Hochschule Düsseldorf
University of Applied Sciences

HSD

Sicherheitsstandards Identifikation und Authentifikation

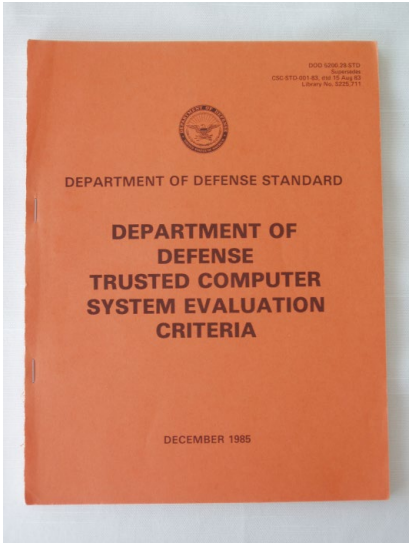
Modul D3.2

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.

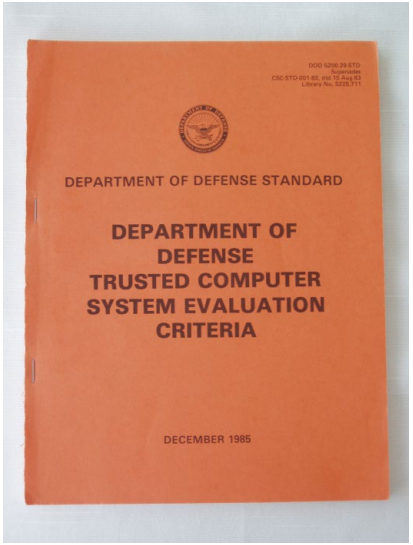


Auf dem Weg zu ISO 27000

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

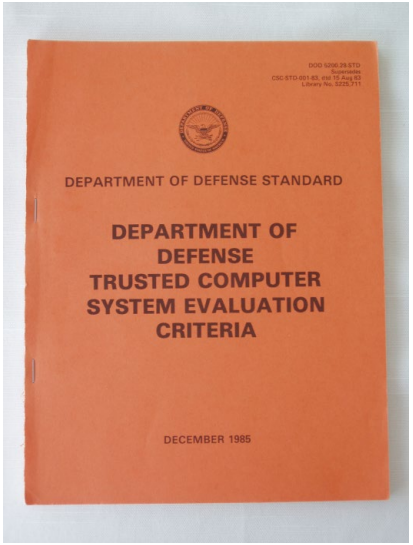


Auf dem Weg zu ISO 27000

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

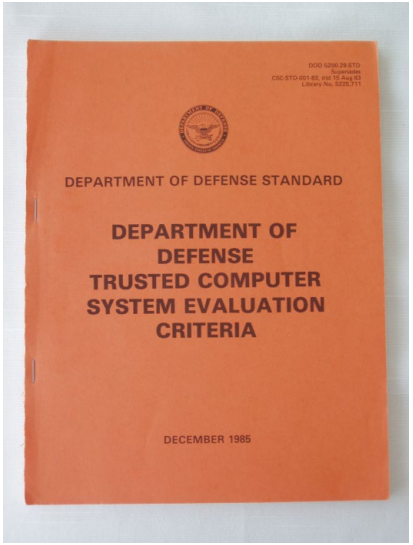


Auf dem Weg zu ISO 27000

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

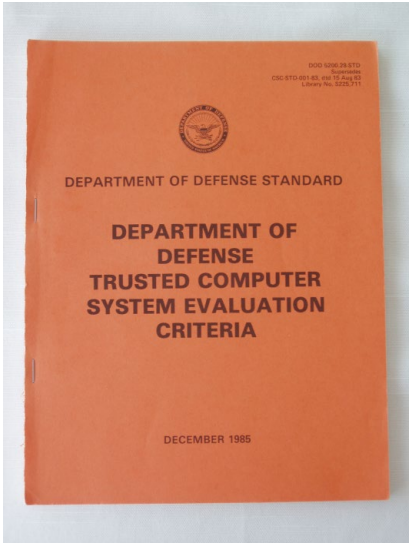


Auf dem Weg zu ISO 27000

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

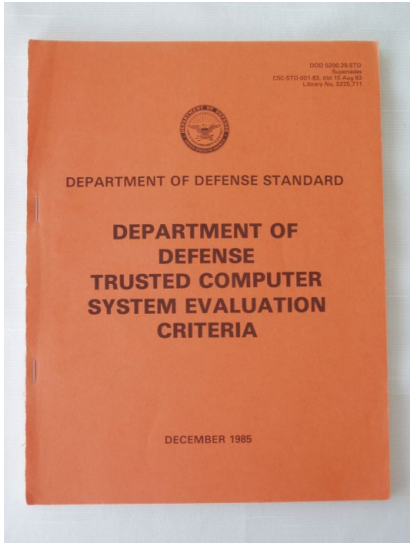
TCSEC ordnet Computersysteme in Stufen A, B, C und D ein:

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



Auf dem Weg zu ISO 27000

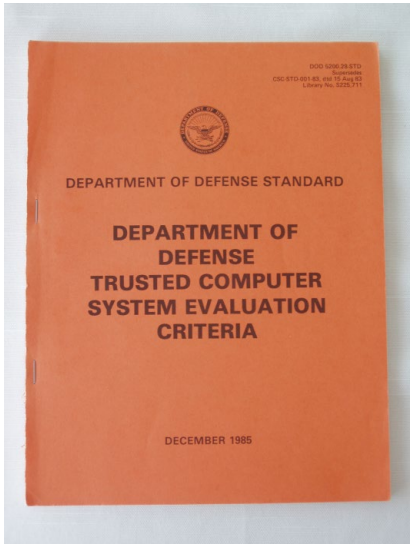
Ablösung durch die Common Criteria im Jahr 1996



Common Criteria

Auf dem Weg zu ISO 27000

Ablösung durch die Common Criteria im Jahr 1996



Common Criteria

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

Common Criteria

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

Common Criteria

MICROSOFT WINDOWSNT

Microsoft Wind[illegible]NT[illegible]t 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	Anforderungen	Leitfäden	Bereichspez. Leitfäden	Spezielle Leitfäden
ISO 27000	ISO 27001	ISO 27002-5	ISO 27010-11	ISO 2702x
	ISO 27006	ISO 27007-8	ISO 27017-19	ISO 2703x
	ISO 27006-2	ISO 27013-14	ISO 27701 A6	ISO 2704x
	ISO 27009	ISO 27021	ISO 27799	ISO 2710x
	ISO 27701-9			

Familie der ISO 2700-X

Übersicht	Anforderungen	Leitfäden	Bereichspez. Leitfäden	Spezielle Leitfäden
ISO 27000	**ISO 27001**	**ISO 27002-5**	ISO 27010-11	ISO 2702x
	ISO 27006	ISO 27007-8	ISO 27017-19	ISO 2703x
	ISO 27006-2	ISO 27013-14	ISO 27701 A6	ISO 2704x
	ISO 27009	ISO 27021	**ISO 27799**	ISO 2710x
	ISO 27701-9			

Familie der ISO 2700-X

Übersicht	Anforderungen	Leitfäden	Bereichspez. Leitfäden	Spezielle Leitfäden
ISO 27000	**ISO 27001**	**ISO 27002-5**	ISO 27010-11	ISO 2702x
	ISO 27006	ISO 27007-8	ISO 27017-19	ISO 2703x
	ISO 27006-2	ISO 27013-14	ISO 27701 A6	ISO 2704x
	ISO 27009	ISO 27021	**ISO 27799**	ISO 2710x
	ISO 27701-9			

Anforderungen an den Gesunheitssektor

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

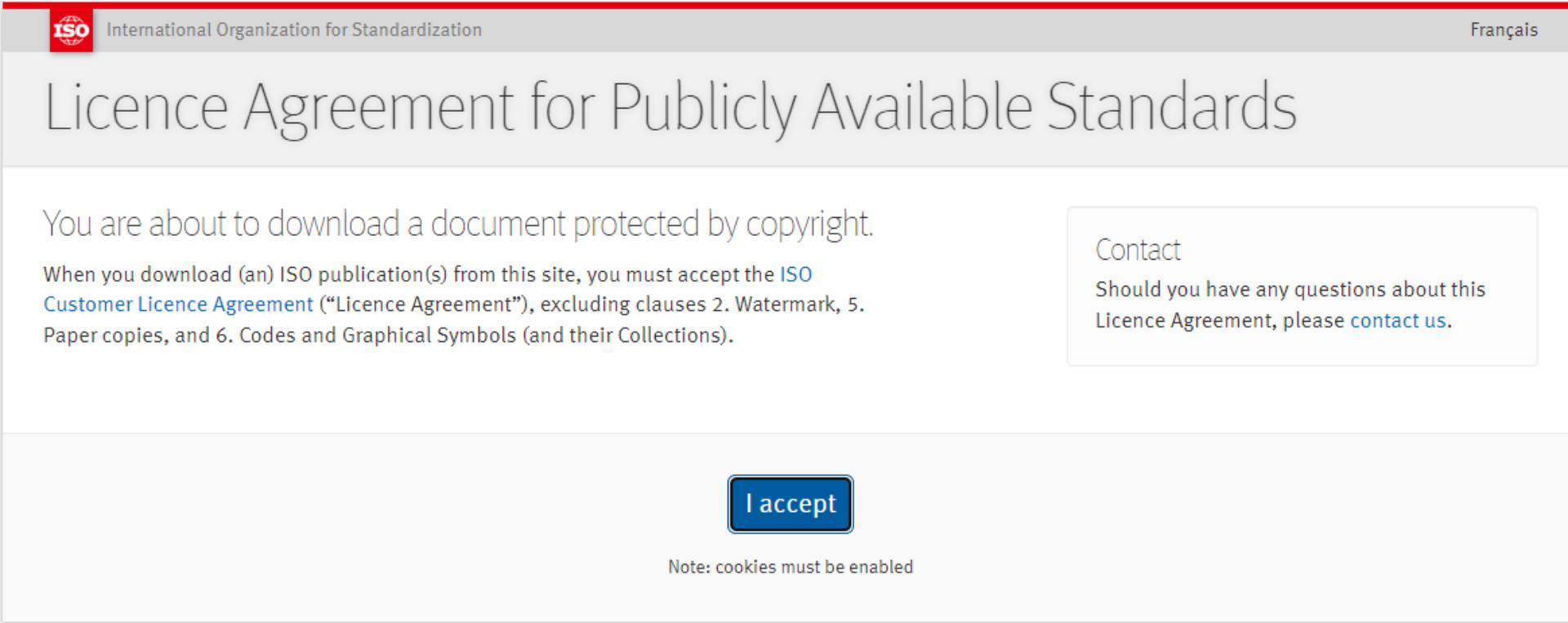
- Einsehbar in Norm Infopoints

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



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;

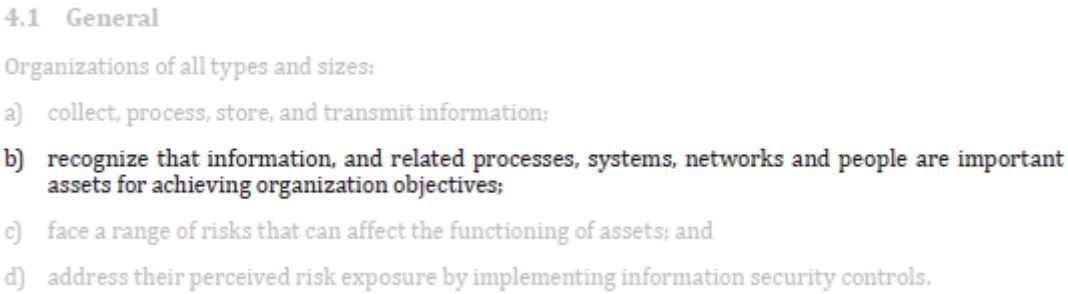
c) face a range of risks that can affect the functioning of assets; and

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.

Informationen

Prozesse

Netzwerke

Mitarbeiter

Risiken erkennen

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

Risiken erkennen

Sicherheit kontrollieren

Blick auf ISO 27000

Auszug aus Abschnitt 4

Informationen

Prozesse

Netzwerke

Mitarbeiter

Risiken erkennen

Sicherheit kontrollieren

Einbetten eines ISMS in die Organisation

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

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

Ausblick:

Infromationen – Verbindung zu Big Data und Data Sciences

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	Anforderungen	Leitfäden	Bereichspez. Leitfäden	Spezielle Leitfäden
ISO 27000	**ISO 27001**	ISO 27002-5	ISO 27010-11	ISO 2702x
	ISO 27006	ISO 27007-8	ISO 27017-19	ISO 2703x
	ISO 27006-2	ISO 27013-14	ISO 27701 A6	ISO 2704x
	ISO 27009	ISO 27021	ISO 27799	ISO 2710x
	ISO 27701-9			

Familie der ISO 2700-X

Übersicht

Anforderungen

ISO 27000

ISO 27001

DS-VGO

- Physische Sicherheit / Sicherheit in der Umgebung ⟷ Zutrittskontrolle
- Steuerung des Zugangs ⟷ Zugang und Zugriffskontrolle
- Kryptografie ⟷ Verschlüsselung
- Sicherheit der Kommunikation ⟷ Weitergabekontrolle
- Beziehung zu Lieferanten ⟷ Auftragskontrolle

Familie der ISO 2700-X

Übersicht

Anforderungen

Vieles ist parallel

ISO 27000 **ISO 27001** **DS-VGO**

- Physische Sicherheit / Sicherheit in der Umgebung ⟷ Zutrittskontrolle
- Steuerung des Zugangs ⟷ Zugang und Zugriffskontrolle
- Kryptografie ⟷ Verschlüsselung
- Sicherheit der Kommunikation ⟷ Weitergabekontrolle
- Beziehung zu Lieferanten ⟷ 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.

Sicherheitsüberprüfung im Ministerium

Familie der ISO 2700-X

Übersicht	Anforderungen	Leitfäden	Bereichspez. Leitfäden	Spezielle Leitfäden
ISO 27000	ISO 27001	**ISO 27002**-5	ISO 27010-11	ISO 2702x
	ISO 27006	ISO 27007-8	ISO 27017-19	ISO 2703x
	ISO 27006-2	ISO 27013-14	ISO 27701 A6	ISO 2704x
	ISO 27009	ISO 27021	ISO 27799	ISO 2710x
	ISO 27701-9			

Familie der ISO 2700-X

Leitfäden

ISO 27002

Kernleitfaden und
Hilfestellung bei der
Umsetzung von ISO 27001

Familie der ISO 2700-X

ISO 27002

- 9.3 Verantwortlichkeit des Benutzers

Kernleitfaden und Hilfestellung bei der Umsetzung von ISO 27001

Familie der ISO 2700-X

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

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 notwenigen Schutz Ihrer Anmeldedaten hingewiesen worden.“

Familie der ISO 2700-X

Leitfäden

ISO 27002

Familie der ISO 2700-X

Themen werden in späteren Vorlesungen diskutiert.

Leitfäden

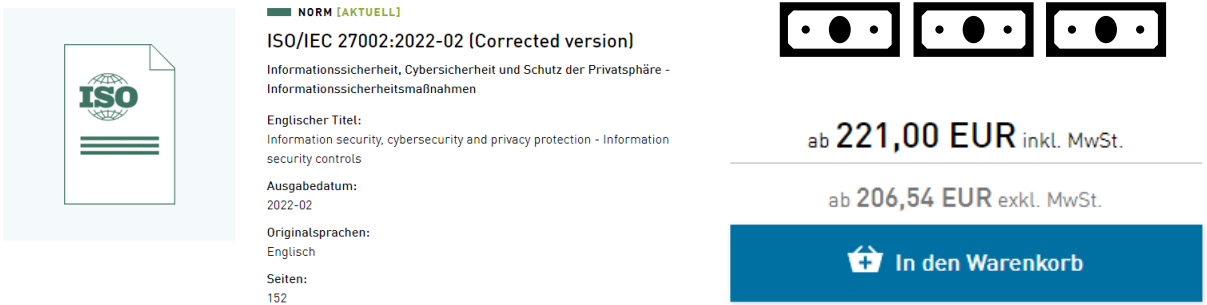
ISO 27002

Familie der ISO 2700-X

Leitfäden

ISO 27002

Spezifische Anleitung sind teuer.

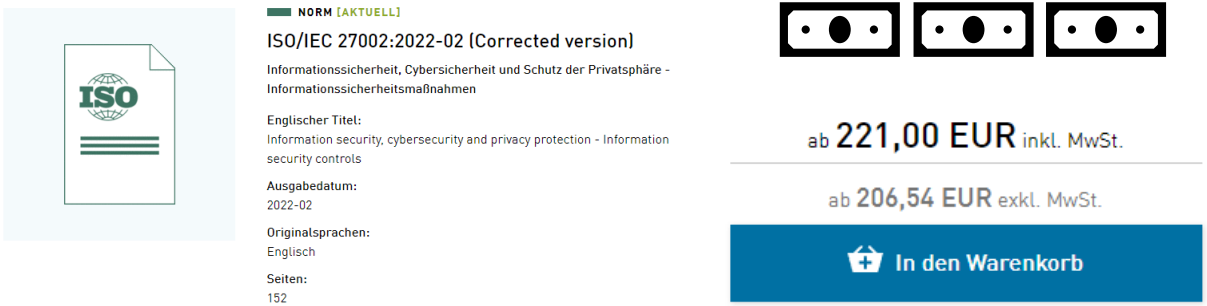


Familie der ISO 2700-X

Leitfäden

ISO 27002

Spezifische Anleitung sind teuer.



Familie der ISO 2700-X

Übersicht	Anforderungen	Leitfäden	Bereichspez. Leitfäden	Spezielle Leitfäden
ISO 27000	ISO 27001	ISO 27002-5	ISO 27010-11	ISO 2702x
	ISO 27006	ISO 27007-8	ISO 27017-19	ISO 2703x
	ISO 27006-2	ISO 27013-14	**ISO 27701 A6**	ISO 2704x
	ISO 27009	ISO 27021	ISO 27799	ISO 2710x
	ISO 27701-9			

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

Leitfäden

ISO 27002

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.

Familie der ISO 2700-X

Diskussion Home-Office

Leitfäden

ISO 27002

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.

- 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

Leitfäden

ISO 27002

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.

Familie der ISO 2700-X

Diskussion Home-Office

Leitfäden

ISO 27002

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;

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;

Leitfäden

ISO 27002

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.

Leitfäden

ISO 27002

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

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.

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.

Was schlagen Sie vor?

Familie der ISO 2700-X

Diskussion Home-Office

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.

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.

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.