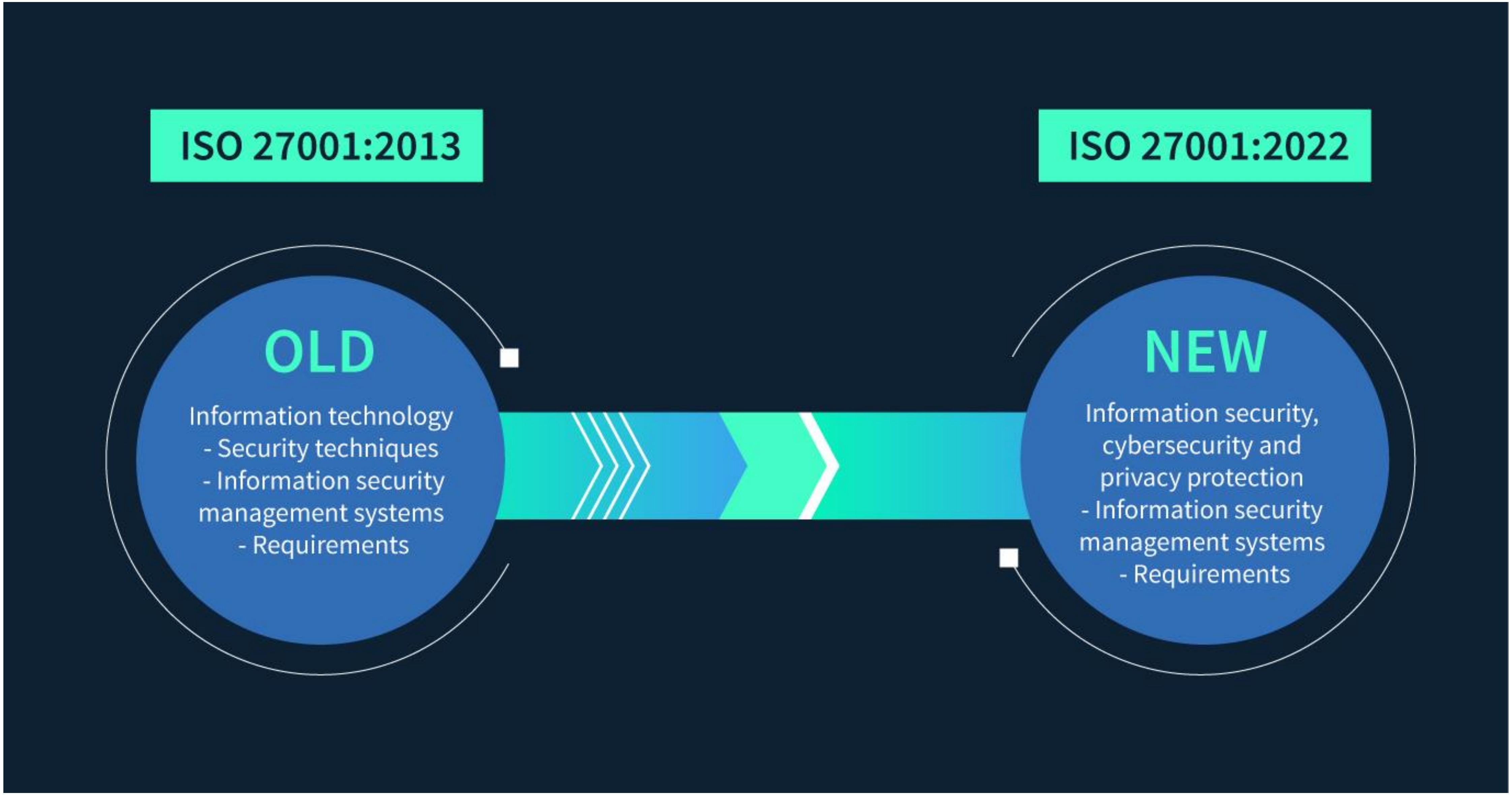
Wissen Baum

Key Changes:
Upgrading for ISO 27001:2013 to ISO 27001:2022

Key Changes : 27001:2013 to ISO 27001:2022



ISO 27001:2013

OLD

Information technology - Security techniques - Information security management systems - Requirements

ISO 27001:2022

NEW

Information security, cybersecurity and privacy protection - Information security management systems - Requirements

Key Changes : 27001:2013 to ISO 27001:2022

ISO 27001:2013

1. Name

Information technology — Security techniques — Information security management systems — Requirements

2. New terminology databases

Terms and conditions

- For the purposes of this document, the terms and definitions given in ISO/IEC 27000 apply

ISO 27001:2022

1. Name

Information security, cybersecurity and privacy protection — Information security management systems — Requirements

2. New terminology databases

Terms and conditions

- For the purposes of this document, the terms and definitions given in ISO/IEC 27000 apply.
- ISO and IEC maintain terminology databases for use in standardization at the following addresses:
- — ISO Online browsing platform: available at https://www.iso.org/obp
- — IEC Electropedia: available at https://www.electropedia.org

Key Changes : 27001:2013 to ISO 27001:2022

ISO 27001:2013

4.2 Understanding the needs and expectations of interested parties

The organization shall determine:

a) interested parties that are relevant to the information security management system

b) The requirements of these interested parties relevant to information security

4.4 Information Security Management System

The organization shall establish, implement, maintain and continually improve an information security management system, in accordance with the requirements of this International Standard.

ISO 27001:2022

4.2 Understanding the needs and expectations of interested parties

The organization shall determine:

a) Interested parties that are relevant to the information security management system

b) The relevant requirements of these interested parties;

c) Which of these requirements will be addressed through the information security management system.

4.4 Information Security Management System

The organization shall establish, implement, maintain and continually improve an information security management system, including the processes needed and their interactions, in accordance with the requirements of this document.

Key Changes : 27001:2013 to ISO 27001:2022

ISO 27001:2013

6.2 Information security objectives

The organization shall establish information security objectives at relevant functions and levels.

The information security objectives shall:

a) be consistent with the information security policy
b) be measurable (if practicable);
c) take into account applicable information security requirements, and results from risk assessment and risk treatment
d) be communicated
e) be updated as appropriate.

ISO 27001:2022

6.2 Information security objectives

The organization shall establish information security objectives at relevant functions and levels.

The information security objectives shall:

a) be consistent with the information security policy
b) be measurable (if practicable)
c) take into account applicable information security requirements, and results from risk assessment and risk treatment
d) be monitored
e) be communicated
f) be updated as appropriate
g) be available as documented information.

Key Changes : 27001:2013 to ISO 27001:2022

ISO 27001:2013

7.4 Communication

The organization shall determine the need for internal and external communications relevant to the information security management system including:

a) on what to communicate;
b) when to communicate;
c) with whom to communicate;
d) who shall communicate; and
e) the processes by which communication shall be effected

ISO 27001:2022

7.4 Communication

The organization shall determine the need for internal and external communications relevant to the information security management system including:

a) on what to communicate;
b) when to communicate;
c) with whom to communicate;
d) how to communicate.

Key Changes : 27001:2013 to ISO 27001:2022

ISO 27001:2013

8.1 Operational planning and control

The organization shall plan, implement and control the processes needed to meet information security requirements, and to implement the actions determined in 6.1. The organization shall also implement plans to achieve information security objectives determined in 6.2.

The organization shall keep documented information to the extent necessary to have confidence that the processes have been carried out as planned. The organization shall control planned changes and review the consequences of unintended changes, taking action to mitigate any adverse effects, as necessary.

The organization shall ensure that outsourced processes are determined and controlled.

ISO 27001:2022

8.1 Operational planning and control

The organization shall plan, implement and control the processes needed to meet requirements, and to implement the actions determined in Clause 6, by:

— establishing criteria for the processes;

— implementing control of the processes in accordance with the criteria.

Documented information shall be available to the extent necessary to have confidence that the processes have been carried out as planned. The organization shall control planned changes and review the consequences of unintended changes, taking action to mitigate any adverse effects, as necessary.

The organization shall ensure that externally provided processes, products or services that are relevant to the information security management system are controlled.

Key Changes : 27001:2013 to ISO 27001:2022

ISO 27001:2013

Structure of 9.2 and 9.3

- **9.2 Internal audit**
- **9.3 Management review**

Structure of 10 Improvement

- **10.1 Nonconformity and corrective action**
- **10.2 Continual improvement**

ISO 27001:2022

Structure of 9.2 and 9.3

- **9.2 Internal audit**
  - 9.2.1 General
  - 9.2.2 Internal audit programme
- **9.3 Management review**
  - 9.3.1 General
  - 9.3.2 Management review inputs
  - 9.3.3 Management review results

Structure of 10 Improvement

- **10.1 Continual improvement**
- **10.2 Nonconformity and corrective action**

Key Changes: Information security controls

ISO 27001:2013

1. Total number of controls – **114**

Domains:

A.5 Information security policies
A.6 Organisation of information security
A.7 Human resource security
A.8 Asset management
A.9 Access control
A.10 Cryptography
A.11 Physical and environmental security
A.12 Operations security
A.13 Communications security
A.14 System acquisition, development, and maintenance
A.15 Supplier relationships
A.16 Information security incident management
A.17 Information security aspects of business continuity management
A.18 Compliance

ISO 27001:2022

1. Total number of controls – **93**, (11 new)

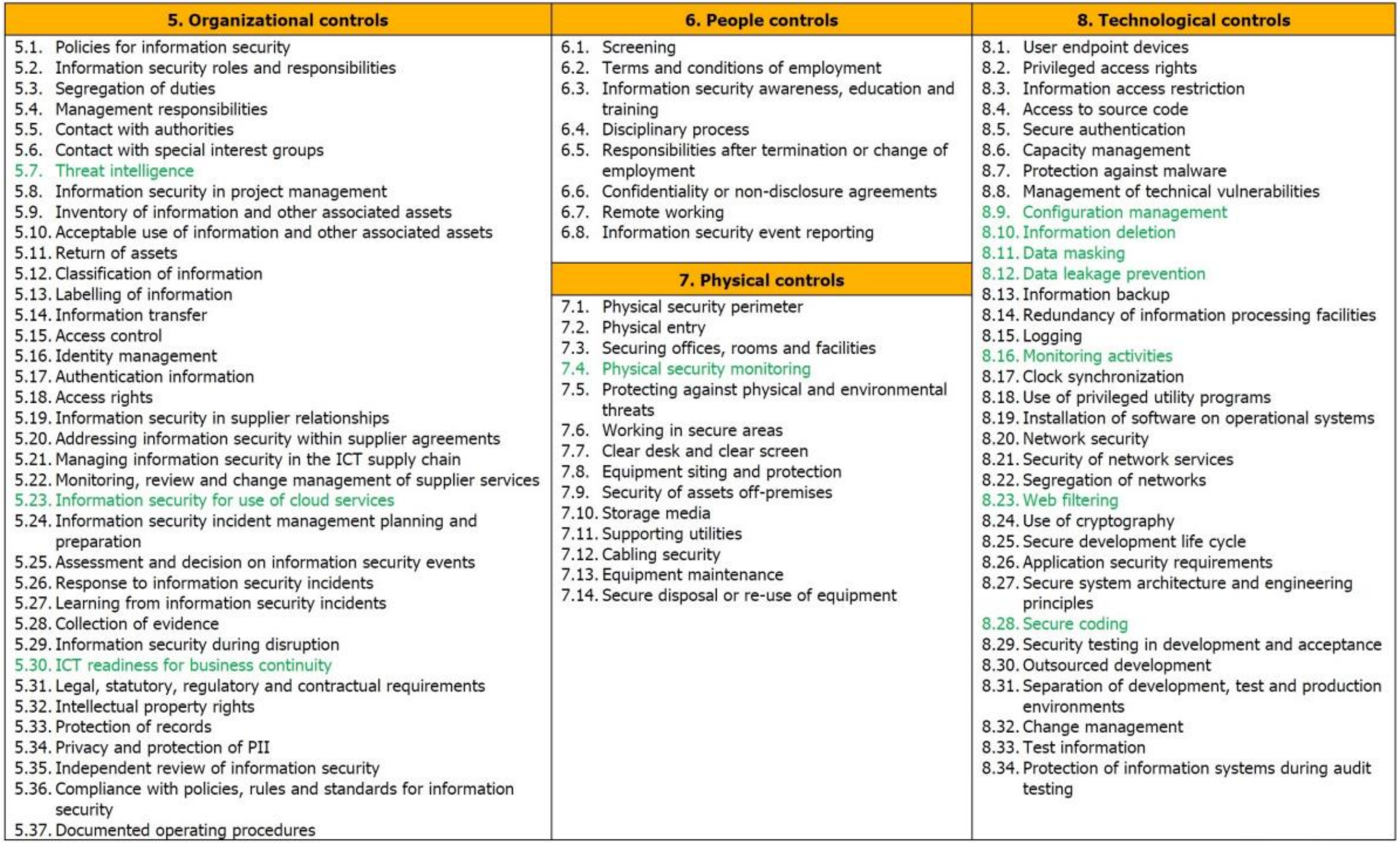
New control Addition in ISO 27001:2022

1. Threat Intelligence (A.5.7)
2. Information Security for Use of Cloud Services (A.5.23)
3. ICT Readiness for Business Continuity (A.5.30)
4. Physical Security Monitoring (A.7.4)
5. Configuration Management (A.8.9)
6. Information Deletion (A.8.10)
7. Data Masking (A.8.11)
8. Data Leakage Prevention (A.8.12)
9. Monitoring Activities (A.8.16)
10. Web Filtering (A.8.23)
11. Secure Coding (A.8.28)

Controls are categorized as:

1. **People**, if they concern individual people
2. **Physical**, if they concern physical objects
3. **Technological,** if they concern technology
4. **Organizational,** If they concern organization

Information Security ontrols : ISO 27001:2022



5. Organizational controls

- 5.1. Policies for information security
- 5.2. Information security roles and responsibilities
- 5.3. Segregation of duties
- 5.4. Management responsibilities
- 5.5. Contact with authorities
- 5.6. Contact with special interest groups
- 5.7. Threat intelligence
- 5.8. Information security in project management
- 5.9. Inventory of information and other associated assets
- 5.10. Acceptable use of information and other associated assets
- 5.11. Return of assets
- 5.12. Classification of information
- 5.13. Labelling of information
- 5.14. Information transfer
- 5.15. Access control
- 5.16. Identity management
- 5.17. Authentication information
- 5.18. Access rights
- 5.19. Information security in supplier relationships
- 5.20. Addressing information security within supplier agreements
- 5.21. Managing information security in the ICT supply chain
- 5.22. Monitoring, review and change management of supplier services
- 5.23. Information security for use of cloud services
- 5.24. Information security incident management planning and preparation
- 5.25. Assessment and decision on information security events
- 5.26. Response to information security incidents
- 5.27. Learning from information security incidents
- 5.28. Collection of evidence
- 5.29. Information security during disruption
- 5.30. ICT readiness for business continuity
- 5.31. Legal, statutory, regulatory and contractual requirements
- 5.32. Intellectual property rights
- 5.33. Protection of records
- 5.34. Privacy and protection of PII
- 5.35. Independent review of information security
- 5.36. Compliance with policies, rules and standards for information security
- 5.37. Documented operating procedures

6. People controls

- 6.1. Screening
- 6.2. Terms and conditions of employment
- 6.3. Information security awareness, education and training
- 6.4. Disciplinary process
- 6.5. Responsibilities after termination or change of employment
- 6.6. Confidentiality or non-disclosure agreements
- 6.7. Remote working
- 6.8. Information security event reporting

7. Physical controls

- 7.1. Physical security perimeter
- 7.2. Physical entry
- 7.3. Securing offices, rooms and facilities
- 7.4. Physical security monitoring
- 7.5. Protecting against physical and environmental threats
- 7.6. Working in secure areas
- 7.7. Clear desk and clear screen
- 7.8. Equipment siting and protection
- 7.9. Security of assets off-premises
- 7.10. Storage media
- 7.11. Supporting utilities
- 7.12. Cabling security
- 7.13. Equipment maintenance
- 7.14. Secure disposal or re-use of equipment

8. Technological controls

- 8.1. User endpoint devices
- 8.2. Privileged access rights
- 8.3. Information access restriction
- 8.4. Access to source code
- 8.5. Secure authentication
- 8.6. Capacity management
- 8.7. Protection against malware
- 8.8. Management of technical vulnerabilities
- 8.9. Configuration management
- 8.10. Information deletion
- 8.11. Data masking
- 8.12. Data leakage prevention
- 8.13. Information backup
- 8.14. Redundancy of information processing facilities
- 8.15. Logging
- 8.16. Monitoring activities
- 8.17. Clock synchronization
- 8.18. Use of privileged utility programs
- 8.19. Installation of software on operational systems
- 8.20. Network security
- 8.21. Security of network services
- 8.22. Segregation of networks
- 8.23. Web filtering
- 8.24. Use of cryptography
- 8.25. Secure development life cycle
- 8.26. Application security requirements
- 8.27. Secure system architecture and engineering principles
- 8.28. Secure coding
- 8.29. Security testing in development and acceptance
- 8.30. Outsourced development
- 8.31. Separation of development, test and production environments
- 8.32. Change management
- 8.33. Test information
- 8.34. Protection of information systems during audit testing

Thank You

Team Wissen Baum