malean

ISO 27001 / 27002 Normrevision 2022

Änderungen von Version 2013 zu 2022

malean.org

DARÜBER SPRECHEN WIR HEUTE

AGENDA

1. ISO/IEC 27001 Normteil
2. ISO/IEC 27001 Anhang A & ISO/IEC 27002
3. Control Layout
4. Attribute
5. Auditplanung und Nutzung von Attributen
6. Die 11 neuen Kontrollen
7. Auswirkungen

DAS LERNEN WIR HEUTE

LERNZIELE

- ✓ Die Änderungen an ISO/IEC 27001:2022 gegenüber Version 2013 kennen
- ✓ Die neue Struktur der Kontrollen verstehen (Anhang A bzw. ISO/IEC 27002:2022)
- ✓ Den Nutzen der Attribute von Kontrollen erkennen
- ✓ Den Inhalt der neuen Kontrollen kennen
- ✓ Die Auswirkungen der Normänderung auf zertifizierte Unternehmen verstehen

malean

WER WIR SIND

KOMPETENT. KREATIV. MENSCHLICH.

Sandra Thurnheer, Gründerin und Geschäftsführerin

Mit umfassendem Know-how, exzellenter Methodenkompetenz und rund 15-jähriger Berufserfahrung unterstützt Sandra Thurnheer Ihr Unternehmen als Beraterin und Coach bei der Erfüllung Ihrer Sicherheitsanforderungen. Sandra Thurnheer hat in Zürich und Rotterdam studiert und einen Masterabschluss in Betriebswirtschaft. Gemeinsam mit ihrem Team bringt sie einen kontinuierlichen Optimierungsprozess in Ihrem Unternehmen in Gang und sichert gemeinsam mit Ihnen dessen Zukunftsfähigkeit. Das alles macht sie mit Charme, Empathie und Sinn für Humor.

+41 76 321 39 40

sandra.thurnheer@malean.org

UNSER ANGEBOT

Damit Sie sich ganz Ihren Kernaufgaben widmen können, stehen wir als Team von Expertinnen und Experten mit Kompetenz und Leidenschaft an Ihrer Seite. Wir beraten Sie in den Bereichen Informationssicherheit, Service Management und Datenschutz. Wir begleiten Sie ausserdem auf dem Weg zu einer international anerkannten Zertifizierung nach den entsprechenden ISO-Normen. Und Sie können sich ganz auf Ihre Unternehmensziele konzentrieren und so die Innovationsfähigkeit stärken.

UNSERE DISZIPLINEN

INFORMATIONSSICHERHEIT

Wir helfen Ihnen, die Informationen Ihres Unternehmens zu sichern und den Umgang mit vertraulichen Informationen und Daten angemessen zu schützen. Gerne zeigen wir Ihnen Ihnen Konzepte und Techniken auf, die Best Practice sind.

- ISO 27001:2013
- ISO 27017:2015
- ISO 27018:2019
- ISO 27001:2022

SERVICE MANAGEMENT

Wir helfen Ihrem Unternehmen dabei, die wertvollen Gedanken aus den Service-Management-Ansätzen nach ITIL oder der ISO 20000-1-Norm umzusetzen. Dabei steht für uns der betriebswirtschaftliche Nutzen dieser Practices im Vordergrund.

- ITIL UND ISO 20000-1:2018

DATENSCHUTZ

Wir helfen Ihnen, die Rollen und die damit verbundenen Pflichten Ihres Unternehmens als Datenverarbeiter oder datenverantwortliche Stelle zu erfüllen.

- VDSZ
- ISO 27701:2019
- GoodPriv@cy

malean

ISO/IEC 27001 NORMTEIL

Änderungen ISO/IEC 27001:2013 → 2022

neu

geändert

GENERELLE ÄNDERUNGEN

- Das Wort **“may”** wurde durch **“can”** ersetzt.
- Die Erwähnung des **“international Standard”** wurde durch **“this document”** ersetzt.

Änderungen ISO/IEC 27001:2013 → 2022

neu

geändert

ÄNDERUNGEN IN KAPITEL 4

4.1 Understanding the organization and its context

The organization shall determine external and internal issues that are relevant to its purpose and that affect its ability to achieve the intended outcome(s) of its information security management system.

NOTE Determining these issues refers to establishing the external and internal context of the organization considered in **Clause 5.4.1 of ISO 31000:2018.**

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;

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 process needed and their interactions, in accordance with the requirements of this document.**

Änderungen ISO/IEC 27001:2013 → 2022

neu

geändert

ÄNDERUNGEN IN KAPITEL 6

6.1.3 Information security risk treatment

The organization shall define and apply an information security risk treatment process to:

a) select appropriate information security risk treatment options, taking account of the risk assessment results;

b) determine all controls that are necessary to implement the information security risk treatment option(s) chosen;

NOTE 1 Organizations can design controls as required, or identify them from any source

c) compare the controls determined in 6.1.3 b) above with these in Annex A and verify that no necessary controls have been omitted;

NOTE 2 Annex A contains a list of possible information security controls. Users of this document are directed to Annex A to ensure that no necessary information security controls are overlooked.

NOTE 3 The information security controls listed in Annex A are not exhaustive and additional information security controls can be included if needed.

6.2 Information security objectives and planning to achieve them

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

The information security objectives shall:

a) be consistent with the information security policy;

b) be measursable (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.

6.3 Planning of changes

When the organization determines the need for changes to the information security management system, the changes shall be carried out in a planned manner.

Änderungen ISO/IEC 27001:2013 → 2022

neu

geändert

ÄNDERUNGEN IN KAPITEL 7

7.4 Communication

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

a) on what to communicate;

b) when to communicate;

c) with whom to communicate;

d) how to communicate.

Änderungen ISO/IEC 27001:2013 → 2022

neu

geändert

ÄNDERUNGEN IN KAPITEL 8

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:

a) establishing criteria for the processes;

b) 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.

Änderungen ISO/IEC 27001:2013 → 2022

neu

geändert

ÄNDERUNGEN IN KAPITEL 9 (I)

9.1 Monitoring, measurement, analysis and evaluation

The organization shall determine:

a) what needs to be monitored and measured, including information security processes and controls;

b) the methods for monitoring, measurement, analysis and evaluation, as applicable, to ensure valid results. The methods selected should produce comparable and reproducible results to be considered valid;

c) when the monitoring and measuring shall be performed;

d) who shall monitor and measure;

e) when the results from monitoring and measurement shall be analysed and evaluated;

f) who shall analyse and evaluate these results.

Documented information shall be available as evidence of the results.

The organization shall evaluate the information security performance and effectiveness of the information security management system.

9.2 Internal Audit

9.2.1 General

The organization shall conduct internal audits at planned intervals to provide information on whether the information security management system:

a) Conforms to

1) the organization's own requirements for its information security management system;

2) the requirements of this document;

b) is effectively implemented and maintained.

9.2.2 Internal audit programme

The organization shall plan, establish, implement and maintain an audit programme(s), including the frequency, method, responsibilities, planning requirements and reporting.

When establishing the internal audit programme(s), the organization shall consider the importance of the processes concerned and the results of previous audits.

Änderungen ISO/IEC 27001:2013 → 2022

neu

geändert

ÄNDERUNGEN IN KAPITEL 9 (II)

The organization shall:

a) define the audit criteria and scope for each audit;

b) select auditors and conduct audits that ensure objectivity and the impartiality of the audit process;

c) ensure that the results of the audits are reported to relevant management;

Documented information shall be available as evidence of the implementation of the audit programme(s) and the audit results.

9.3 Management review

9.3.1 General

Top management shall review the organization's information security management system at planned intervals to ensure its continuing suitability, adequacy and effectiveness.

9.3.2 Management review inputs

The management review shall include consideration of:

a) the status of actions from previous management reviews;

b) changes in external and internal issues that are relevant to the information security management system;

c) changes in needs and expectations of interested parties that are relevant to the information security management system;

d) feedback on the information security performance, including trends in:

1) nonconformities and corrective actions;

2) monitoring and measurement results;

3) audit results;

4) fulfilment of information security objectives;

Änderungen ISO/IEC 27001:2013 → 2022

neu

geändert

ÄNDERUNGEN IN KAPITEL 9 (III)

e) feedback from interested parties;

f) results of risk assessment and status of risk treatment plan;

g) opportunities for continual improvement.

9.3.3 Management review results

The results of the management review shall include decisions related to continual improvement opportunities and any needs for changes to the information security management system.

Documented information shall be available as evidence of the results of management reviews.

Änderungen ISO/IEC 27001:2013 → 2022

neu

geändert

ÄNDERUNGEN IN KAPITEL 10

10 Improvement

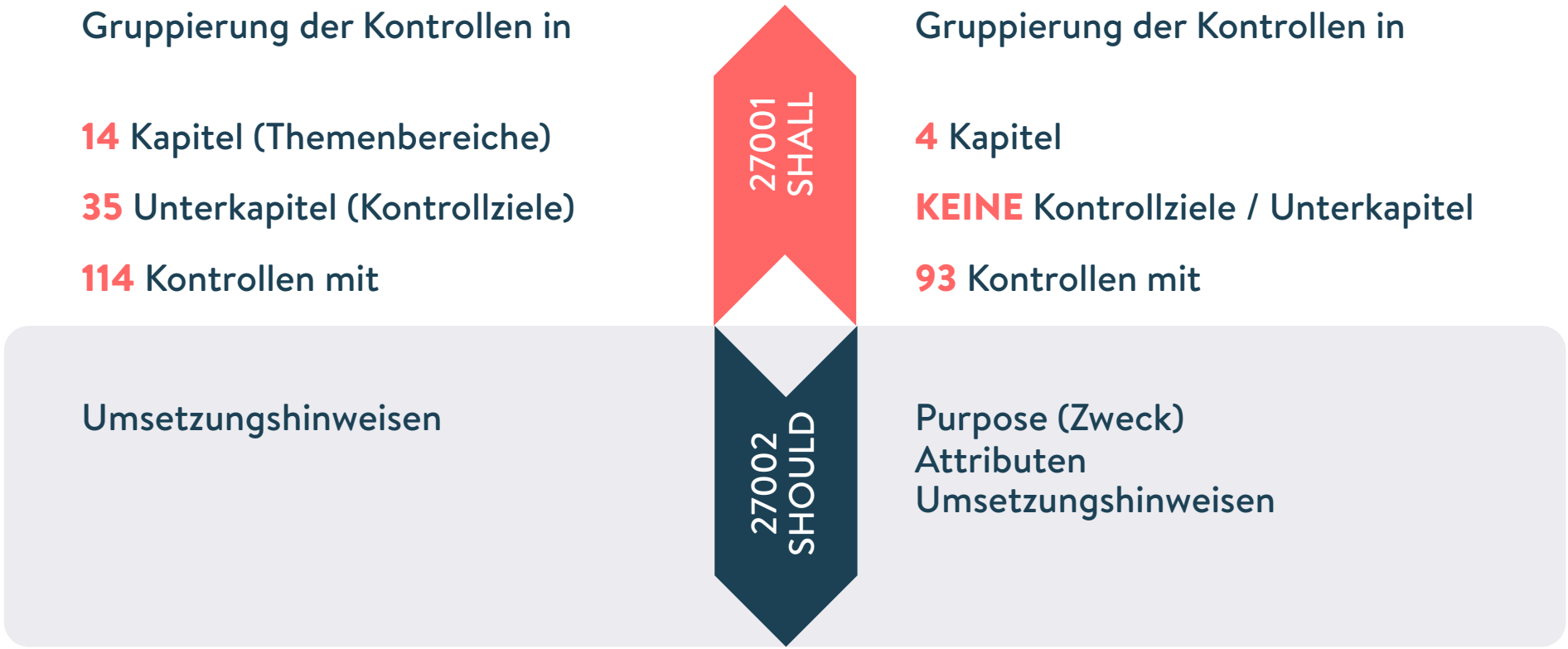
10.1 Continual improvement

The organization shall continually improve the suitability, adequacy and effectiveness of the information security management system.

malean

ISO/IEC 27001 Anhang A
ISO/IEC 27002

ISO/IEC 27001 Anhang A & ISO/IEC 27002



malean

CONTROL LAYOUT

27002:2022 | Layout der Kontrollen

Titel der Kontrolle

Atrribute und Werte

WAS ist zu tun?

WARUM ist es zu tun?

WIE soll es getan werden?

8.8 Management of technical vulnerabilities

Control type	Information security properties	Cybersecurity concepts	Operational capabilites	Security domains
#Preventitive	#Confidentiality #Integrity #Availability	#Identify #Protect	#Threat_and_ vulnerability_ management	#Governance_ and_Ecosystem #Proctection #Defence

Control
Information about technical vulnerabilites of information systems in use **should** be obtained, the organization‘s exposure to such vulnerabilites **should** be evaluated and appropriate measures **should** be taken.

Purpose
To prevent exploitation of technical vulnerabilites.

Guidance

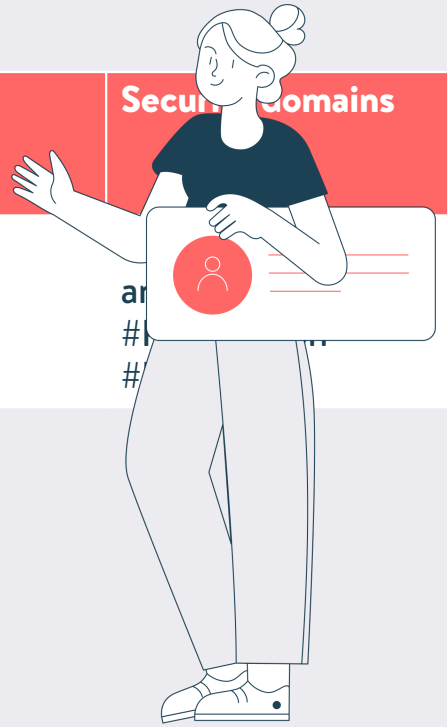
Identifying technical vulnerabilites
The organization **should** have an accurate inventory of assets (see 5.9 to 5.14) as a prerequisite for effective technical vulnerability management; the inventory **should** include the software vendor, software name, version numbers, current state of deployment (e.g. what software is installed on what systems) and the person(s) within the organization responsible for the software.

malean

ATTRIBUTE

27002:2022 | Attributstypen

Control type	Information security properties	Cybersecurity concepts	Operational capabilites	Secu domains
#Preventitive	#Confidentiality #Integrity #Availability	#Identify #Protect	#Threat_and_ vulnerability_ management	ar #I #I



27002:2022 | Attributstypen

Wann und wie wird ein Risiko durch die Kontrolle modifiziert, wenn ein Ereignis eintritt?

Control type	Information security properties	Cybersecurity concepts	Operational capabilites	Security domains
#Preventitive	#Confidentiality #Integrity #Availability	#Identify #Protect	#Threat_and_ vulnerability_ management	#Governance_ and_Ecosystem #Proctection #Defence

27002:2022 | Attributstypen

Wann und wie wird ein Risiko durch die Kontrolle modifiziert, wenn ein Ereignis eintritt?

Control type	Information security properties	Cybersecurity concepts	Operational capabilites	Security domains
#Preventitive	#Confidentiality #Integrity	#Identify #Protect	#Threat_and_ vulnerability_ management	#Governance_ and_Ecosystem #Proctection #Defence

Welches Merkmal der Information wird durch die Kontrolle bewahrt?

27002:2022 | Attributstypen

Wann und wie wird ein Risiko durch die Kontrolle modifiziert, wenn ein Ereignis eintritt?

Welcher Cybersecurity-Funktion sind welche Kontrollen zuzuordnen?

Control type	Information security properties	Cybersecurity concepts	Operational capabilites	Security domains
#Preventitive	#Confidentiality #Integrity	#Identify #Protect	#Threat_and_ vulnerability_ management	#Governance_ and_Ecosystem #Proctection #Defence

Welches Merkmal der Information wird durch die Kontrolle bewahrt?

27002:2022 | Attributstypen

Wann und wie wird ein Risiko durch die Kontrolle modifiziert, wenn ein Ereignis eintritt?

Welcher Cybersecurity-Funktion sind welche Kontrollen zuzuordnen?

Control type	Information security properties	Cybersecurity concepts	Operational capabilites	Security domains
#Preventitive	#Confidentiality #Integrity	#Identify #Protect	#Threat_and_ vulnerability_	#Governance_ and_Ecosystem #Proctection #Defence

Welches Merkmal der Information wird durch die Kontrolle bewahrt?

Welchen praktischen, operationellen Fähigkeiten sind welche Kontrollen zuzuordnen?

27002:2022 | Attributstypen

Wann und wie wird ein Risiko durch die Kontrolle modifiziert, wenn ein Ereignis eintritt?

Welcher Cybersecurity-Funktion sind welche Kontrollen zuzuordnen?

Welcher Sicherheitsdomäne sind welche Kontrollen zuzuordnen?

Control type	Information security properties	Cybersecurity concepts	Operational capabilites	Security domains
#Preventitive	#Confidentiality #Integrity	#Identify #Protect	#Threat_and_ vulnerability_	#Governance_ and_Ecosystem #Proctection #Defence

Welches Merkmal der Information wird durch die Kontrolle bewahrt?

Welchen praktischen, operationellen Fähigkeiten sind welche Kontrollen zuzuordnen?

27002:2022 | Attributstypen

Wann und wie wird ein Risiko durch die Kontrolle modifiziert, wenn ein Ereignis eintritt?

Welcher Cybersecurity-Funktion sind welche Kontrollen zuzuordnen?

Welcher Sicherheitsdomäne sind welche Kontrollen zuzuordnen?

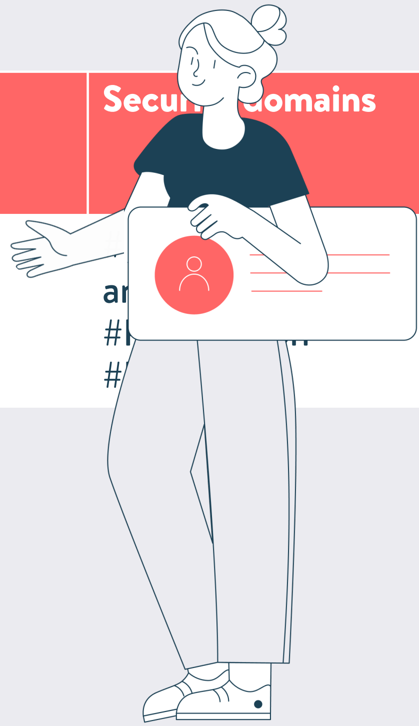
Control type	Information security properties	Cybersecurity concepts	Operational capabilites	Security domains
#Preventitive	#Confidentiality #Integrity	#Identify #Protect	#Threat_and_ vulnerability_	#Governance_ and_Ecosystem #Proctection #Defence

Welches Merkmal der Information wird durch die Kontrolle bewahrt?

Welchen praktischen, operationellen Fähigkeiten sind welche Kontrollen zuzuordnen?

27002:2022 | Attribute und deren Werte

Control type	Information security properties	Cybersecurity concepts	Operational capabilites	Secu domains
#Preventitive	#Confidentiality #Integrity #Availability	#Identify #Protect	#Threat_and_ vulnerability_ management	# ar # #



27002:2022 | Attribute und deren Werte

#Preventitive
#Detective
#Corrective

Control type	Information security properties	Cybersecurity concepts	Operational capabilites	Security domains
#Preventitive	#Confidentiality #Integrity #Availability	#Identify #Protect	#Threat_and_ vulnerability_ management	#Governance_ and_Ecosystem #Proctection #Defence

27002:2022 | Attribute und deren Werte

#Preventitive
#Detective
#Corrective

Control type	Information security properties	Cybersecurity concepts	Operational capabilites	Security domains
#Preventitive	#Confidentiality #Integrity	#Identify #Protect	#Threat_and_ vulnerability_ management	#Governance_ and_Ecosystem #Proctection #Defence

#Confidentiality
#Integrity
#Availability

27002:2022 | Attribute und deren Werte

#Preventitive
#Detective
#Corrective

#Identify
#Protect
#Detect
#Respond
#Recover

NIST CSF

Control type	Information security properties	Cybersecurity concepts	Operational capabilites	Security domains
#Preventitive	#Confidentiality #Integrity	#Identify #Protect	#Threat_and_ vulnerability_ management	#Governance_ and_Ecosystem #Proctection #Defence

#Confidentiality
#Integrity
#Availability

27002:2022 | Attribute und deren Werte

#Preventitive
#Detective
#Corrective

#Identify
#Protect
#Detect
#Respond
#Recover

NIST CSF

Control type	Information security properties	Cybersecurity concepts	Operational capabilites	Security domains
#Preventitive	#Confidentiality #Integrity	#Governance # Asset_management #Information_protection #Human_resource_security #Physical_security #System_and_network_security #Application_security #Secure_configuration	#Identity_and_access_management #Threat_and_vulnerability_management #Continuity #Supplier_relationships_security #Legal_and_compliance #Information_security_event_management #Information_security_assurance	

#Confidentiality
#Integrity
#Availability

27002:2022 | Attribute und deren Werte

#Preventitive
#Detective
#Corrective

#**Identify**
#**Protect**
#**Detect**
#**Respond**
#**Recover**

NIST CSF

#Governance_and_Ecosystem
#Proctection
#Defence
#Resilience

Control type	Information security properties	Cybersecurity concepts	Operational capabilites	Security domains
#Preventitive	#Confidentiality #Integrity			

#Confidentiality
#Integrity
#Availability

#Governance
Asset_management
#Information_protection
#Human_resource_security
#Physical_security
#System_and_network_security
#Application_security
#Secure_configuration

#Identity_and_access_management
#Threat_and_vulnerability_management
#Continuity
#Supplier_relationships_security
#Legal_and_compliance
#Information_security_event_management
#Information_security_assurance

27002:2022 | Attribute und deren Werte

#Preventitive
#Detective
#Corrective

#**Identify**
#**Protect**
#**Detect**
#**Respond**
#**Recover**

NIST CSF

#Governance_and_Ecosystem
#Proctection
#Defence
#Resilience

Control type	Information security properties	Cybersecurity concepts	Operational capabilites	Security domains
#Preventitive	#Confidentiality #Integrity			

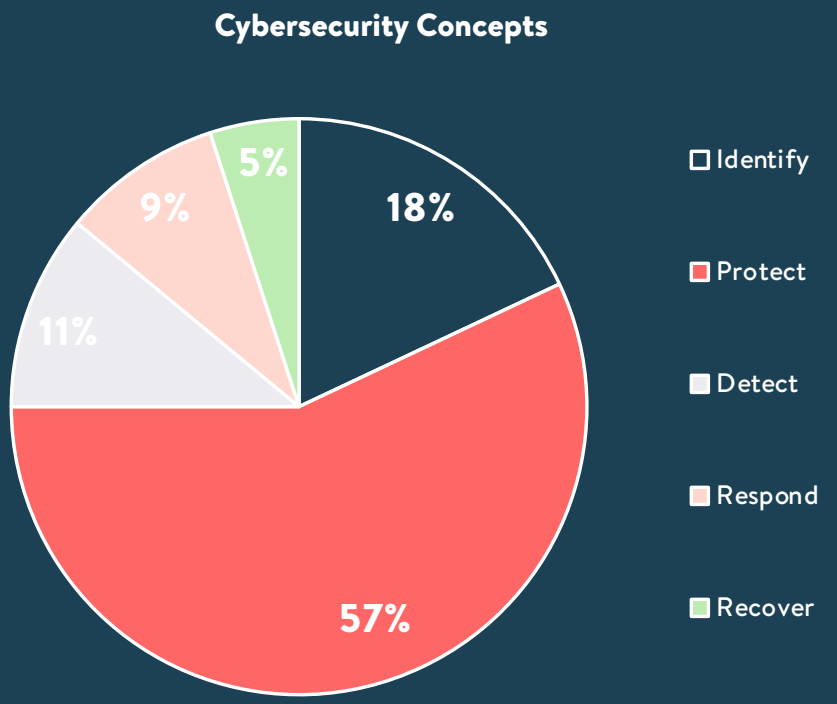
#Confidentiality
#Integrity
#Availability

#Governance
Asset_management
#Information_protection
#Human_resource_security
#Physical_security
#System_and_network_security
#Application_security
#Secure_configuration

#Identity_and_access_management
#Threat_and_vulnerability_management
#Continuity
#Supplier_relationships_security
#Legal_and_compliance
#Information_security_event_management
#Information_security_assurance

27002:2022 | Attribute

Operational capabilites and cybersecurity concepts



malean

AUDITPLANUNG UND NUTZUNG VON ATTRIBUTEN

«Operational capabilities» und Auditplanung

USANZ

Die Auditplanung bzw. Auditsequenzen erfolgen entlang von Organisationseinheiten oder entlang von Geschäftsprozessen.

«OPERATIONAL CAPABILITIES»

Die operationellen Fähigkeiten der Organisation liegen naturgemäss näher an den Geschäfts- bzw. IT-Prozessen, als eine andere (willkürliche) Selektion von Kontrollen für einzelne Auditsequenzen.

EMPFEHLUNG

Kontrollen für Auditsequenzen anhand der «Operational capabilities» auszuwählen erscheint sinnvoll.

ABER...

«Operational capabilities» und Auditplanung

ABER...

Das hätte eine Mehrfachprüfung einiger Kontrollen zur Folge, da einer Kontrolle mehrere Werte pro Attribut zugeordnet sein können.

FRAGEN

- Was wären die Folgen?
- Ist das ein Vor- oder Nachteil?
- Welche (sinnvollen) Alternativen gibt es?

malean

DIE 11 NEUEN KONTROLLEN

27002:2022 | Die 11 neuen Kontrollen

NR.	TITEL	ÜBERSETZUNG
5.7	Threat intelligence	Bedrohungsanalyse
5.23	Information security for use of cloud services	Informationssicherheit für die Nutzung von Clouddiensten
5.30	ICT readiness for business continuity	IKT-Bereitschaft für die Geschäftskontinuität
7.4	Physical security monitoring	Überwachung der physischen Sicherheit
8.9	Configuration management	Konfigurationsmanagement
8.10	Information deletion	Löschen von Informationen
8.11	Data masking	Maskierung von Daten
8.12	Data leakage prevention	Verhinderung von Datenlecks
8.16	Monitoring activities	Überwachungstätigkeiten (Monitoring)
8.23	Web filtering	Web-Filterung
8.28	Secure coding	Sichere Softwareentwicklung (Programmierung)

5.7 Threat intelligence

CONTROL AND PURPOSE

Control

Information relating to information security threats should be collected and analysed to produce threat intelligence.

Purpose

To provide awareness of the organization's threat environment so that the appropriate mitigation actions can be taken.

MÖGLICHE FRAGESTELLUNGEN

- Wann und wie werden Informationen über aktuelle Bedrohungen gesammelt?
- Nach welchen Kriterien werden diese Informationen analysiert?
- Welche Massnahmen werden daraus abgeleitet?
- Erhalten die Verantwortlichen Informationen über die Bedrohungslage?

5.23 Information security for use of cloudservices

CONTROL AND PURPOSE

Control

Processes for acquisition, use, management and exit from cloud services should be established in accordance with the organization's information security requirements.

Purpose

To specify and manage information security for the use of cloud services.

MÖGLICHE FRAGESTELLUNGEN

- Welche Richtlinien und Verfahren bestehen für die Nutzung von Clouddiensten?
- Wird dabei der gesamte Nutzungszyklus von Clouddiensten berücksichtigt, insbesondere auch der Ausstieg?
- Wie werden die Cloud-spezifischen Risiken behandelt?
- Wie wird die rechtliche Compliance sichergestellt, insbesondere hinsichtlich des Datenschutzes?
- Sind die wesentlichen betrieblichen Abhängigkeiten zwischen Clouddiensten und Geschäftsprozessen bekannt und im BCM berücksichtigt?
- Besteht ein Ausstiegsszenario?

5.30 ICT readiness for business continuity

CONTROL AND PURPOSE

Control

ICT readiness should be planned, implemented, maintained, and tested based on business continuity objectives and ICT continuity requirements.

Purpose

To ensure the availability of the organization's information and other associated assets during disruption.

MÖGLICHE FRAGESTELLUNGEN

- Sind für die wesentlichen IKT-Services die Verfügbarkeitsanforderungen systematisch erhoben und festgelegt?
- Wurden die RTOs und RPOs definiert und Abhängig davon Prioritäten einer Wiederherstellung geplant?
- Sind aktuelle Kontinuitätspläne vorhanden?
- Werden die Szenarien regelmässig geübt/getestet?
- Sind Nachweise vorhanden?

7.4 Physical security monitoring

CONTROL AND PURPOSE

Control

Premises should be continuously monitored for unauthorized physical access.

Purpose

To detect and deter unauthorized physical access.

MÖGLICHE FRAGESTELLUNGEN

- Sind die kritischen Einrichtungen identifiziert?
- Welche Überwachungseinrichtungen sind vorhanden und sind diese vor Manipulation geschützt?
- Werden Ereignisse unmittelbar entdeckt und funktioniert die Alarmierung entsprechend?
- Sind die Interventionskräfte informiert und eingebunden? (Polizei, Feuerwehr, etc.)?
- Werden regelmässige Tests durchgeführt?
- Sind bei Videoüberwachung Hinweisschilder gut sichtbar?
- Werden Aufzeichnungen nur im gesetzlich zulässigen Rahmen ausgewertet und aufbewahrt bzw. wieder gelöscht?

8.9 Configuration management

CONTROL AND PURPOSE

Control

Configurations, including security configurations of hardware, software, services, and networks, should be established, documented, implemented, monitored, and reviewed.

Purpose

To ensure hardware, software, services, and networks function correctly with required security settings and configuration is not altered by unauthorized or incorrect changes.

MÖGLICHE FRAGESTELLUNGEN

- Wie wird die korrekte (Sicherheits-)Konfiguration von Hardware, Software, Services, Netzwerken über den gesamten Lebenszyklus hinweg gewährleistet?
- Sind dabei die Aspekte wie Privileged Access Management, Deaktivierung von unnötigen Accounts, Funktionen und Netzwerkdiensten, Nutzung von Systemadministrationstools etc. berücksichtigt?
- Werden hierfür Standard-Templates verwendet?
- Sind Konfigurationsänderungen nachvollziehbar dokumentiert?

8.10 Information deletion

CONTROL AND PURPOSE

Control

Information stored in information systems, devices, or in any other storage media should be deleted when no longer required.

Purpose

To prevent unnecessary exposure of sensitive information and to comply with legal, statutory, regulatory, and contractual requirements for information deletion.

MÖGLICHE FRAGESTELLUNGEN

- Besteht ein Inventar der Datenbestände?
- Sind die Vorgaben bezüglich Löschung bzw. Aufbewahrung definiert und bekannt?
- Besteht ein dokumentiertes und kontrolliertes Verfahren zum Löschen von Daten?
- Kann bei Personendatensammlungen das Recht auf Datenlöschung gem. DSG umgesetzt werden?
- Wird von Cloud-Dienstleistern die Löschung nach Ende des Vertrags eingefordert?
- Sind Nachweise zur Datenlöschung vorhanden?

8.11 Data masking

CONTROL AND PURPOSE

Control

Data masking should be used in accordance with the organization's topic-specific policy on access control and other related topic-specific policies and business requirements, taking applicable legislation into consideration.

Purpose

To limit the exposure of sensitive data, including PII, and to comply with legal, statutory, regulatory, and contractual requirements.

MÖGLICHE FRAGESTELLUNGEN

- Sind die Datenbestände und Informationssysteme identifiziert, welche sensible Daten beinhalten?
- Sind Verfahren etabliert bzw. Techniken implementiert, die eine Unkenntlichmachung von Daten ermöglichen?
- Bei Einsatz von Pseudonymen oder Anonymisierung: Kann eine indirekte Identifikation ausgeschlossen werden?

8.12 Data leakage prevention

CONTROL AND PURPOSE

Control

Data leakage prevention measures should be applied to systems, networks, and any other devices that process, store, or transmit sensitive information.

Purpose

To detect and prevent the unauthorized disclosure and extraction of information by individuals or systems.

MÖGLICHE FRAGESTELLUNGEN

- Sind die Datenbestände und Informationssysteme identifiziert, welche sensible Daten beinhalten?
- Sind mögliche Datenlecks / Kommunikationskanäle bekannt?
- Werden entsprechende Ereignisse erkannt und bestehen definierte Verfahren zu deren Behandlung?
- Sind die Mitarbeitenden über derartige Überwachungsmaßnahmen informiert und werden die Persönlichkeitsrechte angemessen geschützt?

8.16 Monitoring activities

CONTROL AND PURPOSE

Control

Networks, systems, and applications should be monitored for anomalous behaviour, and appropriate actions taken to evaluate potential information security incidents.

Purpose

To detect anomalous behaviour and potential information security incidents.

MÖGLICHE FRAGESTELLUNGEN

- Ist die Organisation in der Lage, Auffälligkeiten und potenzielle Sicherheitsereignisse innert nützlicher Frist zu erkennen und angemessene Entscheide zu fällen?
- Sind alle für die sicherheitsbezogene Überwachung relevanten Systeme, Netzwerke, Applikationen und weiteren Quellen von Protokolldaten integriert?

8.23 Web filtering

CONTROL AND PURPOSE

Control

Access to external websites should be managed to reduce exposure to malicious content.

Purpose

To protect systems from being compromised by malware and to prevent access to unauthorized web resources.

MÖGLICHE FRAGESTELLUNGEN

- Ist die Organisation in der Lage, Auffälligkeiten und potenzielle Sicherheitsereignisse innert nützlicher Frist zu erkennen und angemessene Entscheide zu Ist die Organisation in der Lage, den Zugang zu externen Websites gezielt zu steuern?
- Ist die Verletzbarkeit gegenüber schädigenden Inhalten auf das erforderliche Minimum reduziert?
- Bestehen Vorkehrungen, welche die Kommunikation zu schädigenden Websites wie bspw. C&C Servern, Malware, Phishing-Sites aktiv und dynamisch verhindern?

8.28 Secure coding

CONTROL AND PURPOSE

Control

Secure coding principles should be applied to software development.

Purpose

To ensure software is written securely, thereby reducing the number of potential information security vulnerabilities in the software.

MÖGLICHE FRAGESTELLUNGEN

- Ist die Organisation in der Lage, Software so zu erstellen, dass potenzielle Schwachstellen gezielt vermieden bzw. reduziert werden?
- Welche Codierungsprinzipien und Best Practices werden hierfür angewandt?
- Welche Qualitäts- und Sicherheitskontrollen sind in den Entwicklungszyklen integriert?

malean

AUSWIRKUNGEN

Auswirkungen der Normänderung für Sie

Sich mit der neuen Struktur, den geänderten, weggefallenen und neuen Kontrollen vertraut machen.

Den Prozess zur Informationssicherheits-Risikobehandlung (ISO/IEC 27001:2022, Kapitel 6.1.3) unter Berücksichtigung der Neugestaltung der Kontrollen durchführen.

SoA (= Ergebnis des Prozesses) neu erstellen.

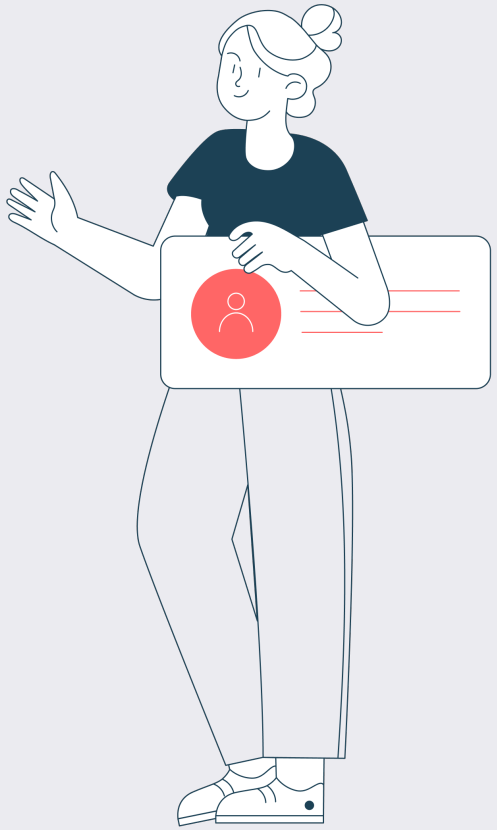
- Erforderliche Kontrollen je Risiko
- Gründe für den Einbezug bzw. Nicht-Einbezug von Kontrollen
- Status der Umsetzung

Risikobehandlungsplan aktualisieren und genehmigen lassen.

Dokumentation des Prozesses aktualisieren und Nachweise erbringen.

KONTINUIERLICHE VERBESSERUNG

- Inhalt von ISO/IEC 27002 und die Empfehlungen zur Umsetzung (Guidance) kennen.
- Kontrollen gemäss 27001 Anhang A richtig verstehen und interpretieren.



malean

FRAGEN?

Wie finden Sie die neue Norm 27001:2022 / 27002:2022?

malean

VIELEN DANK FÜR IHRE AUFMERKSAMKEIT.

+41 76 321 3940

sandra.thurnheer@malean.org

malean | c/o iresults GmbH | Industriering 20 | 9491 Ruggell