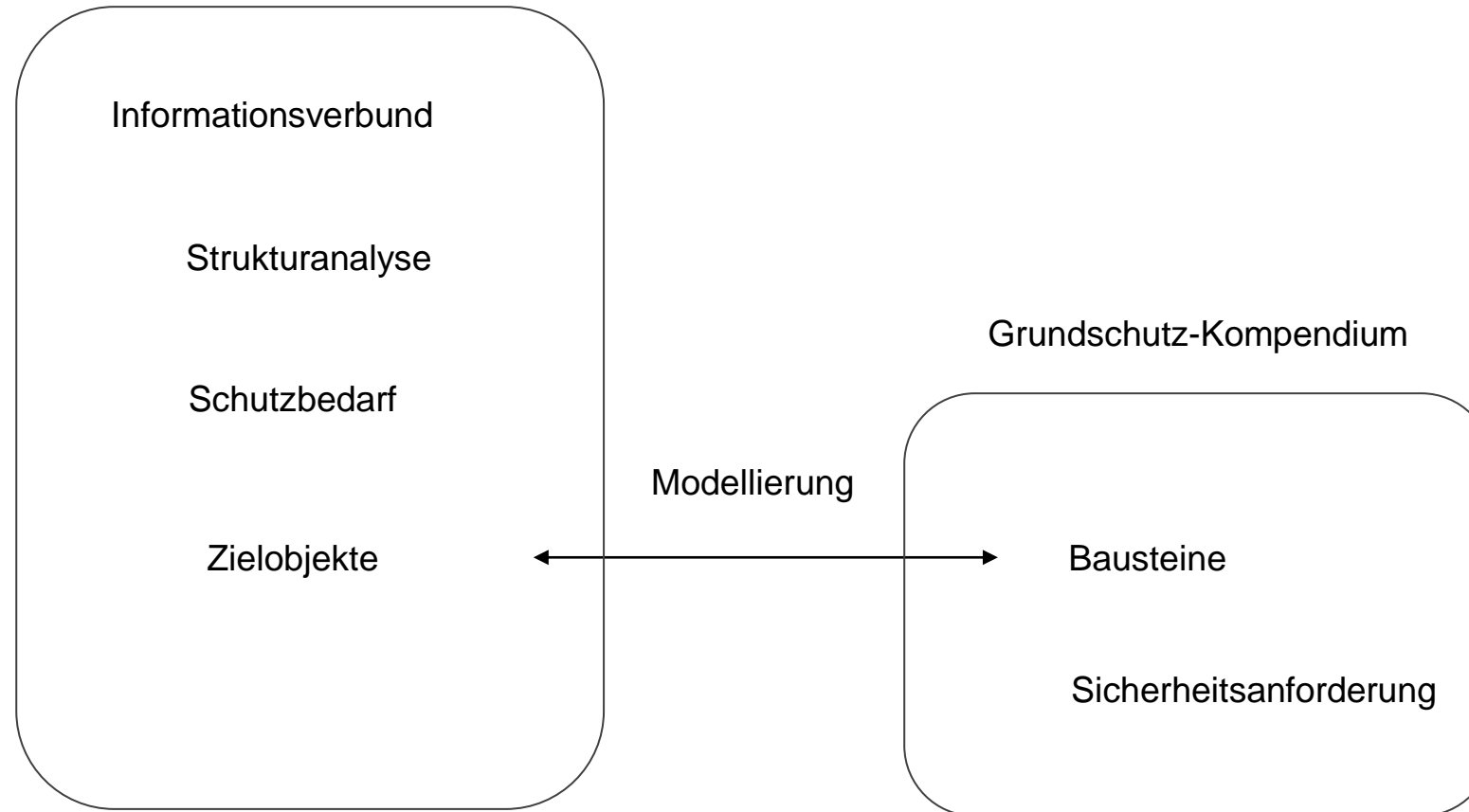


Unternehmen / zu untersuchender Bereich



- Unter einem **Informationsverbund** ist die Gesamtheit von infrastrukturellen, organisatorischen, personellen und technischen Objekten zu verstehen, die der Aufgabenerfüllung in einem bestimmten Anwendungsbereich der Informationsverarbeitung dienen.
- Ein Informationsverbund kann dabei als Ausprägung die gesamte Institution oder auch einzelne Bereiche, die durch organisatorische Strukturen (z. B. Abteilungen) oder gemeinsame Geschäftsprozesse bzw. Anwendungen (z. B. Personalinformationssystem) gegliedert sind, umfassen.

- In einer **Strukturanalyse** werden die erforderlichen Informationen über den ausgewählten Informationsverbund, die Geschäftsprozesse, Anwendungen, IT-Systeme, Netze, Räume, Gebäude und Verbindungen erfasst und so aufbereitet, dass sie die weiteren Schritte gemäß IT-Grundschutz unterstützen.

- Der **Schutzbedarf** beschreibt, welcher Schutz für die Geschäftsprozesse, die dabei verarbeiteten Informationen und die eingesetzte Informationstechnik ausreichend und angemessen ist.
- Bei der **Schutzbedarfsfeststellung** wird der Schutzbedarf der Geschäftsprozesse, der verarbeiteten Informationen und der IT-Komponenten bestimmt. Hierzu werden für jede Anwendung und die verarbeiteten Informationen die zu erwartenden Schäden betrachtet, die bei einer Beeinträchtigung der **Grundwerte der Informationssicherheit – Vertraulichkeit, Integrität oder Verfügbarkeit** – entstehen können. Wichtig ist es dabei auch, die möglichen Folgeschäden realistisch einzuschätzen. Bewährt hat sich eine Einteilung in die drei Schutzbedarfskategorien „normal“, „hoch“ und „sehr hoch“.

- Bei den Vorgehensweisen nach IT-Grundschutz wird bei der **Modellierung** der betrachtete Informationsverbund eines Unternehmens oder einer Behörde mit Hilfe der Bausteine aus dem IT-Grundschutz-Kompendium nachgebildet. Hierzu enthält Kapitel 2.2 des IT-Grundschutz-Kompendiums für jeden Baustein einen Hinweis, auf welche Zielobjekte er anzuwenden ist und welche Voraussetzungen dabei gegebenenfalls zu beachten sind.

Bundesamt für Sicherheit in der Informationstechnik: IT-Grundschutz-Kompendium, Glossar

- **Zielobjekte** sind Teile des Informationsverbunds, denen im Rahmen der Modellierung ein oder mehrere Bausteine aus dem IT-Grundschutz-Kompendium zugeordnet werden können. Zielobjekte können dabei physische Objekte sein, wie beispielsweise Netze oder IT-Systeme. Häufig sind Zielobjekte jedoch logische Objekte, wie beispielsweise Organisationseinheiten, Anwendungen oder der gesamte Informationsverbund.

- Das IT-Grundschutz-Kompendium enthält für unterschiedliche Vorgehensweisen, Komponenten und IT-Systeme Erläuterungen zur Gefährdungslage, Sicherheitsanforderungen und weiterführende Informationen, die jeweils in einem **Baustein** zusammengefasst sind.
- Das IT-Grundschutz-Kompendium ist aufgrund der Baustein-Struktur modular aufgebaut und legt einen Fokus auf die Darstellung der wesentlichen Sicherheitsanforderungen in den Bausteinen. Die grundlegende Struktur des IT-Grundschutz-Kompendiums sieht eine Unterteilung in prozess- und systemorientierte Bausteine vor, zudem sind sie nach Themen in ein Schichtenmodell einsortiert.

Bundesamt für Sicherheit in der Informationstechnik: IT-Grundschutz-Kompendium, Glossar

- Als **Sicherheitsanforderung** werden Anforderungen für den organisatorischen, personellen, infrastrukturellen und technischen Bereich bezeichnet, deren Erfüllung zur Erhöhung der Informationssicherheit notwendig ist bzw. dazu beiträgt. Eine Sicherheitsanforderung beschreibt also, was getan werden muss, um ein bestimmtes Niveau bezüglich der Informationssicherheit zu erreichen. Wie die Anforderungen im konkreten Fall erfüllt werden können, ist in entsprechenden Sicherheitsmaßnahmen beschrieben (siehe dort). Im englischen Sprachraum wird für Sicherheitsanforderungen häufig der Begriff „control“ verwendet.
- Der IT-Grundschutz unterscheidet zwischen **Basis-Anforderungen**, **Standard-Anforderungen** und **Anforderungen bei erhöhtem Schutzbedarf**. Basis-Anforderungen sind fundamental und stets umzusetzen, sofern nicht gravierende Gründe dagegen sprechen. Standard-Anforderungen sind für den normalen Schutzbedarf grundsätzlich umzusetzen, sofern sie nicht durch mindestens gleichwertige Alternativen oder die bewusste Akzeptanz des Restrisikos ersetzt werden. Anforderungen bei erhöhtem Schutzbedarf sind exemplarische Vorschläge, was bei entsprechendem Schutzbedarf zur Absicherung sinnvoll umzusetzen ist.

Bundesamt für Sicherheit in der Informationstechnik: IT-Grundschutz-Kompendium, Glossar

- **Basis-Absicherung**

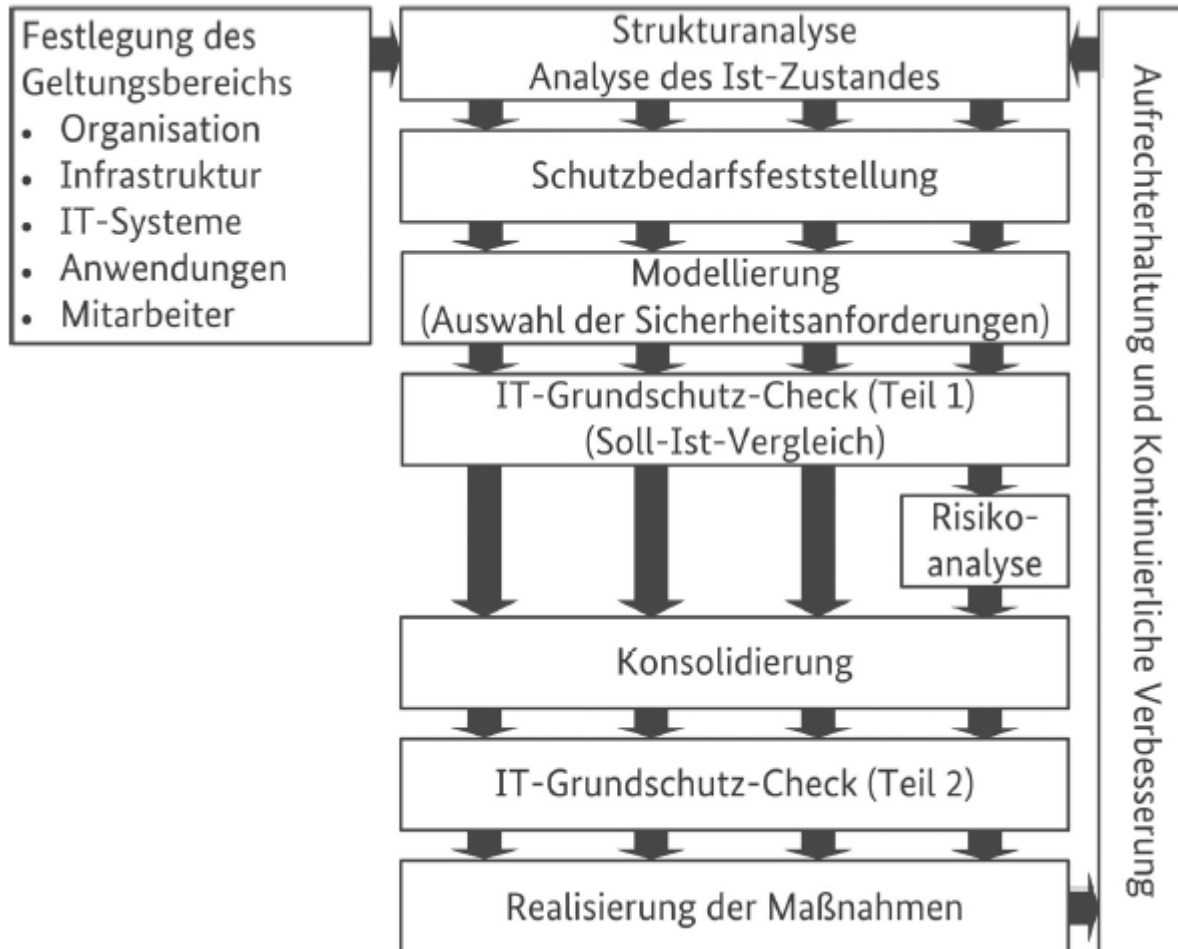
Die Basis-Absicherung ermöglicht es, als Einstieg in den IT-Grundschutz zunächst eine breite, grundlegende Erst-Absicherung über alle Geschäftsprozesse bzw. Fachverfahren einer Institution vorzunehmen

- **Kern-Absicherung**

Im Fokus der Kern-Absicherung stehen zunächst die besonders gefährdeten Geschäftsprozesse und Assets.

- **Standard-Absicherung**

Die Standard-Absicherung entspricht im Wesentlichen der klassischen IT-Grundschutz-Vorgehensweise des BSI-Standards 100-2. Mit der Standard-Absicherung kann ein ISB die Assets und Prozesse einer Institution sowohl umfassend als auch in der Tiefe absichern

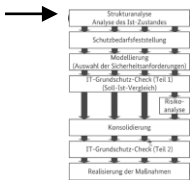


Modellierung = Nachbildung des Informationsverbundes mit Hilfe der Bausteine

- Für jeden Baustein des IT-Grundschutz-Kompendiums ermitteln, auf welche Zielobjekte er im betrachteten Informationsverbund anzuwenden ist
- Zuordnung von Bausteinen zu Zielobjekten („IT-Grundschutz-Modell“) sowie die entsprechenden Ansprechpartner dokumentieren
- Zielobjekte, die nicht geeignet modelliert werden können, für eine Risikoanalyse vormerken
- Festlegung einer Reihenfolge für die Umsetzung der Bausteine
- Sicherheitsanforderungen aus den identifizierten Bausteinen sorgfältig lesen und darauf aufbauend passende Sicherheitsmaßnahmen festlegen

Quelle: BSI-Standard 200-2: IT-Grundschutz-Methodik, S. 76, S. 145

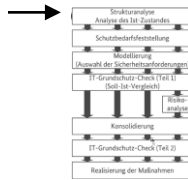
A.1 Geschäftsprozesse der RECPLAST GmbH				
Bezeichnung	Beschreibung des Prozesses	Prozess-Art	Prozessverantwortlicher	Mitarbeiter
GP001	Produktion: Die Produktion der Kunststoffartikel umfasst alle Phasen von der Materialbereitstellung bis hin zur Einlagerung des produzierten Materials. Hierzu gehören innerhalb der Produktion die internen Transportwege, die Produktion und Fertigung der verschiedenen Komponenten und das Verpacken der Teile.	Kerngeschäft	Leiter Produktion	Alle Mitarbeiter
GP002	Angebotswesen: In der Angebotsabwicklung werden die Kundenanfragen für Produkte verarbeitet. Im Regelfall werden Kundenanfragen formlos per E-Mail oder Fax geschickt. Die Angebote werden elektronisch erfasst und ein schriftliches Angebot per Post an den Kunden versendet.	Unterstützender Prozess	Leiter Angebotswesen	Vertrieb
	Auftragsabwicklung: Kunden schicken die Bestellungen im Regelfall per E-Mail oder Fax.			

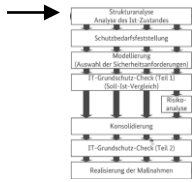


Quelle: BSI-Standard 200-2: IT-Grundschutz-Methodik, S. 84

A.1 Strukturanalyse der RECPLAST GmbH									
Bezeichnung	Beschreibung des Zielobjektes / der Gruppe der Zielobjekte	Plattform / Baustein	Ort	Gebäude	Raum	Anzahl	Status	Benutzer	Verantwortlich / Administrator
A003	Textverarbeitung, Tabellenkalkulation: Alle geschäftlichen Informationen werden in einem Office-Produkt verarbeitet, Geschäftsbriefe, Analysen oder Präsentationen	Office-Produkt 2010	-	-	-	130	in Betrieb	Alle Mitarbeiter	IT-Betrieb
A004	Chat-Anwendung: Eine Chat-Anwendung soll den Kontakt zwischen den Mitarbeitern vereinfachen. Die E-Mails werden standardmäßig nur zwei Mal pro Tag abgerufen. Diese Anwendung wird als virtualisierte Anwendung eingesetzt.	Standardsoftware	-	-	-	130	in Betrieb	Alle Mitarbeiter	IT-Betrieb
A008	Active Directory: Diese Anwendung soll dem IT-Betrieb die Arbeit erleichtern und doppelte Benutzereingaben reduzieren.	Active Directory	Bonn	BG	Büro	5	Test	Administratoren	IT-Betrieb

Quelle: BSI-Standard 200-2: IT-Grundschutz-Methodik, S. 86



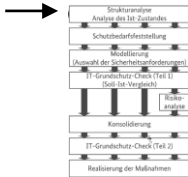


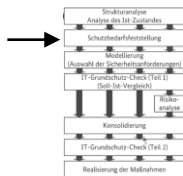
A.1 Zuordnungen Geschäftsprozesse zu Anwendungen der RECPLAST GmbH										
Geschäftsprozess / Anwendung	A001	A002	A003	A004	A005	A006	A007	A008	A009	A010
GP001	x					x	x			x
GP002					x	x	x		x	
GP003					x	x	x		x	
GP004			x	x		x	x	x	x	
GP005			x			x	x	x	x	

Quelle: BSI-Standard 200-2: IT-Grundschutz-Methodik, S. 87

A.1 Strukturanalyse der RECPLAST GmbH									
Bezeichnung	Beschreibung des Zielobjektes / der Gruppe der Zielobjekte	Plattform / Baustein	Ort	Gebäude	Raum	Anzahl	Status	Benutzer	Verantwortlich / Administrator
N001	Router Internetanbindung: Dieser Router regelt die Kommunikation zwischen dem Internet und den internen Prozessen	Router und Switches	Bonn	BG	Server-raum	1	in Betrieb	Administratoren	IT-Betrieb
N002	Firewall Internet-Eingang: Diese Firewall dient als Schutz zwischen dem Internet und dem internen Netz	Firewall	Bonn	BG	Server-raum	1	in Betrieb	Administratoren	IT-Betrieb
N003	Switch – Verteilung Der Datenfluss in Richtung Internet und internes Netz wird über den Switch gesteuert	Router und Switches	Bonn	BG	Server-raum	1	in Betrieb	Administratoren	IT-Betrieb
N004	Router Bonn BG – Beuel Über eine Standleitung sind die beiden Standorte in Bonn verbunden. Diese Router sichern die Verbindung ab.	Router und Switches	Bonn	-	Server-raum	2	in Betrieb	Administratoren	IT-Betrieb
S008	Print-Server: Server für die Druckerdienste, die zentral gesteuert werden.	Windows Server 2012	Bonn	BG	Server-raum	1	in Betrieb	Alle Mitarbeiter	IT-Betrieb

Quelle: BSI-Standard 200-2: IT-Grundschutz-Methodik, S. 93





8.2 Schutzbedarfsfeststellung

Ziel der Schutzbedarfsfeststellung ist es, für die erfassten Objekte im Informationsverbund zu entscheiden, welchen Schutzbedarf sie bezüglich Vertraulichkeit, Integrität und Verfügbarkeit besitzen. Dieser Schutzbedarf orientiert sich an den möglichen Schäden, die mit einer Beeinträchtigung der betroffenen Anwendungen und damit der jeweiligen Geschäftsprozesse verbunden sind.

1. Schutzbedarfsfeststellung für den Informationsverbund gliedert sich in mehrere Schritte:
 2. Definition der Schutzbedarfskategorien
 3. Schutzbedarfsfeststellung für Geschäftsprozesse und Anwendungen
 4. Schutzbedarfsfeststellung für IT-Systeme, IoT- und ICS-Geräte
 5. Schutzbedarfsfeststellung für Gebäude, Räume, Werkhallen usw.
 6. Schutzbedarfsfeststellung für Kommunikationsverbindungen
- Schlussfolgerungen aus den Ergebnissen der Schutzbedarfsfeststellung

Nach der Definition der Schutzbedarfskategorien wird anhand von typischen Schadensszenarien zunächst der Schutzbedarf der Geschäftsprozesse und Anwendungen bestimmt. Anschließend wird daraus der Schutzbedarf der einzelnen IT-Systeme, Räume und Kommunikationsverbindungen abgeleitet.

→ gehenweise hierfür wird in den folgenden Abschnitten detailliert dargestellt.

8.2.1 Definition der Schutzbedarfskategorien

Da der Schutzbedarf meist nicht quantifizierbar ist, beschränkt sich der IT-Grundsicherheitschutz somit auf eine qualitative Aussage, indem der Schutzbedarf in drei Kategorien unterteilt wird:

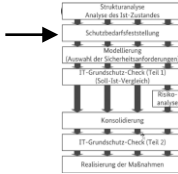
Schutzbedarfskategorien	
„normal“	Die Schadensauswirkungen sind begrenzt und überschaubar.
„hoch“	Die Schadensauswirkungen können beträchtlich sein.
„sehr hoch“	Die Schadensauswirkungen können ein existenziell bedrohliches, katastrophales Ausmaß erreichen.

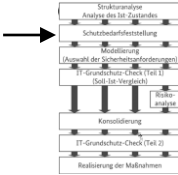
Quelle: BSI-Standard 200-2: IT-Grundsicherheits-Methodik, S. 104

Schutzbedarfskategorie „normal“	
1. Verstoß gegen Gesetze/ Vorschriften/Verträge	<ul style="list-style-type: none"> • Verstöße gegen Vorschriften und Gesetze mit geringfügigen Konsequenzen • Geringfügige Vertragsverletzungen mit maximal geringen Konventionalstrafen
2. Beeinträchtigung des informationellen Selbstbestimmungsrechts	<ul style="list-style-type: none"> • Es handelt sich um personenbezogene Daten, durch deren Verarbeitung der Betroffene in seiner gesellschaftlichen Stellung oder in seinen wirtschaftlichen Verhältnissen beeinträchtigt werden kann.
3. Beeinträchtigung der persönlichen Unversehrtheit	<ul style="list-style-type: none"> • Eine Beeinträchtigung erscheint nicht möglich.
4. Beeinträchtigung der Aufgabenerfüllung	<ul style="list-style-type: none"> • Die Beeinträchtigung würde von den Betroffenen als tolerabel eingeschätzt werden. • Die maximal tolerierbare Ausfallzeit liegt zwischen 24 und 72 Stunden.
5. Negative Innen- oder Außenwirkung	<ul style="list-style-type: none"> • Eine geringe bzw. nur interne Ansehens- oder Vertrauensbeeinträchtigung ist zu erwarten.
6. Finanzielle Auswirkungen	<ul style="list-style-type: none"> • Der finanzielle Schaden bleibt für die Institution tolerabel.

Tabelle 2: Schutzbedarfskategorie „normal“

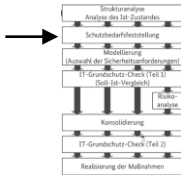
Quelle: BSI-Standard 200-2: IT-Grundschutz-Methodik, S. 106





Schutzbedarfskategorie „hoch“	
1. Verstoß gegen Gesetze/Vorschriften/Verträge	<ul style="list-style-type: none"> • Verstöße gegen Vorschriften und Gesetze mit erheblichen Konsequenzen • Vertragsverletzungen mit hohen Konventionalstrafen
2. Beeinträchtigung des informationellen Selbstbestimmungsrechts	<ul style="list-style-type: none"> • Es handelt sich um personenbezogene Daten, bei deren Verarbeitung der Betroffene in seiner gesellschaftlichen Stellung oder in seinen wirtschaftlichen Verhältnissen erheblich beeinträchtigt werden kann.
3. Beeinträchtigung der persönlichen Unversehrtheit	<ul style="list-style-type: none"> • Eine Beeinträchtigung der persönlichen Unversehrtheit kann nicht absolut ausgeschlossen werden.
4. Beeinträchtigung der Aufgabenerfüllung	<ul style="list-style-type: none"> • Die Beeinträchtigung würde von einzelnen Betroffenen als nicht tolerabel eingeschätzt. • Die maximal tolerierbare Ausfallzeit liegt zwischen einer und 24 Stunden.
5. Negative Innen- oder Außenwirkung	<ul style="list-style-type: none"> • Eine breite Ansehens- oder Vertrauensbeeinträchtigung ist zu erwarten.
6. Finanzielle Auswirkungen	<ul style="list-style-type: none"> • Der Schaden bewirkt beachtliche finanzielle Verluste, ist jedoch nicht existenzbedrohend.

Quelle: BSI-Standard 200-2: IT-Grundsicherheits-Methodik, S. 106

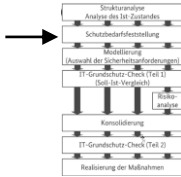


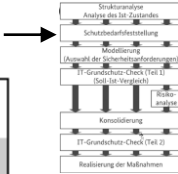
Schutzbedarfskategorie „sehr hoch“	
1. Verstoß gegen Gesetze/ Vorschriften/Verträge	<ul style="list-style-type: none"> Fundamentaler Verstoß gegen Vorschriften und Gesetze Vertragsverletzungen, deren Haftungsschäden ruinös sind
2. Beeinträchtigung des infor- mationellen Selbstbestim- mungsrechts	<ul style="list-style-type: none"> Es handelt sich um personenbezogene Daten, bei deren Verar- beitung eine Gefahr für Leib und Leben oder die persönliche Frei- heit des Betroffenen gegeben ist.
3. Beeinträchtigung der per- sönlichen Unversehrtheit	<ul style="list-style-type: none"> Gravierende Beeinträchtigungen der persönlichen Unversehr- theit sind möglich. Gefahr für Leib und Leben
4. Beeinträchtigung der Auf- gabenerfüllung	<ul style="list-style-type: none"> Die Beeinträchtigung würde von allen Betroffenen als nicht tole- rabel eingeschätzt werden. Die maximal tolerierbare Ausfallzeit ist kleiner als eine Stunde.
5. Negative Innen- oder Au- ßenwirkung	<ul style="list-style-type: none"> Eine landesweite Ansehens- oder Vertrauensbeeinträchtigung, eventuell sogar existenzgefährdender Art, ist denkbar.
6. Finanzielle Auswirkungen	<ul style="list-style-type: none"> Der finanzielle Schaden ist für die Institution existenzbedrohend.

Quelle: BSI-Standard 200-2: IT-Grundschutz-Methodik, S. 107

A.2 Schutzbedarfsfeststellung der RECPLAST GmbH									
Bezeichnung	Beschreibung des Zielobjektes / der Gruppe der Zielobjekte	Plattform / Baustein	Verantwortlich / Administrator	Vertraulichkeit	Begründung für die Vertraulichkeit	Integrität	Begründung für die Integrität	Verfügbarkeit	Begründung für die Verfügbarkeit
A003	Textverarbeitung, Tabellenkalkulation	Office-Produkt 2010	IT-Betrieb	normal	Die Anwendung selbst enthält keine Informationen.	normal	Die Anwendung selbst enthält keine Informationen	normal	Die Anwendung wird lokal installiert. Die Lizenzen sind entsprechend aufgehoben, so dass eine Neuinstallation schnell ermöglicht werden kann. Eine Ausfallzeit von mehr als 24 Stunden ist tolerierbar.
A007	Lotus Notes	Lotus Notes	IT-Betrieb	hoch	Über das E-Mailsystem werden viele, teilweise vertrauliche Informationen versendet. Durch die Anwendung werden alle E-Mails verschlüsselt.	normal	Durch eine Signatur kann die Integrität einer E-Mail festgestellt werden.	sehr hoch	Das Mailsystem sollte auch dann zur Verfügung stehen, falls andere Kommunikationsmittel ausfallen (z.B. Faxserver)
C002	Laptop Verwaltung	Client unter Windows 10	IT-Betrieb	normal	Maximumprinzip Auf dem Arbeitsplatzrechner werden keine Informationen gespeichert	normal	Maximumprinzip Auf dem Arbeitsplatzrechner werden keine Informationen gespeichert	normal	Es ist ein Ausfall von höchstens 4 Stunden tolerierbar.

Quelle: BSI-Standard 200-2: IT-Grundschutz-Methodik, S. 107

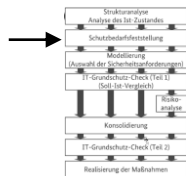




A.2 Schutzbedarfsfeststellung der RECLAST GmbH

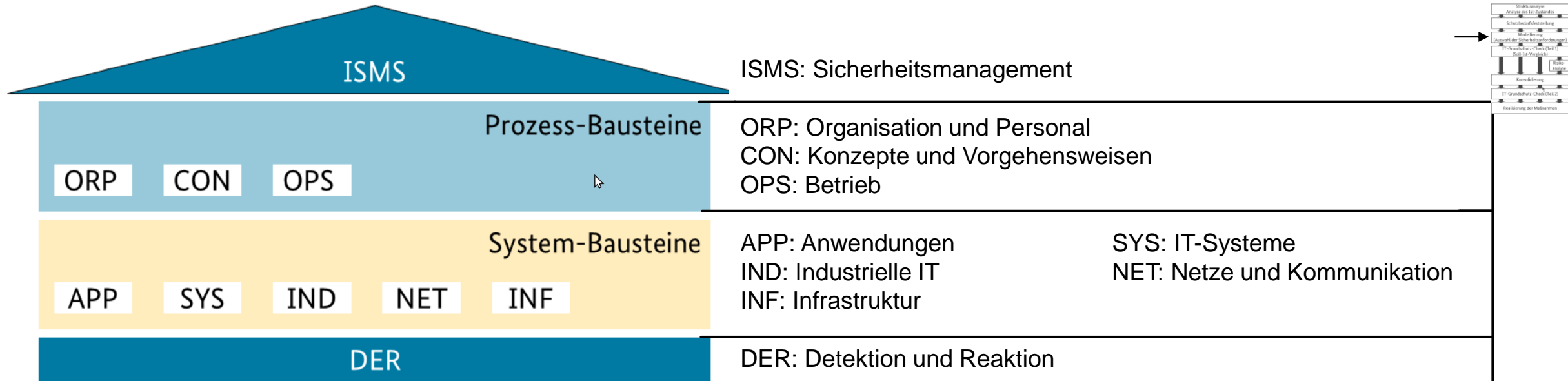
Bezeichnung	Beschreibung des Ziel- objektes / der Gruppe der Zielobjekte	Plattform / Baustein	Vertraulich- keit	Begründung für die Vertraulichkeit	Integrität	Begründung für die Integrität	Verfügbar- keit	Begründung für die Verfügbar- keit
N001	Router Internetanbin- dung	Router und Switches	hoch	Zutritt, Zugang und Zu- griff nur für autorisierte Personen möglich	normal	Zutritt, Zugang und Zugriff nur für auto- risierte Personen möglich	normal	Ersatzgerät liegt auf Lager und kann schnell durch den IT-Betrieb aus- getauscht werden
N002	Firewall Internet- Eingang	Firewall	hoch	Die Konfigurationsei- genschaften müssen vertraulich bleiben. Diese regeln den Da- tenverkehr zwischen dem Internet und der RECLAST	normal	Zutritt, Zugang und Zugriff nur für auto- risierte Personen möglich	normal	Ersatzgerät liegt auf Lager und kann schnell durch den IT-Betrieb aus- getauscht werden
N003	Switch – Verteilung	Router und Switches	normal	Zutritt, Zugang und Zu- griff nur für autorisierte Personen möglich	normal	Zutritt, Zugang und Zugriff nur für auto- risierte Personen möglich	normal	Ersatzgerät liegt auf Lager und kann schnell durch den IT-Betrieb aus- getauscht werden

Quelle: BSI-Standard 200-2: IT-Grundschutz-Methodik, S. 116



Schutzwirkung von Sicherheitsanforderungen nach IT-Grundschutz	
Schutzbedarfskategorie „normal“	Sicherheitsanforderungen nach IT-Grundschutz sind im Allgemeinen ausreichend und angemessen.
Schutzbedarfskategorie „hoch“	Sicherheitsanforderungen nach IT-Grundschutz liefern eine Standard-Absicherung, sind aber unter Umständen alleine nicht ausreichend. Weitergehende Maßnahmen sollten auf Basis einer Risikoanalyse ermittelt werden.
Schutzbedarfskategorie „sehr hoch“	Sicherheitsanforderungen nach IT-Grundschutz liefern eine Standard-Absicherung, reichen aber alleine im Allgemeinen nicht aus. Die erforderlichen zusätzlichen Sicherheitsmaßnahmen müssen individuell auf der Grundlage einer Risikoanalyse ermittelt werden.

Quelle: BSI-Standard 200-2: IT-Grundschutz-Methodik, S. 130



Elementare Gefährdungen (Auszug)

- G 0.14 Ausspähen von Informationen (Spionage)
- G 0.21 Manipulation von Hard- oder Software
- G 0.22 Manipulation von Informationen
- G 0.23 Unbefugtes Eindringen in IT-Systeme
- G 0.25 Ausfall von Geräten oder Systemen
- G 0.28 Software-Schwachstellen oder -Fehler
- 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 0.39 Schadprogramme
- G 0.43 Einspielen von Nachrichten
- G 0.45 Datenverlust
- G 0.46 Integritätsverlust schützenswerter Informationen

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
- APP.3.2 Webserver
- APP.3.3 Fileserver
- APP.3.4 Samba
- APP.3.6 DNS-Server

APP.4 Business-Anwendungen

- APP.4.2 SAP-ERP-System
- APP.4.3 Relationale Datenbanken
- 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

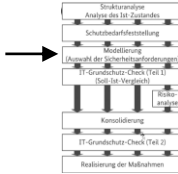
APP.6 Allgemeine Software

APP.7 Entwicklung von Individualsoftware

Beispiel: SAP-ERP-System x elementare Gefährdungen

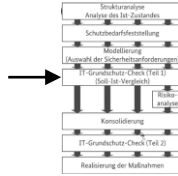
-> APP.4.2 SAP-ERP-System

Basis:	 	Anforderungen
Standard:	 	für jede
hoch:	 	Schutzbedarfskategorie

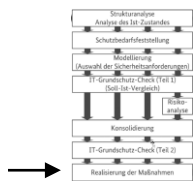


Baustein	APP.4.2 SAP-ERP-System Enterprise-Resource-Planning-Systeme von SAP (kurz SAP-ERP-Systeme) werden eingesetzt, um interne und externe Geschäftsabläufe zu automatisieren und technisch zu unterstützen. SAP-ERP-Systeme verarbeiten daher typischerweise vertrauliche Informationen, sodass alle Komponenten und Daten geeignet geschützt werden müssen.
Gefährdungslage (Beispiel)	2 3 Mangelnde Planung, Umsetzung und Dokumentation eines SAP-Berechtigungskonzeptes Wird das SAP-Berechtigungskonzept nicht ausreichend dokumentiert, können vergebene Berechtigungen nicht mehr nachvollzogen und somit gepflegt werden. So ist es z. B. möglich, dass bereits ausgeschiedene oder mit neuen Aufgaben betraute Mitarbeiter noch auf SAP-ERP-Systeme zugreifen können.
Anforderung (Beispiel)	APP.4.2.A6 Erstellung und Umsetzung eines Benutzer- und Berechtigungskonzeptes [Fachabteilung, Entwickler, Leiter IT] Für SAP-ERP-Systeme MUSS ein Benutzer- und Berechtigungskonzept ausgearbeitet und umgesetzt werden. Dabei MÜSSEN folgende Punkte berücksichtigt werden: <ul style="list-style-type: none"> • ... • Benutzer-, Berechtigungs- und ggf. Profiladministrator MÜSSEN getrennte Verantwortlichkeiten und damit Berechtigungen haben. • ... Es SOLLTEN geeignete Kontrollmechanismen angewandt werden, um SoD-Konfliktfreiheit von Rollen und die Vergabe von kritischen Berechtigungen an Benutzer zu überwachen.
Maßnahme (Beispiel)	Maßnahmen für eine sichere Administration der Benutzer-IDs im SAP-ERP-System Systemzugriffe sind nur autorisierten Personen gestattet, die sich im SAP-ERP-System mit einer Benutzer-ID und einem gültigen Passwort authentisieren müssen. Unberechtigte Systemzugriffe können durch bestimmten Sicherheitsmechanismen verhindert werden. Benutzeradministratoren sollten sich an folgende Empfehlung halten: <ul style="list-style-type: none"> • Jede Benutzer-ID ist einer realen Person zugeordnet. • Es sollten keine Sammelkonten angelegt werden • ...
Verantwortung	Bausteinverantwortlicher IT-Betrieb Weitere Verantwortliche Entwickler, Fachabteilung, Leiter IT, Notfallbeauftragter

A.4 IT-Grundschutz-Check der RECPLAST GmbH				
Baustein: Sicherheitsmanagement				
Anforderung	Anforderungstitel	Verantwortung	Status	Umsetzung
ISMS.1.A1	Übernahme der Gesamtverantwortung für Informationssicherheit durch die Leitungsebene	Institutionsleitung	umgesetzt	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 Umsetzungsstatus der Maßnahmen und initiiert ggf. weitere Maßnahmen und bewilligt das entsprechende Budget.
ISMS.1.A5	Vertragsgestaltung bei Bestellung eines externen Informationssicherheitsbeauftragten	Institutionsleitung	entbehrlich	Der Informationssicherheitsbeauftragte ist ein interner Mitarbeiter der RECPLAST GmbH.
ISMS.1.A7	Festlegung von Sicherheitsmaßnahmen	ISB	teilweise	Alle Mitarbeiter, die Maßnahmen im Sinne der Informationssicherheit umsetzen, sind verpflichtet, diese zu dokumentieren und dem ISB per E-Mail zuzusenden. Eine Auswertung und ausreichende Dokumentation der eingehenden umgesetzten Maßnahmen gibt es nicht. Umsetzungszeitpunkt für ausführliche Dokumentation: 30.04.



A.6 Realisierungsplan der RECPLAST GmbH						
Ziel- objekt	Baustein	Anforde- rungstext	umzusetzende Maßnahmen	Termin- planung	Budget	Verant- wortlich für die Um- setzung
S008 – Print-- Server	SYS.1.1 Allgemei- ner Server	SYS.1.1.A3 Restriktive Rechtverga- be	In der Rechtevergabe müssen die letzten Gruppenberech- tigungen aufgelöst werden.	Q3 des Jahres	- €	Herr Schmidt (IT-Betrieb)
S008 – Print-- Server	SYS.1.1 Allgemei- ner Server	SYS.1.1.A4 Rollentren- nung	Es sind noch nicht für jeden Ad- ministrator separate Benut- zer-Kennungen eingerichtet.	31.07. des Jahres	- €	Herr Schmidt (IT-Betrieb)
S008 – Print-- Server	SYS.1.1 Allgemei- ner Server	SYS.1.1.A8 Regelmäße- ge Datensi- cherung	Die Datensicherungen werden derzeit auf Bändern innerhalb des Serverraumes aufbewahrt. Geplant ist hierzu ein externes Backup-System. Ein Angebot für die Initialisierung liegt be- reits vor (15.000 €). Die Be- triebskosten müssen noch ver- handelt werden.	Q1 Folge- jahr	Anschaf- fung: 15.000 € Betriebs- kosten: noch offen	Frau Meyer (Einkauf)



Quelle: BSI-Standard 200-2: IT-Grundschutz-Methodik

Möglichkeiten



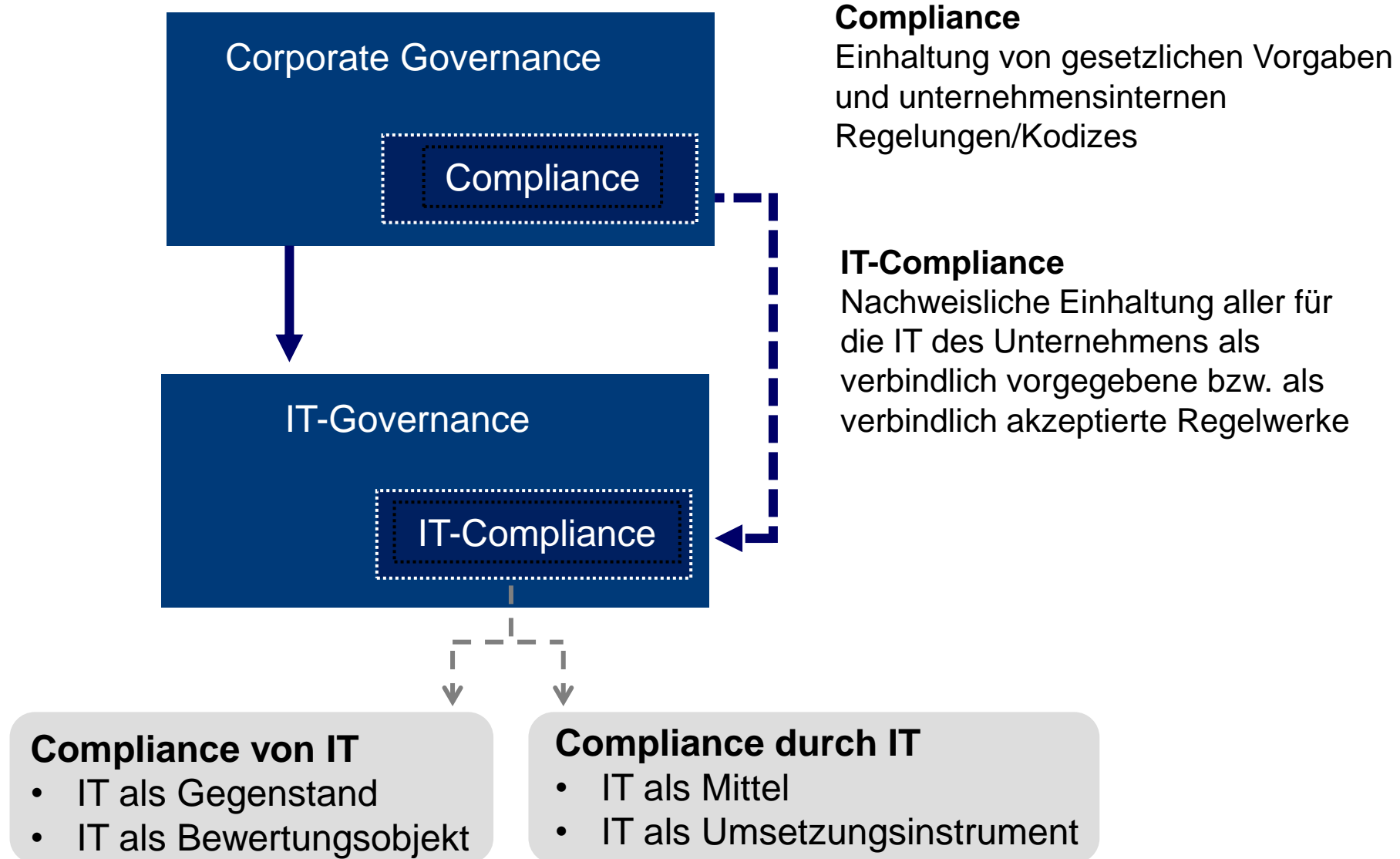
- Systematischer Aufbau
- Stufenweises Vorgehen
- „Checkliste“, kann verwendet werden, um eigenen Stand im Thema IT-Sicherheit zu beurteilen
- Grundlage für Zertifizierung, Dokumentation/Nachweis für Stakeholder
- Fokus auf operative Umsetzung
- Materialien sind kostenlos verfügbar
- Unterstützung des gesamten Zyklus (Identifikation/Analyse/Steuerung/Überwachung)

Grenzen



- Komplexität, ggf. überdimensioniert
- Gefahr des „Ausruhens“ nach erstmaliger Umsetzung, Kontinuität muss sichergestellt werden

- Überblick
- IT-Strategie
- IT-Governance, Risikomanagement und Compliance
 - IT-Governance
 - IT-Risikomanagement
 - IT-Compliance
- IT-Organisation
- IT-Outsourcing
- IT-Servicemanagement



Kodizes

Normen

(ISO 19600, ISO/IEC 2700x,...)

Standards

(CobiT, ITIL, COSO, IDW PS, BSI-GS)...

Richtlinien (E-Mail-, Passwort-RL,...)

Service Level Agreements,

Verfahrensanweisungen,

...

Unternehmensexterne
Regelwerke

Unternehmensinterne
Regelwerke

Rechtliche Vorgaben
(Extern)

Rechnungswesen/

Unternehmensorganisation

GoBS, GoB, GDPdU, E-Mail-
Archivierungsvorschr., BilMoG, IFRS/IAS,
Basel II, Solvency II, KonTraG, AktG,
HGB, BilReG, Empfehlungen DCGK,
KWG, AO, UStg

Supranationales

Recht

8. EU-Richtlinie, SOX,
APAG, FINRA(NASD/SEC),
IFRS, EU-DSGVO,
EU-ePrivacy-Verordnung

Datenschutz/ -sicherheit

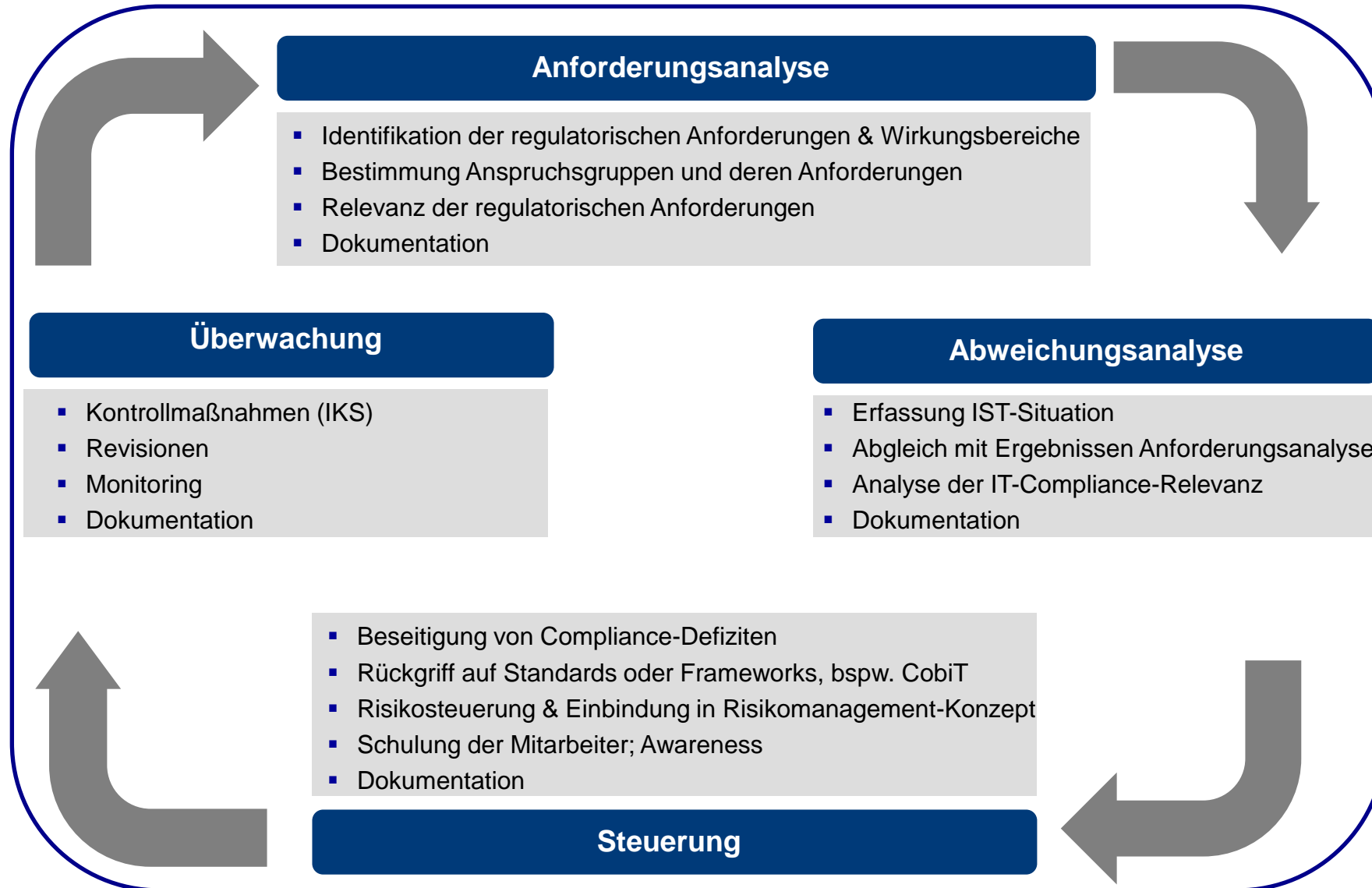
BDSG, TKG, UrhG
IT-Sicherheitsgesetz,
StGB

Arbeits- Recht

BetrVG §§80 (1,2)
§87 (6)
Bildschirmarbv

Branchen-/ Größenspezifisch

WpHG, BaFin, FdA, GMP,
MARisk, EU-
Vermittlerrichtlinie,
Produkthaftungsgesetz



- Überblick
- IT-Strategie
- IT-Governance, Risikomanagement und Compliance
 - IT-Governance
 - IT-Risikomanagement
 - IT-Compliance
- IT-Organisation
- IT-Outsourcing
- IT-Servicemanagement