

ISW Mit Sicherheit
ein Blick fürs Ganze

Praktische Umsetzung des Risikomanagements – vom kritischen Prozess zum Schutzbedarf der IT-Assets

Marion Steiner - Workshop GI-SECMGT am 08.11.2024

Navigieren durch den Regularien-Dschungel:

DORA, NIS2 und CRA als Wegweiser für Informationssicherheit

– öffentlich –

(IKT-)Risikomanagement im ISMS

Übersicht des „Toolkits“

Der IKT-Risikoprozess

... in der Praxis

Einbindung in die Organisation und Vorgabenwelt



Marion Steiner

Generalbevollmächtigte, IT-Security Expertin, eISB und eDSB

marion.steiner@isw-online.de

+49 151 58487603

Marion Steiner ist Dipl. Informatikerin und seit zwanzig Jahren Beraterin mit Schwerpunkt Informationssicherheit.

Aktuell ist sie bei der IT-Security@Work GmbH (ISW) (www.isw-online.de) als Fachexpertin in Projekten im Einsatz sowie für die fachliche Ausrichtung des Unternehmens zuständig.

Ihr erklärtes Ziel ist es, dass Informationssicherheit und Compliance nicht als Störfaktoren, sondern als Mehrwert für ein Unternehmen wahrgenommen werden. Bei ihrer Arbeit stehen daher risikobasierte Verfahren sowie Vereinbarkeit von Geschäftsprozessen, IT-Betrieb und Compliance (inklusive Informationssicherheit und Datenschutz) im Vordergrund.

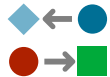
Die **Einführung eines ISMS** ist eine **strategische Entscheidung** der Organisation.
Insbesondere die Erstellung und Umsetzung eines ISMS richtet sich stark nach den



Bedürfnissen und Zielen,



Sicherheitsanforderungen,



Organisatorischen Abläufen



sowie Größe und Struktur ... einer Organisation.

Diese Einflussgrößen sollten als **Variablen** betrachtet werden,
welche sich im Laufe der Zeit ändern können.

Warum die ganze Mühe?

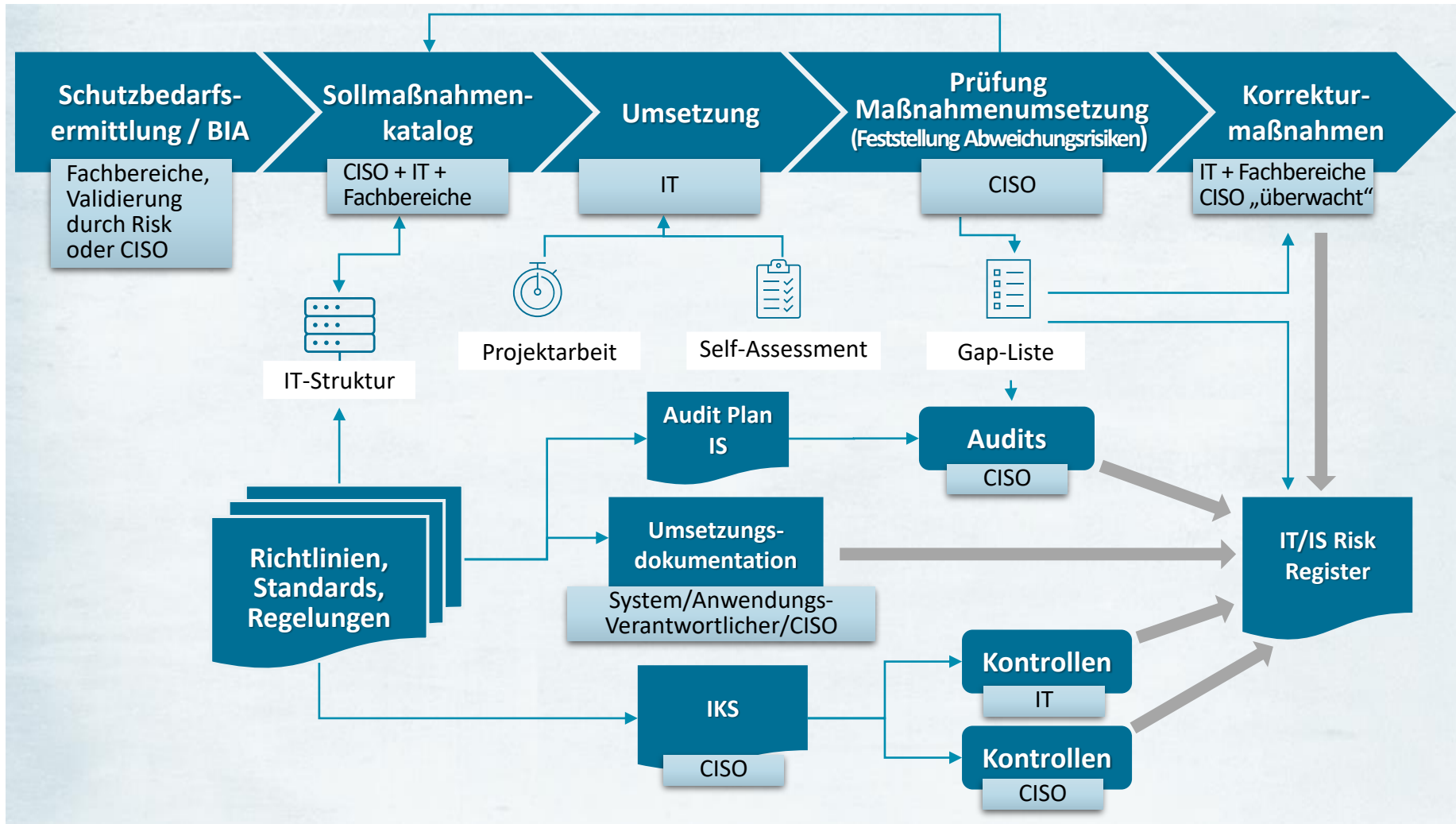
- **Risikominimierung** z. B. durch
 - Identifikation kritischer Prozesse und Abläufe
 - Systematische Erkennung von Bedrohungen und Schwachstellen
- **Kostenreduzierung** z. B. durch
 - Aufdeckung und Verbesserung ineffizienter Prozesse
 - Produktionssteigerung/ Geschäftsoptimierung durch strukturiertere Unternehmensprozesse
 - Verbesserung der Systemverfügbarkeit (Produktivitätssteigerung)
 - Geringere Haftungsrisiken ➔ geringere Versicherungsbeiträge
- **Steigerung des Sicherheitsniveaus** z. B. durch
 - Schutz vor steigender Cyber-Kriminalität und Attacken
 - Schutz aller Arten von digitalen und physischen Informationen / geistigem Eigentum
- **Verbesserte Außenwirkung** z. B. durch
 - Beweise für hohe Qualitäts- und Sicherheitsstandards
 - Erhöhtes Vertrauen durch Kunden, Dienstleister, Vertragspartner, Versicherungen usw.
- **Erhöhte Transparenz** z. B. durch
 - Einführung organisationsweiter Strukturen
 - Nachweise interner Kontrollen
 - Kontinuierliche Überwachung und Verbesserung der Prozesse (Qualitätssicherung)

Bestandsaufnahme, Risikoeinschätzung, Konzeption

- Prozesse, benötigte Informationswerte und deren Eigentümer im Kontext der kDL (Geltungsbereichs ISMS) identifizieren
- Bedrohungen und Schwachstellen identifizieren
- Eigentümer der Risiken identifizieren
- Bewertung der aktuell umgesetzten Maßnahmen (GAP-Analyse, Reifegradanalyse)
- Bewertung von Auswirkungen und Eintrittswahrscheinlichkeiten
- Entscheidung über nicht akzeptable Risiken (Schutzbedarf vs. Risiko)
- Risikobehandlung für jedes nicht akzeptable Risiko definieren; Maßnahmen auswählen und Restrisiko abschätzen
- Bericht zu Risikoeinschätzung und -behandlung
- Restrisiken genehmigen

Lfd. Nummer
Kernprozesse
Prozessschritte (Kernprozess)
Support-Prozesse
Prozessschritte (Support-Prozess)
Beschreibung
Prozessverantwortlicher
Beteiligte Organisation
Räume / Lokation
Verarbeitete Daten / Informationen (Kategorien)
Anwendungen
Verfügbarkeit (mit Begründung)
Integrität (mit Begründung)
Authentizität (mit Begründung)
Vertraulichkeit (mit Begründung)
Patientensicherheit (mit Begründung)
Behandlungseffektivität (mit Begründung)
Kritikalität

IKT-Risikomanagement-Framework



Gewährleistung der **Vertraulichkeit, Integrität, Authentizität** und **Verfügbarkeit** von internen Informationen, Daten und Arbeitsabläufen.

- Schutz der Informationen von Kunden/Klienten, Mitarbeitern und Partnern.
- Zuverlässige Unterstützung der Geschäftsprozesse durch die IT und Sicherstellung der Kontinuität der Arbeitsabläufe innerhalb der Organisation.
- Werterhaltung der Investitionen in Technik, Arbeitsprozesse, Informationen und Wissen.
- Einhaltung der aus gesetzlichen Vorgaben resultierenden Anforderungen.
- Gewährleistung des informationellen Selbstbestimmungsrechts der Betroffenen bei der Verarbeitung personenbezogener Daten.
- Reduzierung der im Schadensfall entstehenden Auswirkungen.

Dazu bedarf es Maßnahmen zur **Prävention**, zur **Erkennung** und zur **Reaktion** auf sicherheitsrelevante Ereignisse.

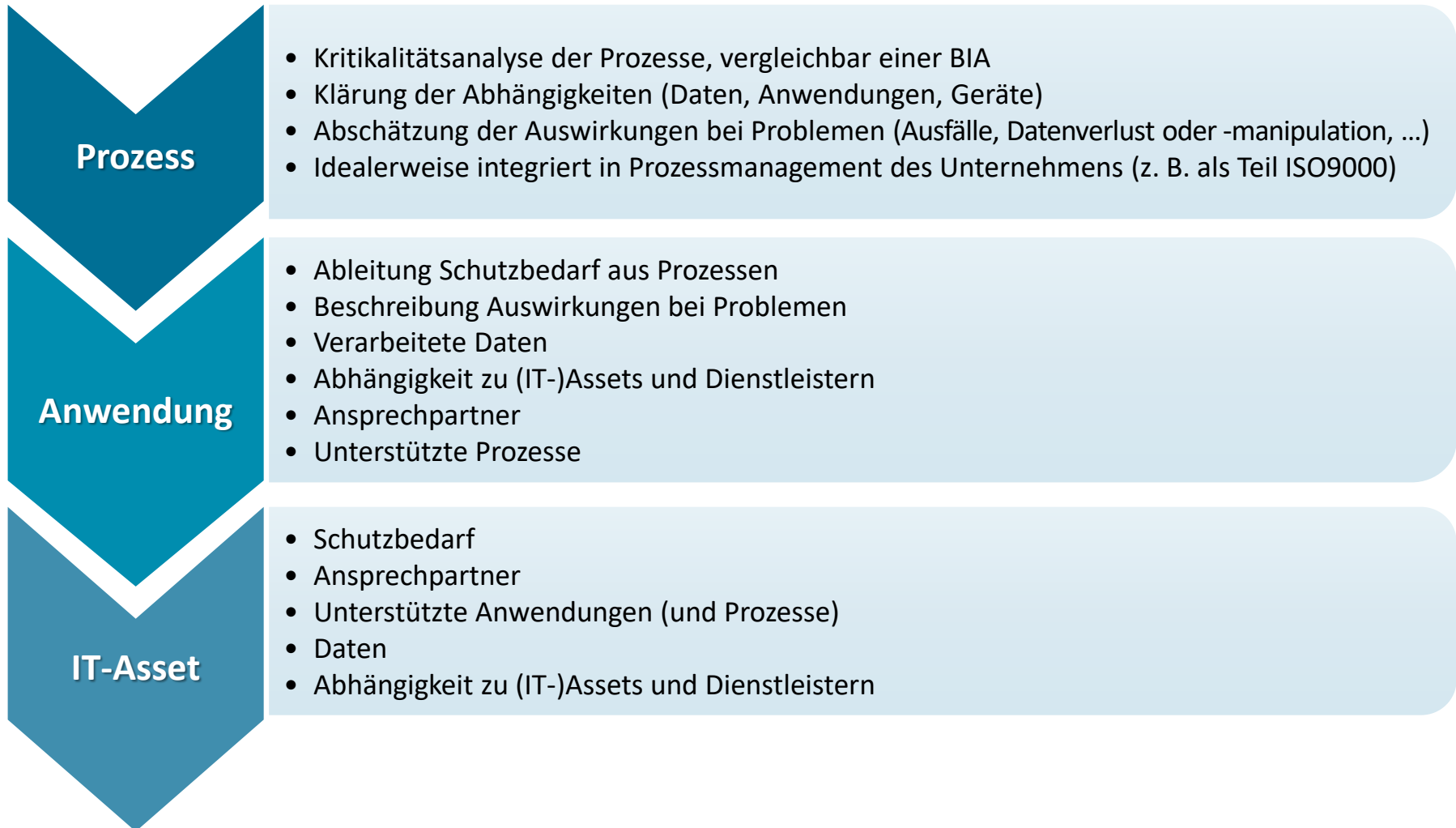
Erfassung der Prozesse und Abläufe, sowie der involvierten Daten, Informationen und Systeme

Bestimmung der schützenswerten Daten, Informationen, Geräte, Netzwerke ...

Bewertung des Risikos bei einem Angriff auf Vertraulichkeit, Integrität, Authentizität und Verfügbarkeit

Ableitung eines Maßnahmenplans und Planung der Umsetzung

! Wichtig ist daher die fachliche Einschätzung der Abhängigkeit von Informationen, Geräten und Anwendungen, um einen angemessenen Schutz umzusetzen.



Business Impact Analysis (BIA)

Fachbereich 1

Prozess A

Prozess B

Prozess C

Fachbereich 2

Prozess D

Prozess E

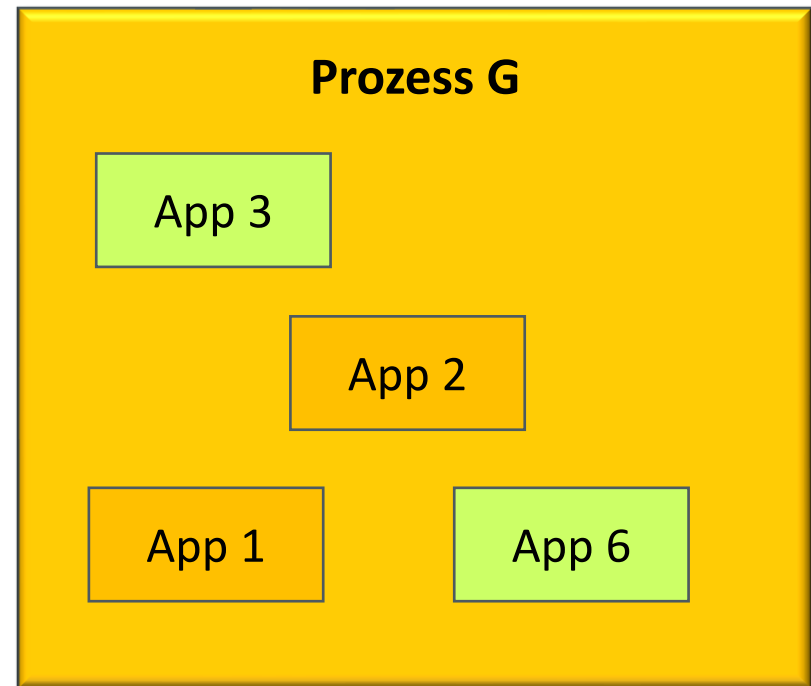
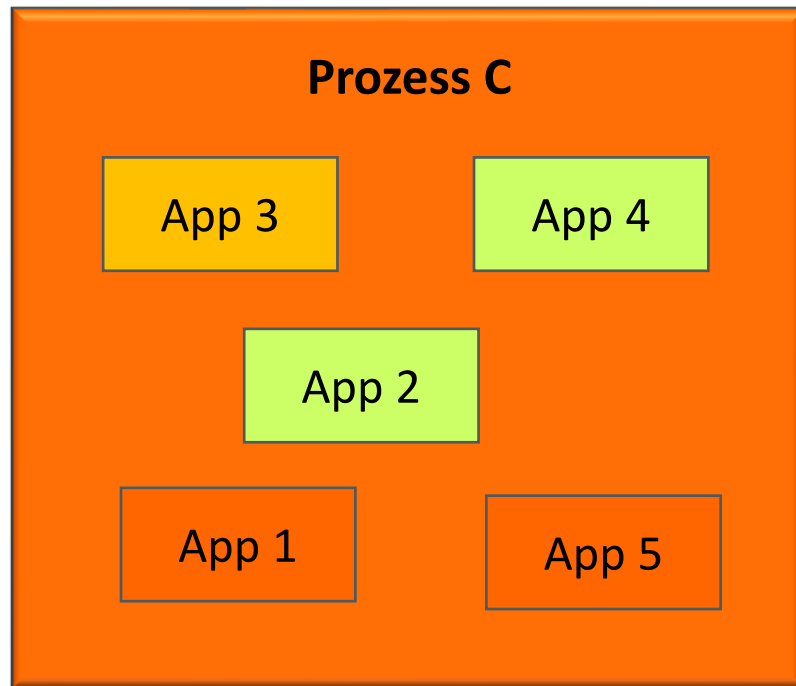
Fachbereich 2

Prozess F

Prozess G

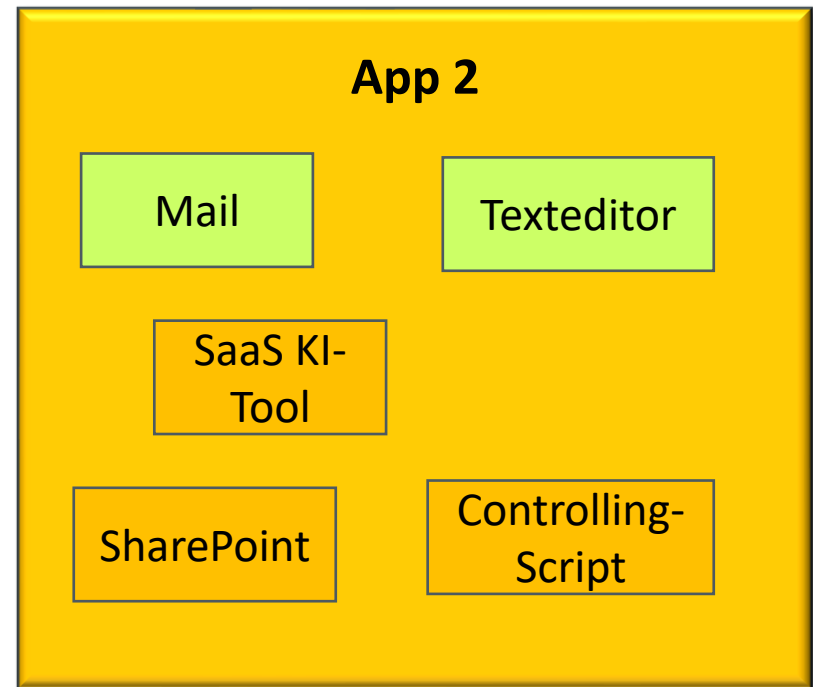
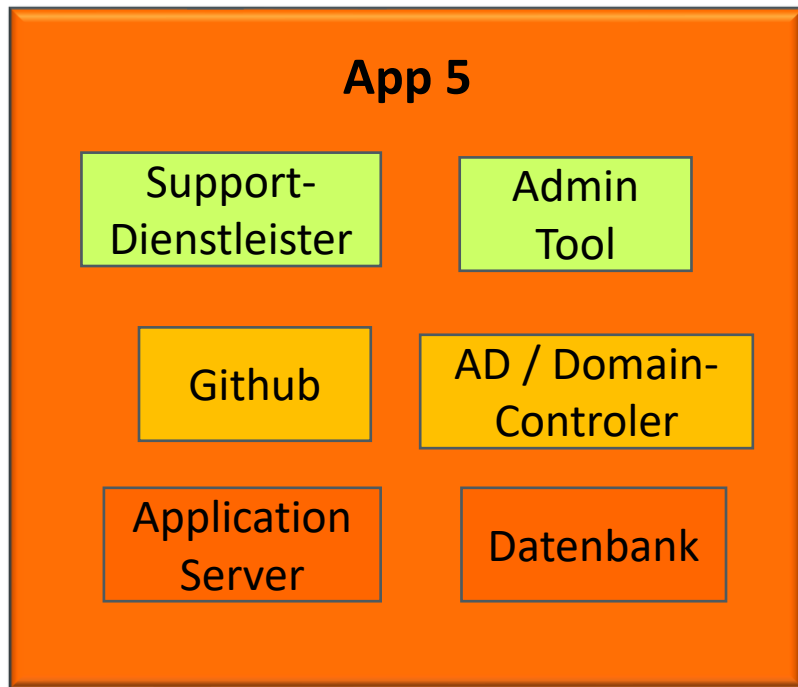
Prozess H

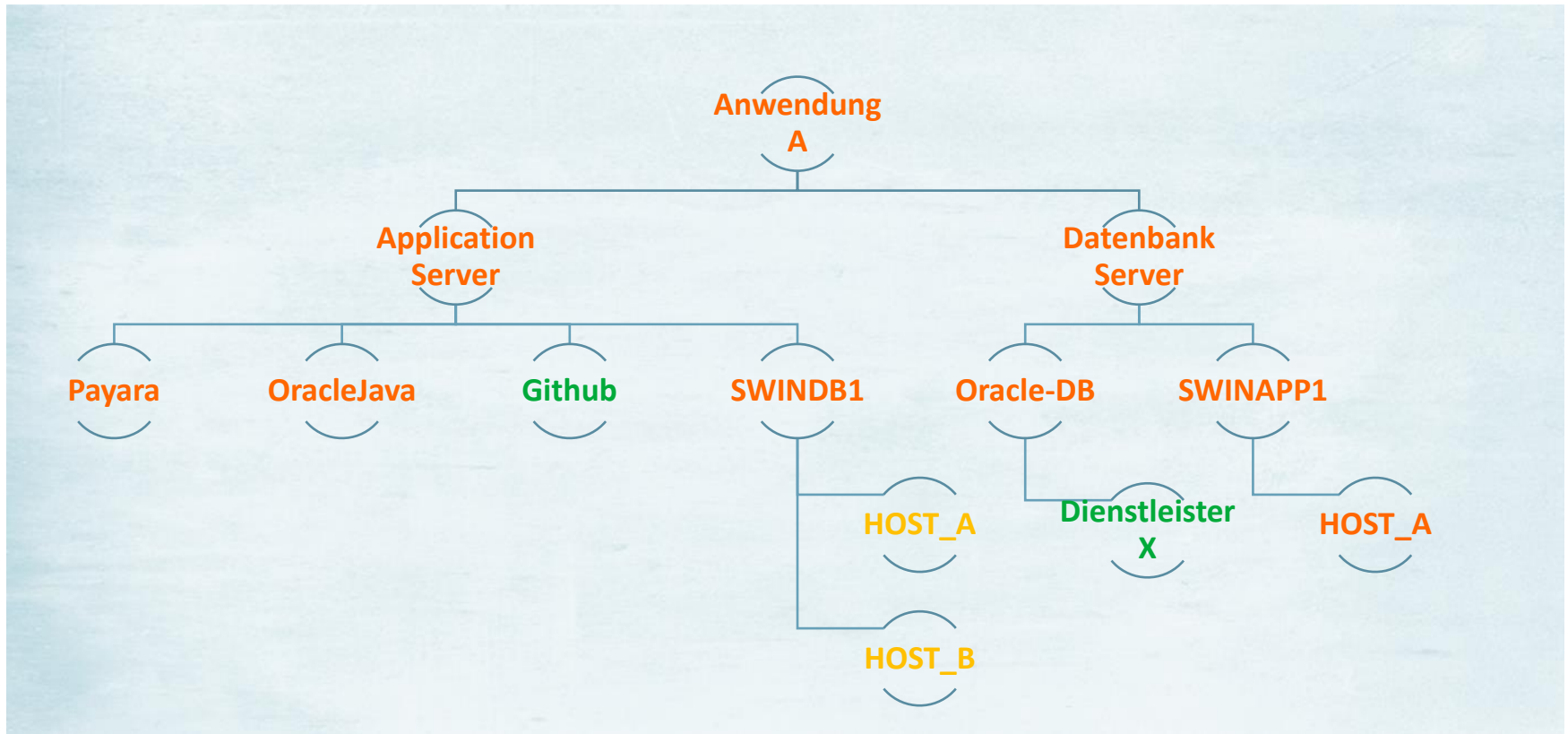
„Wenn alles wichtig ist, ist nichts wichtig“



Ableitung der Kritikalität einer Anwendung

		Potenzielles Schadensausmaß bei Systemfehlern / Kompromittierung des Systems – Abhängigkeit des Prozesses von der Anwendung			
		Nicht signifikant	Geringe Abhängigkeit	Erhebliche Beeinträchtigung	Vollständige Abhängigkeit
Kritikalität	Sehr gering	Sehr gering	Sehr gering	Sehr gering	Normal
	Gering	Sehr gering	Sehr gering	Sehr gering	Normal
	Mittel	Sehr gering	Sehr gering	Normal	Normal
	Hoch	Sehr gering	Normal	Normal	Hoch
	Sehr hoch	Sehr gering	Normal	Hoch	Sehr hoch





- Erfassung des Ergebnisses erfolgt in der Regel in Prozesstool und/oder Asset-Management Tool/CMDB
- Erfassung selber erfolgt je nach Aufstellung des Unternehmens unterschiedlich
 - Prozesse im Rahmen des Qualitätsmanagements oder der Unternehmensorganisations-Prozesse oder der BIA -im Rahmen DORA aktuell häufig auch parallele Aktivitäten
 - Im Rahmen des ISMS mit Tool oder Excel
 - Anwendungen und IT-Assets Top-Down im Rahmen der Prozesserfassung und mehr Bottom-Up im Rahmen der IT-Prozesse

WICHTIG

Über Top-Down Ansatz von den Prozessen her erfasst man auf jeden Fall die kritischen Komponenten!

Beispiel für Prozesserrfassungsbogen

Prozesse																									
Lfd. Nr.	Phase/Geschäftsprozess	Prozess	Beschreibung des Prozesses und Arbeitsschritte	Informationen zur kritischen Prozessschritten	Datum	Prozessverantwortlicher	Kritikalität des Prozesses	Begründung	Verarbeitete Daten / Informationen (Kategorien)																
	Aktivitäten und geschäftliche Ziele	Kritikalitätsanalyse betrachtet wird.	nachgelagert und werden aus darstellerischen Gründen vorab aufgeführt.	Prozess identifiziert wurden. Dazu gehören beispielsweise Details zu potenziellen Risiken, Auswirkungen von Störungen oder geplanten Maßnahmen zur Risikominderung.	einzutragen.	der für die Durchführung und Überwachung des jeweiligen Prozesses zuständig ist.	bewertet. Hoch: Der Prozess ist für die Funktionsfähigkeit des Unternehmens unerlässlich. Mittel: Der Prozess beeinflusst die Funktionsfähigkeit des Unternehmens in gewissem Maße.	Kritikalität des Prozesses erklärt.	verarbeitet werden.																
<table border="1"> <thead> <tr> <th>Datenschutzklasse</th> <th>Bewertung Vertraulichkeit</th> <th>Begründung Vertraulichkeit</th> <th>Bewertung der Integrität</th> <th>Begründung der Integrität</th> <th>Bewertung der Authentizität</th> <th>Begründung Authentizität</th> <th>B</th> </tr> </thead> <tbody> <tr> <td> Öffentlich: Allgemein zugängliche Daten ohne sensiblen Inhalt. Interne Daten: Vertrauliche Informationen für die Organisation. Private Daten: Persönliche Informationen, die geschützt werden müssen. Sensible personenbezogene Daten: Hochsensible Informationen mit schwerwiegenden Folgen. Keine personenbezogenen Daten: Daten, die keine personenbezogenen Daten sind und keine Schutzmaßnahmen erfordern. </td> <td>Informationen gemäß folgender Kategorien anzugeben: Öffentlich: Frei zugänglich, kein Sicherheitsrisiko. Intern: Nur für Unternehmensangehörige, </td> <td>ist.</td> <td>Prozesses anzugeben. Niedrig: Fehler in den Informationen haben minimale oder keine Auswirkungen. Mittel: Ungenauigkeiten können zu spürbaren, aber beherrschbaren </td> <td>gewählt wurde.</td> <td>im Rahmen des Prozesses anzugeben: Niedrig: Die Authentizität ist nicht kritisch, geringe Auswirkungen bei Fälschung. Mittel: Authentizität ist wichtig. </td> <td>Authentizität gewählt wurde.</td> <td>Nu im an Ni mi ge Mi be ab Hc st Ä err Se No Ve</td> </tr> </tbody> </table>										Datenschutzklasse	Bewertung Vertraulichkeit	Begründung Vertraulichkeit	Bewertung der Integrität	Begründung der Integrität	Bewertung der Authentizität	Begründung Authentizität	B	Öffentlich: Allgemein zugängliche Daten ohne sensiblen Inhalt. Interne Daten: Vertrauliche Informationen für die Organisation. Private Daten: Persönliche Informationen, die geschützt werden müssen. Sensible personenbezogene Daten: Hochsensible Informationen mit schwerwiegenden Folgen. Keine personenbezogenen Daten: Daten, die keine personenbezogenen Daten sind und keine Schutzmaßnahmen erfordern.	Informationen gemäß folgender Kategorien anzugeben: Öffentlich: Frei zugänglich, kein Sicherheitsrisiko. Intern: Nur für Unternehmensangehörige,	ist.	Prozesses anzugeben. Niedrig: Fehler in den Informationen haben minimale oder keine Auswirkungen. Mittel: Ungenauigkeiten können zu spürbaren, aber beherrschbaren	gewählt wurde.	im Rahmen des Prozesses anzugeben: Niedrig: Die Authentizität ist nicht kritisch, geringe Auswirkungen bei Fälschung. Mittel: Authentizität ist wichtig.	Authentizität gewählt wurde.	Nu im an Ni mi ge Mi be ab Hc st Ä err Se No Ve
Datenschutzklasse	Bewertung Vertraulichkeit	Begründung Vertraulichkeit	Bewertung der Integrität	Begründung der Integrität	Bewertung der Authentizität	Begründung Authentizität	B																		
Öffentlich: Allgemein zugängliche Daten ohne sensiblen Inhalt. Interne Daten: Vertrauliche Informationen für die Organisation. Private Daten: Persönliche Informationen, die geschützt werden müssen. Sensible personenbezogene Daten: Hochsensible Informationen mit schwerwiegenden Folgen. Keine personenbezogenen Daten: Daten, die keine personenbezogenen Daten sind und keine Schutzmaßnahmen erfordern.	Informationen gemäß folgender Kategorien anzugeben: Öffentlich: Frei zugänglich, kein Sicherheitsrisiko. Intern: Nur für Unternehmensangehörige,	ist.	Prozesses anzugeben. Niedrig: Fehler in den Informationen haben minimale oder keine Auswirkungen. Mittel: Ungenauigkeiten können zu spürbaren, aber beherrschbaren	gewählt wurde.	im Rahmen des Prozesses anzugeben: Niedrig: Die Authentizität ist nicht kritisch, geringe Auswirkungen bei Fälschung. Mittel: Authentizität ist wichtig.	Authentizität gewählt wurde.	Nu im an Ni mi ge Mi be ab Hc st Ä err Se No Ve																		
<table border="1"> <thead> <tr> <th colspan="2">IT-Anwendungen</th> <th>Weitere genutzte Assets (Dienste)</th> <th>Kommentar</th> </tr> </thead> <tbody> <tr> <td> Bewertung Verfügbarkeit Nutzbarkeit der Informationen im Rahmen des Prozesses anzugeben. Niedrig: Ausfallzeiten haben minimale oder keine geschäftlichen Auswirkungen. Mittel: Mäßige Auswirkungen bei Ausfallzeiten, erfordern aber Aufmerksamkeit. Hoch: Hohe Bedeutung der ständigen Verfügbarkeit; Ausfallzeiten können ernsthafte Folgen haben. Sehr hoch: Kritische Notwendigkeit der ständigen Verfügbarkeit; Ausfälle hätten </td> <td> Begründung Verfügbarkeit Authentizität gewählt wurde. </td> <td> Gerätschaften Einsatz kommen. </td> <td> (ergänzende Informationen) Hinweise zum jeweiligen Prozess oder den zugehörigen Einträgen gemacht werden. </td> </tr> </tbody> </table>										IT-Anwendungen		Weitere genutzte Assets (Dienste)	Kommentar	Bewertung Verfügbarkeit Nutzbarkeit der Informationen im Rahmen des Prozesses anzugeben. Niedrig: Ausfallzeiten haben minimale oder keine geschäftlichen Auswirkungen. Mittel: Mäßige Auswirkungen bei Ausfallzeiten, erfordern aber Aufmerksamkeit. Hoch: Hohe Bedeutung der ständigen Verfügbarkeit; Ausfallzeiten können ernsthafte Folgen haben. Sehr hoch: Kritische Notwendigkeit der ständigen Verfügbarkeit; Ausfälle hätten	Begründung Verfügbarkeit Authentizität gewählt wurde.	Gerätschaften Einsatz kommen.	(ergänzende Informationen) Hinweise zum jeweiligen Prozess oder den zugehörigen Einträgen gemacht werden.								
IT-Anwendungen		Weitere genutzte Assets (Dienste)	Kommentar																						
Bewertung Verfügbarkeit Nutzbarkeit der Informationen im Rahmen des Prozesses anzugeben. Niedrig: Ausfallzeiten haben minimale oder keine geschäftlichen Auswirkungen. Mittel: Mäßige Auswirkungen bei Ausfallzeiten, erfordern aber Aufmerksamkeit. Hoch: Hohe Bedeutung der ständigen Verfügbarkeit; Ausfallzeiten können ernsthafte Folgen haben. Sehr hoch: Kritische Notwendigkeit der ständigen Verfügbarkeit; Ausfälle hätten	Begründung Verfügbarkeit Authentizität gewählt wurde.	Gerätschaften Einsatz kommen.	(ergänzende Informationen) Hinweise zum jeweiligen Prozess oder den zugehörigen Einträgen gemacht werden.																						

Beispiel für Prozesserrfassungsbogen

Kennun	Bezeichnung / Anwendungsname	Type / Anwendungstyp	Kurzbeschreibung	Link IT-Dokumentation im Wiki	Vertraulichkeit	Integrität
Anwendungs-	In dieser Spalte ist die spezifische Bezeichnung der Anwendung einzutragen.	In dieser Spalte ist die Art der Anwendung anzugeben.	In dieser Spalte ist der Verwendungszweck der Einsatzbereich der Software zu beschreiben.	In dieser Spalte ist der direkte Verweis auf die entsprechende Dokumentation der Anwendung im Unternehmens-Wiki einzutragen.	<p>In dieser Spalte ist die Vertraulichkeitsstufe der Anwendung anzugeben, basierend auf der Sensibilität der durch die Anwendung verarbeiteten oder gespeicherten Informationen. Wählen Sie eine der folgenden Stufen:</p> <p>öffentlich: Informationen, die für die allgemeine Öffentlichkeit bestimmt sind und keine Gefahr bei Offenlegung darstellen.</p> <p>intern: Informationen, die für den internen Gebrauch bestimmt sind und bei deren Offenlegung außerhalb des Unternehmens nur geringfügige negative Konsequenzen zu erwarten sind.</p> <p>vertraulich: Informationen, die eine</p>	<p>In dieser Spalte ist die Integritätsstufe der Anwendung anzugeben, basierend auf der Bedeutung der Genauigkeit und Vollständigkeit der durch die Anwendung verarbeiteten oder gespeicherten Informationen. Wählen Sie eine der folgenden Stufen:</p> <p>Niedrig: Fehler in den Informationen haben minimale oder keine Auswirkungen.</p> <p>Mittel: Ungenauigkeiten können zu spürbaren, aber beherrschbaren Problemen führen.</p> <p>Hoch: Hohe Genauigkeit ist kritisch; Fehler könnten erhebliche Folgen haben.</p> <p>Sehr hoch: Absolute Genauigkeit ist essenziell; Fehler hätten gravierende</p>
Authentizität	Verfügbarkeit	Ansprechpartner technisch	Ansprechpartner fachliche	Risikobetrachtung	Prozesse	
<p>In dieser Spalte ist die Authentizitätsstufe der Anwendung anzugeben, basierend auf der Bedeutung der Nachweisbarkeit der Identität von Nutzern und der Herkunft von Daten in der Anwendung. Wählen Sie eine der folgenden Stufen:</p> <p>Niedrig: Die Authentizität ist nicht kritisch, geringe Auswirkungen bei Fälschung.</p> <p>Mittel: Authentizität ist wichtig, Fälschungen können zu Problemen führen.</p> <p>Hoch: Sehr wichtige Authentizität, Fälschungen können ernsthafte Folgen haben.</p> <p>Sehr hoch: Kritische Bedeutung der Authentizität, Fälschungen hätten gravierende Auswirkungen.</p>	<p>In dieser Spalte ist das Maß an Bedeutung der ständigen Zugänglichkeit und Nutzbarkeit der Informationen im Rahmen der Anwendung anzugeben:</p> <p>Niedrig: Ausfallzeiten haben minimale oder keine geschäftlichen Auswirkungen.</p> <p>Mittel: Mäßige Auswirkungen bei Ausfallzeiten, erfordern aber Aufmerksamkeit.</p> <p>Hoch: Hohe Bedeutung der ständigen Verfügbarkeit; Ausfallzeiten können ernsthafte Folgen haben.</p> <p>Sehr hoch: Kritische Notwendigkeit der ständigen Verfügbarkeit; Ausfälle hätten gravierende Konsequenzen.</p>	<p>In dieser Spalte ist der Name des technischen Ansprechpartners für die jeweilige Anwendung einzutragen. Diese Person ist verantwortlich für alle technischen Aspekte der Anwendung, einschließlich Wartung, Konfiguration und Fehlerbehebung.</p>	<p>In dieser Spalte ist der Name des fachlichen Ansprechpartners für die jeweilige Anwendung einzutragen. Diese Person ist verantwortlich für die inhaltlichen und geschäftlichen Aspekte der Anwendung und dient als Bindeglied zwischen den Benutzern und der IT-Abteilung.</p>	<p>In dieser Spalte ist der Status der Risikoanalyse für die jeweilige Anwendung zu dokumentieren. Folgende Eintragungen sind möglich:</p> <p>Erfolgt: Die Risikoanalyse wurde vollständig durchgeführt und alle relevanten Risiken wurden dokumentiert.</p> <p>In Bearbeitung: Die Risikoanalyse ist aktuell im Gange. Risiken werden identifiziert und analysiert.</p> <p>Aktualisierung erforderlich: Die Risikoanalyse ist aktuell im Gange. Risiken werden identifiziert und analysiert.</p> <p>Nicht erforderlich: Für diese Anwendung ist keine Risikoanalyse notwendig, da sie als nicht kritisch oder risikoarm eingestuft wurde.</p>	<p>In dieser Spalte sind die Identifikationsnummern (IDs) aller Geschäftsprozesse einzutragen, in denen die betreffende Anwendung verwendet wird. Diese Informationen sind entscheidend, um die Integration der Anwendung in die Unternehmensabläufe zu verstehen und zu dokumentieren.</p>	

Schutzprofil Normal

App 4

App 6

Schutzprofil Hoch

App 2

App 3

Schutzprofil Sehr Hoch

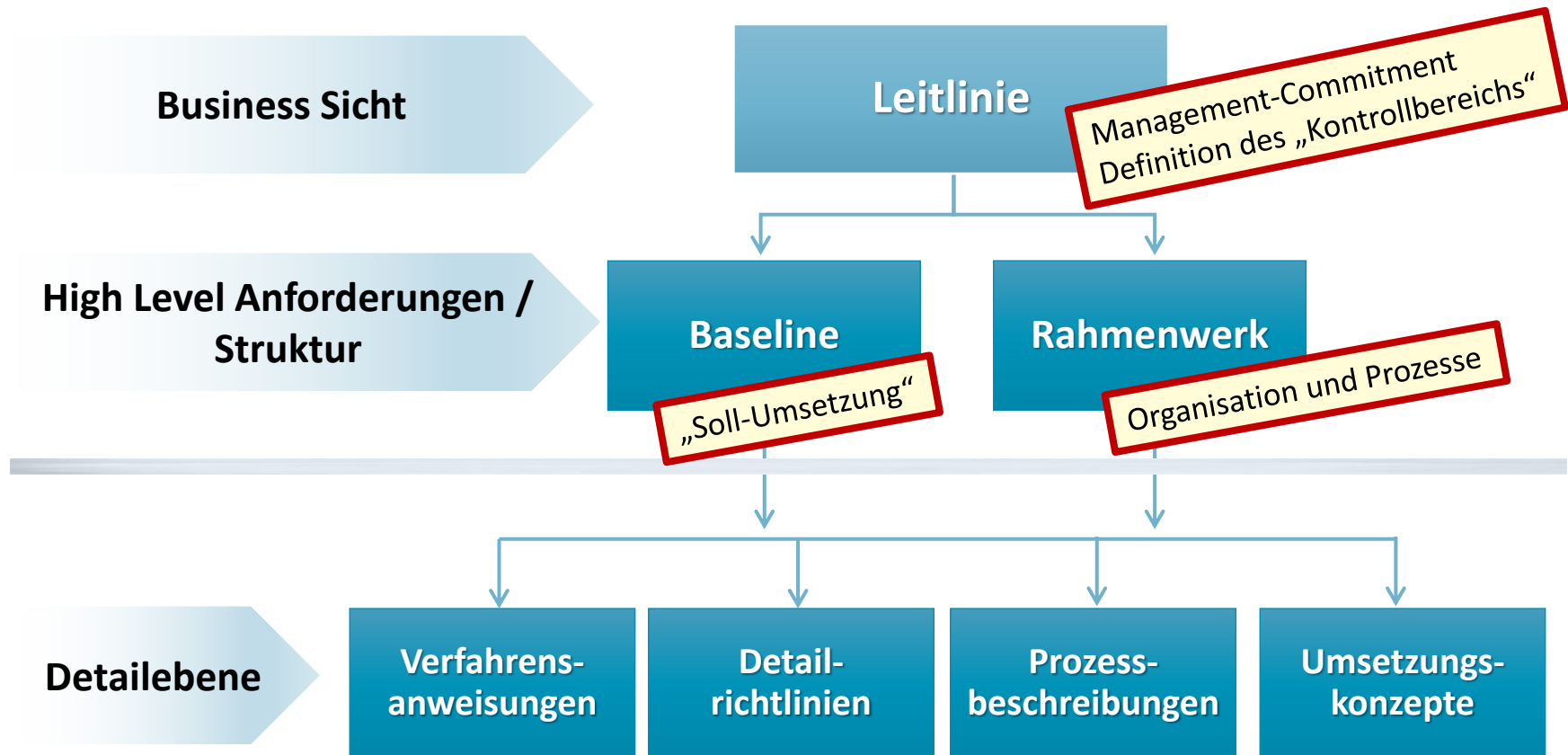
App 1

App 5

Hinweis:

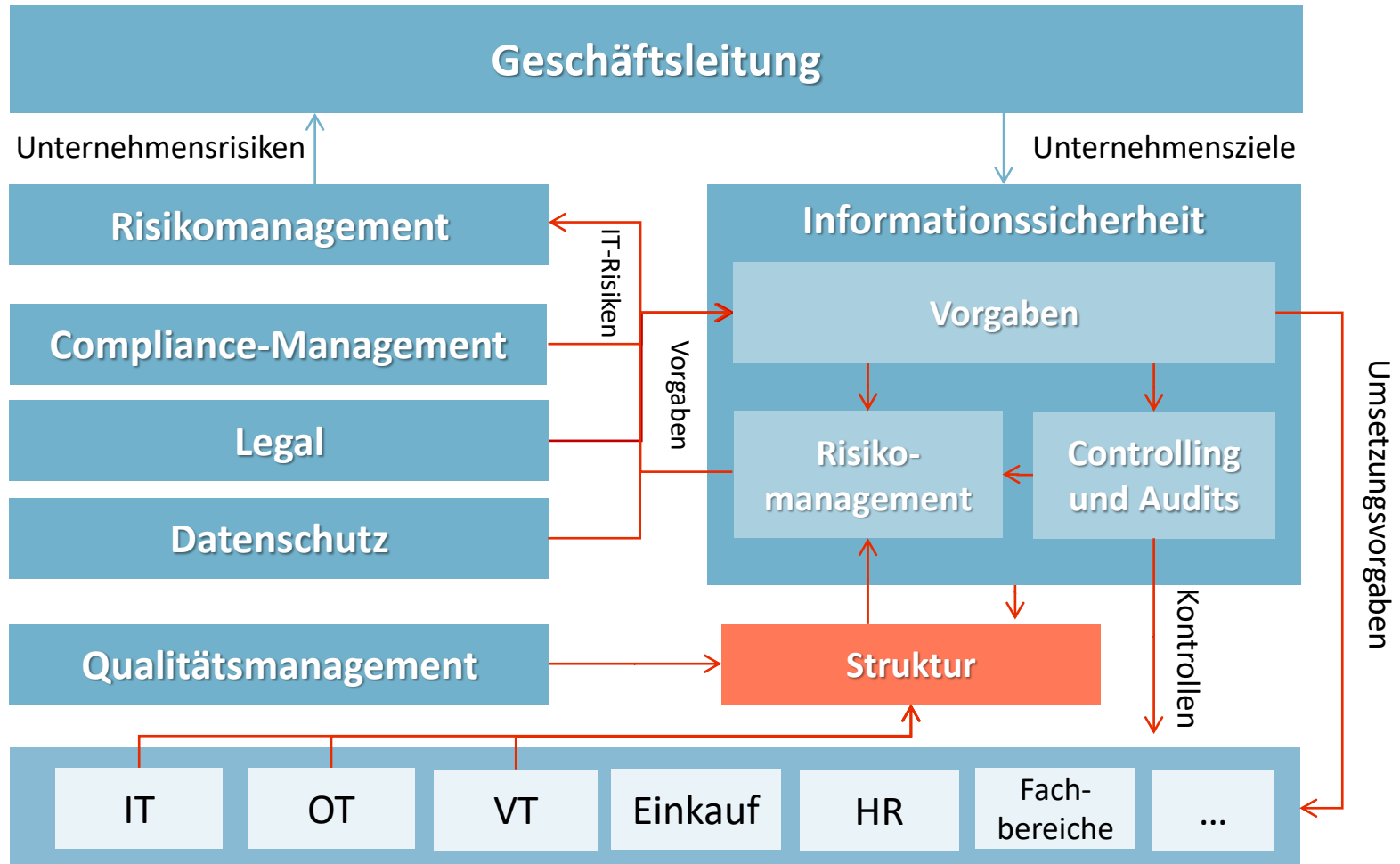
Das Mapping auf das Schutzprofil findet auch auf Asset-Level statt – je nach Anforderung, z. B.

- Auslagerung einer Anwendung – Schutzprofil der Anwendung
- Absicherung eigene IT – Mapping auf Assets (ggf. geringere Anforderungen ausreichend)



**Die umzusetzenden Schutzprofile werden in den Policies beschrieben –
Diese können auch als „Anforderung“ an den Dienstleister weitergegeben werden.**

Einbindung in die Organisation



Urheberrecht

Die Bilder und Inhalte dieser Präsentation unterliegen dem deutschen Urheberrecht. Beiträge von Dritten sind als solche gekennzeichnet. Die Vervielfältigung, Bearbeitung, Verbreitung und jede Art der Verwertung außerhalb der Grenzen des Urheberrechts bedürfen der schriftlichen Zustimmung der IT-Security@Work GmbH (ISW).