Praktische Umsetzung IKT-Risikomanagement und ISMS anhand von Umsetzungsbeispielen

Marion Steiner – 21.11.2024

CAST. e.V. Workshop „Cybersicherheit für den Mittelstand“

– öffentlich –

Agenda

- (IKT-)Risikomanagement im ISMS
- Der IKT-Risikoprozess
- Übersicht des „Toolkits“
- … in der Praxis
- … Verzahnung zu Sicherheitsmaßnahmen

Ihre Referentin

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.

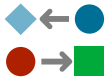
Ihr erklärtes Ziel ist es, dass Informationssicherheit und Compliance nicht als Störfaktoren, sondern als Mehrwert für ein Unternehmen wahrgenommen werden. Bei ihrer Arbeit stehen daher risikobasierte Verfahren sowie Vereinbarkeit von Geschäftsprozessen, IT-Betrieb und Compliance (inklusive Informationssicherheit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

Das ISMS

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

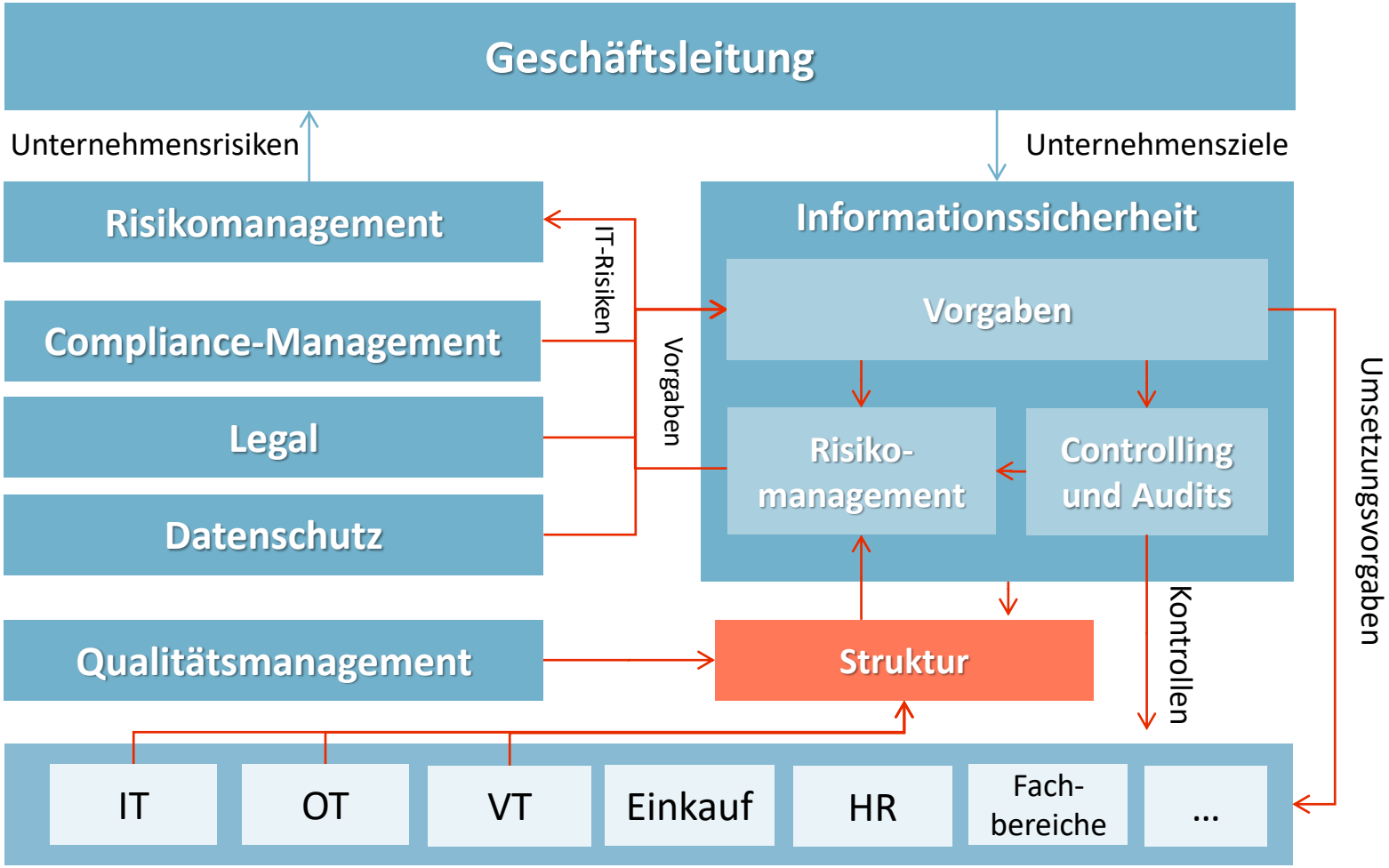
sowie Größe und Struktur … einer Organisation.

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)

Einbindung in die Organisation



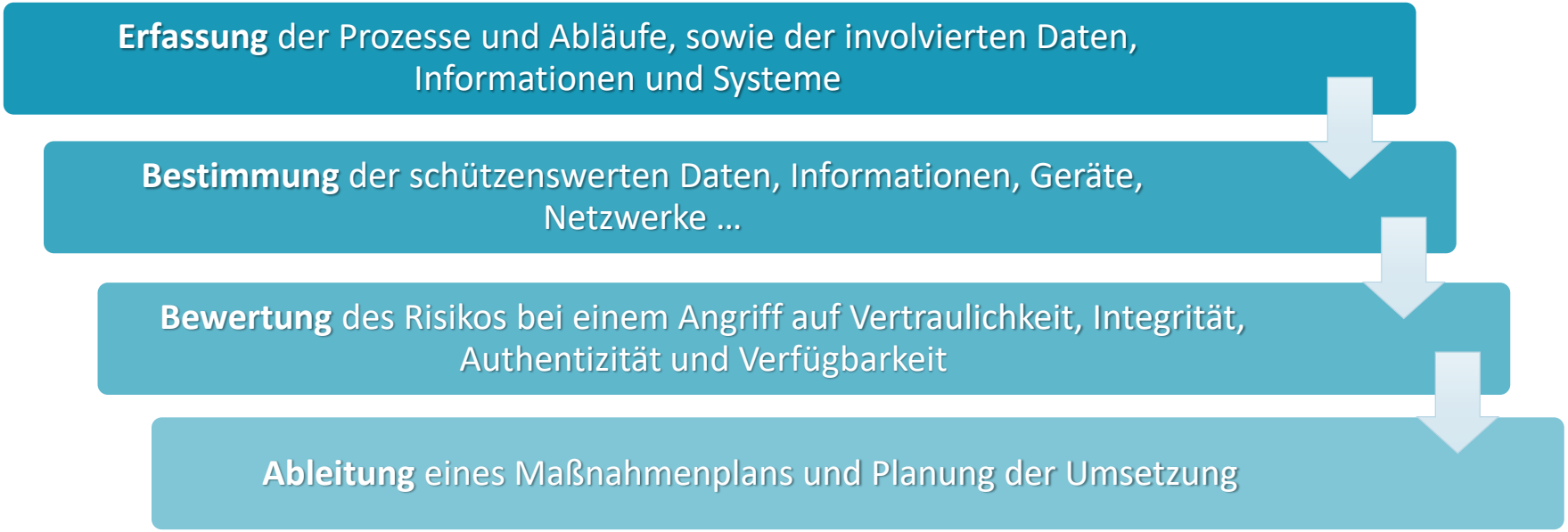
Ziele der Informationssicherheit

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.

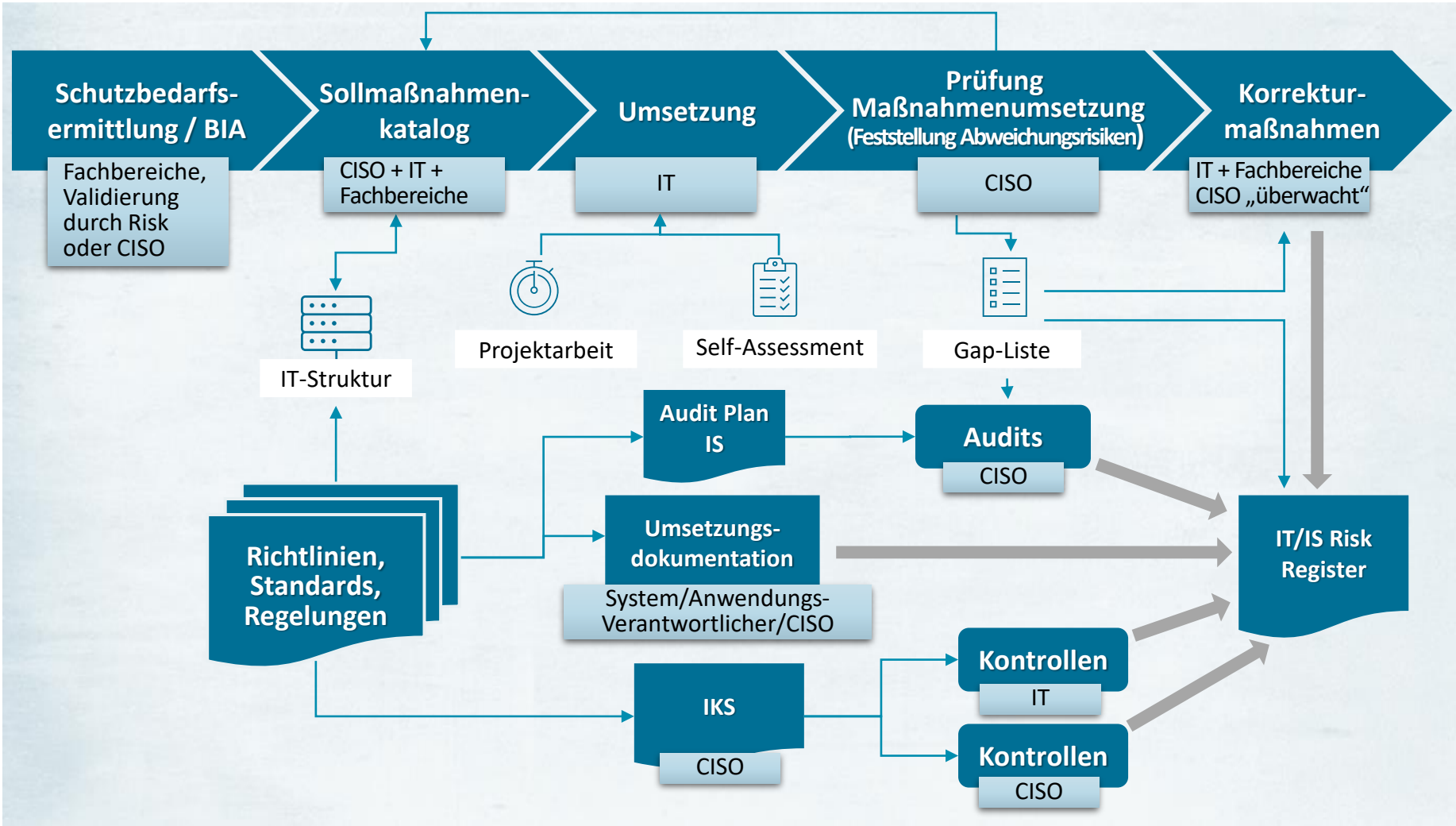
Dazu bedarf es Maßnahmen zur **Prävention**, zur **Erkennung** und zur **Reaktion** auf sicherheitsrelevante Ereignisse.

Der Risikoprozess

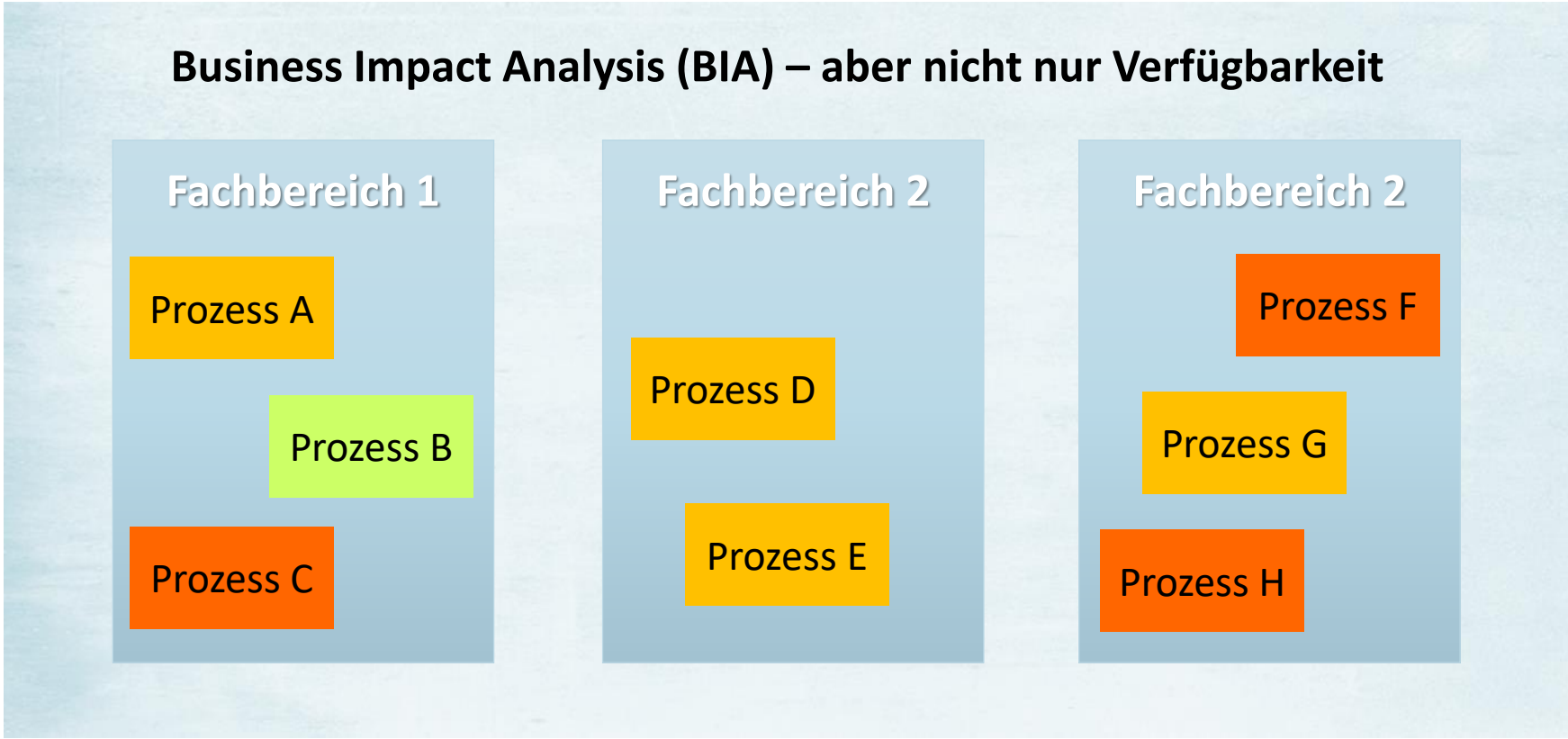


! Wichtig ist die fachliche Einschätzung der Abhängigkeit von Informationen, Geräten und Anwendungen, um einen angemessenen Schutz umzusetzen.

IKT-Risikomanagement-Framework



… in der Praxis



„Wenn alles wichtig ist, ist nichts wichtig“

Vom Prozess zu den IT-Assets

- Kritikalitätsanalyse der Prozesse, vergleichbar einer BIA
- Klärung der Abhängigkeiten (Daten, Anwendungen, Geräte)
- Abschätzung der Auswirkungen bei Problemen (Ausfälle, Datenverlust oder -manipulation, …)
- Idealerweise integriert in Prozessmanagement des Unternehmens (z. B. als Teil ISO9000)

Fachliche Bewertung

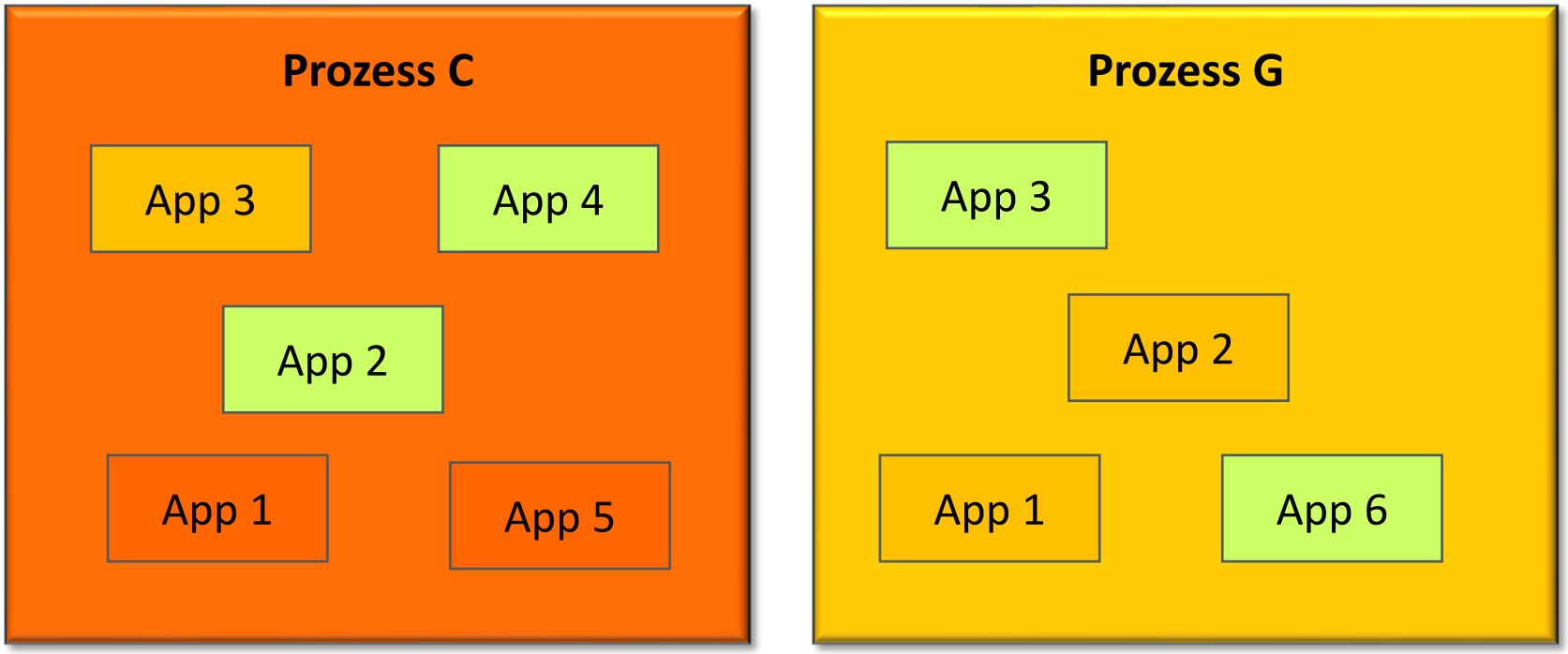
- Ableitung Schutzbedarf aus Prozessen
- Beschreibung Auswirkungen bei Problemen
- Verarbeitete Daten
- Abhängigkeit zu (IT-)Assets und Dienstleistern
- Ansprechpartner
- Unterstützte Prozesse

Fachliche und technische Bewertung

- Schutzbedarf
- Ansprechpartner
- Unterstützte Anwendungen (und Prozesse)
- Daten
- Abhängigkeit zu (IT-)Assets und Dienstleistern

Technische Bewertung

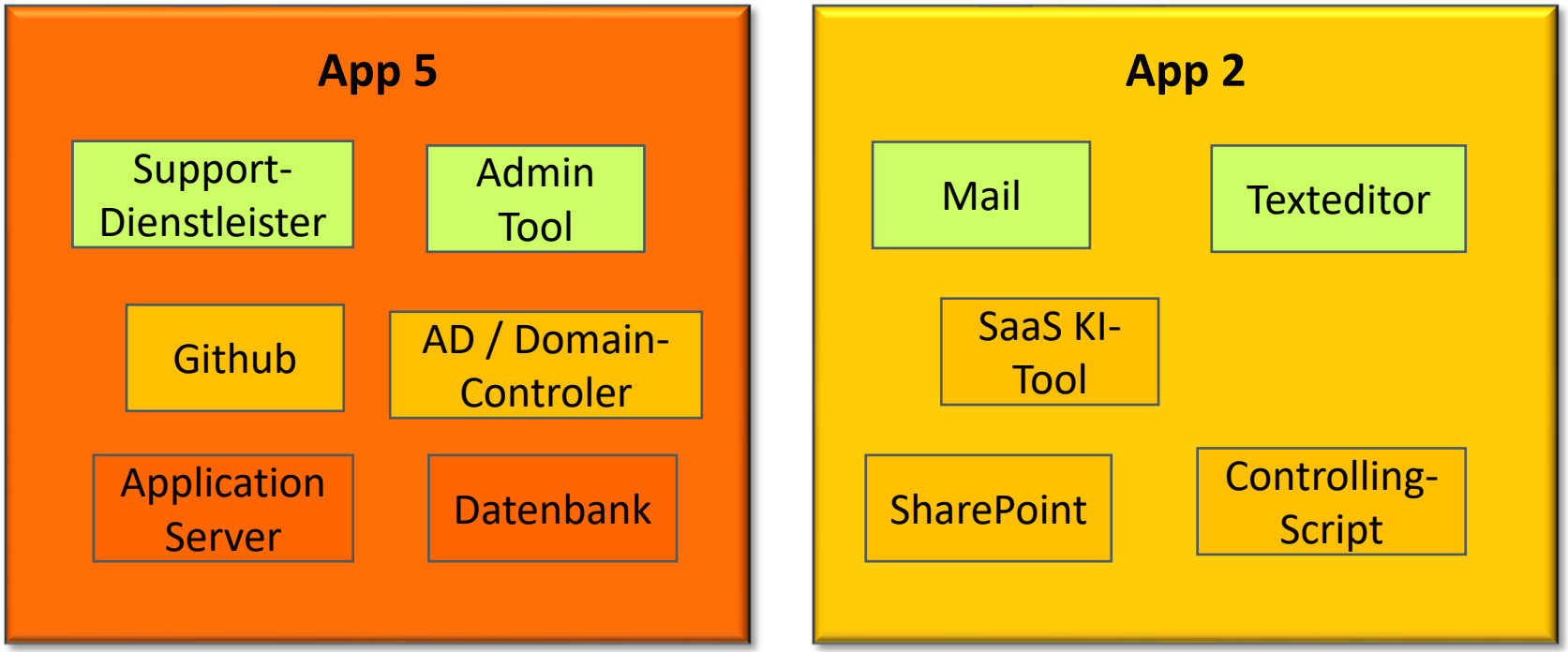
… in der Praxis



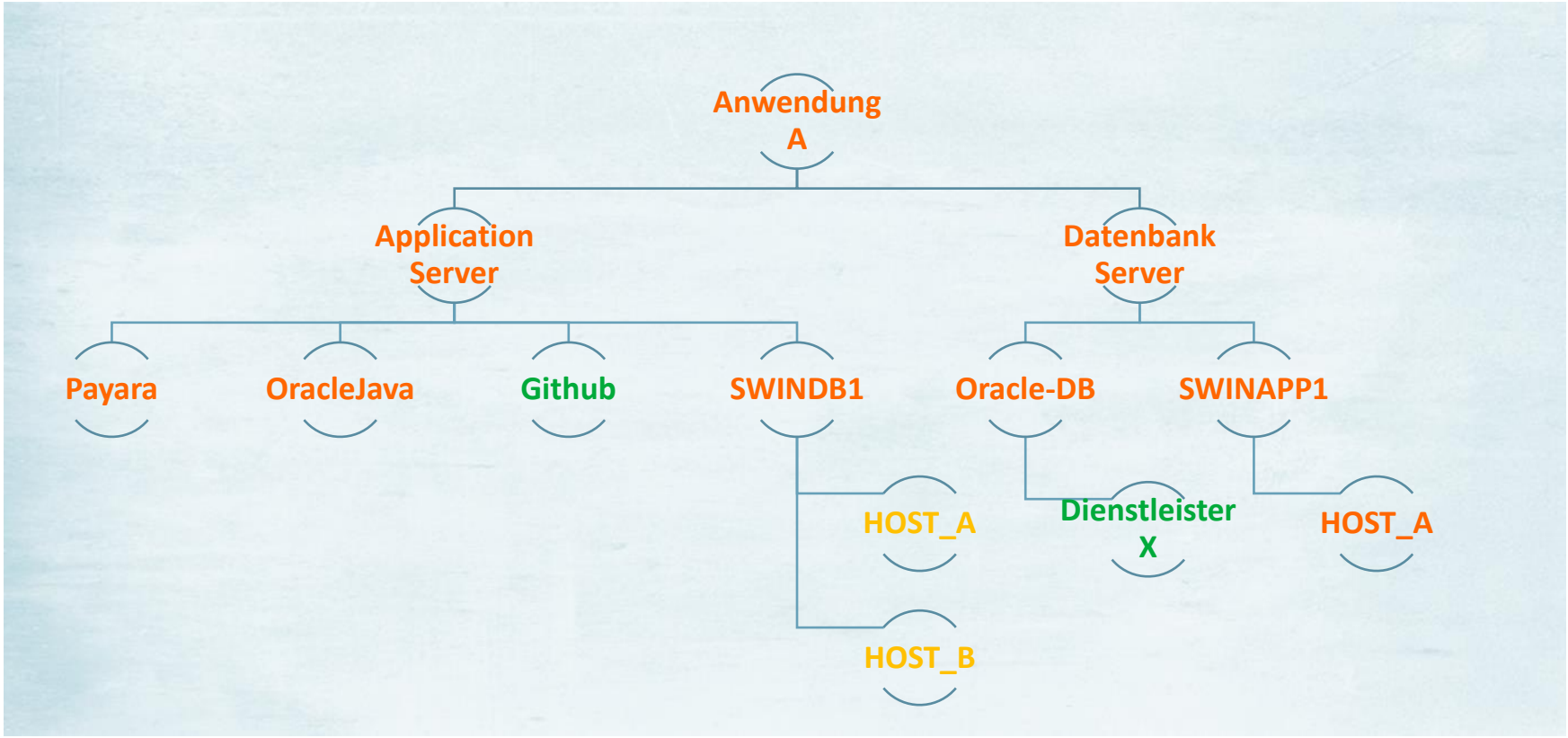
Ableitung der Kritikalität einer Anwendung

		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

… in der Praxis



… in der Praxis



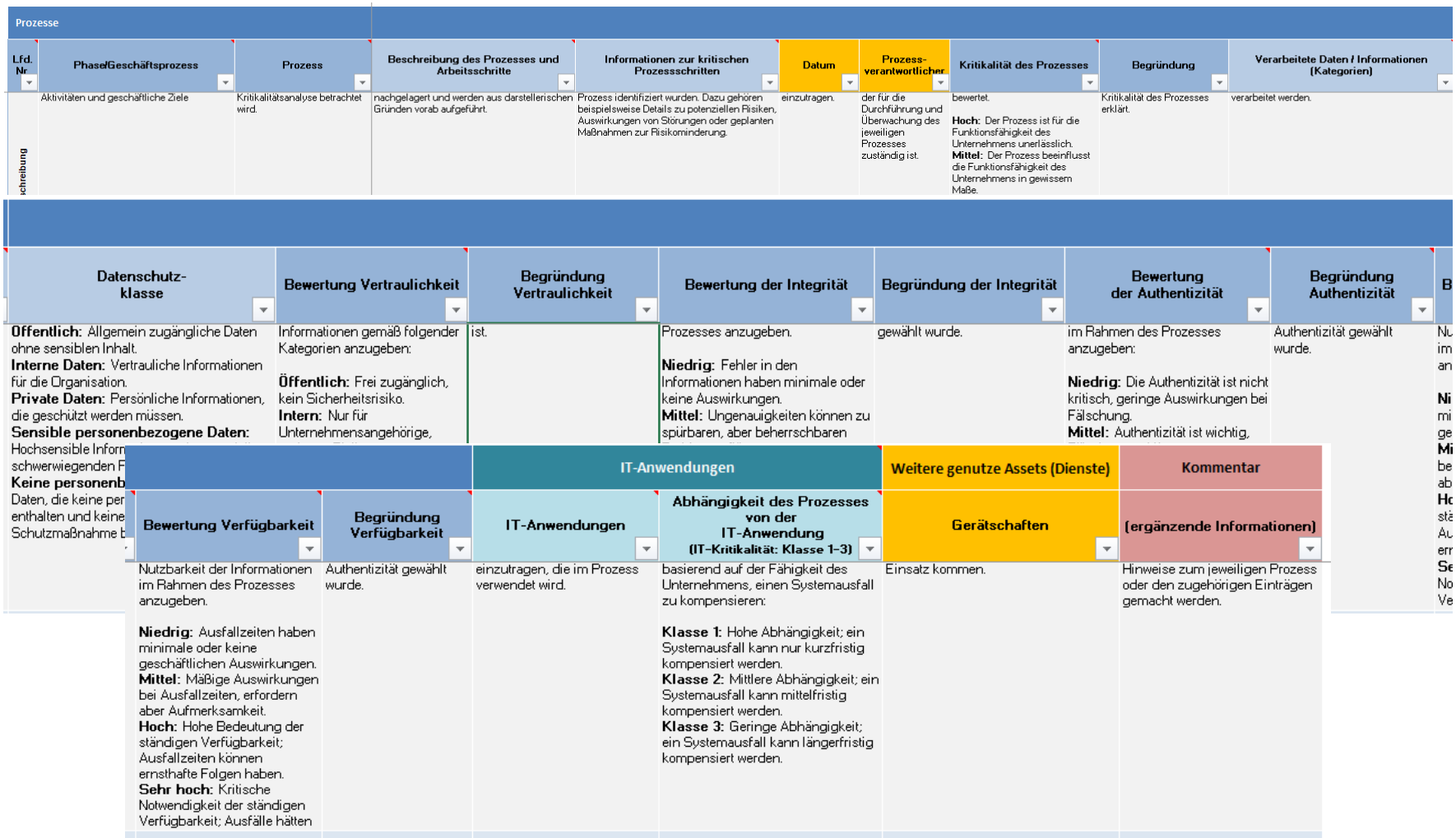
… in der Praxis

- 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 Prozesserfassungsbogen



Prozesse									
Lfd. Nr.	Phase/Geschäftsprozess	Prozess	Beschreibung des Prozesses und Arbeitsschritte	Informationen zur kritischen Prozessschritten	Datum	Prozess-verantwortlicher	Kritikalität des Prozesses	Begründung	Verarbeitete Daten / Informationen (Kategorien)
schreibung	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.

	Datenschutz-klasse	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 Inform schwerwiegenden F **Keine personenb** Daten, die keine per enthalten und keine Schutzmaßnahme b	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** stä Au err **Se** No Ve

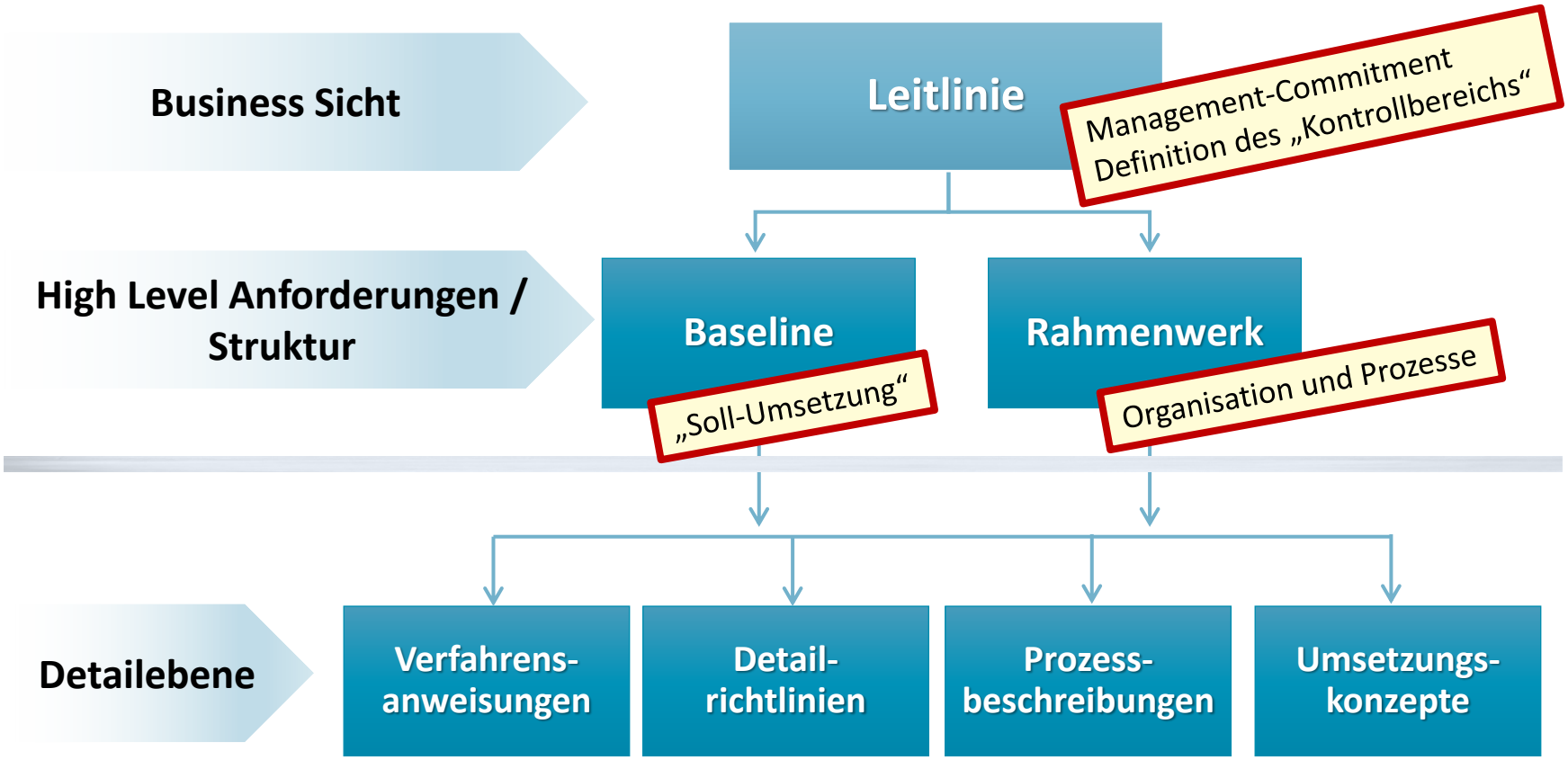
			IT-Anwendungen		Weitere genutze Assets (Dienste)	Kommentar
	Bewertung Verfügbarkeit	Begründung Verfügbarkeit	IT-Anwendungen	Abhängigkeit des Prozesses von der IT-Anwendung (IT-Kritikalität: Klasse 1-3)	Gerätschaften	(ergänzende Informationen)
	Nutzbarkeit der Informationen im Rahmen des Prozesses anzugeben. **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	Authentizität gewählt wurde.	einzutragen, die im Prozess verwendet wird.	basierend auf der Fähigkeit des Unternehmens, einen Systemausfall zu kompensieren: **Klasse 1:** Hohe Abhängigkeit; ein Systemausfall kann nur kurzfristig kompensiert werden. **Klasse 2:** Mittlere Abhängigkeit; ein Systemausfall kann mittelfristig kompensiert werden. **Klasse 3:** Geringe Abhängigkeit; ein Systemausfall kann längerfristig kompensiert werden.	Einsatz kommen.	Hinweise zum jeweiligen Prozess oder den zugehörigen Einträgen gemacht werden.

Beispiel für Prozesserfassungsbogen

Kennun	Bezeichnung / Anwendungsname	Type / Anwendungsl	Kurzbeschreibung	Link IT-Dokumentation im Wiki	Vertraulichkeit	Integrität
Anwendungs-ID	In dieser Spalte ist die spezifische Bezeichnung der Anwendung einzutragen.	In dieser Spalte ist die Art der Anwendunge 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.	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: **öffentlich:** Informationen, die für die allgemeine Öffentlichkeit bestimmt sind und keine Gefahr bei Offenlegung darstellen. **intern:** Informationen, die für den internen Gebrauch bestimmt sind und bei deren Offenlegung außerhalb des Unternehmens nur geringfügige negative Konsequenzen zu erwarten sind. **vertraulich:** Informationen, die eine	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: **Niedrig:** Fehler in den Informationen haben minimale oder keine Auswirkungen. **Mittel:** Ungenauigkeiten können zu spürbaren, aber beherrschbaren Problemen führen. **Hoch:** Hohe Genauigkeit ist kritisch; Fehler könnten erhebliche Folgen haben. Sehr hoch: Absolute Genauigkeit ist essenziell; Fehler hätten gravierende

Authentizität	Verfügbarkeit	Ansprechpartner technisch	Ansprechpartner fachliche	Risikobetrachtung	Prozesse
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: **Niedrig:** Die Authentizität ist nicht kritisch, geringe Auswirkungen bei Fälschung. **Mittel:** Authentizität ist wichtig, Fälschungen können zu Problemen führen. **Hoch:** Sehr wichtige Authentizität, Fälschungen können ernsthafte Folgen haben. **Sehr hoch**: Kritische Bedeutung der Authentizität, Fälschungen hätten gravierende Auswirkungen.	In dieser Spalte ist das Maß an Bedeutung der ständigen Zugänglichkeit und Nutzbarkeit der Informationen im Rahmen der Anwendung 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 gravierende Konsequenzen.	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.	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.	In dieser Spalte ist der Status der Risikoanalyse für die jeweilige Anwendung zu dokumentieren. Folgende Eintragungen sind möglich: **Erfolgt**: Die Risikoanalyse wurde vollständig durchgeführt und alle relevanten Risiken wurden dokumentiert. **In Bearbeitung:** Die Risikoanalyse ist aktuell im Gange. Risiken werden identifiziert und analysiert. **Aktualisierung erforderlich:** Die Risikoanalyse ist aktuell im Gange. Risiken werden identifiziert und analysiert. **Nicht erforderlich:** Für diese Anwendung ist keine Risikoanalyse notwendig, da sie als nicht kritisch oder risikoarm eingestuft wurde.	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.

Umsetzung in die Vorgabenwelt



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

Von der Schutzanforderung zu Maßnahmen

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

Patchmanagement – Ziele

Ziele des Patchmanagement

- Sicherstellung der Funktionsstabilität
- Verringerung der Angriffsfläche
- Vermeidung von Haftungsrisiken

Abgeleitete Anforderungen

- **kritische Patches** sollten nach **spätestens 30 Tagen** eingespielt sein
- Notfallpatches **„Sofort“**
- ausreichendes Testen von Änderungen (und damit auch bei Patch-Anwendung)
- Roll-Back-Planung – Was ist zu tun, wenn der Patch doch schief geht?

Schwachstellenmanagement

IT-SECURITY @ WORK

Konzept

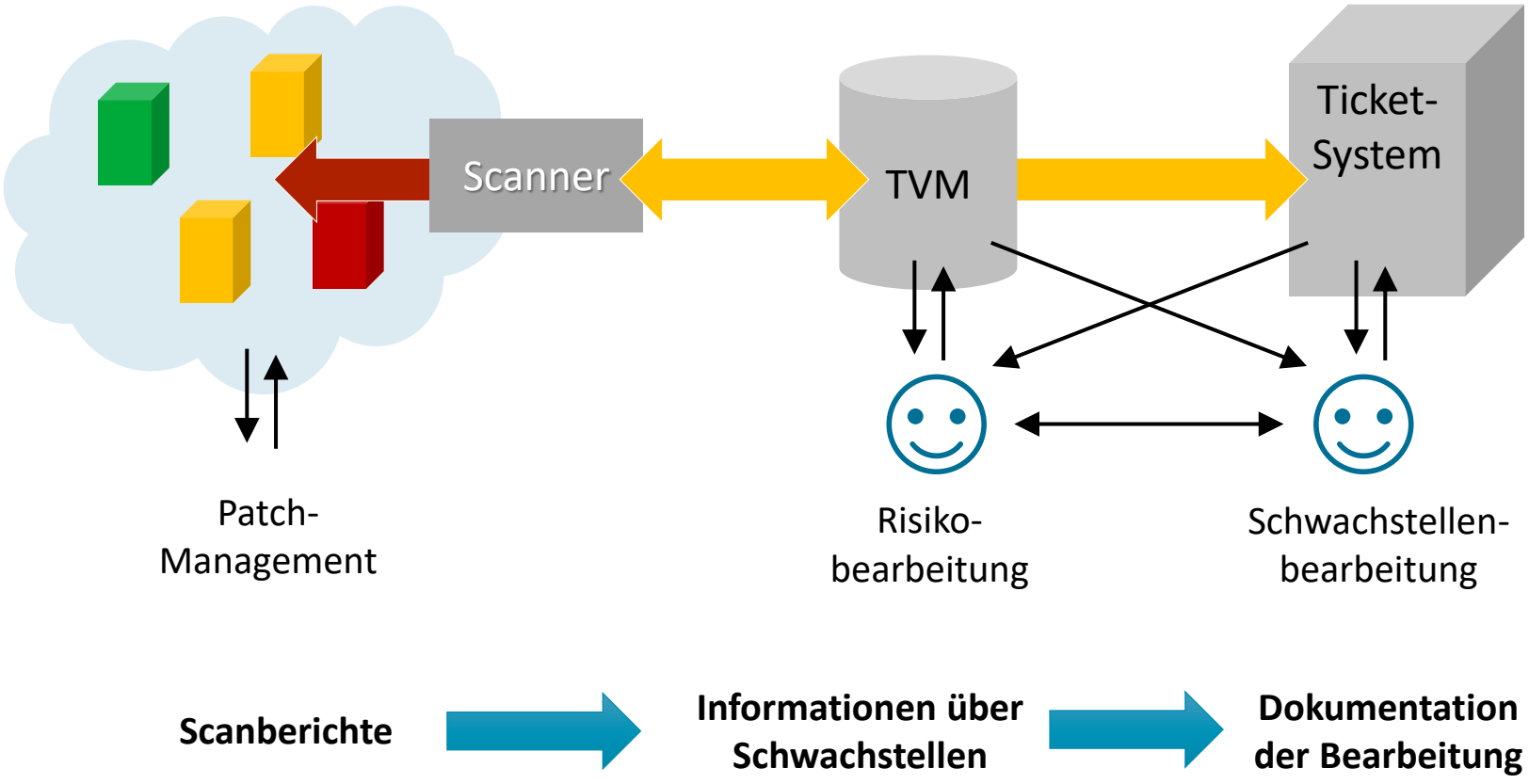
- Test der Systeme auf Verwundbarkeiten – „Vulnerability Scans“.
- Durchführung per Scan über Netzwerk oder Prüfung über Agenten auf dem System.
- Einzelne Scan-Reports oder zentrales Verwaltungssystem mit Übersichten.
- Information zu den Lücken wird bereitgestellt (Schweregrad, Angriffsvektor, etc.).
- Informationen können den relevanten Stakeholdern direkt geliefert werden.

Hinweis

Schwachstellenmanagement kümmert sich nicht um Patches, sondern Schwachstellen – teils können die gefundenen Punkte daher nicht direkt behoben werden!

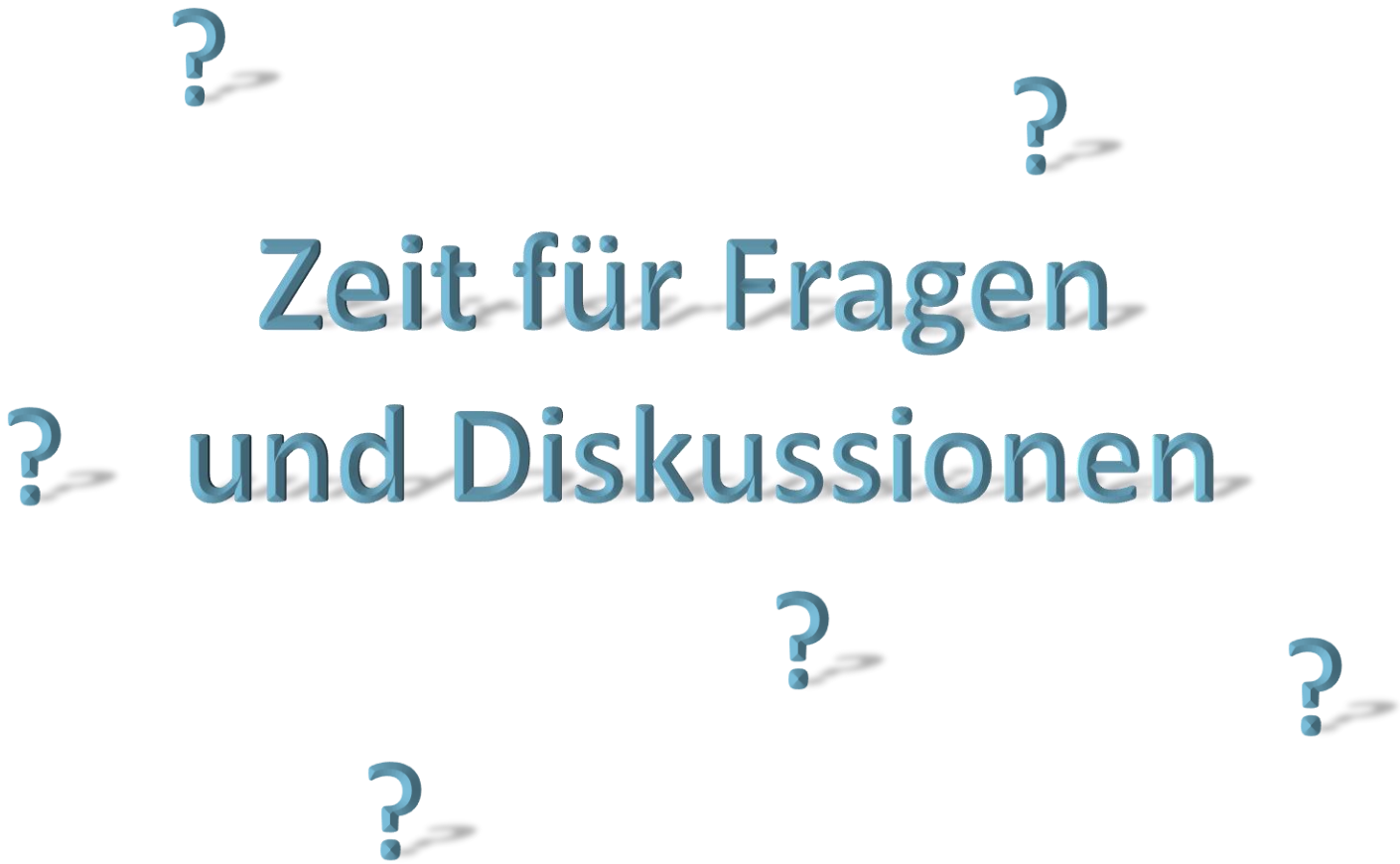
Sichtumkehrung zum Patchmanagement –
nicht „was habe ich bereits geschlossen“, sondern „was ist noch offen“

Schwachstellenmanagement – Umsetzung



Patch- und Schwachstellenmanagement

- Schwachstellenmanagement soll Überblick über Risiken geben.
- Patchmanagement schließt einige der Risiken – je größer die Lücke, desto wichtiger und zeitnaher das Patching.
- Schwachstellen-Prüfung kann Erfolg des Patchens prüfen und Fehler aufdecken.
  - Haben die Updates für alle Systeme stattgefunden? Wird nach Patch-Anwendung die Lücke nicht mehr gemeldet?
  - Priorisierung bei „kritischen“ Systemen“
- Bei zentralem Management System für Schwachstellen:
  - Risikomanagement möglich: Schwachstellen können (zeitlich begrenzt) aus dem Reporting genommen werden (mit Begründung).
  - Report kann daher um bekannte und „akzeptierte“ Lücken verringert werden.
- Systemverantwortliche können Patch-Relevanz auf Basis der konkreten Risiken einschätzen und Patchplan erstellen (Emergency-Patch, normaler Patch-Zyklus, kein Patch, …).
- Ggf. Funktion, unbekannte Assets im Netz zu identifizieren (Discovery-Scan).



Urheberrechtshinweis

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).

Bildquellen

- **(Patchmanagement Ziele)** – Update on Light Box – © patpitchaya – stock.adobe.com