



Sicherheitsstandards Identifikation und Authentifikation

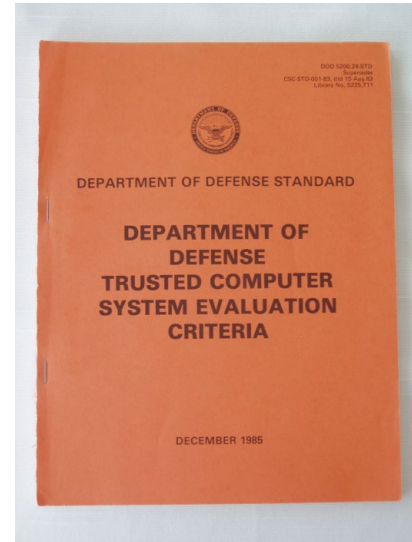
Modul D3.2

Referent: Dr. Jörg Cosfeld

Auf dem Weg zu ISO 27000

Startschuss zu den IT Sicherheitsstandards war das Jahr 1985 – Orange Book

USA haben erste Kriterien vor.

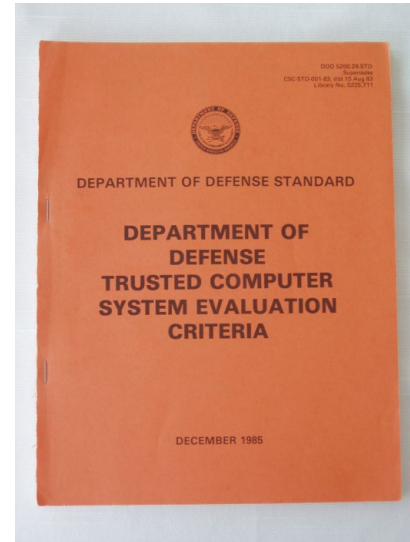


Auf dem Weg zu ISO 27000

Startschuss zu den IT Sicherheitsstandards war das Jahr 1985 – Orange Book

TCSEC ordnet Computersysteme in Stufen A, B, C und D ein:

D = unsicheres System



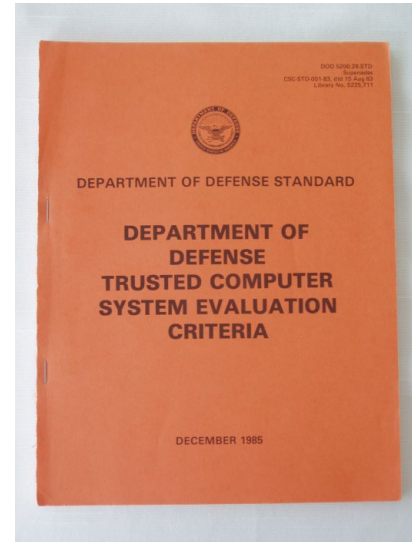
Auf dem Weg zu ISO 27000

Startschuss zu den IT Sicherheitsstandards war das Jahr 1985 – Orange Book

TCSEC ordnet Computersysteme in Stufen A, B, C und D ein:

C = einfacher Schutz

C1 / C2 = Login Sicherung

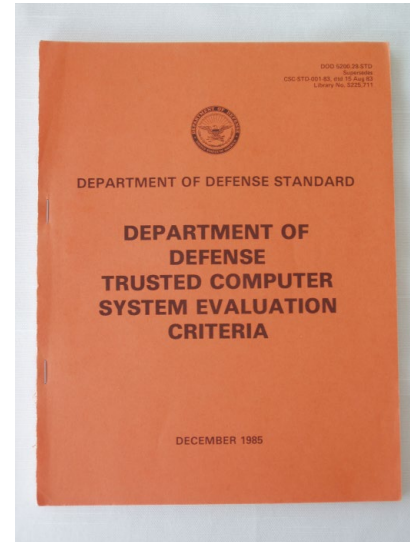


Auf dem Weg zu ISO 27000

Startschuss zu den IT Sicherheitsstandards war das Jahr 1985 – Orange Book

TCSEC ordnet Computersysteme in Stufen A, B, C und D ein:

B = Verwaltung von Zugriffsrechten

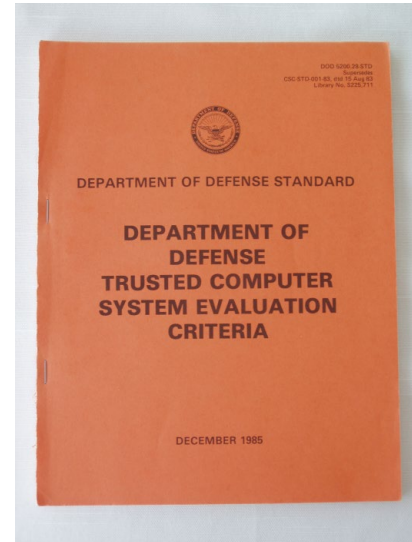


Auf dem Weg zu ISO 27000

Startschuss zu den IT Sicherheitsstandards war das Jahr 1985 – Orange Book

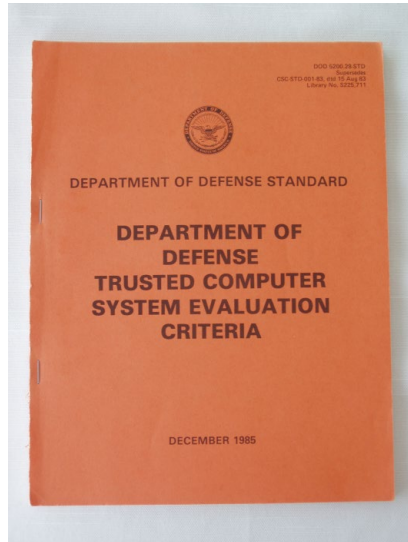
TCSEC ordnet Computersysteme in Stufen A, B, C und D ein:

A = Gesamtsystem hat ein FallBack System (Backup) und ist verifizierbar



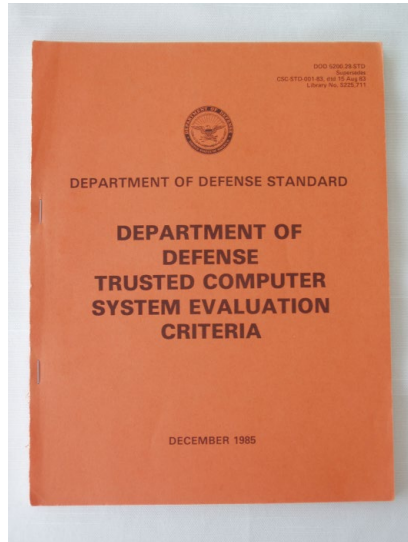
Auf dem Weg zu ISO 27000

Ablösung durch die Common Criteria im Jahr 1996



Auf dem Weg zu ISO 27000

Ablösung durch die Common Criteria im Jahr 1996



Weg zu ISO Normen

Auf dem Weg zu ISO 27000

Aktuelle Version ist am 2017 veröffentlicht worden

- Version 3.1 Release 5
- Alle Normen sind entstanden
 - Zur Prüfung von:
 - IT Sicherheit von Netzwerken
 - IT Sicherheit von Geräten



Auf dem Weg zu ISO 27000

Aktuelle Version ist am 2017 veröffentlicht worden

- Version 3.1 Release 5
- Alle Normen sind entstanden
 - Zur Prüfung von:
 - IT Sicherheit von Netzwerken
 - IT Sicherheit von Geräten



Microsoft Windows NT ist C2 zertifiziert.

Bill Gates - 1995

Auf dem Weg zu ISO 27000

Aktuelle Version ist am 2017 veröffentlicht worden

- Version 3.1 Release 5
- Alle Normen sind entstanden
 - Zur Prüfung von:
 - IT Sicherheit von Netzwerken
 - IT Sicherheit von Geräten



Microsoft Windows NT ist C2 zertifiziert.



Bill Gates - 1995

Auf dem Weg zu ISO 27000

Aktuelle Version ist am 2017 veröffentlicht worden

- Version 3.1 Release 5
- Alle Normen sind entstanden
 - Zur Prüfung von:
 - IT Sicherheit von Netzwerken
 - IT Sicherheit von Geräten



Motivation:

IT Sicherheitsstandards sind dazu da, **IT Sicherheit zu systematisieren** und methodisch **sauber zu gestalten**.

Auf dem Weg zu ISO 27000

Aktuelle Version ist am 2017 veröffentlicht worden

- Version 3.1 Release 5
- Alle Normen sind entstanden
 - Zur Prüfung von:
 - IT Sicherheit von Netzwerken
 - IT Sicherheit von Geräten



Motivation:

IT Sicherheitsstandards sind dazu da, **IT Sicherheit zu systematisieren** und methodisch **sauber zu gestalten**.

Vergleichbarkeit.

Auf dem Weg zu ISO 27000

Aktuelle Version ist am 2017 veröffentlicht worden

- Version 3.1 Release 5
- Alle Normen sind entstanden
 - Zur Prüfung von:
 - IT Sicherheit von Netzwerken
 - IT Sicherheit von Geräten



Motivation:

IT Sicherheitsstandards sind dazu da, **IT Sicherheit zu systematisieren** und methodisch **sauber zu gestalten**.

Vergleichbarkeit.

Familie der ISO 2700-X

Übersicht

ISO 27000

Anforderungen

ISO 27001

ISO 27006

ISO 27006-2

ISO 27009

ISO 27701-9

Leitfäden

ISO 27002-5

ISO 27007-8

ISO 27013-14

ISO 27021

Bereichspez. Leitfäden

ISO 27010-11

ISO 27017-19

ISO 27701 A6

ISO 27799

Spezielle Leitfäden

ISO 2702x

ISO 2703x

ISO 2704x

ISO 2710x

Familie der ISO 2700-X

Übersicht

ISO 27000

Anforderungen

ISO 27001

ISO 27006

ISO 27006-2

ISO 27009

ISO 27701-9

Leitfäden

ISO 27002-5

ISO 27007-8

ISO 27013-14

ISO 27021

Bereichspez. Leitfäden

ISO 27010-11

ISO 27017-19

ISO 27701 A6

ISO 27799

Spezielle Leitfäden

ISO 2702x

ISO 2703x

ISO 2704x

ISO 2710x

Familie der ISO 2700-X

Übersicht

ISO 27000

Anforderungen

ISO 27001

ISO 27006

ISO 27006-2

ISO 27009

ISO 27701-9

Leitfäden

ISO 27002-5

ISO 27007-8

ISO 27013-14

ISO 27021

Bereichspez. Leitfäden

ISO 27010-11

ISO 27017-19

ISO 27701 A6

ISO 27799



Anforderungen an den
Gesundheitssektor

Spezielle Leitfäden

ISO 2702x

ISO 2703x

ISO 2704x

ISO 2710x

Familie der ISO 2700-X

Es gilt:

- Jahreszahl der Norm wird hinter die Bezeichnung geschrieben
 - Doppelpunkt beachten!
- Korrekturen sind durch **cor1** oder **cor2**, etc. markiert

Familie der ISO 2700-X

Es gilt:

- Jahreszahl der Norm wird hinter die Bezeichnung geschrieben
 - Doppelpunkt beachten!
- Korrekturen sind durch **cor1** oder **cor2**, etc. markiert
- Englischer Standard schreibt die Jahreszahl nach vorne
- Nicht frei zugänglich
 - Kosten entstehen für Unternehmen / Institutionen

Familie der ISO 2700-X

Es gilt:

- Jahreszahl der Norm wird hinter die Bezeichnung geschrieben
 - Doppelpunkt beachten!
- Korrekturen sind durch **cor1** oder **cor2**, etc. markiert
- Englischer Standard schreibt die Jahreszahl nach vorne
- Nicht frei zugänglich
 - Kosten entstehen für Unternehmen / Institutionen
- Einsehbar in Norm Infopoints

Blick auf ISO 27000

Was ist der Inhalt von ISO 27000

- Definition von rund 77 Kenngrößen
- Definition eines Informationssicherheit-Management Systems (ISMS)
- Definition des Scopes (Anwendungsbereich) und Purpose (Zweck)

Blick auf ISO 27000



International Organization for Standardization

Français

Licence Agreement for Publicly Available Standards

You are about to download a document protected by copyright.

When you download (an) ISO publication(s) from this site, you must accept the [ISO Customer Licence Agreement](#) ("Licence Agreement"), excluding clauses 2. Watermark, 5. Paper copies, and 6. Codes and Graphical Symbols (and their Collections).

Contact

Should you have any questions about this Licence Agreement, please [contact us](#).

I accept

Note: cookies must be enabled

Blick auf ISO 27000

Auszug aus Abschnitt 4

4.1 General

Organizations of all types and sizes:

- a) collect, process, store, and transmit information;
- b) recognize that information, and related processes, systems, networks and people are important assets for achieving organization objectives;
- c) face a range of risks that can affect the functioning of assets; and
- d) address their perceived risk exposure by implementing information security controls.

Informationen

Blick auf ISO 27000

Auszug aus Abschnitt 4

4.1 General

Organizations of all types and sizes:

- a) collect, process, store, and transmit information;
- b) recognize that information, and related processes, systems, networks and people are important assets for achieving organization objectives;
- c) face a range of risks that can affect the functioning of assets; and
- d) address their perceived risk exposure by implementing information security controls.

Informationen
Prozesse
Netzwerke

Mitarbeiter

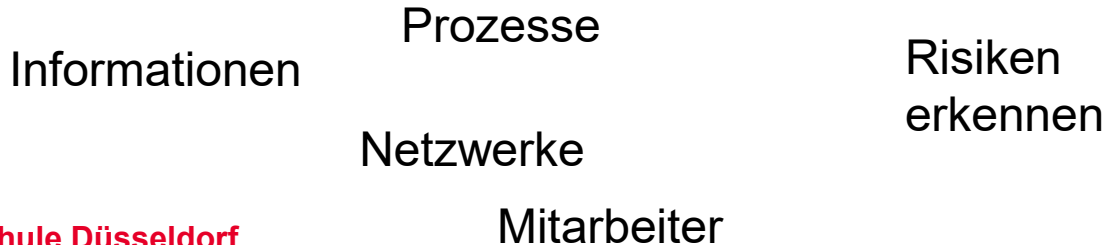
Blick auf ISO 27000

Auszug aus Abschnitt 4

4.1 General

Organizations of all types and sizes:

- a) collect, process, store, and transmit information;
- b) recognize that information, and related processes, systems, networks and people are important assets for achieving organization objectives;
- c) face a range of risks that can affect the functioning of assets; and
- d) address their perceived risk exposure by implementing information security controls.



Blick auf ISO 27000

Auszug aus Abschnitt 4

4.1 General

Organizations of all types and sizes:

- a) collect, process, store, and transmit information;
- b) recognize that information, and related processes, systems, networks and people are important assets for achieving organization objectives;
- c) face a range of risks that can affect the functioning of assets; and
- d) address their perceived risk exposure by implementing information security controls.

Informationen

Prozesse

Netzwerke

Risiken
erkennen

Sicherheit
kontrollieren

Mitarbeiter

Blick auf ISO 27000

Auszug aus Abschnitt 4



**Einbetten eines ISMS in die
Organisation**

Blick auf ISO 27000

Auszug aus Abschnitt 4



**Einbetten eines ISMS
in die Organisation**

5	ISMS family of standards	18
5.1	General information	18
5.2	Standard describing an overview and terminology: ISO/IEC 27000 (this document)	19
5.3	Standards specifying requirements	19
5.3.1	ISO/IEC 27001	19
5.3.2	ISO/IEC 27006	20
5.3.3	ISO/IEC 27009	20
5.4	Standards describing general guidelines	20
5.4.1	ISO/IEC 27002	20
5.4.2	ISO/IEC 27003	20
5.4.3	ISO/IEC 27004	21
5.4.4	ISO/IEC 27005	21
5.4.5	ISO/IEC 27007	21
5.4.6	ISO/IEC TR 27008	21
5.4.7	ISO/IEC 27013	22
5.4.8	ISO/IEC 27014	22
5.4.9	ISO/IEC TR 27016	22
5.4.10	ISO/IEC 27021	22
5.5	Standards describing sector-specific guidelines	23
5.5.1	ISO/IEC 27010	23
5.5.2	ISO/IEC 27011	23
5.5.3	ISO/IEC 27017	23
5.5.4	ISO/IEC 27018	24
5.5.5	ISO/IEC 27019	24
5.5.6	ISO 27799	25

Blick auf ISO 27000

Auszug aus Abschnitt 4



Einbetten eines ISMS in die Organisation

An **ISMS** consists of the **policies, procedures, guidelines**, and **associated** resources and activities, **collectively managed** by an organization, in the pursuit of protecting its **information assets**.

Blick auf ISO 27000

Ausblick:

Auszug aus Abschnitt 4

Informationen – Verbindung zu
Big Data und Data Sciences



**Einbetten eines ISMS
in die Organisation**

An **ISMS** consists of the **policies, procedures, guidelines**, and **associated** resources and activities, **collectively managed** by an organization, in the pursuit of protecting its **information assets**.

Blick auf ISO 27000

Auszug aus Abschnitt 4



**Einbetten eines ISMS
in die Organisation**

An **ISMS** consists of the **policies, procedures, guidelines**, and **associated** resources and activities, **collectively managed** by an organization, in the pursuit of protecting its **information assets**.

Blick auf ISO 27000

Auszug aus Abschnitt 4.2.5



Einbetten eines ISMS in die Organisation

4.2.5 Management system

A management system uses a framework of resources to achieve an organization's objectives. The management system includes organizational structure, policies, planning activities, responsibilities, practices, procedures, processes and resources.

In terms of information security, a management system allows an organization to:

- a) satisfy the information security requirements of customers and other stakeholders;
- b) improve an organization's plans and activities;
- c) meet the organization's information security objectives;
- d) comply with regulations, legislation and industry mandates; and
- e) manage information assets in an organized way that facilitates continual improvement and adjustment to current organizational goals.

Blick auf ISO 27000

Auszug aus Abschnitt 4.2.5



Einbetten eines ISMS in die Organisation

4.2.5 Management system

A management system uses a framework of resources to achieve an organization's objectives. The management system includes organizational structure, policies, planning activities, responsibilities, practices, procedures, processes and resources.

In terms of information security, a management system allows an organization to:

- a) satisfy the information security requirements of customers and other stakeholders;
- b) improve an organization's plans and activities;
- c) meet the organization's information security objectives;
- d) comply with regulations, legislation and industry mandates; and
- e) manage information assets in an organized way that facilitates continual improvement and adjustment to current organizational goals.

Blick auf ISO 27000

Auszug aus Abschnitt 4.2.5



Einbetten eines ISMS in die Organisation

4.2.5 Management system

A management system uses a framework of resources to achieve an organization's objectives. The management system includes organizational structure, policies, planning activities, responsibilities, practices, procedures, processes and resources.

In terms of information security, a management system allows an organization to:

- a) satisfy the information security requirements of customers and other stakeholders;
- b) **improve an organization's plans and activities;**
- c) meet the organization's information security objectives;
- d) comply with regulations, legislation and industry mandates; and
- e) manage information assets in an organized way that facilitates continual improvement and adjustment to current organizational goals.

Blick auf ISO 27000

Auszug aus Abschnitt 4.2.5



Einbetten eines ISMS in die Organisation

4.2.5 Management system

A management system uses a framework of resources to achieve an organization's objectives. The management system includes organizational structure, policies, planning activities, responsibilities, practices, procedures, processes and resources.

In terms of information security, a management system allows an organization to:

- a) satisfy the information security requirements of customers and other stakeholders;
- b) improve an organization's plans and activities;
- c) **meet the organization's information security objectives;**
- d) comply with regulations, legislation and industry mandates; and
- e) manage information assets in an organized way that facilitates continual improvement and adjustment to current organizational goals.

Familie der ISO 2700-X

Übersicht

ISO 27000

Anforderungen

ISO 27001

ISO 27006

ISO 27006-2

ISO 27009

ISO 27701-9

Leitfäden

ISO 27002-5

ISO 27007-8

ISO 27013-14

ISO 27021

Bereichspez. Leitfäden

ISO 27010-11

ISO 27017-19

ISO 27701 A6

ISO 27799

Spezielle Leitfäden

ISO 2702x

ISO 2703x

ISO 2704x

ISO 2710x

Familie der ISO 2700-X

Übersicht

Anforderungen

ISO 27000

ISO 27001

DS-VGO

- Physische Sicherheit / Sicherheit in der Umgebung
- Steuerung des Zugangs
- Kryptografie
- Sicherheit der Kommunikation
- Beziehung zu Lieferanten



- Zutrittskontrolle
- Zugang und Zugriffskontrolle
- Verschlüsselung
- Weitergabekontrolle
- Auftragskontrolle

Familie der ISO 2700-X

Übersicht

Anforderungen

Vieles ist parallel

ISO 27000

ISO 27001

DS-VGO

- Physische Sicherheit / Sicherheit in der Umgebung
- Steuerung des Zugangs
- Kryptografie
- Sicherheit der Kommunikation
- Beziehung zu Lieferanten



- Zutrittskontrolle
- Zugang und Zugriffskontrolle
- Verschlüsselung
- Weitergabekontrolle
- Auftragskontrolle

Familie der ISO 2700-X

Übersicht

Anforderungen

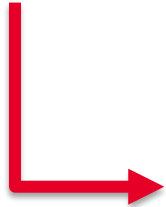
Vieles ist parallel

ISO 27000

ISO 27001

DS-VGO

- Physische Sicherheit / Sicherheit in der Umgebung
- Zutrittskontrolle



Fordert unter „Sicherheitsaspekte beim Personal“ deutlich mehr.

Familie der ISO 2700-X

Übersicht

Anforderungen

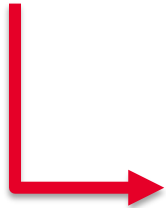
Vieles ist parallel

ISO 27000

ISO 27001

DS-VGO

- Physische Sicherheit / Sicherheit in der Umgebung
- Zutrittskontrolle



Fordert unter „Sicherheitsaspekte beim Personal“ deutlich mehr.

Aufnahme und Beendigung des Arbeitsverhältnisses.

Familie der ISO 2700-X

Übersicht

Anforderungen

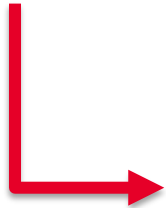
Vieles ist parallel

ISO 27000

ISO 27001

DS-VGO

- Physische Sicherheit / Sicherheit in der Umgebung
- Zutrittskontrolle



Fordert unter „Sicherheitsaspekte beim Personal“
deutlich mehr.

Aufnahme und **Beendigung** des
Arbeitsverhältnisses.

Familie der ISO 2700-X

Übersicht

ISO 27000

Anforderungen

ISO 27001

ISO 27006

ISO 27006-2

ISO 27009

ISO 27701-9

Leitfäden

ISO 27002-5

ISO 27007-8

ISO 27013-14

ISO 27021

Bereichspez. Leitfäden

ISO 27010-11

ISO 27017-19

ISO 27701 A6

ISO 27799

Spezielle Leitfäden

ISO 2702x

ISO 2703x

ISO 2704x

ISO 2710x

Familie der ISO 2700-X



Leitfäden

ISO 27002

Kernleitfaden und
Hilfestellung bei der
Umsetzung von ISO 27001

Familie der ISO 2700-X

Leitfäden

ISO 27002

- 9.3 Verantwortlichkeit des Benutzers

Kernleitfaden und
Hilfestellung bei der
Umsetzung von ISO 27001

Familie der ISO 2700-X

Leitfäden

ISO 27002

- 9.3 Verantwortlichkeit des Benutzers
Kernleitfaden und Hilfestellung bei der Umsetzung von ISO 27001
- User sollen dazu verpflichtet werden, die Regel zum Umgang mit vertraulichen Anmeldedaten einzuhalten.

Familie der ISO 2700-X

Leitfäden

ISO 27002

- 9.3 Verantwortlichkeit des Benutzers
Kernleitfaden und Hilfestellung bei der Umsetzung von ISO 27001
- User sollen dazu verpflichtet werden, die Regel zum Umgang mit vertraulichen Anmeldedaten einzuhalten.
- „User sind auf den notwendigen Schutz Ihrer Anmeldedaten hingewiesen worden.“

Familie der ISO 2700-X

8	Verwaltung der Werte	
8.1	Verantwortlichkeit für Werte	
8.1.1	Inventarisierung der Werte	
8.1.2	Zuständigkeit für Werte	
8.1.3	Zulässiger Gebrauch von Werten	
8.1.4	Rückgabe von Werten	
8.2	Informationsklassifizierung	
8.2.1	Klassifizierung von Information	
8.2.2	Kennzeichnung von Information	
8.2.3	Handhabung von Werten	

Leitfaden

ISO 27002

7	Personalsicherheit	
7.1	Vor der Beschäftigung	
7.1.1	Sicherheitsüberprüfung	
7.1.2	Beschäftigungs- und Vertragsbedingungen	
7.2	Während der Beschäftigung	
7.2.1	Verantwortlichkeiten der Leitung	
7.2.2	Informationssicherheitsbewusstsein, -ausbildung und	
7.2.3	Maßregelungsprozess	
7.3	Beendigung und Änderung der Beschäftigung	
7.3.1	Verantwortlichkeiten bei Beendigung oder Änderung	

14	Anschaffung, Entwicklung und Instandhaltung von Systemen	77
14.1	Sicherheitsanforderungen an Informationssysteme	77
14.1.1	Analyse und Spezifikation von Informationssicherheitsanforderungen	77
14.1.2	Sicherung von Anwendungsdiensten in öffentlichen Netzwerken	78
14.1.3	Schutz der Transaktionen bei Anwendungsdiensten	79
14.2	Sicherheit in Entwicklungs- und Unterstützungsprozessen	80
14.2.1	Richtlinie für sichere Entwicklung	80
14.2.2	Verfahren zur Verwaltung von Systemänderungen	81
14.2.3	Technische Überprüfung von Anwendungen nach Änderungen an der Betriebsplattform	82
14.2.4	Beschränkung von Änderungen an Softwarepaketen	83
14.2.5	Grundsätze für die Analyse, Entwicklung und Pflege sicherer Systeme	83
14.2.6	Sichere Entwicklungsumgebung	84
14.2.7	Ausgegliederte Entwicklung	85
14.2.8	Testen der Systemsicherheit	85
14.2.9	Systemabnahmetest	86
14.3	Testdaten	86
14.3.1	Schutz von Testdaten	86

12	Betriebssicherheit	58
12.1	Betriebsabläufe und -verantwortlichkeiten	58
12.1.1	Dokumentierte Betriebsabläufe	58
12.1.2	Änderungssteuerung	59
12.1.3	Kapazitätssteuerung	59
12.1.4	Trennung von Entwicklungs-, Test- und Betriebsumgebungen	60
12.2	Schutz vor Schadsoftware	61
12.2.1	Maßnahmen gegen Schadsoftware	61
12.3	Datensicherung	63

16	Handhabung von Informationssicherheitsvorfällen	93
16.1	Handhabung von Informationssicherheitsvorfällen und -verbesserungen	93
16.1.1	Verantwortlichkeiten und Verfahren	93
16.1.2	Meldung von Informationssicherheitsereignissen	94
16.1.3	Meldung von Schwächen in der Informationssicherheit	95
16.1.4	Beurteilung von und Entscheidung über Informationssicherheitsereignisse	95

Familie der ISO 2700-X

Themen werden in
späteren Vorlesungen
diskutiert.

Leitfäden

ISO 27002

8	Verwaltung der Werte	
8.1	Verantwortlichkeit für Werte	
8.1.1	Inventarisierung der Werte	
8.1.2	Zuständigkeit für Werte	
8.1.3	Zulässiger Gebrauch von Werten	
8.1.4	Rückgabe von Werten	
8.2	Informationsklassifizierung	
8.2.1	Klassifizierung von Information	
8.2.2	Kenzeichnung von Information	
8.2.3	Handhabung von Werten	
14	Anschaffung, Entwicklung und Instandhaltung von Systemen	77
14.1	Sicherheitsanforderungen an Informationssysteme	77
14.1.1	Analyse und Spezifikation von Informationssicherheitsanforderungen	77
14.1.2	Sicherung von Anwendungsdiensten in öffentlichen Netzwerken	78
14.1.3	Schutz der Transaktionen bei Anwendungsdiensten	79
14.2	Sicherheit in Entwicklungs- und Unterstützungsprozessen	80
14.2.1	Richtlinie für sichere Entwicklung	80
14.2.2	Verfahren zur Verwaltung von Systemänderungen	81
14.2.3	Technische Überprüfung von Anwendungen nach Änderungen an der Betriebsplattform	82
14.2.4	Beschränkung von Änderungen an Softwarepaketen	83
14.2.5	Grundsätze für die Analyse, Entwicklung und Pflege sicherer Systeme	83
14.2.6	Sichere Entwicklungsumgebung	84
14.2.7	Ausgegliederte Entwicklung	85
14.2.8	Testen der Systemicherheit	85
14.2.9	Systemnahmetest	86
14.3	Testdaten	86
14.3.1	Schutz von Testdaten	86

7	Personalsicherheit	
7.1	Vor der Beschäftigung	
7.1.1	Sicherheitsüberprüfung	
7.1.2	Beschäftigungs- und Vertragsbedingungen	
7.2	Während der Beschäftigung	
7.2.1	Verantwortlichkeiten der Leitung	
7.2.2	Informationssicherheitsbewusstsein, -ausbildung und	
7.2.3	Maßregelungsprozess	
7.3	Beendigung und Änderung der Beschäftigung	
7.3.1	Verantwortlichkeiten bei Beendigung oder Änderung	

12	Betriebsicherheit	58
12.1	Betriebsabläufe und -verantwortlichkeiten	58
12.1.1	Dokumentierte Betriebsabläufe	58
12.1.2	Änderungssteuerung	59
12.1.3	Kapazitätssteuerung	59
12.1.4	Trennung von Entwicklungs-, Test- und Betriebsumgebungen	60
12.2	Schutz vor Schadsoftware	61
12.2.1	Maßnahmen gegen Schadsoftware	61
12.3	Datensicherung	63

16	Handhabung von Informationssicherheitsvorfällen	93
16.1	Handhabung von Informationssicherheitsvorfällen und -verbesserungen	93
16.1.1	Verantwortlichkeiten und Verfahren	93
16.1.2	Meldung von Informationssicherheitsereignissen	94
16.1.3	Meldung von Schwächen in der Informationssicherheit	95
16.1.4	Beurteilung von und Entscheidung über Informationssicherheitsereignisse	95

Familie der ISO 2700-X

8	Verwaltung der Werte
8.1	Verantwortlichkeit für Werte
8.1.1	Inventarisierung der Werte
8.1.2	Zuständigkeit für Werte
8.1.3	Zulässiger Gebrauch von Werten
8.1.4	Rückgabe von Werten
8.2	Informationsklassifizierung
8.2.1	Klassifizierung von Information
8.2.2	Kennzeichnung von Information
8.2.3	Handhabung von Werten

Leitfäden

ISO 27002

7	Personalsicherheit
7.1	Vor der Beschäftigung
7.1.1	Sicherheitsüberprüfung
7.1.2	Beschäftigungs- und Vertragsbedingungen
7.2	Während der Beschäftigung
7.2.1	Verantwortlichkeiten der Leitung
7.2.2	Informationssicherheitsbewusstsein, -ausbildung und
7.2.3	Maßregelungsprozess
7.3	Beendigung und Änderung der Beschäftigung
7.3.1	Verantwortlichkeiten bei Beendigung oder Änderung

Spezifische Anleitung sind teuer.



NORM [AKTUELL]

ISO/IEC 27002:2022-02 (Corrected version)

Informationssicherheit, Cybersicherheit und Schutz der Privatsphäre -
Informationssicherheitsmaßnahmen

Englischer Titel:

Information security, cybersecurity and privacy protection - Information
security controls

Ausgabedatum:

2022-02

Originalsprachen:

Englisch


Seiten:

152



ab **221,00 EUR** inkl. MwSt.

ab **206,54 EUR** exkl. MwSt.

 In den Warenkorb

Familie der ISO 2700-X

8	Verwaltung der Werte
8.1	Verantwortlichkeit für Werte
8.1.1	Inventarisierung der Werte
8.1.2	Zuständigkeit für Werte
8.1.3	Zulässiger Gebrauch von Werten
8.1.4	Rückgabe von Werten
8.2	Informationsklassifizierung
8.2.1	Klassifizierung von Information
8.2.2	Kennzeichnung von Information
8.2.3	Handhabung von Werten

Leitfäden

ISO 27002

7	Personalsicherheit
7.1	Vor der Beschäftigung
7.1.1	Sicherheitsüberprüfung
7.1.2	Beschäftigungs- und Vertragsbedingungen
7.2	Während der Beschäftigung
7.2.1	Verantwortlichkeiten der Leitung
7.2.2	Informationssicherheitsbewusstsein, -ausbildung und
7.2.3	Maßregelungsprozess
7.3	Beendigung und Änderung der Beschäftigung
7.3.1	Verantwortlichkeiten bei Beendigung oder Änderung

Spezifische Anleitung sind teuer.



NORM [AKTUELL]

ISO/IEC 27002:2022-02 (Corrected version)

Informationssicherheit, Cybersicherheit und Schutz der Privatsphäre -
Informationssicherheitsmaßnahmen

Englischer Titel:

Information security, cybersecurity and privacy protection - Information
security controls

Ausgabedatum:

2022-02

Originalsprachen:

Englisch


Seiten:

152



ab **221,00 EUR** inkl. MwSt.

ab **206,54 EUR** exkl. MwSt.

 In den Warenkorb

Familie der ISO 2700-X

Übersicht

ISO 27000

Anforderungen

ISO 27001

ISO 27006

ISO 27006-2

ISO 27009

ISO 27701-9

Leitfäden

ISO 27002-5

ISO 27007-8

ISO 27013-14

ISO 27021

Bereichspez. Leitfäden

ISO 27010-11

ISO 27017-19

ISO 27701 A6

ISO 27799

Spezielle Leitfäden

ISO 2702x

ISO 2703x

ISO 2704x

ISO 2710x

Familie der ISO 2700-X

- Erweiterung von ISO 27001 um den Datenschutz
- ISMS wird dann um Datenschutz erweitert

Bereichspez.
Leitfäden

ISO 27010-11

ISO 27017-19

ISO 27701 A6

ISO 27799

Familie der ISO 2700-X

Diskussion Home-Office

Leitfäden

ISO 27002

Familie der ISO 2700-X

Diskussion Home-Office

6 Organization of information security

6.1 Internal organization

Objective: To establish a management framework to initiate and control the implementation and operation of information security within the organization.

Leitfäden

ISO 27002

Familie der ISO 2700-X

Diskussion Home-Office

Leitfäden

6 Organization of information security

6.1 Internal organization

Objective: To establish a management framework to initiate and control the implementation and operation of information security within the organization.

ISO 27002

6.1.1 Information security roles and responsibilities ✓

6.1.2 Segregation of duties ✓

6.1.3 Contact with authorities ✓

6.1.4 Contact with special interest groups ✓

6.1.5 Information security in project management ✓

Familie der ISO 2700-X

Diskussion Home-Office

6.2 Mobile devices and teleworking

Objective: To ensure the security of teleworking and use of mobile devices.

Leitfäden

ISO 27002

Familie der ISO 2700-X

Diskussion Home-Office

6.2 Mobile devices and teleworking

Objective: To ensure the security of teleworking and use of mobile devices.

6.2.1 Mobile device policy

Control

A policy and supporting security measures should be adopted to manage the risks introduced by using mobile devices.

Leitfäden

ISO 27002

Familie der ISO 2700-X

Diskussion Home-Office

6.2 Mobile devices and teleworking

Objective: To ensure the security of teleworking and use of mobile devices.

6.2.1 Mobile device policy

Control

A policy and supporting security measures should be adopted to manage the risks introduced by using mobile devices.

Implementation guidance

When using mobile devices, special care should be taken to ensure that business information is not compromised. The mobile device policy should take into account the risks of working with mobile devices in unprotected environments.

Leitfäden

ISO 27002

Familie der ISO 2700-X

Diskussion Home-Office

6.2 Mobile devices and teleworking

Objective: To ensure the security of teleworking and use of mobile devices.

6.2.1 Mobile device policy

Control

A policy and supporting security measures should be adopted to manage the risks introduced by using mobile devices.

Implementation guidance

When using mobile devices, special care should be taken to ensure that business information is not compromised. The mobile device policy should take into account the risks of working with mobile devices in unprotected environments.

The mobile device policy should consider:

- a) registration of mobile devices;
- b) requirements for physical protection;
- c) restriction of software installation;

Leitfäden

ISO 27002

Familie der ISO 2700-X

Diskussion Home-Office

Leitfäden

ISO 27002

The mobile device policy should consider:

- a) registration of mobile devices;
- b) requirements for physical protection;
- c) restriction of software installation;
- d) requirements for mobile device software versions and for applying patches;
- e) restriction of connection to information services;

Familie der ISO 2700-X

Diskussion Home-Office

Leitfäden

ISO 27002

The mobile device policy should consider:

- a) registration of mobile devices;
- b) requirements for physical protection;
- c) restriction of software installation;
- d) requirements for mobile device software versions and for applying patches;
- e) restriction of connection to information services;
- f) access controls;
- g) cryptographic techniques;
- h) malware protection;
- i) remote disabling, erasure or lockout;
- j) backups;
- k) usage of web services and web apps.

Familie der ISO 2700-X

Diskussion Home-Office

The mobile device policy should consider:

- a) registration of mobile devices;
- b) requirements for physical protection;
- c) restriction of software installation;
- d) requirements for mobile device software versions and for applying patches;
- e) restriction of connection to information services;
- f) access controls;
- g) cryptographic techniques;
- h) malware protection;
- i) remote disabling, erasure or lockout;
- j) backups;
- k) usage of web services and web apps.

Der User wird mit einem Endgerät ausgestattet welches bei der Ausgabe, von nun an *mobile device* genannt, registriert wird.

Familie der ISO 2700-X

Diskussion Home-Office

The mobile device policy should consider:

- a) registration of mobile devices;
- b) requirements for physical protection;
- c) restriction of software installation;
- d) requirements for mobile device software versions and for applying patches;
- e) restriction of connection to information services;
- f) access controls;
- g) cryptographic techniques;
- h) malware protection;
- i) remote disabling, erasure or lockout;
- j) backups;
- k) usage of web services and web apps.

Der User wird mit einem Endgerät ausgestattet welches bei der Ausgabe, von nun an *mobile device* genannt, registriert wird.

Das mobile device ist in auf den Transportwege zu schützen.

Familie der ISO 2700-X

Diskussion Home-Office

The mobile device policy should consider:

- a) registration of mobile devices;
- b) requirements for physical protection;
- c) restriction of software installation;
- d) requirements for mobile device software versions and for applying patches;
- e) restriction of connection to information services;
- f) access controls;
- g) cryptographic techniques;
- h) malware protection;
- i) remote disabling, erasure or lockout;
- j) backups;
- k) usage of web services and web apps.

Der User wird mit einem Endgerät ausgestattet welches bei der Ausgabe, von nun an *mobile device* genannt, registriert wird.

Das mobile device ist in auf den Transportwege zu schützen.

Was schlagen Sie vor?

Familie der ISO 2700-X

Diskussion Home-Office

The mobile device policy should consider:

- a) registration of mobile devices;
- b) requirements for physical protection;
- c) restriction of software installation;
- d) requirements for mobile device software versions and for applying patches;
- e) restriction of connection to information services;
- f) access controls;
- g) cryptographic techniques;
- h) malware protection;
- i) remote disabling, erasure or lockout;
- j) backups;
- k) usage of web services and web apps.

Der User wird mit einem Endgerät ausgestattet welches bei der Ausgabe, von nun an *mobile device* genannt, registriert wird.

Das mobile device ist in auf den Transportwege zu schützen.

Das mobile device wird über einen VPN Client logisch in die Netzwerkstruktur des Unternehmens eingefügt.

Familie der ISO 2700-X

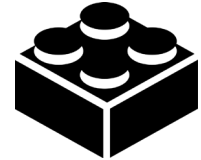
Diskussion Home-Office

Bausteine für eine Leitlinie

Der User wird mit einem Endgerät ausgestattet welches bei der Ausgabe, von nun an *mobile device* genannt, registriert wird.



Das mobile device ist in auf den Transportwege zu schützen.



Das mobile device wird über einen VPN Client logisch in die Netzwerkstruktur des Unternehmens eingefügt.

