

# Organisatorische Richtlinien und Rechtliche Rahmenbedingungen

## **Modul D3.2**

Referent: Dr. Jörg Cosfeld

# Bundesamt für Sicherheit in der Informationstechnik



Bundesamt  
für Sicherheit in der  
Informationstechnik

Das **Bundesamt für Sicherheit in der Informationstechnik** (BSI) ist eine deutsche **Bundesoberbehörde** im Geschäftsbereich des Bundesministeriums des Innern und für Heimat mit Sitz in Bonn

# Bundesamt für Sicherheit in der Informationstechnik



Bundesamt  
für Sicherheit in der  
Informationstechnik

Das **Bundesamt für Sicherheit in der Informationstechnik** (BSI) ist eine deutsche **Bundesoberbehörde** im Geschäftsbereich des Bundesministeriums des Innern und für Heimat mit Sitz in Bonn

**1.290 Stellen**

# Bundesamt für Sicherheit in der Informationstechnik



Bundesamt  
für Sicherheit in der  
Informationstechnik

Das BSI veröffentlicht  
regelmäßig Studien,  
Richtlinien, Infoblätter und  
Broschüren zum Thema IT-  
Sicherheit.

# Bundesamt für Sicherheit in der Informationstechnik

Vorgabe einer  
Sicherheitslinie



Ziel anzustrebendes Niveau der  
**Informationssicherheit** in einer **Institution**  
heben.



Das BSI veröffentlicht  
regelmäßig Studien,  
Richtlinien, Infoblätter und  
Broschüren zum Thema IT-  
Sicherheit.

# Bundesamt für Sicherheit in der Informationstechnik

Vorgabe einer  
Sicherheitslinie



Ziel anzustrebendes Niveau der  
**Informationssicherheit** in einer **Institution**  
heben.



Das BSI veröffentlicht  
regelmäßig Studien,  
Richtlinien, Infoblätter und  
Broschüren zum Thema IT-  
Sicherheit.

# Bundesamt für Sicherheit in der Informationstechnik

Eine Sicherheitsrichtlinie umfasst folgende Elemente:

- Wenige Seite fassen Maßnahmen treffend zusammen
- Leitung definiert und updated die Linie

Zitat:

Die Leitlinie muss **allen betroffenen Mitarbeitern bekannt gegeben** und **kontinuierlich aktualisiert** werden.

# Bundesamt für Sicherheit in der Informationstechnik

Eine Sicherheitsrichtlinie umfasst folgende Elemente:

- Wenige Seite fassen Maßnahmen treffend zusammen
- Leitung definiert und updated die Linie
- Geltungsbereich definieren
- Definition wann Verletzungen vorliegen
- Initiierung von Sicherheitsprozessen
  - Schulungen etc.
- Organisationsstrukturen und Sicherheitsverantwortliche werden vorgestellt



# Bundesamt für Sicherheit in der Informationstechnik

Eine Sicherheitsrichtlinie umfasst folgende Elemente:

- Wenige Seite fassen Maßnahmen treffend zusammen
- Leitung definiert und updated die Linie
- Geltungsbereich definieren
- Definition wann Verletzungen vorliegen
- Initiierung von Sicherheitsprozessen
  - Schulungen etc.
- Organisationsstrukturen und Sicherheitsverantwortliche werden vorgestellt

# Bundesamt für Sicherheit in der Informationstechnik

Auf dem Weg zur Sicherheitslinie

**Schnell verloren im umfangreichen BSI Grundschutz.**

Nehmen wir an jede  
Seite des BSI  
Grundschutzes ist  
ein Baum.

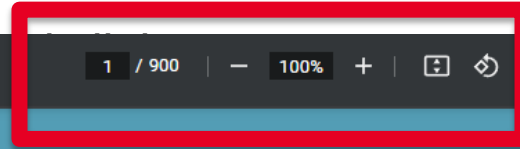


# Bundesamt für Sicherheit in der Informationstechnik

Auf dem Weg z

Schnell verloren

Nehm  
Seite o  
Grund  
ein Ba



Bundesamt  
für Sicherheit in der  
Informationstechnik

## IT-Grundschutz- Kompodium



# Bundesamt für Sicherheit in der Informationstechnik

Auf dem Weg zur Sicherheitslinie

**Schnell verloren im umfangreichen BSI  
Grundschutz.**

# Bundesamt für Sicherheit in der Informationstechnik

## Elementare Gefährdungen

- G 0.1 Feuer
- G 0.2 Ungünstige klimatische Bedingungen
- G 0.3 Wasser
- G 0.4 Verschmutzung, Staub, Korrosion
- G 0.5 Naturkatastrophen
- G 0.6 Katastrophen im Umfeld
- G 0.7 Großereignisse im Umfeld
- G 0.8 Ausfall oder Störung der Stromversorgung
- G 0.9 Ausfall oder Störung von Kommunikationsnetzen
- G 0.10 Ausfall oder Störung von Versorgungsnetzen
- G 0.11 Ausfall oder Störung von Dienstleistern
- G 0.12 Elektromagnetische Störstrahlung
- G 0.13 Abfangen kompromittierender Strahlung
- G 0.14 Ausspähen von Informationen (Spionage)
- G 0.15 Abhören
- G 0.16 Diebstahl von Geräten, Datenträgern oder Dokumenten
- G 0.17 Verlust von Geräten, Datenträgern oder Dokumenten
- G 0.18 Fehlplanung oder fehlende Anpassung
- G 0.19 Offenlegung schützenswerter Informationen
- G 0.20 Informationen oder Produkte aus unzuverlässiger Quelle
- G 0.21 Manipulation von Hard- oder Software
- G 0.22 Manipulation von Informationen
- G 0.23 Unbefugtes Eindringen in IT-Systeme
- G 0.24 Zerstörung von Geräten oder Datenträgern
- G 0.25 Ausfall von Geräten oder Systemen
- G 0.26 Fehlfunktion von Geräten oder Systemen
- G 0.27 Ressourcenmangel
- G 0.28 Software-Schwachstellen oder -Fehler
- G 0.29 Verstoß gegen Gesetze oder Regelungen
- G 0.30 Unberechtigte Nutzung oder Administration von Geräten und Systemen
- G 0.31 Fehlerhafte Nutzung oder Administration von Geräten und Systemen
- G 0.32 Missbrauch von Berechtigungen
- G 0.33 Personalausfall
- G 0.34 Anschlag
- G 0.35 Nötigung, Erpressung oder Korruption
- G 0.36 Identitätsdiebstahl
- G 0.37 Abstreiten von Handlungen
- G 0.38 Missbrauch personenbezogener Daten

- G 0.39 Schadprogramme
- G 0.40 Verhinderung von Diensten (Denial of Service)
- G 0.41 Sabotage
- G 0.42 Social Engineering
- G 0.43 Einspielen von Nachrichten
- G 0.44 Unbefugtes Eindringen in Räumlichkeiten
- G 0.45 Datenverlust
- G 0.46 Integritätsverlust schützenswerter Informationen
- G 0.47 Schädliche Seiteneffekte IT-gestützter Angriffe

## Prozess-Bausteine

- ISMS: Sicherheitsmanagement
- ISMS.1 Sicherheitsmanagement
- ORP: Organisation und Personal
- ORP.1 Organisation
- ORP.2 Personal
- ORP.3 Sensibilisierung und Schulung zur Informationssicherheit
- ORP.4 Identitäts- und Berechtigungsmanagement
- ORP.5 Compliance Management (Anforderungsmanagement)
- CON: Konzepte und Vorgehensweisen
- CON.1 Kryptokonzept
- CON.2 Datenschutz
- CON.3 Datensicherungskonzept
- CON.6 Löschen und Vernichten
- CON.7 Informationssicherheit auf Auslandsreisen
- CON.8 Software-Entwicklung
- CON.9 Informationsaustausch
- CON.10 Entwicklung von Webanwendungen

## OPS: Betrieb

- OPS.1 Eigener Betrieb
- OPS.1.1 Kern-IT-Betrieb
  - OPS.1.1.2 Ordnungsgemäße IT-Administration
  - OPS.1.1.3 Patch- und Änderungsmanagement
  - OPS.1.1.4 Schutz vor Schadprogrammen
  - OPS.1.1.5 Protokollierung
  - OPS.1.1.6 Software-Tests und -Freigaben
  - OPS.1.1.7 Systemmanagement
- OPS.1.2 Weiterführende Aufgaben
  - OPS.1.2.2 Archivierung
  - OPS.1.2.4 Telearbeit
  - OPS.1.2.5 Fernwartung
  - OPS.1.2.6 NTP-Zeitsynchronisation
- OPS.2 Betrieb von Dritten
  - OPS.2.1 Outsourcing für Kunden
  - OPS.2.2 Cloud-Nutzung
- OPS.3 Betrieb für Dritte
  - OPS.3.1 Outsourcing für Dienstleister

## DER: Detektion und Reaktion

- DER.1 Detektion von sicherheitsrelevanten Ereignissen
- DER.2 Security Incident Management
  - DER.2.1 Behandlung von Sicherheitsvorfällen
  - DER.2.2 Vorsorge für die IT-Forensik
  - DER.2.3 Bereinigung weitreichender Sicherheitsvorfälle
- DER.3 Sicherheitsprüfungen
  - DER.3.1 Audits und Revisionen
  - DER.3.2 Revisionen auf Basis des Leitfadens IS-Revision
- DER.4 Notfallmanagement

## System-Bausteine

### APP: Anwendungen

- APP.1 Client-Anwendungen
  - APP.1.1 Office-Produkte
  - APP.1.2 Webbrowser
  - APP.1.4 Mobile Anwendungen (Apps)
- APP.2 Verzeichnisdienst
  - APP.2.1 Allgemeiner Verzeichnisdienst
  - APP.2.2 Active Directory
  - APP.2.3 OpenLDAP
- APP.3 Netzbasierte Dienste
  - APP.3.1 Webanwendungen und Webservices
  - APP.3.2 Webserver
  - APP.3.3 Fileserver
  - APP.3.4 Samba
  - APP.3.6 DNS-Server
- APP.4 Business-Anwendungen
  - APP.4.1 SAP-ERP-System
  - APP.4.3 Relationale Datenbanken
  - APP.4.4 Kubernetes
  - APP.4.6 SAP ABAP-Programmierung
- APP.5 E-Mail/Groupware/Kommunikation
  - APP.5.2 Microsoft Exchange und Outlook
  - APP.5.3 Allgemeiner E-Mail-Client und -Server
- APP.6 Allgemeine Software
- APP.7 Entwicklung von Individualsoftware

### SYS: IT-Systeme

- SYS.1 Server
  - SYS.1.1 Allgemeiner Server
  - SYS.1.2 Windows Server
    - SYS.1.2.2 Windows Server 2012
  - SYS.1.3 Server unter Linux und Unix
  - SYS.1.5 Virtualisierung
  - SYS.1.6 Containerisierung
  - SYS.1.7 IBM Z
  - SYS.1.8 Speicherlösungen

### SYS.2 Desktop-Systeme

- SYS.2.1 Allgemeiner Client
- SYS.2.2 Windows-Clients
  - SYS.2.2.2 Clients unter Windows 8.1
  - SYS.2.2.3 Clients unter Windows 10
- SYS.2.3 Clients unter Linux und Unix
- SYS.2.4 Clients unter macOS
- SYS.3 Mobile Devices
  - SYS.3.1 Laptops
  - SYS.3.2 Tablet und Smartphone
    - SYS.3.2.1 Allgemeine Smartphones und Tablets
    - SYS.3.2.2 Mobile Device Management (MDM)
    - SYS.3.2.3 iOS (for Enterprise)
    - SYS.3.2.4 Android
  - SYS.3.3 Mobiltelefon
- SYS.4 Sonstige Systeme
  - SYS.4.1 Drucker, Kopierer und Multifunktionsgeräte
  - SYS.4.3 Eingebettete Systeme
  - SYS.4.4 Allgemeines IoT-Gerät
  - SYS.4.5 Wechseldatenträger

### IND: Industrielle IT

- IND.1 Prozessleit- und Automatisierungstechnik
- IND.2 ICS-Komponenten
  - IND.2.1 Allgemeine ICS-Komponente
  - IND.2.2 Speicherprogrammierbare Steuerung (SPS)
  - IND.2.3 Sensoren und Aktoren
  - IND.2.4 Maschine
  - IND.2.7 Safety Instrumented Systems
- IND.3 Produktionsnetze
  - IND.3.2 Fernwartung im industriellen Umfeld

### NET: Netze und Kommunikation

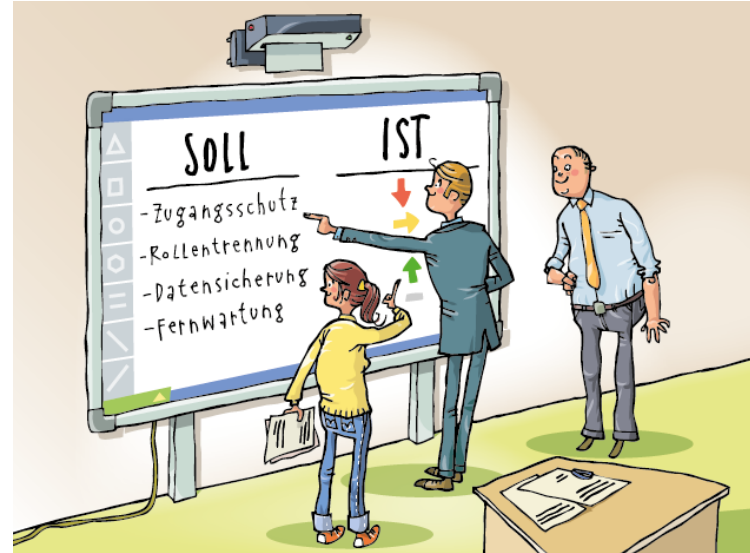
- NET.1 Netze
  - NET.1.1 Netzarchitektur und -design
  - NET.1.2 Netzmanagement
- NET.2 Funknetze
  - NET.2.1 WLAN-Betrieb
  - NET.2.2 WLAN-Nutzung
- NET.3 Netzkomponenten
  - NET.3.1 Router und Switches
  - NET.3.2 Firewall
  - NET.3.3 VPN
- NET.4 Telekommunikation
  - NET.4.1 TK-Anlagen
  - NET.4.2 VoIP
  - NET.4.3 Faxgeräte und Faxserver

### INF: Infrastruktur

- INF.1 Allgemeines Gebäude
- INF.2 Rechenzentrum sowie Serverraum
- INF.5 Raum sowie Schrank für technische Infrastruktur
- INF.6 Datenträgerarchiv
- INF.7 Büroarbeitsplatz
- INF.8 Häuslicher Arbeitsplatz
- INF.9 Mobiler Arbeitsplatz
- INF.10 Besprechungs-, Veranstaltungs- und Schulungsräume
- INF.11 Allgemeines Fahrzeug
- INF.12 Verkabelung
- INF.13 Technisches Gebäudemanagement
- INF.14 Gebäudeautomation

# Bundesamt für Sicherheit in der Informationstechnik

Lassen Sie uns versuchen die Kernbausteine zu verstehen.



# Bundesamt für Sicherheit in der Informationstechnik

Es gilt zu klären:

Was ergibt eine **Strukturanalyse** der IT Systeme, Räume und Anwendungen?

Bestimmung des **Schutzbedarfes**.

Definition eines **Prüfplans** und dessen Anwendung.

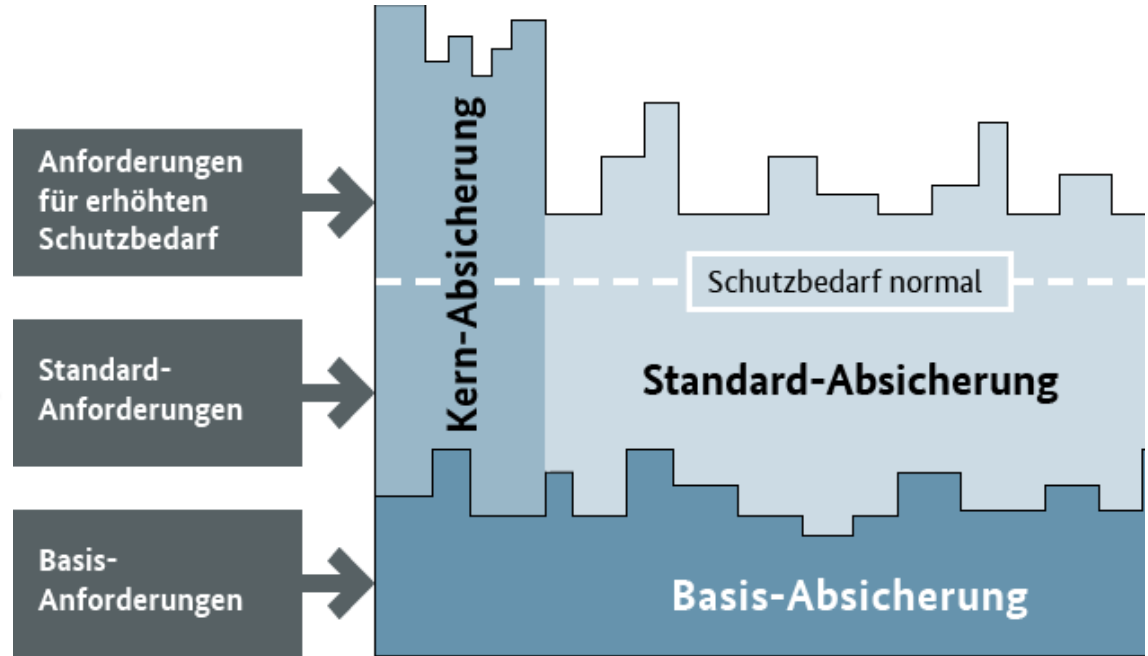


# Bundesamt für Sicherheit in der Informationstechnik

Die Grundsatzfrage ist ein Soll-Ist Vergleich der Anforderungen und des bereits Erreichten.

# Bundesamt für Sicherheit in der Informationstechnik

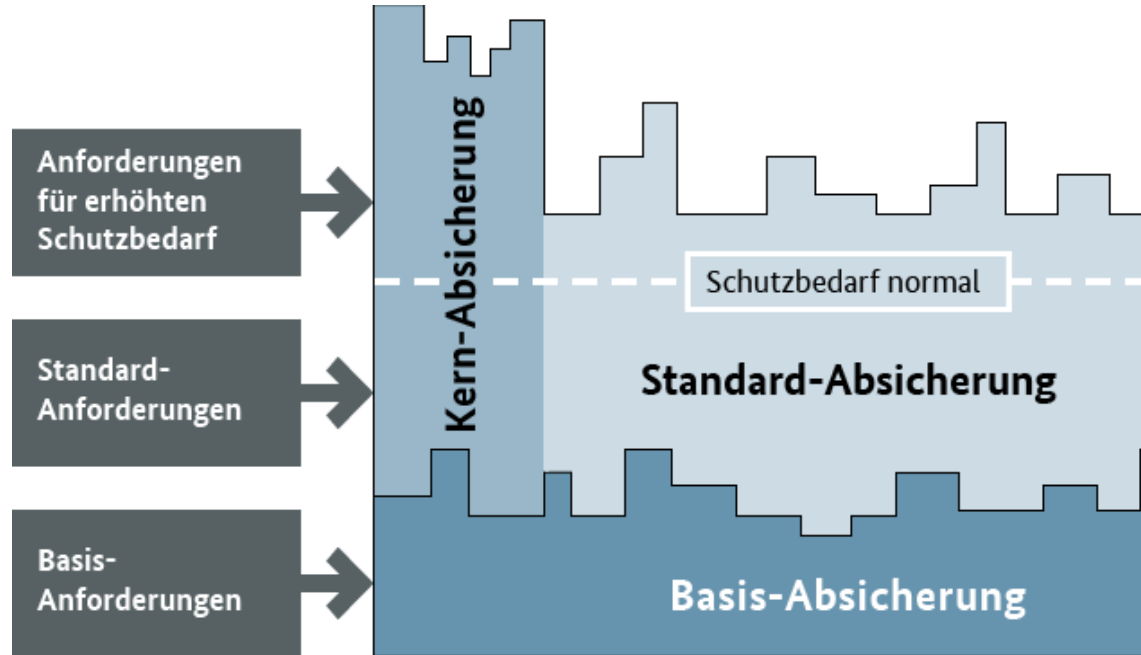
Ein Unternehmen gliedert ihre Bedarfe in drei Anforderungsstufen.



# Bundesamt für Sicherheit in der Informationstechnik

Beispiele:

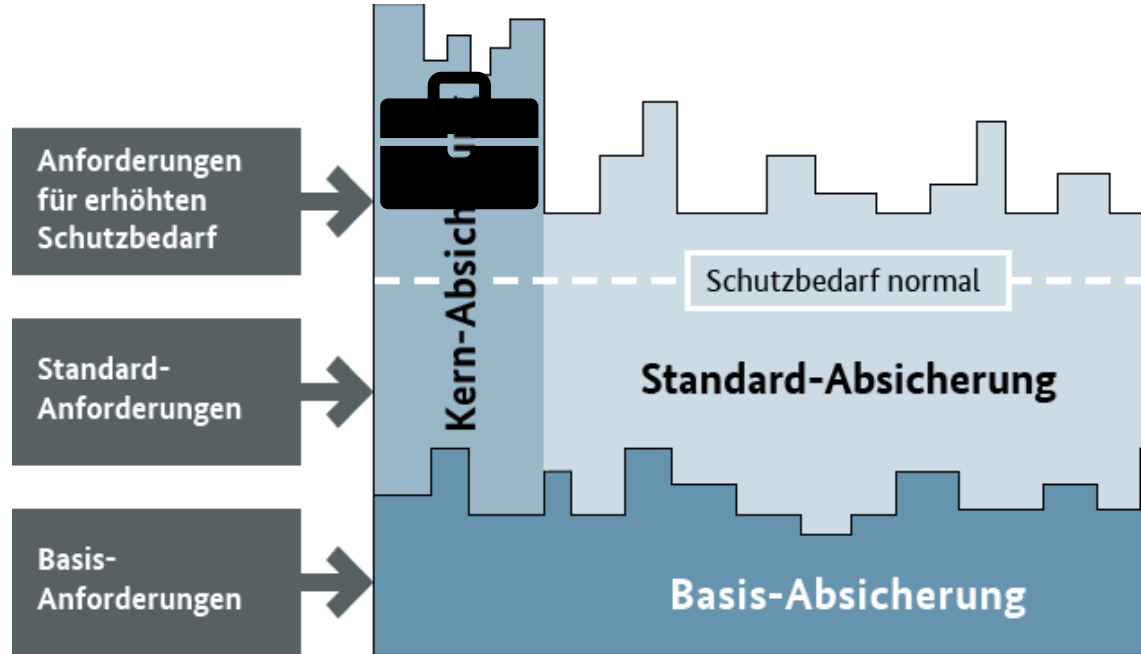
Personalak  
ten?



# Bundesamt für Sicherheit in der Informationstechnik

Beispiele:

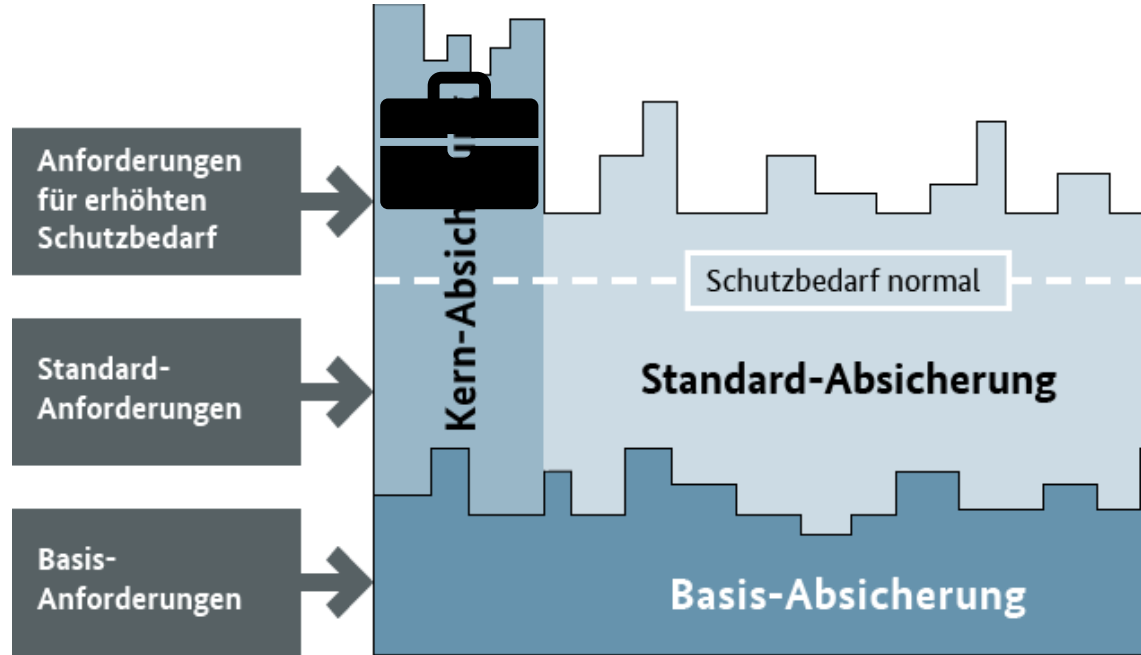
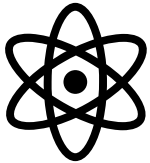
Personalak  
ten?



# Bundesamt für Sicherheit in der Informationstechnik

Beispiele:

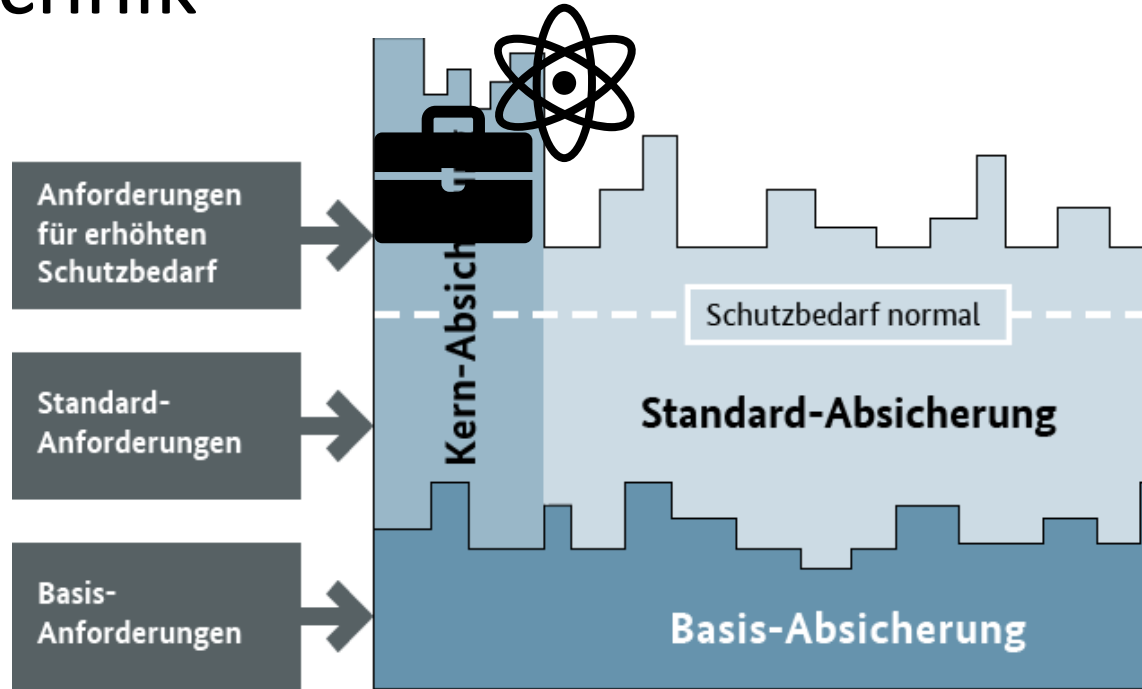
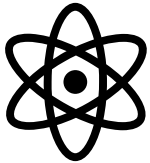
Gedanken  
gut von  
Wissensch  
aftlern?



# Bundesamt für Sicherheit in der Informationstechnik

Beispiele:

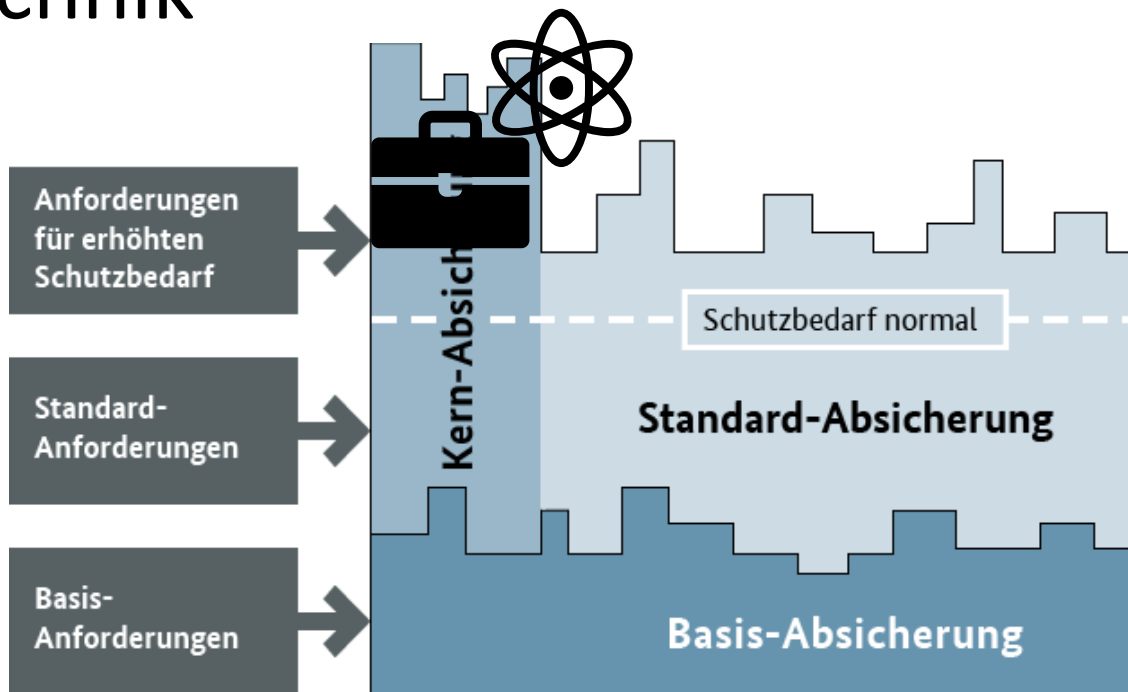
Gedanken  
gut von  
Wissensch  
aftlern?



# Bundesamt für Sicherheit in der Informationstechnik

Beispiele:

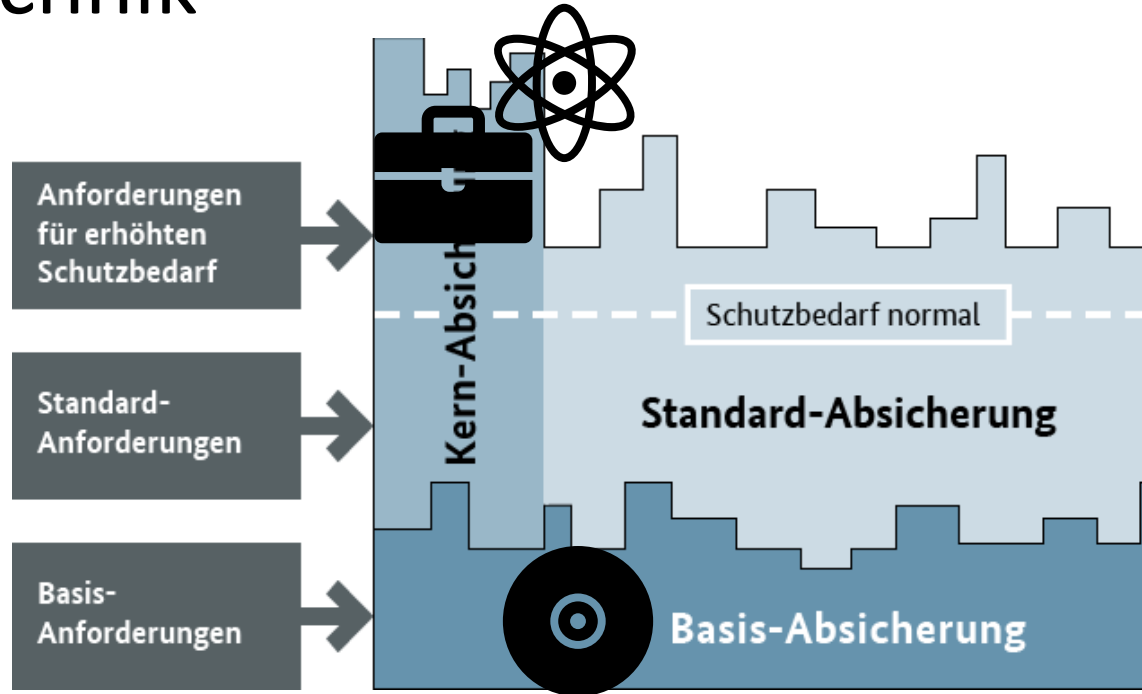
Recherche  
Downloads  
?



# Bundesamt für Sicherheit in der Informationstechnik

Beispiele:

Recherche  
Downloads  
?

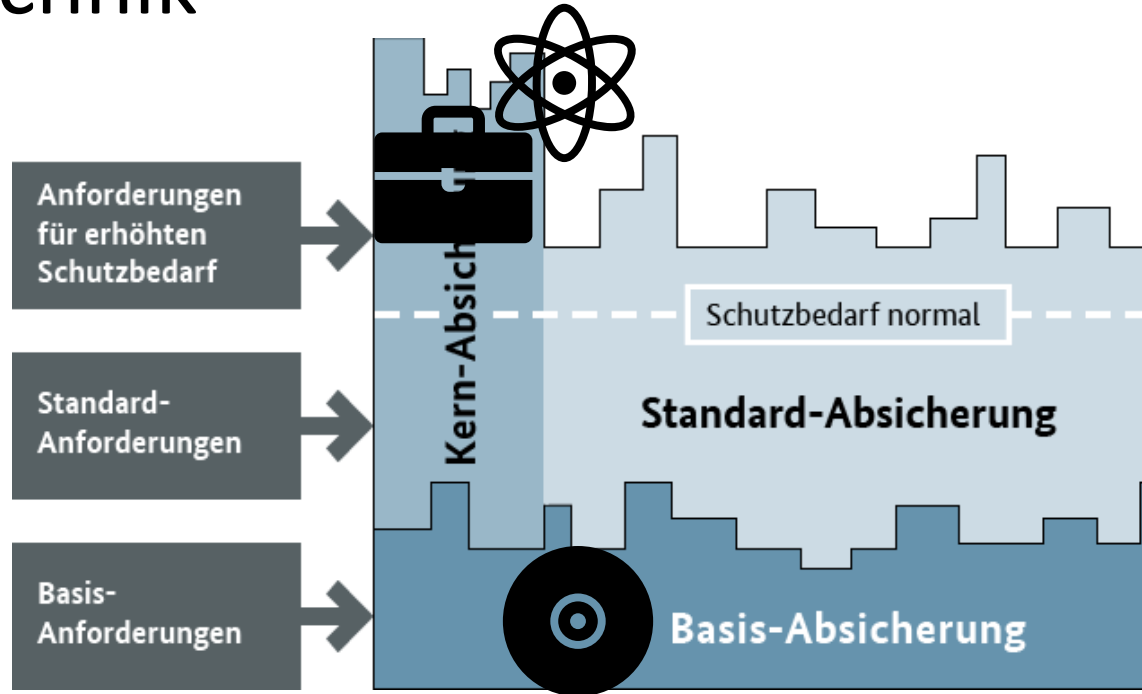




# Bundesamt für Sicherheit in der Informationstechnik

Beispiele:

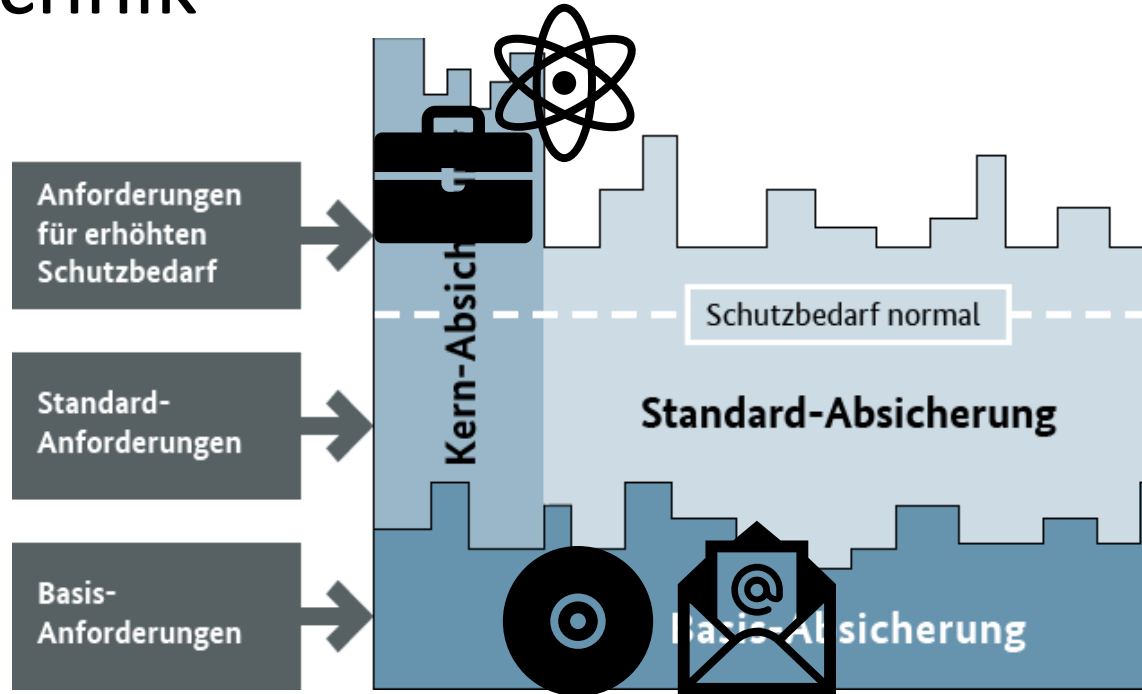
WerbeMail  
s?



# Bundesamt für Sicherheit in der Informationstechnik

Beispiele:

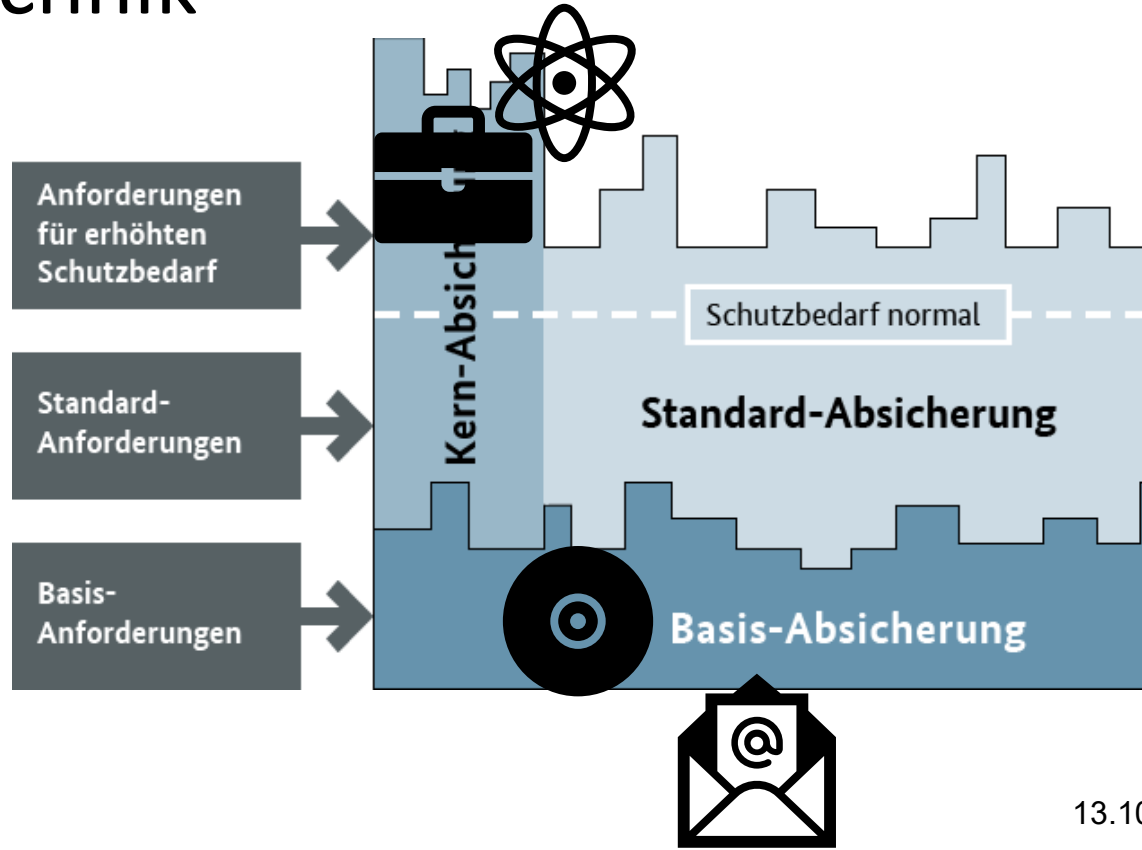
WerbeMail  
s?



# Bundesamt für Sicherheit in der Informationstechnik

Beispiele:

WerbeMail  
s?



# Bundesamt für Sicherheit in der Informationstechnik

Wie geht man nach den  
Empfehlungen des BSI  
vor?

# Bundesamt für Sicherheit in der Informationstechnik

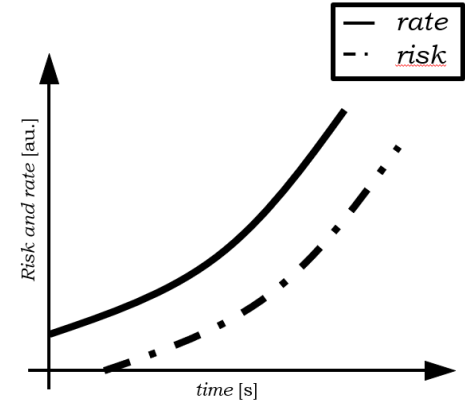
Wie geht man nach den  
Empfehlungen des BSI  
vor?

Die Informationstechnik ändert sich  
**kontinuierlich**, sodass **regelmäßig geprüft**  
werden muss, ob die eingeführten  
Sicherheitsmaßnahmen noch einen  
angemessenen Schutz bieten.

# Bundesamt für Sicherheit in der Informationstechnik

Wie geht man nach den Empfehlungen des BSI vor?

**Reminder**

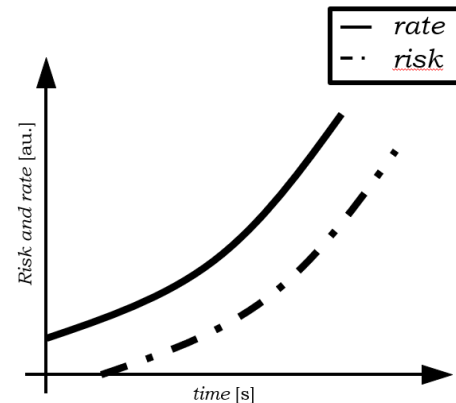


Die Informationstechnik ändert sich **kontinuierlich**, sodass **regelmäßig geprüft** werden muss, ob die eingeführten Sicherheitsmaßnahmen noch einen angemessenen Schutz bieten.

# Bundesamt für Sicherheit in der Informationstechnik

Wie geht man nach den Empfehlungen des BSI vor?

Reminder



Die Informationstechnik ändert sich **kontinuierlich**, sodass **regelmäßig geprüft** werden muss, ob die eingeführten Sicherheitsmaßnahmen noch einen angemessenen Schutz bieten.



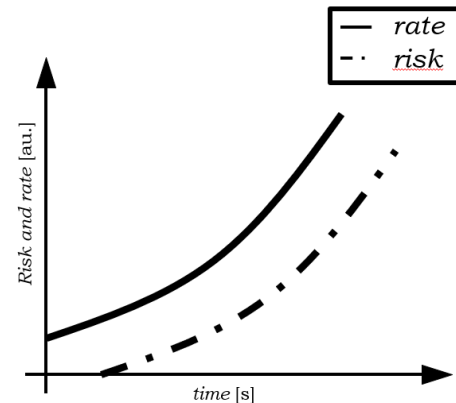
**IT-Grundschutz-  
Kompodium**

wird  
angepasst.

# Bundesamt für Sicherheit in der Informationstechnik

Wie geht man nach den Empfehlungen des BSI vor?

Reminder



Die Informationstechnik ändert sich **kontinuierlich**, sodass **regelmäßig geprüft** werden muss, ob die eingeführten Sicherheitsmaßnahmen noch einen angemessenen Schutz bieten.



**Wald wird noch dichter.**



# Bundesamt für Sicherheit in der Informationstechnik

Wie geht man nach den Empfehlungen des BSI vor?

Wählen Sie geeignete Ansprechpartner aus. Klären Sie in diesem Zusammenhang auch, ob externe Stellen **hinzuzuziehen** sind, z. B. **Fremdfirmen**,

# Bundesamt für Sicherheit in der Informationstechnik

Wie geht man nach den Empfehlungen des BSI vor?

**Vier Augen und Ohren sehen und hören** mehr als zwei. Führen Sie die **Interviews** nach Möglichkeit daher **nicht alleine durch**.

# Bundesamt für Sicherheit in der Informationstechnik

Wie geht man nach den Empfehlungen des BSI vor?

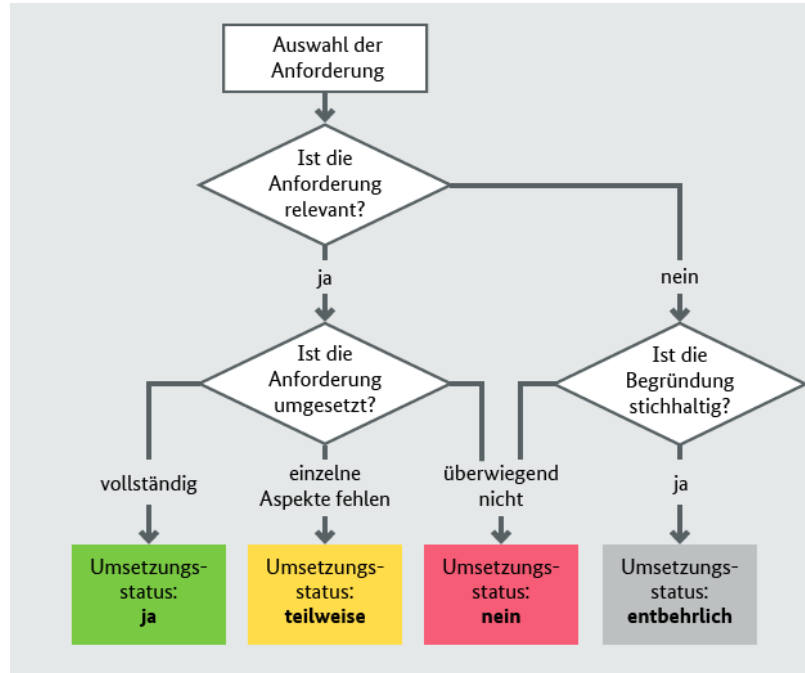
**Vier Augen und Ohren sehen und hören** mehr als zwei. Führen Sie die **Interviews** nach Möglichkeit daher **nicht alleine durch**.



BSI leitet klaren Bedarf an „Manpower“ ab

# Bundesamt für Sicherheit in der Informationstechnik

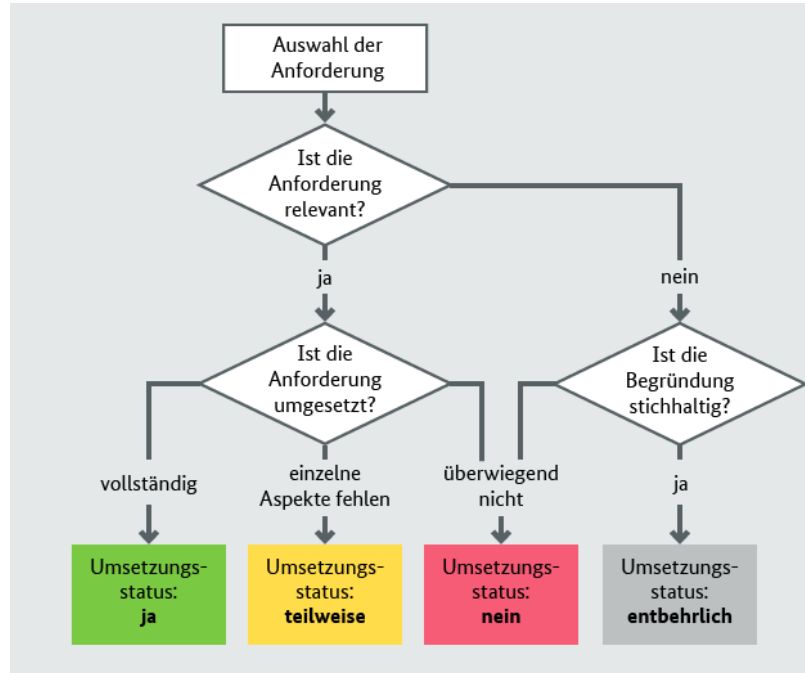
Informationen sind dann in folgende Kategorien zu unterteilen.



# Bundesamt für Sicherheit in der Informationstechnik

Informationen sind dann in folgende Kategorien zu unterteilen.

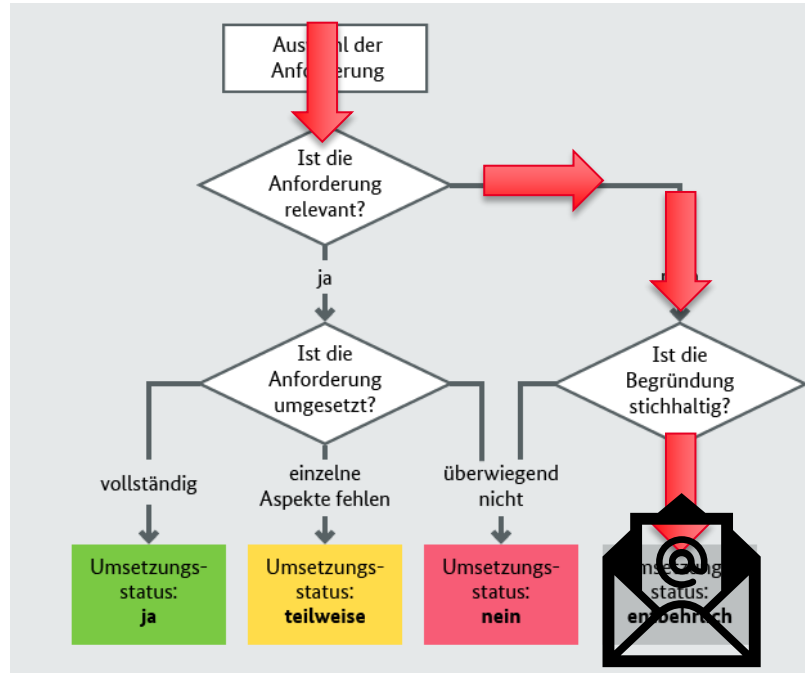
WerbeMail  
s?



# Bundesamt für Sicherheit in der Informationstechnik

Informationen sind dann  
in folgende Kategorien  
zu unterteilen.

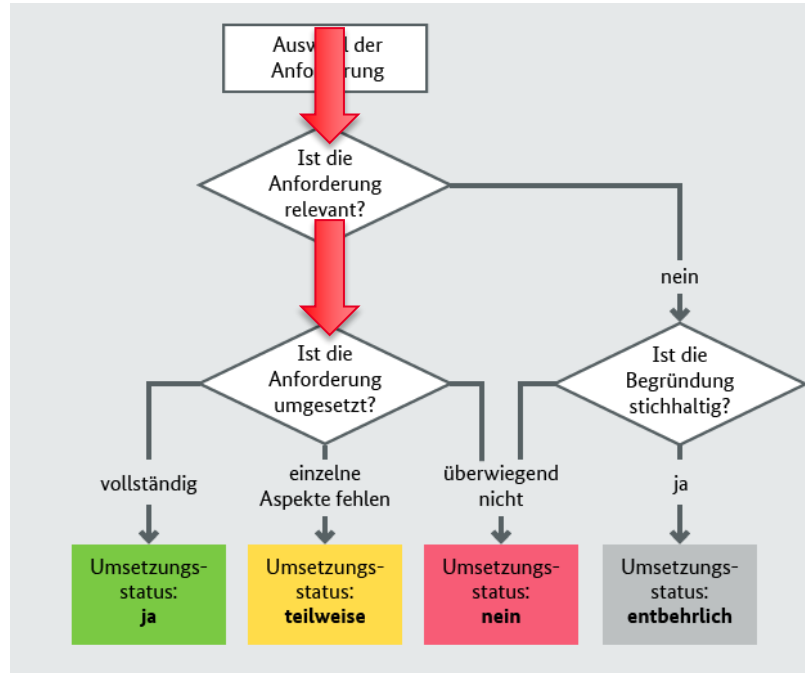
WerbeMail  
s?



# Bundesamt für Sicherheit in der Informationstechnik

Informationen sind dann  
in folgende Kategorien  
zu unterteilen.

Personalak  
ten?



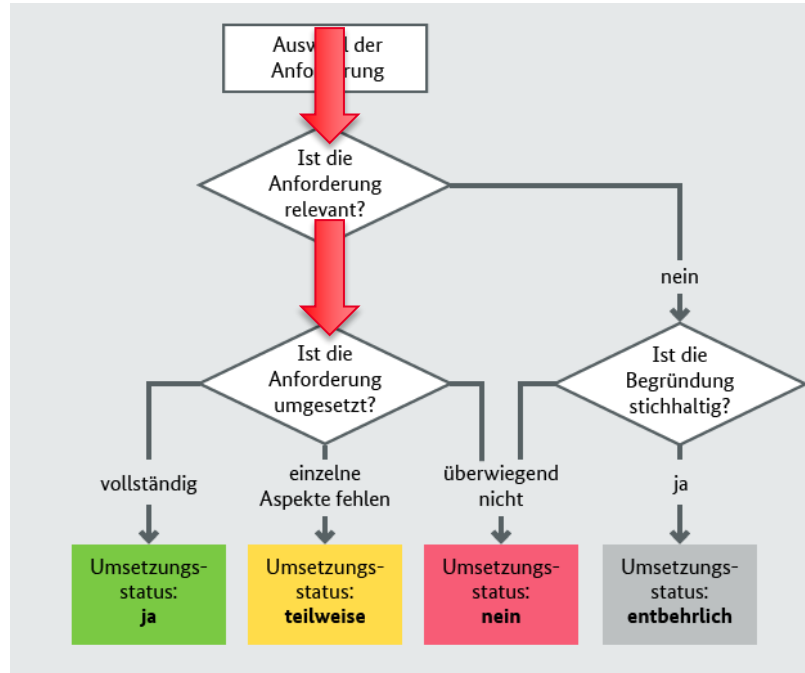
# Bundesamt für Sicherheit in der Informationstechnik

Informationen sind dann in folgende Kategorien zu unterteilen.

Personalakten?



**Liegen auf  
Immutable Backup  
Server mit  
Schleusensystem.**





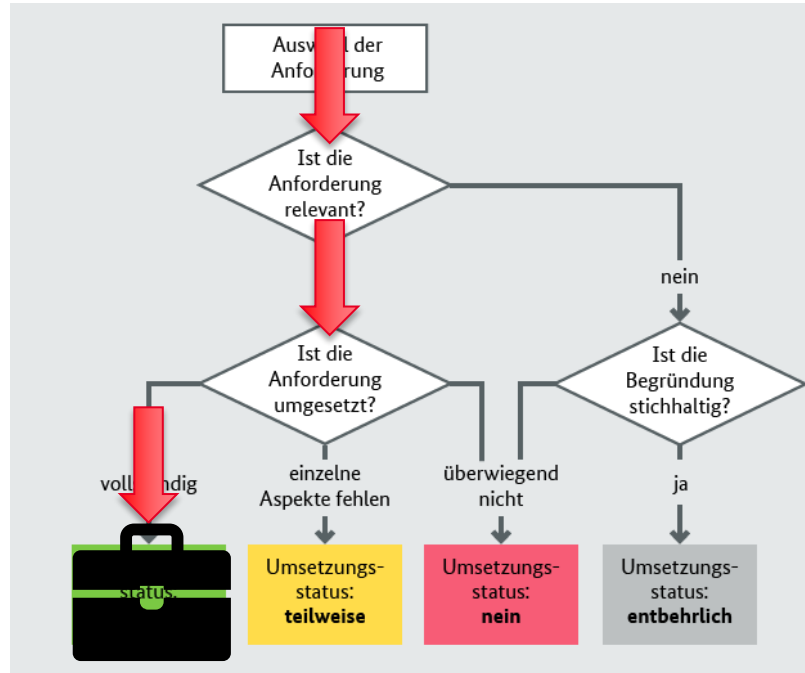
# Bundesamt für Sicherheit in der Informationstechnik

Informationen sind dann in folgende Kategorien zu unterteilen.

Personalakten?



Liegen auf  
Immutable Backup  
Server mit  
Schleusensystem.



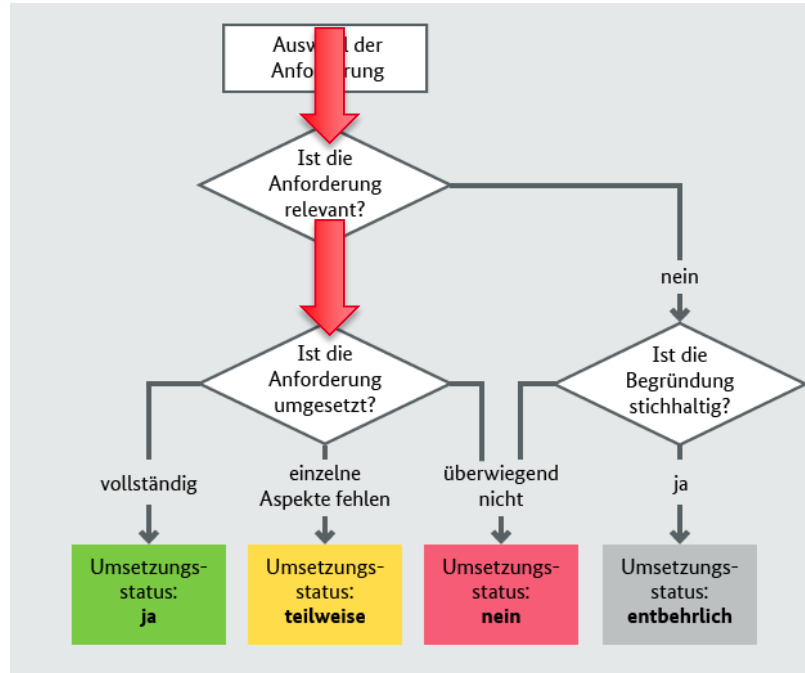
# Bundesamt für Sicherheit in der Informationstechnik

Informationen sind dann in folgende Kategorien zu unterteilen.

Personalakten?



**Liegen auf HDD eines PCs in der Personalverwaltung.**



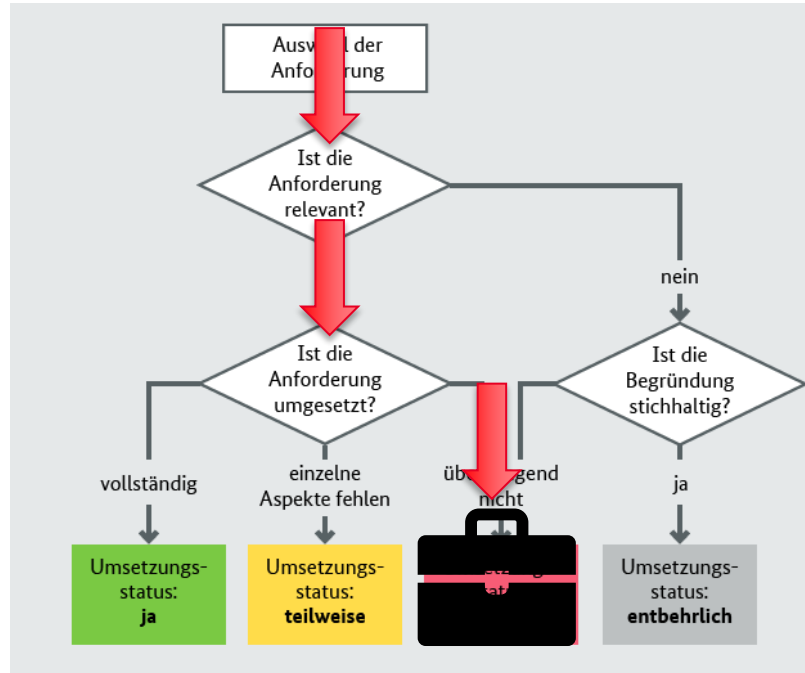
# Bundesamt für Sicherheit in der Informationstechnik

Informationen sind dann in folgende Kategorien zu unterteilen.

Personalakten?



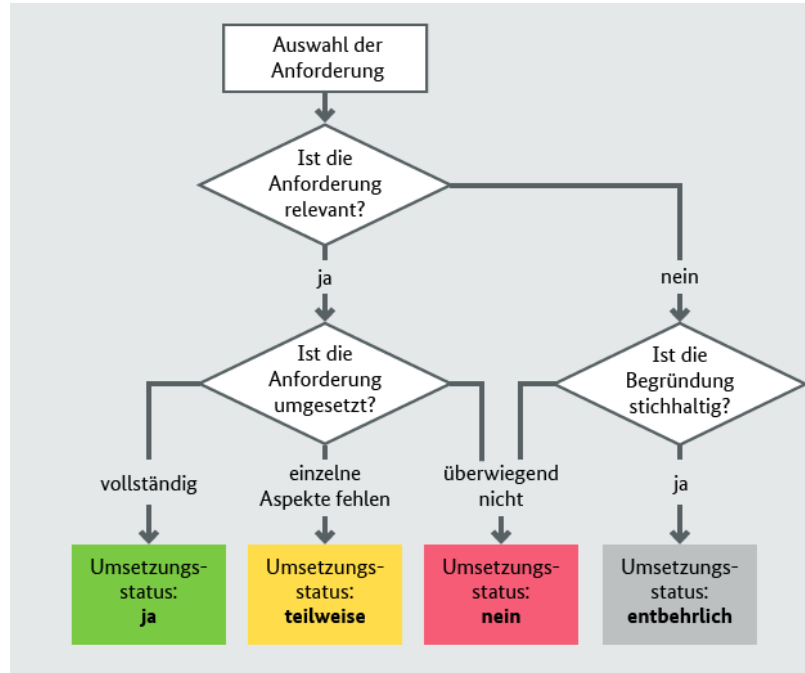
Liegen auf HDD eines PCs in der Personalverwaltung.



# Bundesamt für Sicherheit in der Informationstechnik

Informationen sind dann in folgende Kategorien zu unterteilen.

Festhalten in Checklisten.



# Bundesamt für Sicherheit in der Informationstechnik

Informationen sind dann  
in folgende Kategorien  
zu unterteilen.


Festhalten in  
Checklisten.

# Bundesamt für Sicherheit in der Informationstechnik

Informationen sind dann  
in folgende Kategorien  
zu unterteilen.

Festhalten in  
Checklisten.

ITIS-Check_APP.1.1 Office-Produkte	18.01.2021 16:53	OpenDocument-T...	73 KB
ITIS-Check_APP.1.2 Webbrowser	18.01.2021 16:53	OpenDocument-T...	73 KB
ITIS-Check_APP.1.4 Mobile Anwendungen (Apps)	18.01.2021 16:53	OpenDocument-T...	73 KB
ITIS-Check_APP.2.1 Allgemeiner Verzeichnisdienst	18.01.2021 16:53	OpenDocument-T...	73 KB
ITIS-Check_APP.2.2 Active Directory	18.01.2021 16:53	OpenDocument-T...	73 KB
ITIS-Check_APP.2.3 OpenLDAP	18.01.2021 16:53	OpenDocument-T...	73 KB
ITIS-Check_APP.3.1 Webanwendungen	18.01.2021 16:53	OpenDocument-T...	73 KB
ITIS-Check_APP.3.2 Webserver	18.01.2021 16:53	OpenDocument-T...	73 KB
ITIS-Check_APP.3.3 Fileserver	18.01.2021 16:53	OpenDocument-T...	73 KB
ITIS-Check_APP.3.4 Samba	18.01.2021 16:53	OpenDocument-T...	73 KB
ITIS-Check_APP.3.6 DNS-Server	18.01.2021 16:53	OpenDocument-T...	74 KB
ITIS-Check_APP.4.2 SAP-ERP-System	18.01.2021 16:53	OpenDocument-T...	74 KB
ITIS-Check_APP.4.3 Relationale Datenbanken	18.01.2021 16:53	OpenDocument-T...	74 KB
ITIS-Check_APP.4.6 SAP ABAP-Programmierung	18.01.2021 16:53	OpenDocument-T...	74 KB
ITIS-Check_APP.5.2 Microsoft Exchange und Outlook	18.01.2021 16:53	OpenDocument-T...	73 KB
ITIS-Check_APP.5.3 Allgemeiner E-Mail-Client und -Server	18.01.2021 16:53	OpenDocument-T...	73 KB
ITIS-Check_APP.6 Allgemeine Software	18.01.2021 16:53	OpenDocument-T...	73 KB
ITIS-Check_APP.7 Entwicklung von Individualsoftware	18.01.2021 16:53	OpenDocument-T...	73 KB
ITIS-Check_CON.1 Kryptokonzept	18.01.2021 16:53	OpenDocument-T...	66 KB
ITIS-Check_CON.2 Datenschutz	18.01.2021 16:53	OpenDocument-T...	63 KB
ITIS-Check_CON.3 Datensicherungskonzept	18.01.2021 16:53	OpenDocument-T...	66 KB
ITIS-Check_CON.6 Löschen und Vernichten	18.01.2021 16:53	OpenDocument-T...	66 KB
ITIS-Check_CON.7 Informationssicherheit auf Auslandsreisen	18.01.2021 16:53	OpenDocument-T...	66 KB
ITIS-Check_CON.8 Software-Entwicklung	18.01.2021 16:53	OpenDocument-T...	66 KB
ITIS-Check_CON.9 Informationsaustausch	18.01.2021 16:53	OpenDocument-T...	66 KB
ITIS-Check_CON.10 Entwicklung von Webanwendungen	18.01.2021 16:53	OpenDocument-T...	66 KB
ITIS-Check_DER.1 Detektion von sicherheitsrelevanten Ereignissen	18.01.2021 16:53	OpenDocument-T...	68 KB
ITIS-Check_DER.2.1 Behandlung von Sicherheitsvorfällen	18.01.2021 16:53	OpenDocument-T...	68 KB
ITIS-Check_DER.2.2 Vorsorge für die IT-Forensik	18.01.2021 16:53	OpenDocument-T...	68 KB
ITIS-Check_DER.2.3 Bereinigung weitreichender Sicherheitsvorfälle	18.01.2021 16:53	OpenDocument-T...	68 KB
ITIS-Check_DER.3.1 Audits und Revisionen	18.01.2021 16:53	OpenDocument-T...	68 KB
ITIS-Check_DER.3.2 Revisionen auf Basis des Leitfadens IS-Revision	18.01.2021 16:53	OpenDocument-T...	68 KB
ITIS-Check_DER.4 Notfallmanagement	18.01.2021 16:53	OpenDocument-T...	68 KB
ITIS-Check_IND.1 Prozesslet- und Automatisierungstechnik	18.01.2021 16:53	OpenDocument-T...	63 KB
ITIS-Check_IND.2.1 Allgemeine ICS-Komponente	18.01.2021 16:53	OpenDocument-T...	63 KB
ITIS-Check_IND.2.2 Speicherprogrammierbare Steuerung (SPS)	18.01.2021 16:53	OpenDocument-T...	63 KB
ITIS-Check_IND.2.3 Sensoren und Aktoren	18.01.2021 16:53	OpenDocument-T...	64 KB
ITIS-Check_IND.2.4 Maschine	18.01.2021 16:53	OpenDocument-T...	64 KB

 checklisten\_2021

15.09.2022 20:38

Dateiordner

<b>Nummer:</b>		<b>Erfasst am:</b>		<b>Befragte Personen:</b>	
<b>Bezeichnung:</b>		<b>Erfasst durch:</b>		- " -	
<b>Standort:</b>				- " -	

Anforderung	Titel	Typ	ent- behl.	ja	teilw.	nein	Umsetzung bis	verantwortlich	Bemerkungen / Begründung für Nicht-Umsetzung	Kostenschätzung
SYS.3.3.A1	Sicherheitsrichtlinien und Regelungen für die Mobiltelefon-Nutzung	Basis								
SYS.3.3.A2	Spermaßnahmen bei Verlust eines Mobiltelefons	Basis								
SYS.3.3.A3	Sensibilisierung und Schulung der Mitarbeiter im Umgang mit Mobiltelefonen	Basis								
SYS.3.3.A4	Aussonderung und ordnungsgemäße Entsorgung von Mobiltelefonen und darin verwendeter Speicherkarten	Basis								
SYS.3.3.A5	Nutzung der Sicherheitsmechanismen von Mobiltelefonen	Standard								
SYS.3.3.A6	Updates von Mobiltelefonen	Standard								

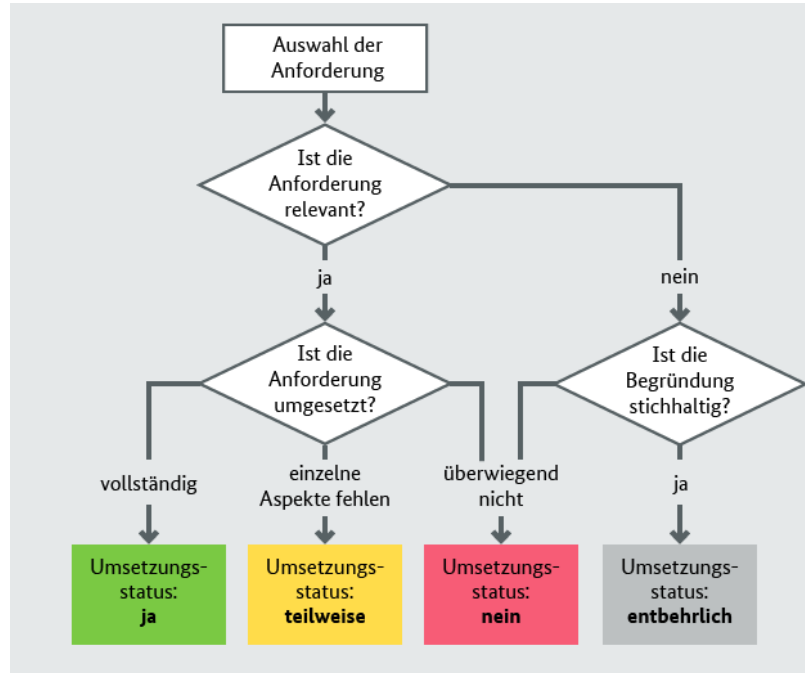
Anforderung	Titel	Typ	ent- behr.	ja	teilw.	nein	Umsetzung bis	verantwortlich	Bemerkungen / Begründung für Nicht-Umsetzung	Kostenschätzung
SYS.3.3.A7	Beschaffung von Mobiltelefonen	Standard								
SYS.3.3.A8	Nutzung drahtloser Schnittstellen von Mobiltelefonen	Standard								
SYS.3.3.A10	Sichere Datenübertragung über Mobiltelefone	Standard								
SYS.3.3.A11	Ausfallvorsorge bei Mobiltelefonen	Standard								
SYS.3.3.A12	Einrichtung eines Mobiltelefon-Pools	Standard								
SYS.3.3.A9	Sicherstellung der Energieversorgung von Mobiltelefonen	Hoch								
SYS.3.3.A13	Schutz vor der Erstellung von Bewegungsprofilen bei der Mobilfunk-Nutzung	Hoch								
SYS.3.3.A14	Schutz vor Rufnummernermittlung bei der Mobiltelefon-Nutzung	Hoch								
SYS.3.3.A15	Schutz vor Abhören der Raumgespräche über Mobiltelefone	Hoch								



# Bundesamt für Sicherheit in der Informationstechnik

Informationen sind dann in folgende Kategorien zu unterteilen.

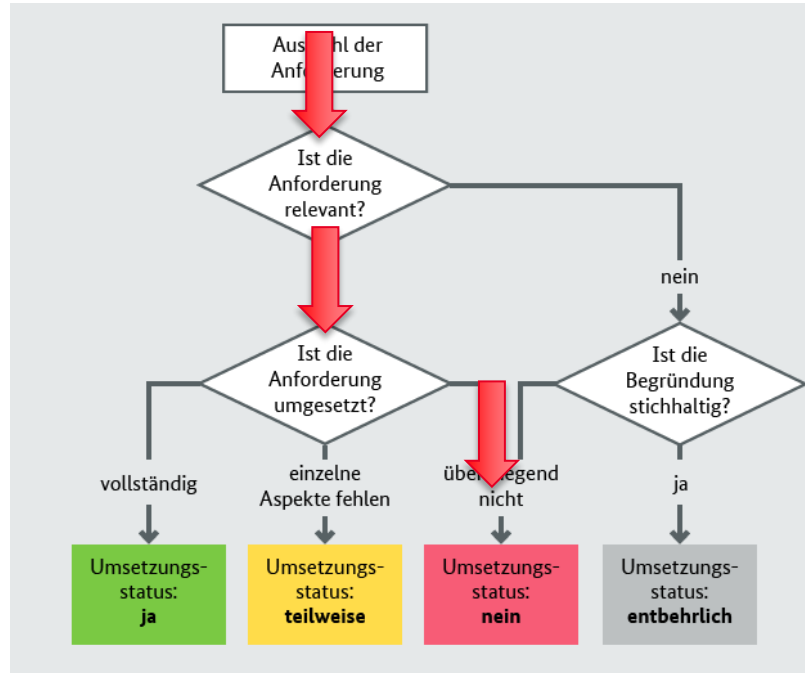
Smartphone?



# Bundesamt für Sicherheit in der Informationstechnik

Informationen sind dann  
in folgende Kategorien  
zu unterteilen.

Smartphone?



# Bundesamt für Sicherheit in der Informationstechnik

Informationen sind dann  
in folgende Kategorien  
zu unterteilen.

## Beispiele

ISMS.1.A1: Übernahme der  
Gesamtverantwortung für  
Informationssicherheit durch die  
Leitungsebene  
(Institutionsleitung)

# Bundesamt für Sicherheit in der Informationstechnik

Informationen sind dann  
in folgende Kategorien  
zu unterteilen.

## Beispiele

ISMS.1.A1: Übernahme der  
*Gesamtverantwortung für*  
*Informationssicherheit durch die* erfüllt  
*Leitungsebene*  
(Institutionsleitung)

# Bundesamt für Sicherheit in der Informationstechnik

Informationen sind dann in folgende Kategorien zu unterteilen.

## Beispiele

ISMS.1.A1: Übernahme der Gesamtverantwortung für Informationssicherheit durch die Leitungsebene  
(Institutionsleitung)

erfüllt

Die Geschäftsführung hat die Erstellung der Leitlinie initiiert. Die Leitlinie wurde von der Geschäftsführung unterzeichnet. Die Geschäftsführung hat die gesamte Verantwortung für das Thema Informationssicherheit übernommen und delegiert an den ISB die Umsetzung der geforderten Maßnahmen. Einmal monatlich erhält die Geschäftsführung einen Management-Report, kontrolliert den Umsetzungsstand der Maßnahmen, initiiert bei Bedarf weitere Maßnahmen und bewilligt das entsprechende Budget.

# Bundesamt für Sicherheit in der Informationstechnik



Bundesamt  
für Sicherheit in der  
Informationstechnik