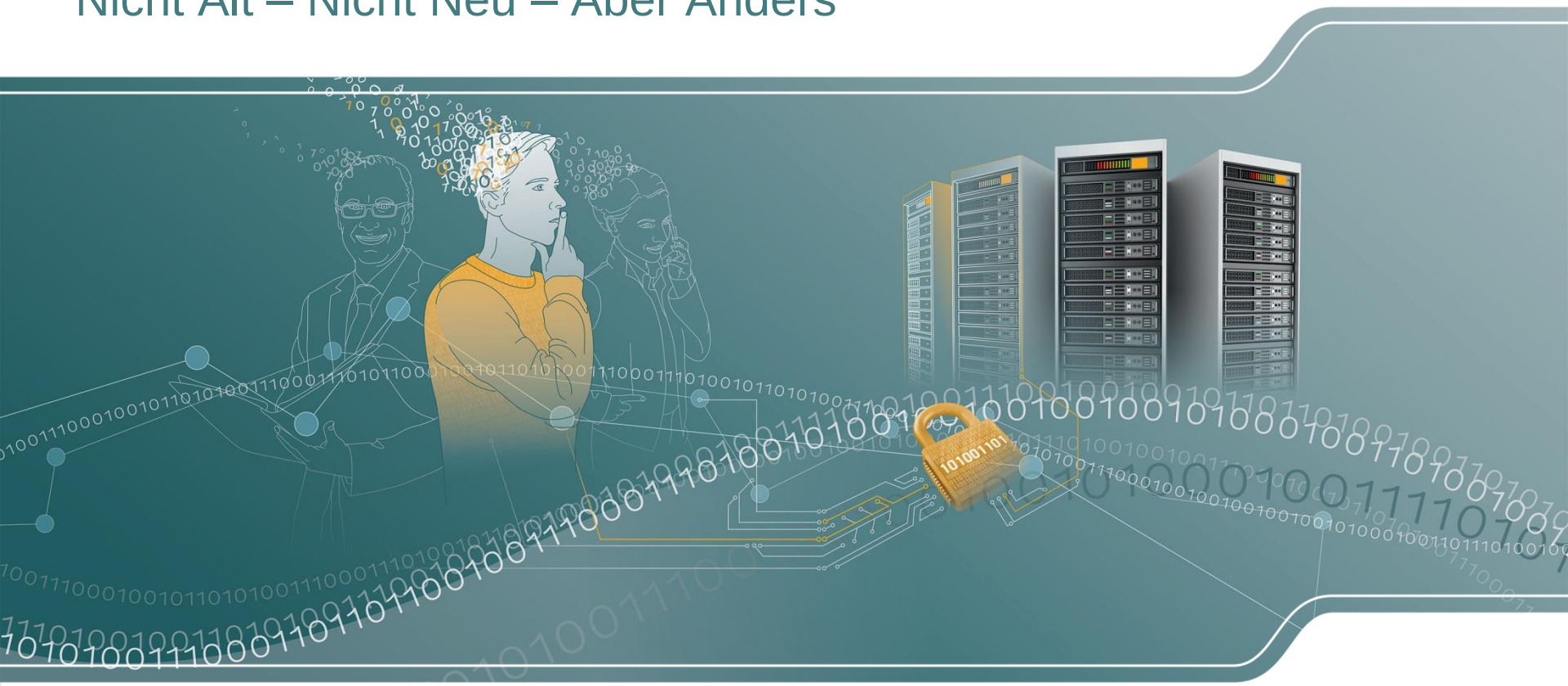
STAATSBETRIEB
SÄCHSISCHE
INFORMATIK DIENSTE

Freistaat
SACHSEN

BSI-Modernisierung Grundschutz:
Nicht Alt – Nicht Neu – Aber Anders



27. September 2016 | Simone Hock & Denny Dittrich

Inhalt

- Darstellung der Neuerungen im IT-Grundschutz im Rahmen der BSI-Modernisierung 2017
- Gegenüberstellung mit dem „klassischen“ IT-Grundschutz

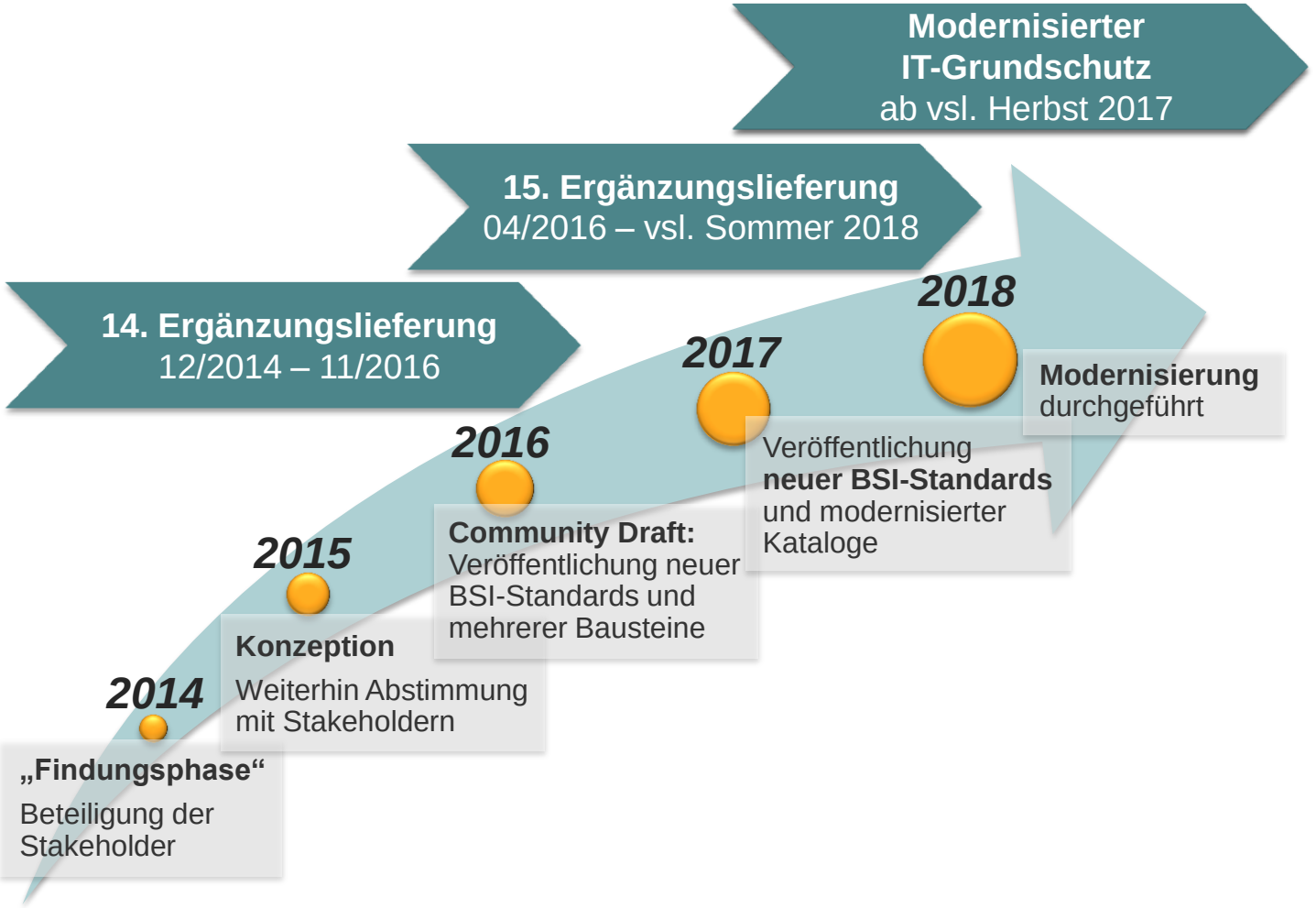
Gliederung

- **Gründe** für die Modernisierung
- **Zeitlicher Verlauf** der Modernisierung
- **Kernaspekte** der Modernisierung
  - Vorgehensweisen
  - Bausteine
  - Profile
- **Ausblick zur Umsetzung** der Modernisierung

Gründe für die Modernisierung

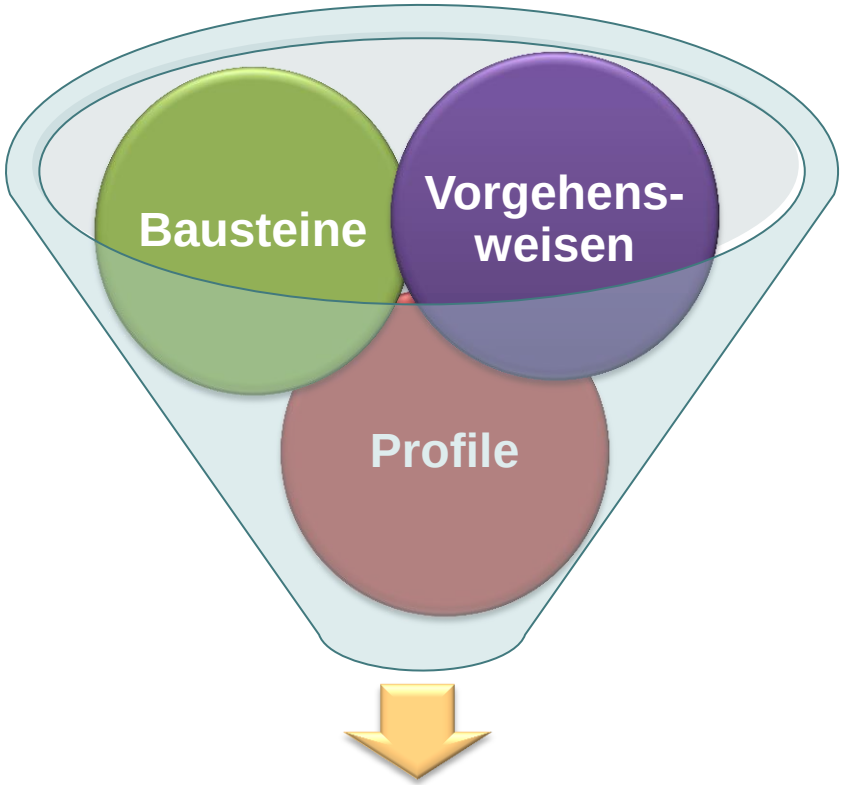
Quelle: Bundesamt für Sicherheit in der Informationstechnik (BSI)

Zeitlicher Verlauf



Quelle: Bundesamt für Sicherheit in der Informationstechnik (BSI)

Kernaspekte der Modernisierung



Quelle: Bundesamt für Sicherheit in der Informationstechnik (BSI)

Kernthema Vorgehensweisen

Quelle: Bundesamt für Sicherheit in der Informationstechnik (BSI)

Vorgehens-
weisen

Neue Absicherung

- IT-Grundschutz-Methodik nach BSI-Standard 100-2

- 3 Arten der Absicherung:
  - Basisabsicherung
  - Kernabsicherung
  - Standardabsicherung

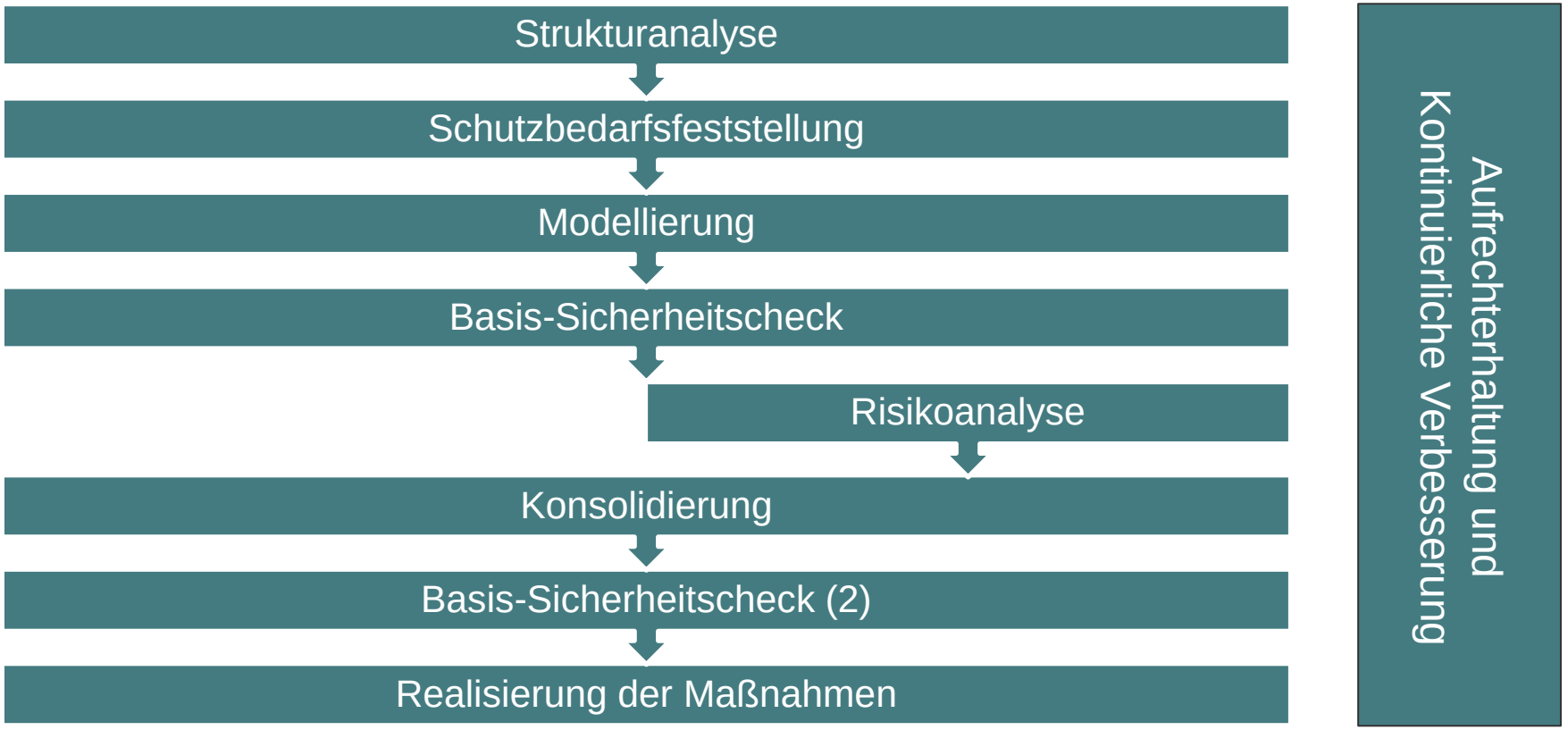
Quelle: Bundesamt für Sicherheit in der Informationstechnik (BSI)

Vorgehens-
weisen

STAATSBETRIEB
SÄCHSISCHE
INFORMATIK DIENSTE

Freistaat
SACHSEN

Neue Absicherung IT-Grundschutz-Methodik



Quelle: Bundesamt für Sicherheit in der Informationstechnik (BSI)

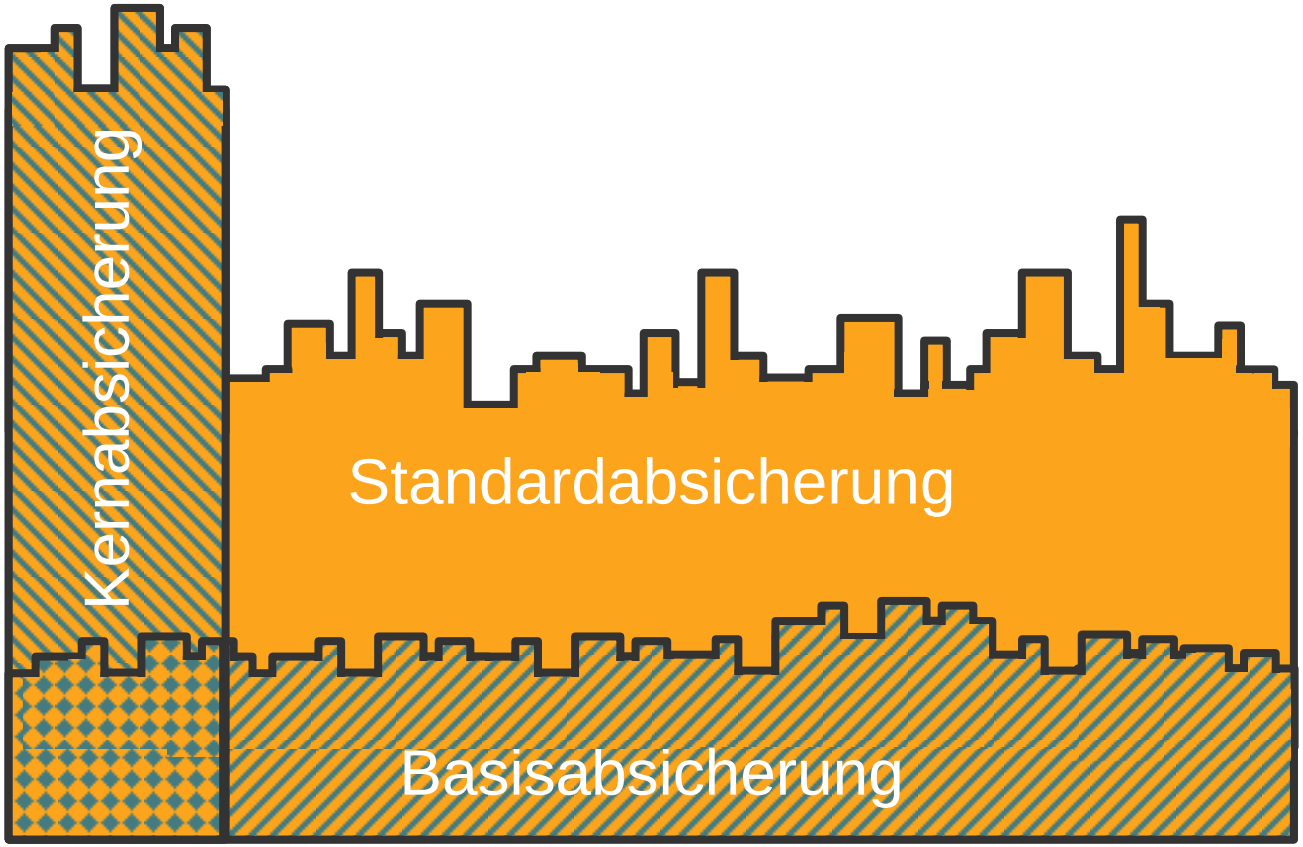
Neue Absicherung

- IT-Grundschutz-Methodik nach BSI-Standard 100-2

- 3 Arten der Absicherung:
  - Basisabsicherung
  - Kernabsicherung
  - Standardabsicherung

Quelle: Bundesamt für Sicherheit in der Informationstechnik (BSI)

Neue Absicherung - Überblick



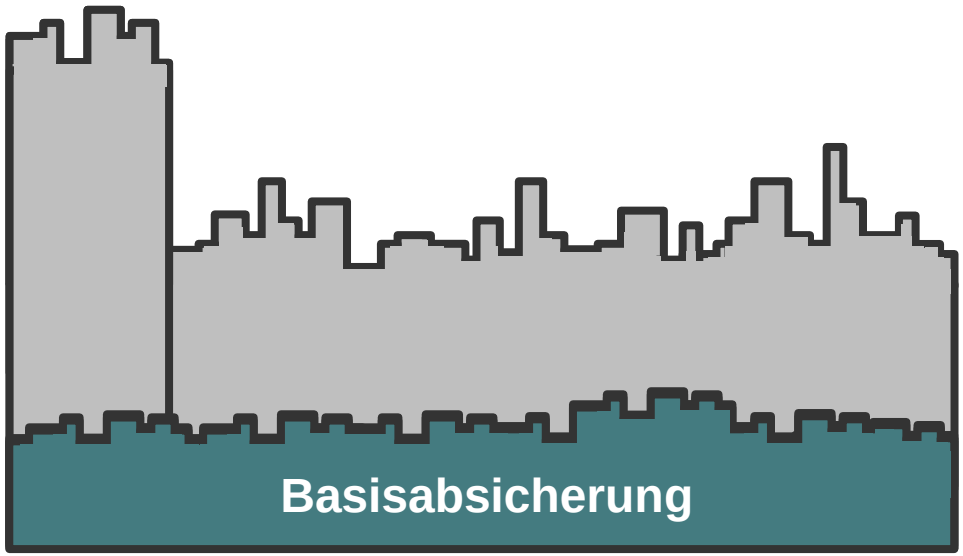
Quelle: Bundesamt für Sicherheit in der Informationstechnik (BSI)

Vorgehens-
weisen

STAATSBETRIEB
SÄCHSISCHE
INFORMATIK DIENSTE

Freistaat
SACHSEN

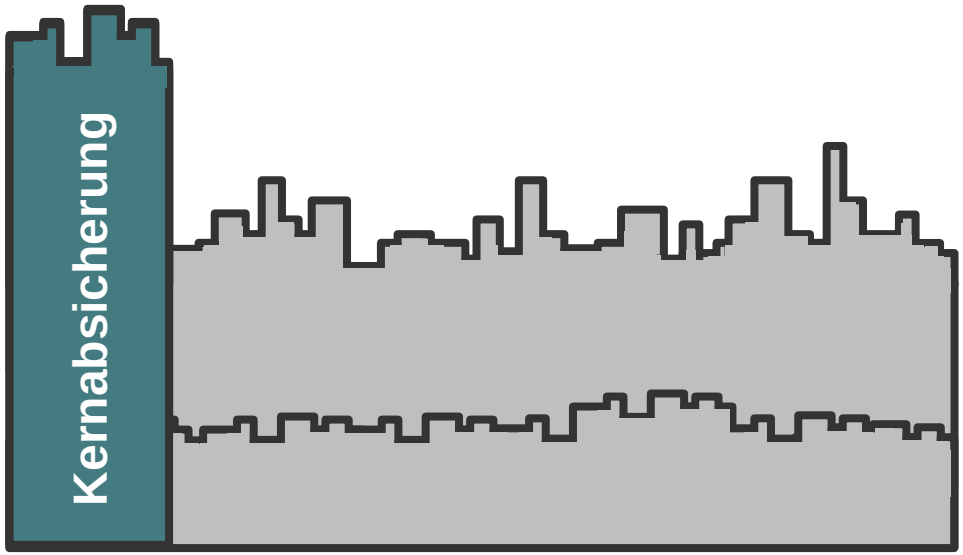
Neue Absicherung - Basisabsicherung



- Vereinfachter Einstieg
- Grundlegende Erstabsicherung der Geschäftsprozesse und Ressourcen
- <u>Vorteil</u>:
  - Zugeschnitten für Bedürfnisse der kleine und mittlere Unternehmen sowie Institutionen

Quelle: Bundesamt für Sicherheit in der Informationstechnik (BSI)

Neue Absicherung - Kernabsicherung



- Konzentration auf kleinen, sehr wichtigen Informationsverbund
- Schutz herausragender, besonders gefährdeter Geschäftsprozesse und Ressourcen (Kronjuwelen)
- Vorteil:
  - Zeitersparnis im Vorgehen
  - Beschleunigte Absicherung

Quelle: Bundesamt für Sicherheit in der Informationstechnik (BSI)

Vorgehens-
weisen

Neue Absicherung - Standardabsicherung

- Methodik in Grundzügen unverändert
- Vollumfänglicher Sicherheitsprozess nach bekannten BSI-Standard 100-2
- Vorteil:
  - Zertifizierung nach ISO 27001 auf Basis von IT-Grundschutz möglich

Quelle: Bundesamt für Sicherheit in der Informationstechnik (BSI)

Neue Umsetzungsreihenfolge

- Bisher keine Vorgaben zur Umsetzungsreihenfolge

- Umsetzung in 3 Phasen
  - Phase 1:
    Vorrangige Umsetzung
  - Phase 2:
    Weitere relevante Bausteine
  - Phase 3:
    Bausteine nachrangig
    für Basisabsicherung nur ggf. relevant

Quelle: Bundesamt für Sicherheit in der Informationstechnik (BSI)

Neue Umsetzungsreihenfolge

Phase 1

- ISMS (Sicherheitsmanagement)
- ORP.1 (Organisation)
- ORP.2 (Personal)
- ORP.3 (Sensibilisierung und Schulung)
- ORP.4 (Identitäts- und Berechtigungsmanagement)
- OPS.1.1 (Kern IT-Betrieb / Kernaufgaben)

Phase 2

- APP (Anwendungen)
- SYS (IT-Systeme)
- NET (Netze und Kommunikation)
- INF (Infrastruktur)
- DER (Detektion und Reaktion)
- ORP.5 (Anforderungs-management (Compliance))
- CON.1 (Kryptokonzept)
- CON.2 (Datenschutz)
- CON.5 (Informationssicherheit im Projektmanagement)
- OPS.2 (IT-Betrieb von Dritten)
- OPS.3 (IT-Betrieb für Dritte)
- OPS.4 (Betriebliche Aspekte)

Phase 3

- CON.3 (Hochverfügbarkeitskonzeption)
- CON.4 (Softwareentwicklung)
- CON.6 (Informationssicherheit auf Auslandsreisen)
- OPS.1.2 (Weiterführende Aufgaben (IT-Betrieb))

Quelle: Bundesamt für Sicherheit in der Informationstechnik (BSI)

Kernthema Bausteine

Quelle: Bundesamt für Sicherheit in der Informationstechnik (BSI)

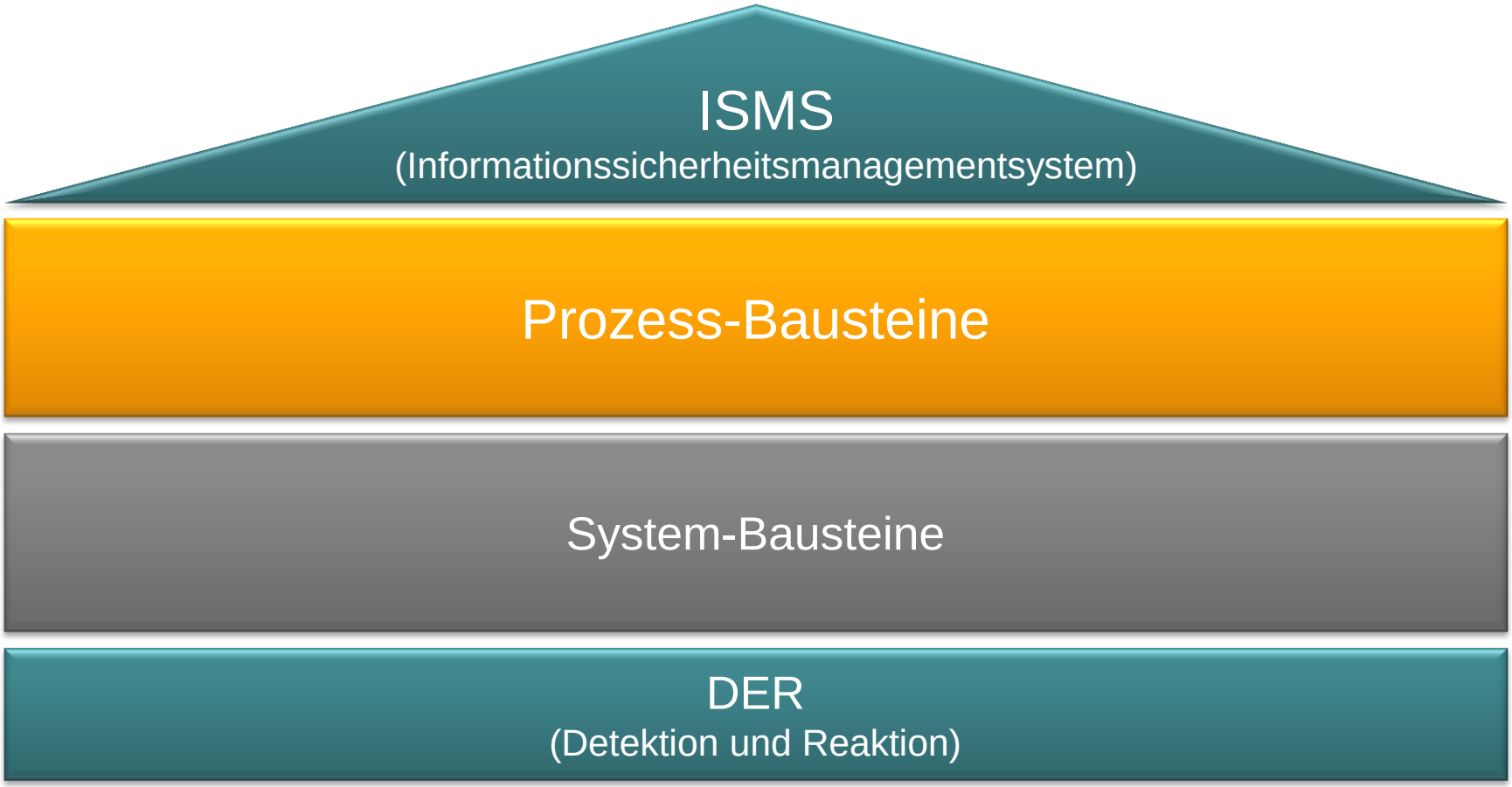
Neue Bausteineinteilung

- 5-teiliges Schichtenmodell:
  - Übergreifende Aspekte
  - Infrastruktur
  - IT-Systeme
  - Netze
  - Anwendungen

- Zweiteilung:
  - Prozess-Bausteine
  - System-Bausteine

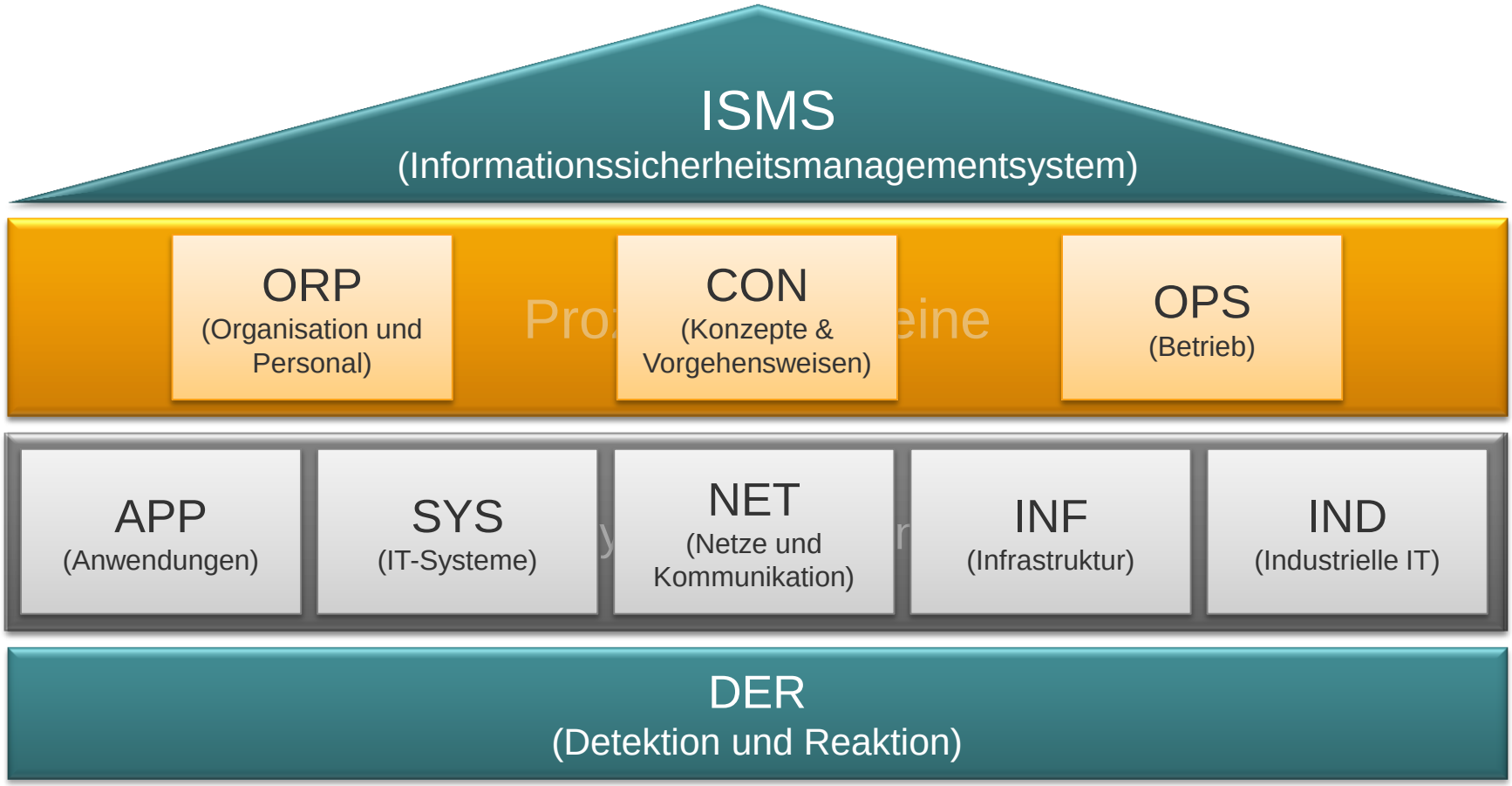
Quelle: Bundesamt für Sicherheit in der Informationstechnik (BSI)

Neue Bausteineinteilung



Quelle: Bundesamt für Sicherheit in der Informationstechnik (BSI)

Neue Bausteineinteilung



Quelle: Bundesamt für Sicherheit in der Informationstechnik (BSI)

Neue Qualifizierungsstufen

- Einstufung der Maßnahmen nach Wichtigkeit für Zertifizierung
  - „A“ ⇨ Einstieg
  - „B“ ⇨ Aufbau
  - „C“ ⇨ Zertifikat
  - „Z“ ⇨ Zusätzlich
  - „W“ ⇨ Wissen

- Basismaßnahmen
  ⇨ Vorrang vor anderen Maßnahmen
- Standardmaßnahmen
  ⇨ Umzusetzen für „normales“ Schutzniveau
- Maßnahmen für erhöhten Schutzbedarf
  ⇨ Umzusetzen für „hohes“ und „sehr hohes“ Schutzniveau

Quelle: Bundesamt für Sicherheit in der Informationstechnik (BSI)

Neue Dokumentenstruktur - Aufbau

- Beschreibung
- Gefährdungslage
  mit Verweis auf
  Gefährdungskataloge
- Maßnahmenempfehlung
  mit Verweis auf
  Maßnahmenkataloge

- Beschreibung
- Spezifische Gefährdungslage
- Anforderungen
- Weiterführende Informationen
  (z.B. Veröffentlichungen)
- Anlagen
  (z.B. Kreuztabellen)

Neue Dokumentenstruktur - Aufbau

Bundesamt für Sicherheit in der Informationstechnik

Community Draft

ISMS: Sicherheitsmanagement

ISMS.1: Sicherheitsmanagement

IT-Grundschutz

1 Beschreibung

1.1 Einleitung

Mit (Informations-)Sicherheitsmanagement oder auch kurz IS-Management wird die Planungs-, Lenkungs- und Kontrollaufgabe bezeichnet, die erforderlich ist, um einen durchdachten und wirksamen Prozess zur Herstellung von Informationssicherheit aufzubauen und kontinuierlich umzusetzen. Ein funktionierendes Sicherheitsmanagement muss in die existierenden Managementstrukturen einer jeden Institution eingebettet werden. Daher ist es praktisch nicht möglich, eine für jede Institution unmittelbar anwendbare Organisationsstruktur für das Sicherheitsmanagement anzugeben. Vielmehr werden häufig Anpassungen an spezifische Gegebenheiten erforderlich sein.

1.2 Zielsetzung

Ziel dieses Bausteins ist es, aufzeigen, wie ein funktionierendes Informationssicherheitsmanagement eingerichtet und im laufenden Betrieb weiterentwickelt werden kann. Er beschreibt dazu sinnvolle Schritte eines systematischen Sicherheitsprozesses und gibt Anleitungen zur Erstellung eines umfassenden Sicherheitskonzeptes.

1.3 Abgrenzung

Der Baustein baut auf dem BSI-Standard 100-1 Managementsysteme für Informationssicherheit und BSI-Standard 100-2 Vorgehensweise nach IT-Grundschutz auf und fasst die wichtigsten Aspekte zum Sicherheitsmanagement hieraus zusammen.

2 Gefährdungslage

Bedrohungen und Schwachstellen im Umfeld des Sicherheitsmanagements können vielfältiger Natur sein. Häufig sind sie Symptom einer mangelhaften Gesamtorganisation des

2.8 Störung der Geschäftsabläufe aufgrund von Sicherheitsvorfällen

Sicherheitsvorfälle können durch ein singuläres Ereignis oder eine Verkettung unglücklicher Umstände ausgelöst werden und dazu führen, dass Vertraulichkeit, Integrität oder Verfügbarkeit von Informationen und IT-Systemen beeinträchtigt werden. Dies wirkt sich dann schnell negativ auf wesentliche Fachaufgaben und Geschäftsprozesse der betroffenen Institution aus. Auch wenn nicht alle Sicherheitsvorfälle in der Öffentlichkeit bekannt werden, können sie trotzdem zu negativen Auswirkungen in den Beziehungen zu Geschäftspartnern und Kunden führen. Dabei ist es nicht einmal so, dass die beträchtlichsten und weitreichendsten Sicherheitsvorfälle durch die größten Sicherheitsschwachstellen ausgelöst wurden. In vielen Fällen hat die Verkettung kleiner Ursachen zu riesigen Schäden geführt.

2.9 Unwirtschaftlicher Umgang mit Ressourcen durch unzureichendes Sicherheitsmanagement

Ein unzureichendes Sicherheitsmanagement kann dazu führen, dass falsche Prioritäten gesetzt werden und nicht an denjenigen Stellen investiert wird, die den größten Mehrwert für die Institution bringen. Dies kann zu folgenden Fehlern führen:

- Es wird in teure Sicherheitslösungen investiert, ohne dass eine Basis an notwendigen organisatorischen Regelungen vorhanden ist. Nicht geklärte Zuständigkeiten und Verantwortlichkeiten können trotz teurer Investitionen zu schweren Sicherheitsvorfällen führen.
- Es wird in den Bereichen einer Institution in Informationssicherheit investiert, die für Informationssicherheit besonders sensibilisiert sind. Andere Bereiche, die vielleicht für die Erfüllung der Fachaufgaben und der Erreichung der Geschäftsziele wichtiger sind, werden aufgrund von knappen Mitteln oder Desinteresse der Verantwortlichen vernachlässigt.
- Es wird nur in einzelne Teilbereiche investiert. Im Gesamtsystem verbleiben jedoch erhebliche Sicherheitslücken.
- Durch die einseitige Erhöhung des Schutzes einzelner Grundwerte kann sich der Gesamtschutz verringern.
- Ein inhomogener und unkoordinierter Einsatz von Sicherheitsprodukten kann zu hohem finanziellen und personellen Ressourceneinsatz führen.

3 Anforderungen

Im Folgenden sind die spezifischen Anforderungen für den Bereich Sicherheitsmanagement aufgeführt. Grundsätzlich ist der Informationssicherheitsbeauftragte (ISB) für die Erfüllung der Anforderungen zuständig. Abweichungen hiervon werden in den entsprechenden Anforderungen gesondert erwähnt. Der ISB ist bei strategischen Entscheidungen stets einzubeziehen. Außerdem ist der ISB dafür verantwortlich, dass alle Anforderungen gemäß dem festlegten Sicherheitskonzept erfüllt und überprüft werden. Zusätzlich kann es noch andere Rollen geben, die weitere Verantwortlichkeiten bei der Umsetzung von Anforderungen haben. Diese sind dann jeweils explizit in eckigen Klammern in der Überschrift der jeweiligen Anforderungen aufgeführt.

Bausteinverantwortlicher	Informationssicherheitsbeauftragter

Quelle: Bundesamt für Sicherheit in der Informationstechnik (BSI)

Neue Dokumentenstruktur - Aufbau

ISMS.1.A6 Aufbau einer geeigneten Organisationsstruktur für Informationssicherheit [Behörden-/Unternehmensleitung]

Es MUSS eine geeignete, übergreifende Organisationsstruktur für Informationssicherheit vorhanden sein. Dafür MÜSSEN Rollen definiert sein, die die verschiedenen Aufgaben für die Erreichung der Sicherheitsziele wahrnehmen. Außerdem MÜSSEN Personen benannt sein, die qualifiziert sind und denen ausreichend Ressourcen zur Verfügung stehen, um diese Rollen auszufüllen. Die Aufgaben, Verantwortungen und Kompetenzen im Sicherheitsmanagement MÜSSEN nachvollziehbar definiert und zugewiesen sein. Für alle wichtigen Funktionen der IS-Organisation MUSS es wirksame Vertretungsregelungen geben.

Kommunikationswege MÜSSEN geplant, beschrieben, eingerichtet und bekannt gemacht werden. Es MUSS für alle Aufgaben und Rollen festgelegt sein, wer wen informiert und wer bei welchen Aktionen in welchen Umfang informiert werden muss.

Es MUSS regelmäßig geprüft werden, ob die Organisationsstruktur für Informationssicherheit noch angemessen ist oder an neue Rahmenbedingungen angepasst werden muss.

ISMS.1.A7 Festlegung von Sicherheitsmaßnahmen

Im Rahmen des Sicherheitsprozesses MÜSSEN für die gesamte Informationsverarbeitung ausführliche und angemessene Sicherheitsmaßnahmen festgelegt werden. Alle Sicherheitsmaßnahmen SOLLTEN systematisch in Sicherheitskonzepten dokumentiert und regelmäßig aktualisiert werden.

ISMS.1.A8 Integration der Mitarbeiter in den Sicherheitsprozess [Vorgesetzte]

Alle Mitarbeiter MÜSSEN in den Sicherheitsprozess integriert sein, dass heißt, sie müssen über Hintergründe und Gefährdungen informiert sein und Sicherheitsmaßnahmen kennen und umsetzen, die ihren Arbeitsplatz betreffen, und sie MÜSSEN Sicherheit aktiv mitgestalten, also in ihre Geschäftsprozesse mit einbringen. Daher SOLLTEN die Mitarbeiter frühzeitig bei der Planung von Sicherheitsmaßnahmen oder der Gestaltung organisatorischer Regelungen beteiligt werden.

Bei der Einführung von Sicherheitsrichtlinien und Sicherheitswerkzeugen MÜSSEN die Mitarbeiter ausreichend informiert sein, wie diese anzuwenden sind.

ISMS.1.A9 Integration der Informationssicherheit in organisationsweite Abläufe und Prozesse [Behörden-/Unternehmensleitung]

Informationssicherheit MUSS in alle Geschäftsprozesse integriert werden. Es MUSS dabei gewährleistet sein, dass nicht nur bei neuen Prozessen und Projekten, sondern auch bei laufenden Aktivitäten alle erforderlichen Sicherheitsaspekte berücksichtigt werden. Informationssicherheit SOLLTE außerdem mit anderen Bereichen in der Institution, die sich mit Sicherheit und Risikomanagement beschäftigen, abgestimmt werden.

Der Informationssicherheitsbeauftragte MUSS an sicherheitsrelevanten Entscheidungen ausreichend beteiligt werden.

3.2 Standard-Anforderungen

Gemeinsam mit den Basisanforderungen entsprechen die folgenden Anforderungen dem Stand der Technik im Bereich Informationssicherheitsmanagement. Sie SOLLTEN grundsätzlich umgesetzt

4 Weiterführende Informationen

Weiterführende Informationen zu Gefährdung und Schutz von iOS finden sich unter anderem in folgenden Veröffentlichungen:

[[ISO/IEC 27000] Information technology — Security techniques — Information security management systems — Overview and vocabulary.
http://www.beuth.de (bzw. auf Englisch als kostenloser Download von www.iso.org).

[ISO/IEC 27001] Information technology – Security techniques – Information security management systems – Requirements

[BSI200-1] BSI-Standard 100-1 Managementsysteme für Informationssicherheit

[BSI200-2] BSI-Standard 200-2: Vorgehensweise nach IT-Grundschutz

Mit dem IT-Grundschutz publiziert das Bundesamt für Sicherheit in der Informationstechnik (BSI) Empfehlungen zur Informationssicherheit. Kommentare und Hinweise können von Lesern an grundschutz@bsi.bund.de gesendet werden.

5 Anlage: Kreuzreferenztabelle zu elementaren Gefährdungen

Die folgenden elementaren Gefährdungen sind für ein ISMS von Bedeutung:

G 0.18 Fehlplanung oder fehlende Anpassung

G 0.27 Ressourcenmangel

G 0.29 Verstoß gegen Gesetze oder Regelungen

Quelle: Bundesamt für Sicherheit in der Informationstechnik (BSI)

Neue Dokumentenstruktur - Umfang

- Je nach Baustein 1-6 Seiten

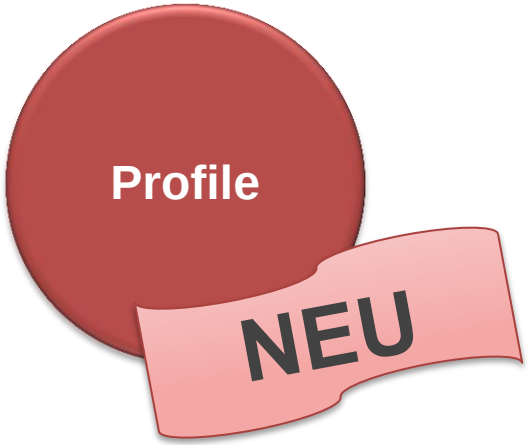
  + Gefährdungen

  + Maßnahmen

- Max. 10 Seiten
- Beschreiben Gefährdungen und Anforderungen ohne Verlinkung
- Ergänzend zu Baustein Umsetzungsempfehlungen mit
  - Lebenszyklus
  - Maßnahmen
  - Weiterführenden Informationen

Quelle: Bundesamt für Sicherheit in der Informationstechnik (BSI)

Kernthema Profile



Neues Klientel

- **Werkzeug** für anwenderspezifische Empfehlungen
- **Individuelle Anpassungen** an die jeweiligen Bedürfnisse
- Berücksichtigung der **Möglichkeiten und Risiken** der Institution
- Bezug auf **typische IT-Szenarien**
- **Profilerstellung** durch Dritte
- Keine **BSI-Vorgabe**
- Eventuell Nachweis für Umsetzung (z.B. Testat) und **Anerkennung ausgewählter Profile durch BSI**

Quelle: Bundesamt für Sicherheit in der Informationstechnik (BSI)

Ausblick

Migration vom alten zum neuen Sicherheitskonzept

- **Parallele Existenz** beider Modelle im **Übergangszeitraum**
- **Zusammenarbeit** zwischen **BSI** und **Herstellern** von IT-Grundschutz-Tools
- **Migrationsleitfaden** zur Überführung (geplant)
- **Migrationstabellen** mit Gegenüberstellung von „klassischen“ Maßnahmen und Anforderungen der modernisierten Bausteinen

Quelle: Bundesamt für Sicherheit in der Informationstechnik (BSI)

Ausblick

Migration vom alten zum neuen Sicherheitskonzept

		M 2.336 (A)	M 2.335 (A)	M 2.192 (A)	M 2.475 (A)	M 2.193 (A)	M 2.337 (A)	M 2.195 (A)	M 2.199 (A)	M 2.200 (C)	M 2.201 (C)	M 2.197 (A)	M 2.338 (Z)	M 2.339 (Z)	M 6.16 (Z)
	Basis-Anforderungen														
ISMS.1.A1	Übernahme der Gesamtverantwortung für Informationssicherheit durch die Leitungsebene	x													
ISMS.1.A2	Festlegung der Sicherheitsziele und -strategie		x												
ISMS.1.A3	Erstellung einer Leitlinie zur Informationssicherheit			x											
ISMS.1.A4	Benennung eines Informationssicherheitsbeauftragten														
ISMS.1.A5	Vertragsgestaltung bei Bestellung eines externen Informationssicherheitsbeauftragten				x										
ISMS.1.A6	Aufbau einer geeigneten Organisationsstruktur für Informationssicherheit					x									
ISMS.1.A7	Festlegung von Sicherheitsmaßnahmen							x							
ISMS.1.A8	Integration der Mitarbeiter in den Sicherheitsprozess											x			
ISMS.1.A9	Integration der Informationssicherheit in organisationsweite Abläufe und Prozesse						x								
	Standard-Anforderungen														
ISMS.1.A10	Erstellung eines Sicherheitskonzepts							x							
ISMS.1.A11	Aufrechterhaltung der Informationssicherheit								x						
ISMS.1.A12	Management-Berichte zur Informationssicherheit									x					
ISMS.1.A13	Dokumentation des Sicherheitsprozesses										x				
ISMS.1.A14	Sensibilisierung zur Informationssicherheit											x			
	Anforderungen bei erhöhtem Schutzbedarf														
ISMS.1.A14	Erstellung von zielgruppengerechten Sicherheitsrichtlinien												x		
ISMS.1.A15	Wirtschaftlicher Einsatz von Ressourcen für Informationssicherheit													x	
ISMS.1.A16	Abschließen von Versicherungen														x

Quelle: Bundesamt für Sicherheit in der Informationstechnik (BSI)

Vielen Dank für Ihre Aufmerksamkeit!

STAATSBETRIEB
SÄCHSISCHE
INFORMATIK DIENSTE

Freistaat
SACHSEN

Erfahren Sie mehr…

Sie finden uns unter:
www.sid.sachsen.de

Riesaer Straße 7

01129 Dresden

Telefon 0351 3264 5101

Telefax 0351 3264 5109