

Neue Wege in den IT-Grundschutz

Weg in die Basis-Absicherung (WiBA)

Omnisecure 2023 | 23.05.2023

Carmen Gros, BSI Referat BL 12 – Informationssicherheitsberatung für Länder und Kommunen

Florian Göhler, BSI Referat SZ 13 – IT-Grundschutz

Leitsatz

Das BSI als die Cyber-Sicherheitsbehörde des Bundes gestaltet Informationssicherheit in der Digitalisierung durch Prävention, Detektion und Reaktion für Staat, Wirtschaft und Gesellschaft.



Kurzprofil des BSI

Gründung
01. Januar 1991

217 Mio.
Euro Budget
Haushalt
2022

Stellen 2022

1733



183

Neue
Stellen
zum Vorjahr

BSI vor Ort

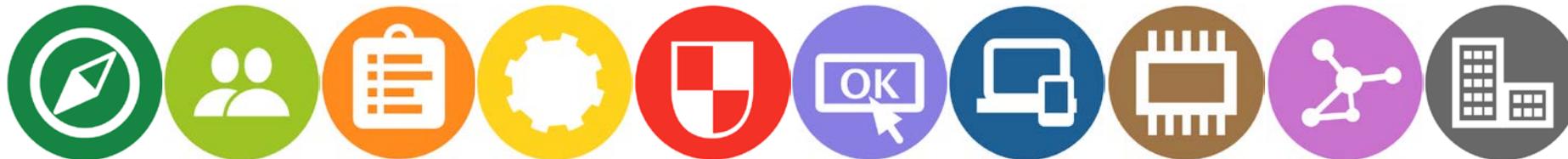
- Standorte
- Stützpunkte
- Verbindungsstellen



Darüber hinaus engagiert sich das BSI seit langem intensiv im internationalen und nationalen Rahmen, unter anderem in enger Zusammenarbeit mit bilateralen Partnern sowie in multilateralen Handlungsfeldern rund um EU und NATO.

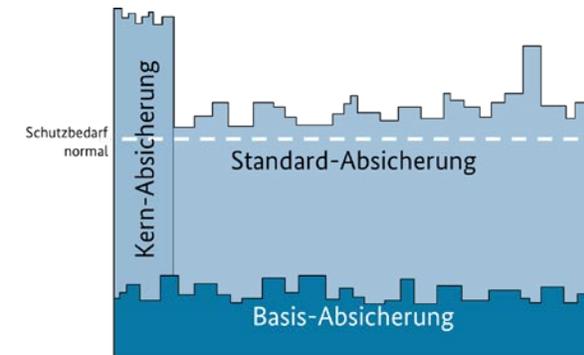
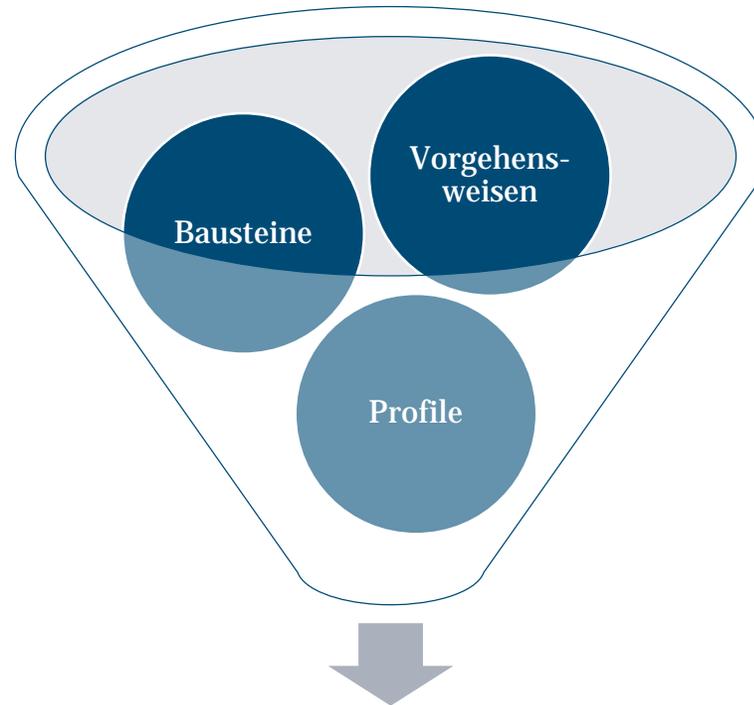
Informationssicherheitsmanagementsystem

- IT ist kein Selbstzweck
- Ein ISMS sichert Informationen
- Organisatorische, Technische und Planerische Aufgaben
- Kontinuierliche Verbesserung



Der Werkzeugkasten für ein ISMS

IT-Grundschutz



IT-Grundschutz



BSI-Standards

Inhalt

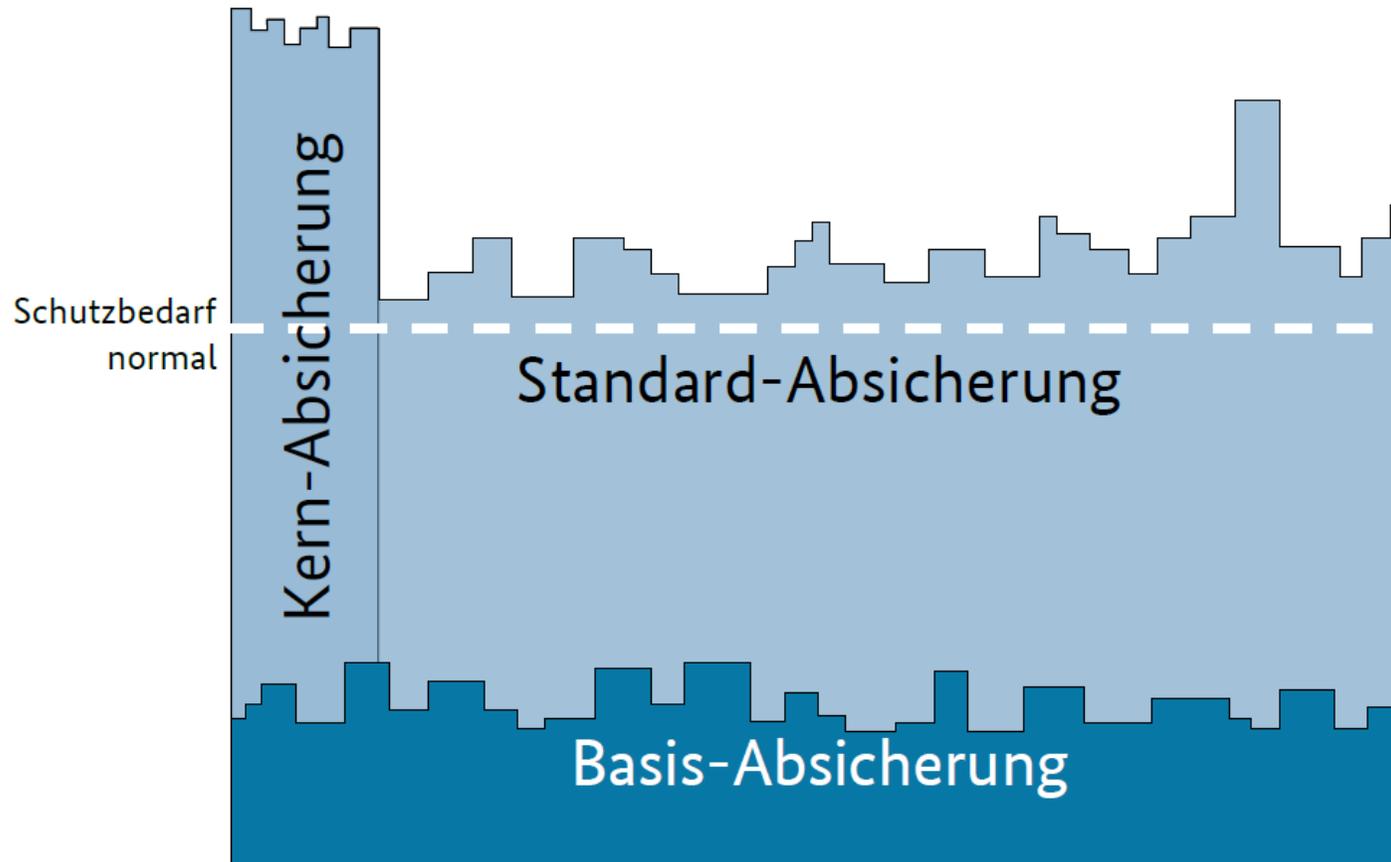
- 200-1: Managementsysteme für Informationssicherheit
- 200-2: IT-Grundschutz-Methodik
- 200-3: Risikoanalyse auf der Basis von IT-Grundschutz

Verfügbare Versionen

- Kostenlos als PDF auf BSI-Webseite
- Kostenpflichtige gedruckte Version über Reguvis / Bundesanzeiger Verlag



BSI-Standard 200-2

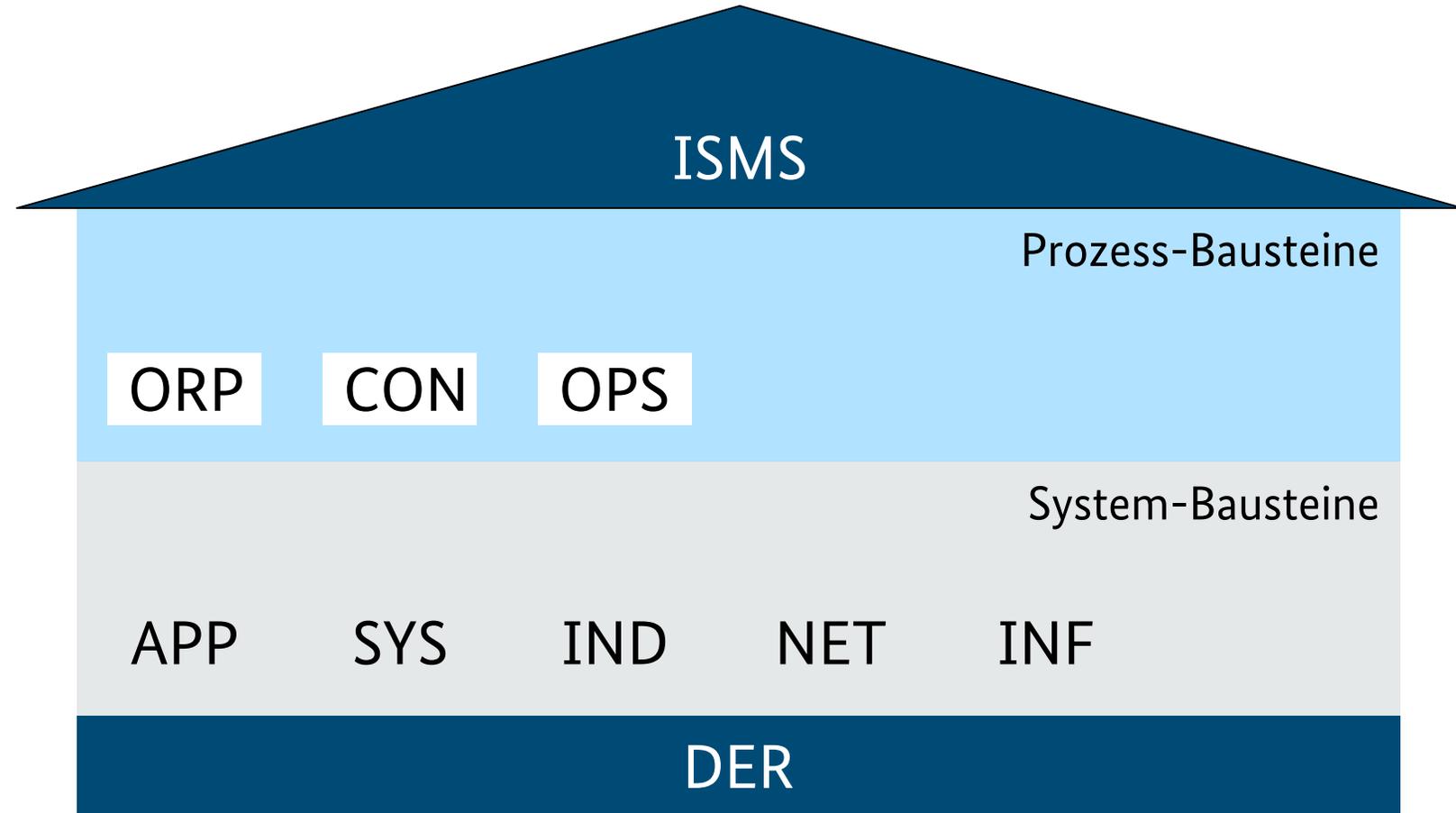


Vorgehensweise



„Arbeitsbuch“

IT-Grundschutz-Kompendium



Anforderungen

3.1 Basis-Anforderungen

Die folgenden Anforderungen MÜSSEN für den Baustein OPS.1.2.5 *Fernwartung* vorrangig erfüllt werden:

OPS.1.2.5.A1 Planung des Einsatzes der Fernwartung (B)

Der Einsatz der Fernwartung MUSS an die Institution angepasst und hinsichtlich technischer und organisatorischer Aspekte bedarfsgerecht geplant werden. Es MUSS geklärt werden, ob In-Band oder Out-Band Administration genutzt wird. Die Institution MUSS geeignete IT-Systemschnittstellen und Protokolle auswählen.

OPS.1.2.5.A2 Sicherer Verbindungsaufbau bei der Fernwartung von Clients [Benutzer] (B)

Wird per Fernwartung auf Clients zugegriffen, MUSS dieser Zugriff vom Benutzer des IT-Systems initiiert werden. Der Benutzer des fernadministrierten Clients MUSS dem Fernzugriff explizit zustimmen.

Weg in die Basis-Absicherung (WiBA)

#WoSollIchAnfangen



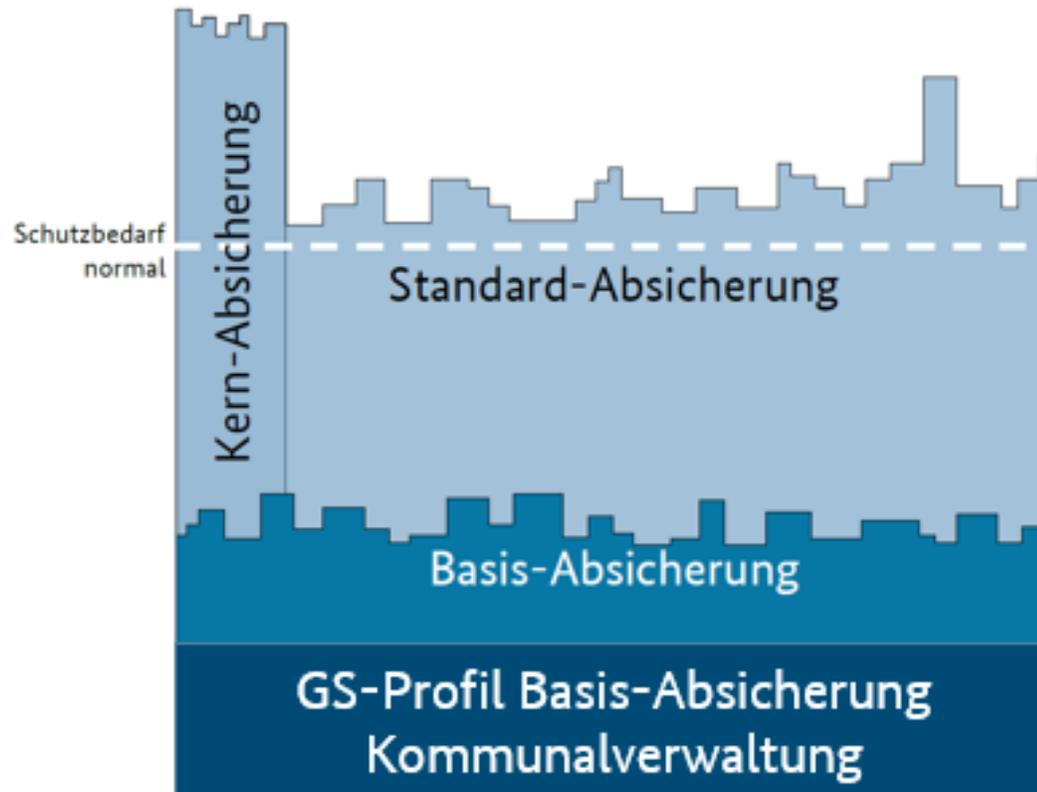
Unsplash / Peter Herrmann



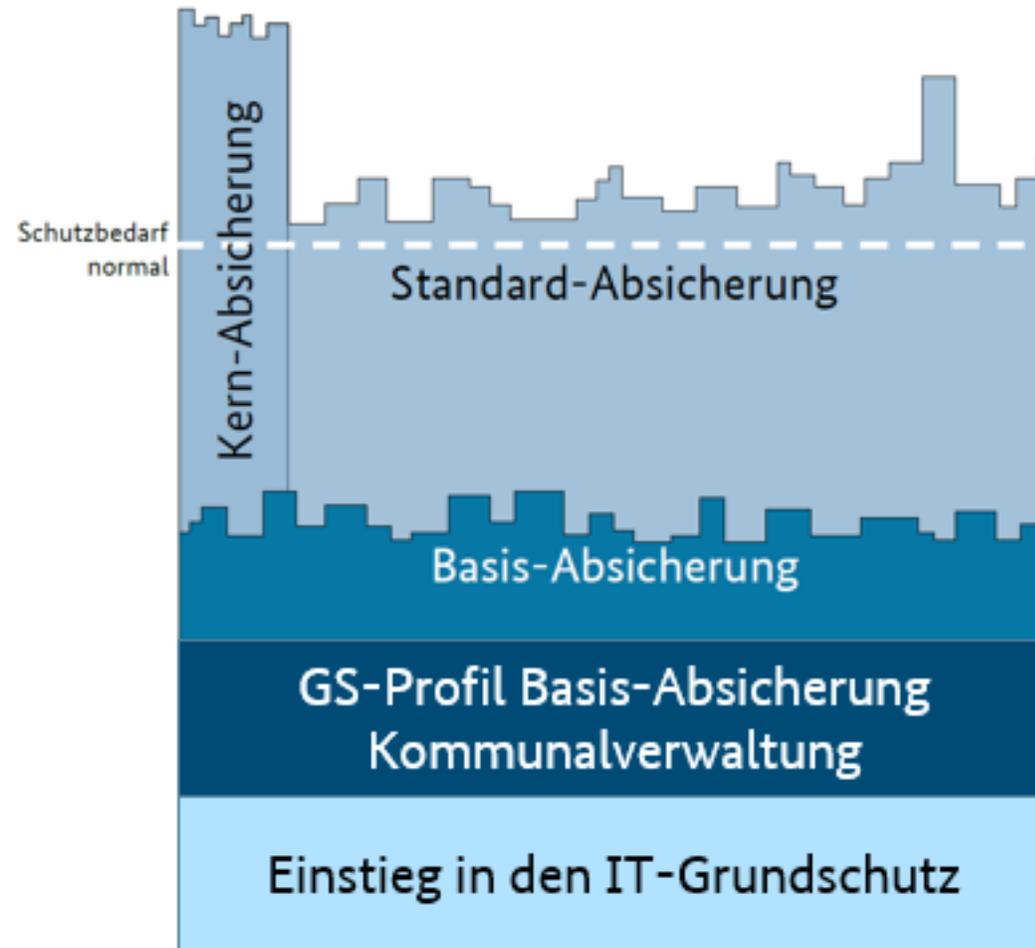
Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

Ausgangslage



Lösungsansatz



Zeitplan



Gründung Projektgruppe

Entwicklung der „Einstiegsmethodik“

Identifizierung relevanter Bausteine und Anforderungen, Formulierung der Fragen

Erstellung der Dokumentation (Dokumente, Checklisten)

Einbindung der kommunalen Stakeholder (AG KoBa, KSV, ggf. IT-SiBe-Forum)

Pilotierung des finalen Produkts mit Modellkommunen

Veröffentlichung

Weg in die Basis-Absicherung



Vorgehensweise



© Bim / E+ / Getty Images

Clusterung der 51 relevanten Bausteine
in 19 themenspezifischen Checklisten

Einbindung von Modellkommunen
über kommunale Spitzenverbände

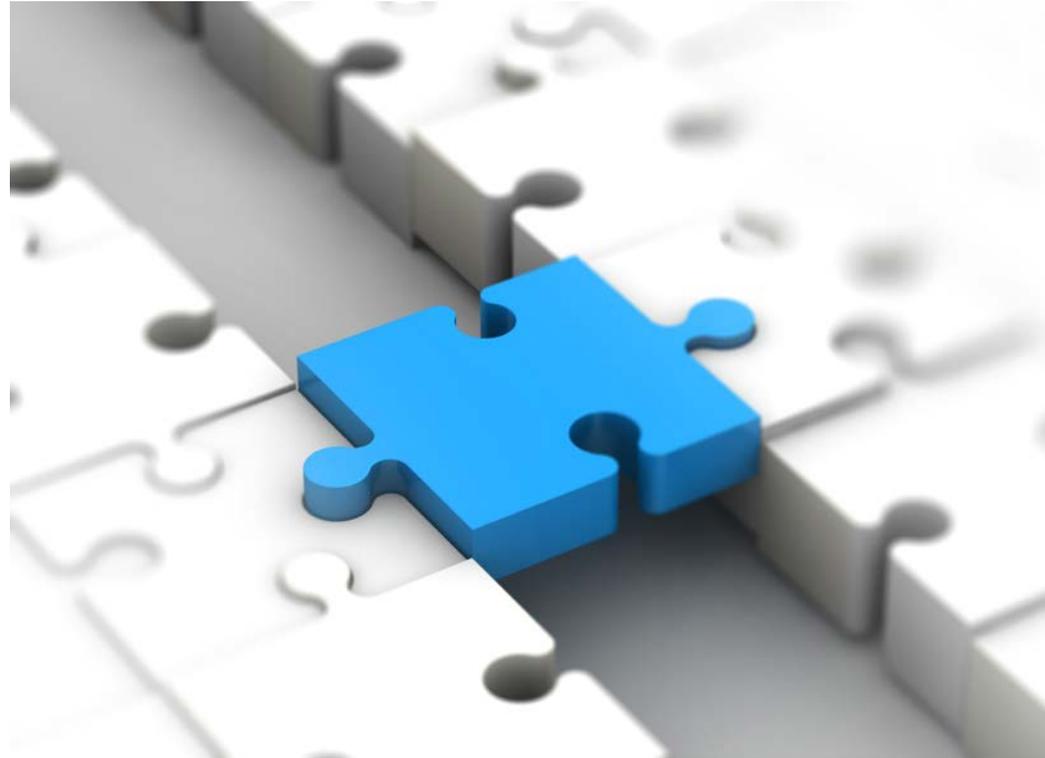
Erstellung eines „Kennzeichens“
bei Umsetzung der Prüffragen



Weg in die Basis-Absicherung (WiBA)

Praxis-Test der Checklisten

Einbindung der
AG koBA



© vegefox / AdobeStock / stock.adobe.com

Einbindung von
Modellkommunen

Checklisten

- „Vorgehensweise“ / Management Summary
- Arbeit außerhalb der Institution
- Arbeit innerhalb der Institution / Haustechnik
- Backup
- Client
- Drucker / Multifunktionsgeräte
- IT-Administration
- Mobile Endgeräte
- Netze
- Organisation und Personal
- Outsourcing und Cloud
- Bürosoftware
- Rollen / Berechtigungen / Authentisierung
- Serverraum
- Serversysteme
- Sicherheitsmechanismen
- Telefonie und Fax
- Umgang mit Informationen
- Vorbereitung für Sicherheitsvorfälle

Clusterbildung: Beispiele

- „Serversysteme“
 - SYS.1.1 allg. Server, SYS.1.5 Virtualisierung, APP 2.1 allg. Verzeichnisdienst, APP.3.3 Fileserver, APP.5.3 Allg. E-Mail-Client und –Server
- „Umgang mit Informationen“
 - CON.6 Löschen und Vernichten, CON.9 Informationsaustausch
- „Arbeit außerhalb der Institution“
 - OPS.1.2.4 Telearbeit, INF.8 Häuslicher Arbeitsplatz, INF.9 Mobiler Arbeitsplatz, INF.11 Allgemeines Fahrzeug
- „Outsourcing und Cloud“
 - OPS.2.1 Outsourcing für Kunden, OPS.2.2 Cloud-Nutzung

Beispiel Herabsenkung von Anforderungen für Einstieg

ID-Anforderung	Titel	Inhalt	Typ	im GS-Profil	berücksichtigen	Begründung für Nicht-Berücksichtigung	Checkfrage
OPS.2.1.A1	Festlegung der Sicherheitsanforderungen für Outsourcing-Vorhaben	Alle Sicherheitsanforderungen für ein Outsourcing-Vorhaben MÜSSEN auf Basis einer Strategie zum Outsourcing festgelegt sein und beide Outsourcing-Parteien MÜSSEN sich vertraglich dazu verpflichten, den IT-Grundschutz oder ein vergleichbares Schutzniveau einzuhalten.	Basis	ja	ja		Werden Sicherheitsanforderungen durch den Outsourcing-Dienstleister erfüllt?



Prüffragen

Nr.	Zu prüfende Anforderung	Aufwand	Erfüllt	
			Ja	Nein
1	Werden die Sicherheitsanforderungen der Institution durch den Outsourcing-Dienstleister erfüllt?	☹️ - ☹️☹️☹️☹️		
	<i>Es sollten mindestens die Anforderungen der Checklisten aus der Einstiegsstufe erfüllt werden. Die Verpflichtung sollte vertraglich erfolgt sein.</i>			
	Notizen			

Beispiel Konsolidierung von Anforderungen

ID-Anforderung	Titel	Inhalt	Typ	im GS-Profil	berücksichtigt	Begründung für Nicht-Berücksichtigung
OPS.1.1.2.A7	Regelung der IT-Administrationstätigkeit	Die Befugnisse, Aufgaben und Pflichten der Administratoren SOLLTEN in einer Arbeitsanweisung oder Richtlinie verbindlich festgeschrieben werden.	Standard	Ja	nein	in Checkliste "Personal und Organisation" in Anforderung 2
OPS.1.1.2.A7	Regelung der IT-Administrationstätigkeit	Die Aufgaben zwischen den einzelnen Administratoren SOLLTEN so verteilt werden, dass einerseits Überschneidungen in den Zuständigkeiten vermieden werden und andererseits keine Administrationslücken entstehen.	Standard	Ja	nein	in Checkliste "Personal und Organisation" in Anforderung 1 (Hilfsmittel) aufgegangen



Nr.	Zu prüfende Anforderung	Aufwand	Erfüllt	
			Ja	Nein
1	Wurde für alle Geschäftsprozesse, Anwendungen, IT-Systeme, Räume und Gebäude sowie Kommunikationsverbindungen festgelegt, wer für diese und deren Sicherheit zuständig ist?	👤 👤		
	<p><i>Die Aufgaben sollten so verteilt werden, dass einerseits Überschneidungen in den Zuständigkeiten vermieden werden und andererseits keine Lücken entstehen.</i></p> <p><i>Die Festlegung kann dabei in verschiedenen Dokumenten bspw. im Geschäftsverteilungsplan oder dem <u>Assetmanagement</u> erfolgen.</i></p> <p><i>Die Zuständigkeit liegt dabei in der Regel nicht allein beim ISB, sondern je nach Zielobjekt (Anwendung, IT-System...) bei Admins, Fachverfahrensverantwortlichen usw.</i></p>			
	Notizen			

Nr.	Zu prüfende Anforderung	Aufwand	Erfüllt	
			Ja	Nein
2	Wurden die Personen darüber informiert, welche Zuständigkeiten sie haben und welche Aufgaben, Pflichten und Befugnisse sie in diesem Kontext wahrnehmen?	👤		
	<i>Die Information sollte schriftlich erfolgen.</i>			
	Notizen			



Vielen Dank für Ihre Aufmerksamkeit!

Deutschland
Digital•Sicher•BSI

Kontakt

Projektgruppe „Weg in die Basis-Absicherung“

Kontakt über:

basisabsicherung@bsi.bund.de

Bundesamt für Sicherheit in der Informationstechnik (BSI)
Godesberger Allee 185-189
53175 Bonn
www.bsi.bund.de

Das BSI als die Cyber-Sicherheitsbehörde des Bundes gestaltet Informationssicherheit in der Digitalisierung durch Prävention, Detektion und Reaktion für Staat, Wirtschaft und Gesellschaft.