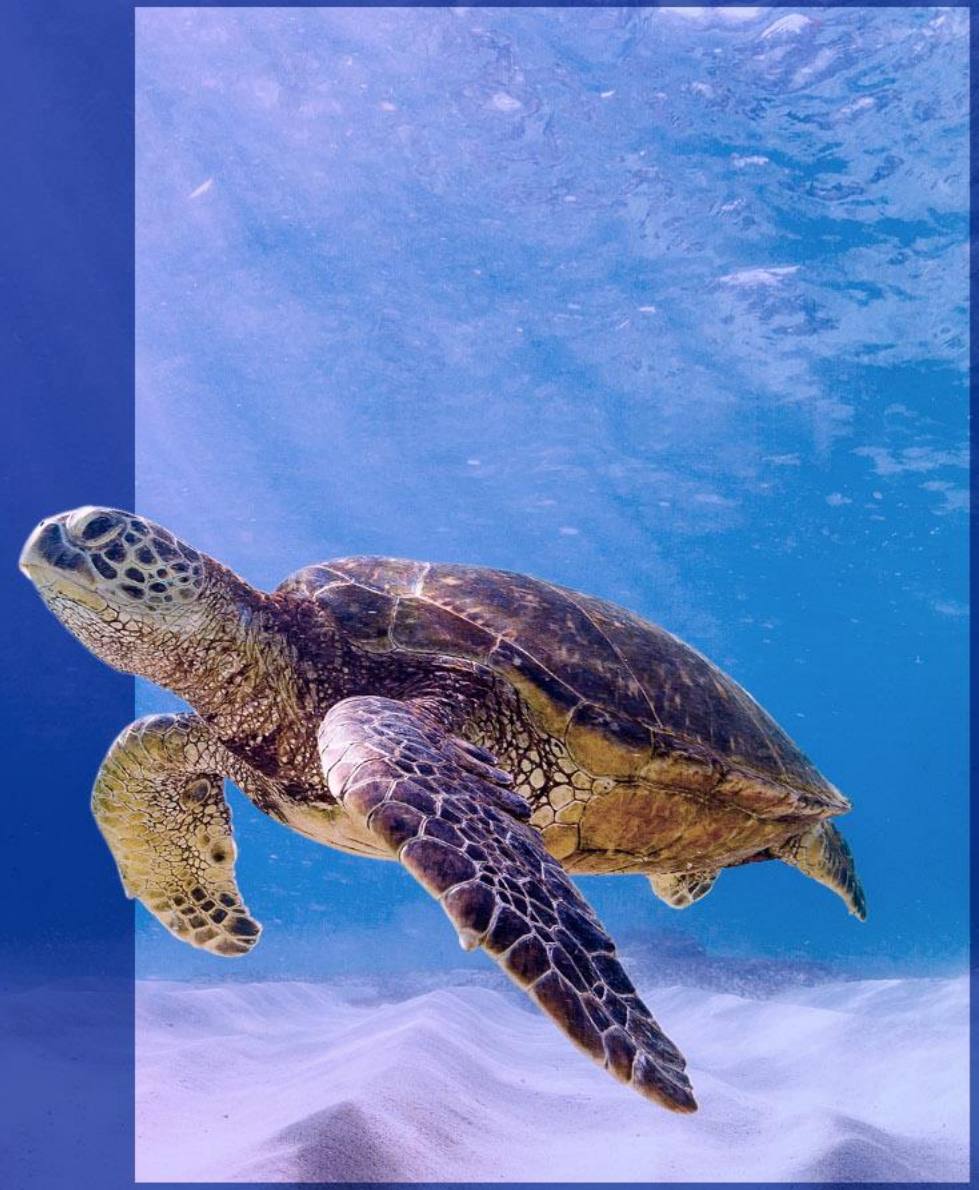
KPMG

DORA Sicherheitsmaßnahmen bei IKT-Dienstleistern



—

04.03.2025

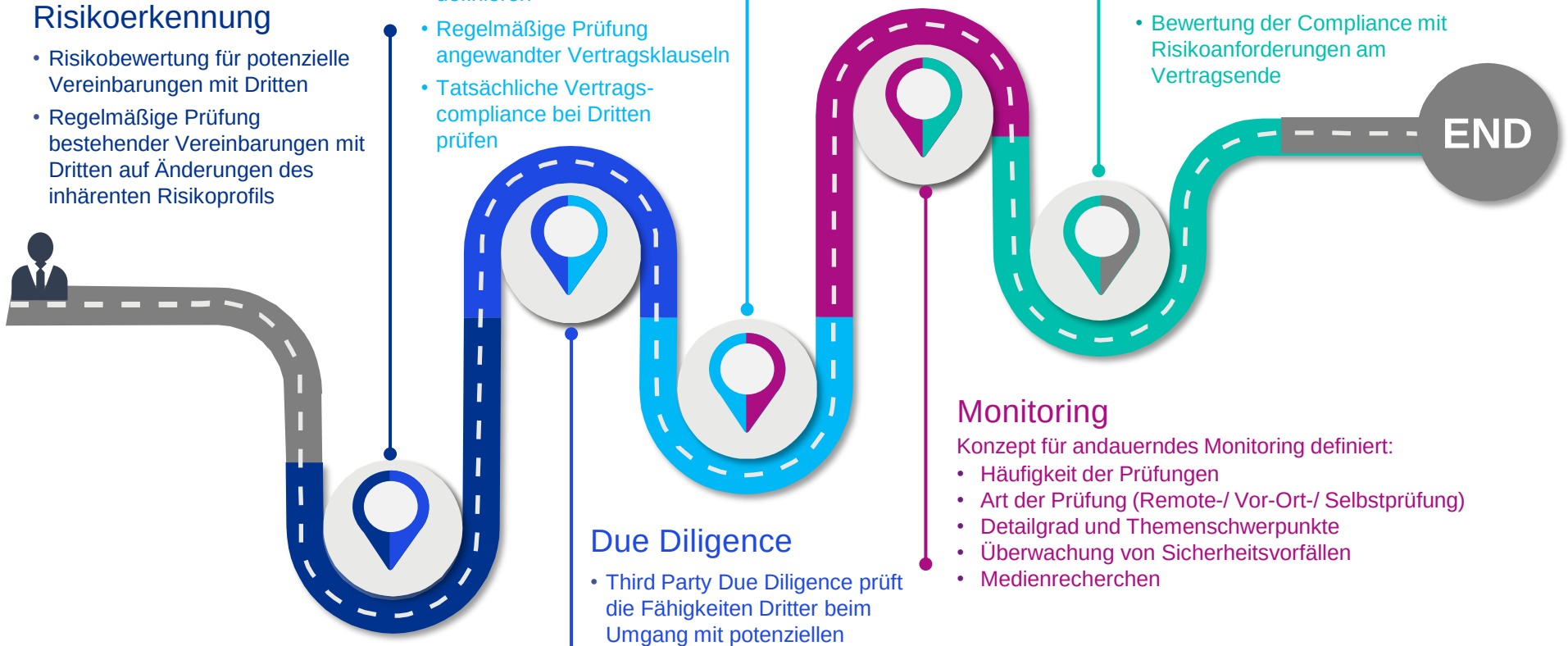
Third Party Risk Management (TPRM) Lebenszyklus

Risikoerkennung

- Risikobewertung für potenzielle Vereinbarungen mit Dritten
- Regelmäßige Prüfung bestehender Vereinbarungen mit Dritten auf Änderungen des inhärenten Risikoprofils

Vertragsabschluss

- Rechtliche Vereinbarungen zwischen Kunden und Dritten definieren
- Regelmäßige Prüfung angewandter Vertragsklauseln
- Tatsächliche Vertrags-compliance bei Dritten prüfen



Due Diligence

- Third Party Due Diligence prüft die Fähigkeiten Dritter beim Umgang mit potenziellen Risiken
- Periodische Due Diligence Prüfungen entsprechend den bestehenden Risikoprofilen

Monitoring

Konzept für andauerndes Monitoring definiert:

- Häufigkeit der Prüfungen
- Art der Prüfung (Remote-/ Vor-Ort-/ Selbstprüfung)
- Detailgrad und Themenschwerpunkte
- Überwachung von Sicherheitsvorfällen
- Medienrecherchen

Vertragsbeendigung

- Anforderungen für die Beendigung von Vereinbarungen mit Dritten definieren
- Bewertung der Compliance mit Risikoanforderungen am Vertragsende

Klassifizierung von IKT-Dienstleistern aufgrund Kritikalität

Beispielhafte Darstellung

„A und B-Lieferanten”

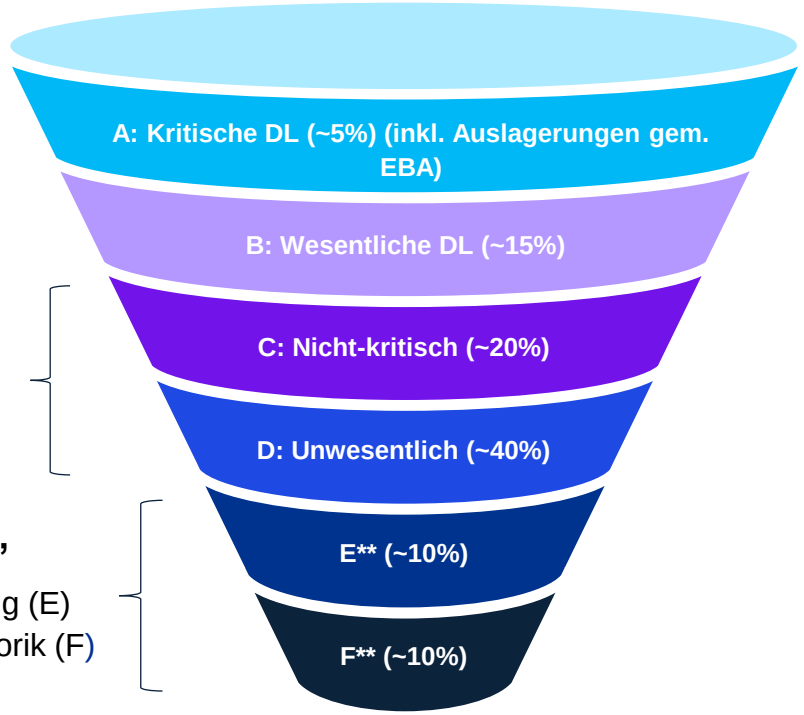
IKT-Dienstleister zur Unterstützung von kritischen und wichtigen Funktionen (DORA) sowie Auslagerungen* (EBA)

„C und D-Lieferanten”

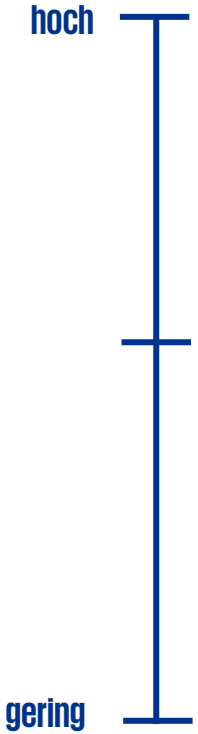
Nicht-kritische Lieferanten (NIS2, DORA, EBA, ISO)

„E und F-Lieferanten”

Lieferanten ohne IKT-Bezug (E) bzw. keine entspr. Regulatorik (F)



Aufwand in den jeweiligen TPRM-Phasen



*Auslagerungen und wesentliche Auslagerungen

**E-F: Keine Dienstleisterprüf- bzw. Monitoringaktivitäten aufgrund von IKT-Regulatorik notwendig

DORA – Welche Sicherheitsmaßnahmen sind bei IKT-Dienstleistern gefordert?

- *DORA Art 28.5: 66: (5) Finanzunternehmen dürfen vertragliche Vereinbarungen nur mit IKT-Drittdienstleistern schließen, die **angemessene Standards** für Informationssicherheit einhalten.*

  *Betreffen diese vertraglichen Vereinbarungen **kritische oder wichtige Funktionen**, so berücksichtigen die Finanzunternehmen vor Abschluss der Vereinbarungen angemessen, ob die IKT-Drittdienstleister die **aktuellsten und höchsten** Qualitätsstandards für die Informationssicherheit anwenden.*

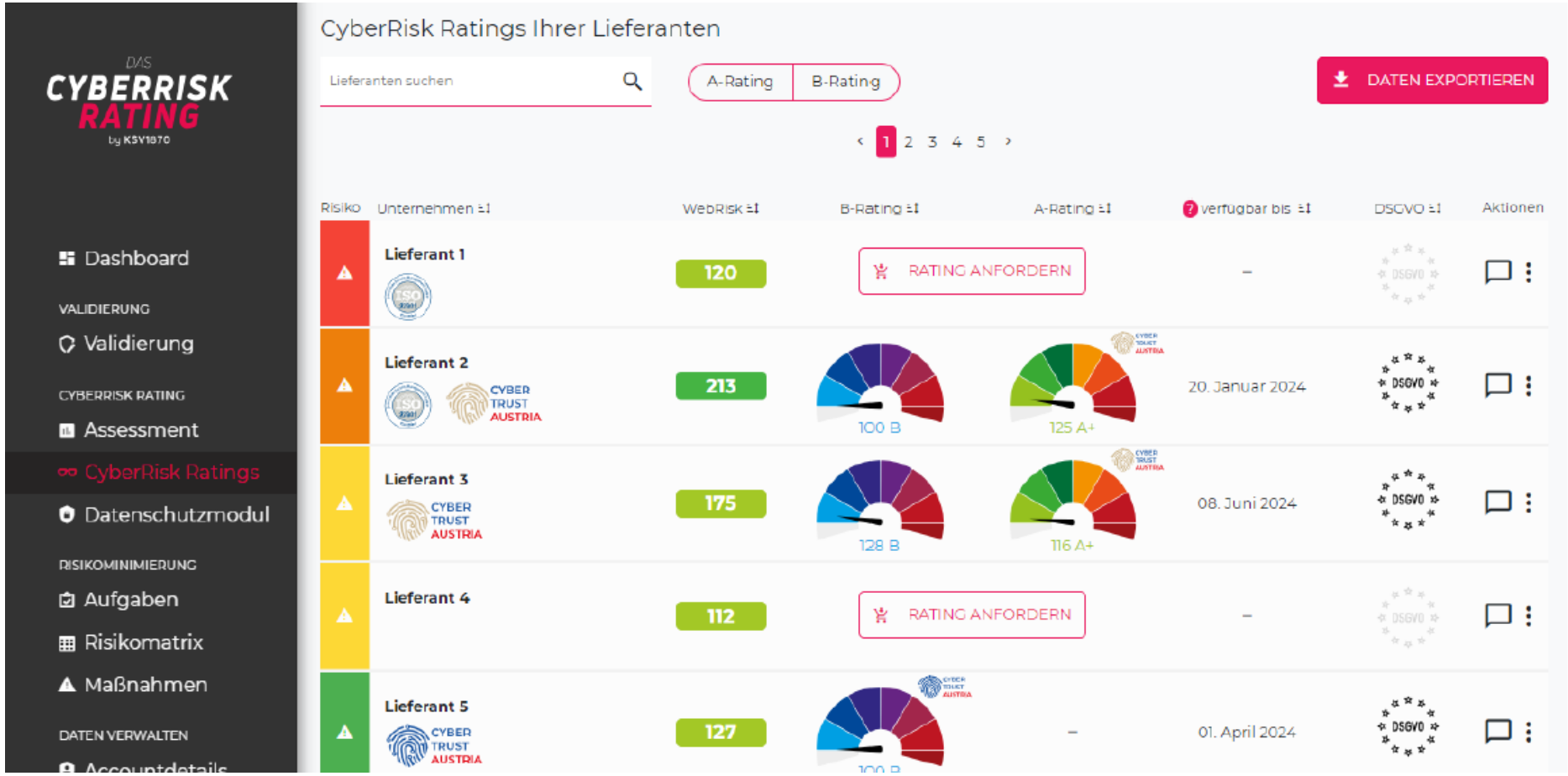
- Formal in der DORA keine Liste dieser Qualitätsstandards (im Detail) oder Vorgabe in welchem Detailgrad diese spezifiziert werden müssen.
- Annäherung via DORA und andere Industriestandards oder Best-Practices (ISO 27.001, BSI-Grundschutz, NIST, …)

- Mögliche Herangehensweise:
  - …angemessene Standards... => ISO 27.001, Cyber Trust Label, ISAE, SOC, …
  - …aktuellste und höchste Standards… => Angemessen + Spezifika der Leistungserbringung

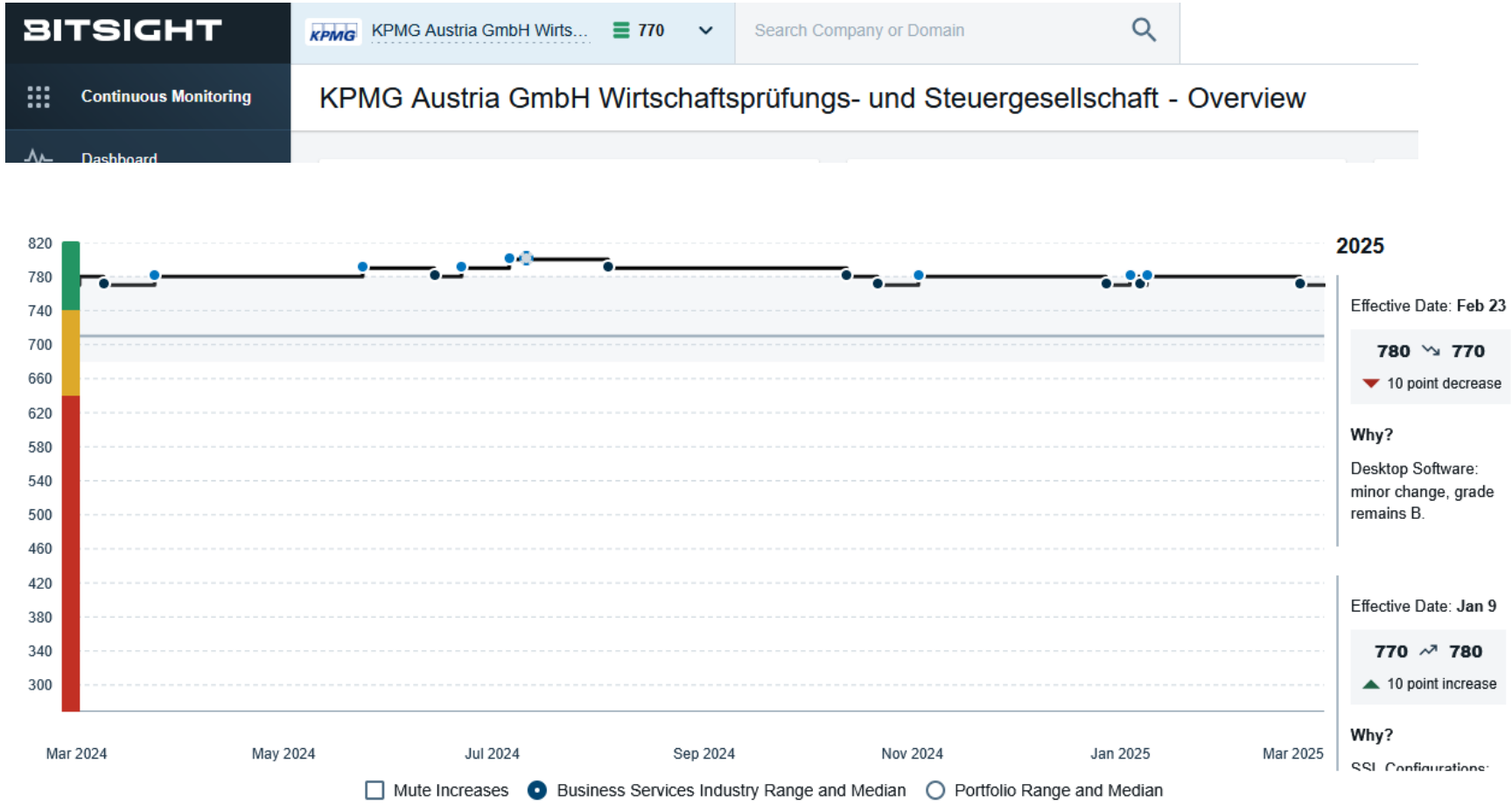
Top 10 Hausaufgaben für die Vorbereitung auf DORA

1	**Informationssicherheits-Risikomanagement** - Identifizieren, analysieren, bewerten und behandeln Sie Ihre Informations-sicherheitsrisiken als Grundlage für weitere Maßnahmen!
2	**Vorbereitung auf Sicherheitsvorfälle** - Legen Sie Verantwortlichkeiten fest und definieren Sie Prozesse zur Erkennung & Bewältigung von Sicherheitsvorfällen!“
3	**Notfallmanagement (Business Continuity, Disaster Recovery, Krisenmanagement)** - Erstellen Sie Abläufe zur Sicherstellung der Betriebskontinuität im Ernstfall & üben Sie diese regelmäßig!
4	**Sicherheitsrichtlinien** - Definieren Sie Vorgaben (Sicherheitsrichtlinien), setzen Sie diese um und überprüfen Sie diese regelmäßig auf Ihre Wirksamkeit!
5	**Risikomanagement für Lieferanten, Dienstleister und Dritte** - Geben Sie Lieferanten, Dienstleistern und Dritten klare Leitlinien, überprüfen Sie deren Einhaltung und analysieren Sie die daraus resultierenden Risiken!
6	**Sicherheitstests** - Führen Sie Sicherheitstests durch um die Effektivät Ihrer Maßnahmen und IKT-Sicherheitsarchitektur zu kennen!
7	**Physische Sicherheit** - Schützen Sie Ihre Infrastruktur durch die Definition klarer, physischer Sicherheitszonen!
8	**Meldewesen** - Bereiten Sie sich auf alle notwendigen (DORA, DSGVO) Meldewege zu diversen Behörden vor!”
9	**Sichere Konfiguration von Systemen und Netzwerken** - Härten & aktualisieren Sie Ihre Systeme und segmentieren Sie diese je nach Schutzbedarf in eigene Netzbereiche!
10	**Asset Management** - Identifizieren, dokumentieren & schützen Sie Ihre Assets und halten Sie Ihr Asset Inventar aktuell!

Mögliche Automatisierungsansätze zum IKT-Dienstleister Monitoring: Beispiel KSV/Nimbusec



Mögliche Automatisierungsansätze zum IKT-Dienstleister Monitoring: Beispiel Bitsight



Anhang: Details zu den Top 10 Maßnahmen

Top 10 Hausaufgaben für die Vorbereitung auf DORA

Bildquelle: https://www.istockphoto.com/

1. Informationssicherheits-Risikomanagement

"Identifizieren, analysieren, bewerten und behandeln Sie Ihre Informations-sicherheitsrisiken als Grundlage für weitere Maßnahmen!"

Bildquelle: https://www.istockphoto.com/

2. Vorbereitung auf Sicherheitsvorfälle

"Legen Sie Verantwortlichkeiten fest und definieren Sie Prozesse zur Erkennung & Bewältigung von Sicherheitsvorfällen!"

Bildquelle: https://www.istockphoto.com/

3. Notfallmanagement (Business Continuity, Disaster Recovery, Krisenmanagement)

“Erstellen Sie Abläufe zur Sicherstellung der Betriebskontinuität im Ernstfall & üben Sie diese regelmäßig!“

Bildquelle: https://www.istockphoto.com/

4. Sicherheitsrichtlinien

“Definieren Sie Vorgaben (Sicherheitsrichtlinien), setzen Sie diese um und überprüfen Sie diese regelmäßig auf Ihre Wirksamkeit!”

Bildquelle: https://www.istockphoto.com/

5. Risikomanagement für Lieferanten, Dienstleister und Dritte

“Geben Sie Lieferanten, Dienstleistern und Dritten klare Leitlinien, überprüfen Sie deren Einhaltung und analysieren Sie die daraus resultierenden Risiken!”

Bildquelle: https://www.istockphoto.com/

6. Sicherheitstests

“Führen Sie Sicherheitstests durch um die Effektivät Ihrer Maßnahmen und IKT-Sicherheitsarchitektur zu kennen!“

Bildquelle: https://www.istockphoto.com/

7. Physische Sicherheit

"Schützen Sie Ihre Infrastruktur durch die Definition klarer, physischer Sicherheitszonen!"

Bildquelle: https://www.istockphoto.com/

8. Meldewesen

"Bereiten Sie sich auf alle notwendigen (DORA, DSGVO) Meldewege zu diversen Behörden vor!"

Bildquelle: https://www.istockphoto.com/

9. Sichere Konfiguration von Systemen und Netzwerken

"Härten & aktualisieren Sie Ihre Systeme und segmentieren Sie diese je nach Schutzbedarf in eigene Netzbereiche!"

Bildquelle: https://www.istockphoto.com/

10. Asset Management

“Identifizieren, dokumentieren & schützen Sie Ihre Assets und halten Sie Ihr Asset Inventar aktuell!”

Bildquelle: https://www.istockphoto.com/

Anhang: Details zur IKT-Drittdienstleistesteuer ung unter DORA

Risiko-Assessment Phase (ex-ante und tourlich)

Third Party Risk Assessment

Aktivitäten:

- Definition von Risiko-Assessment Kriterien in Abhängigkeit von der Kritikalität des Dienstleisters (zB. operationelle Risiken, IKT-Risiken, Reputationsrisiken, Risiken iZh mit der Verfügbarkeit, Vertraulichkeit ect von Daten, Konzentrationsrisiken, Subauslagerung ect)
- Erstellung eines Risikobewertung-Fragebogens
- Definition einer Methodik zur Bewertung und Klassifizierung von Third Parties basierend auf den Ergebnissen des Third Party Risk Assessment Fragebogens
- Definition von IKS-Kontrollen
- Integration der DL IKT-Risiken in das interne IKT-Risikomanagement

Deliverables:

– Prozess zur Risikobewertung(ex-ante als auch tourlich)
– in Abhängigkeit der Klassifizierung ist definiert
– Risiko-Fragebogen ist erstellt
– Rollen und Verantwortlichkeiten sind definiert

Schnittstellen:

- Risiko Management
- Einkauf/Procurement

Artefakte (beispielhaft):

Risiko-Assessment | Due Diligence | Vertragsphase | Dienstleister-steuerung | Vertrags-beendigung & Offboarding

Due Dilligence Phase

Due Dilligence Phase

Aktivitäten:

- Erstellung eines Anforderungskataloges zur Due Diligence Bewertung von Third Parties unter Berücksichtigung der im Rahmen des Risiko-Assessment ermittelten Kritikalität des IKT-Dienstleisters

- Due Diligence Prüfkriterien umfassen zB.:
  - Geschäftlicher Ruf
  - Fachkenntnisse
  - Geeignete Organisationsstruktur
  - Funktionierendes Risikomanagement
  - Angemessene Informationssicherheitsstandards
  - Erforderliche Genehmigungen/Registrierungen

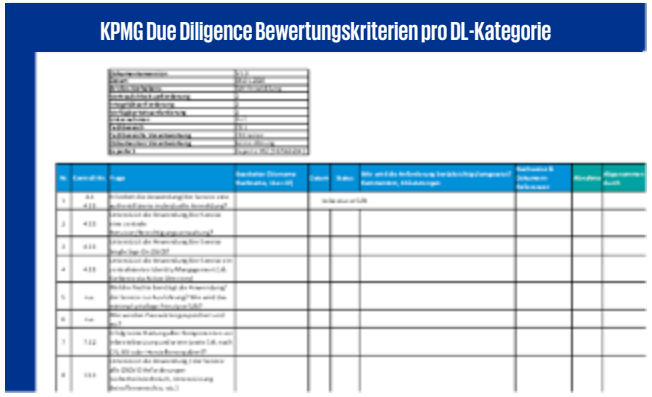
Deliverables:

– Checkliste mit Bewertungskriterien sowie einzuholenden Informationen/Dokumenten pro Dienstleister-Kategorie

Schnittstellen:

- Risiko Management
- Einkauf/Procurement

Artefakte (beispielhaft):



Risiko-Assessment | **Due Diligence** | Vertragsphase | Dienstleister-steuerung | Vertrags-beendigung & Offboarding

Vertragsphase

Vertragsphase

Aktivitäten:

- Definition von (Mindestvertrags)inhalten
- Erstellung allgemeiner Informationssicherheitsanforderungen (als Vertragsanhang)
- Definition von Sicherheitsanforderungen in SLAs (Service Level Agreement) und Lieferantenverträgen von kritischen Dienstleistern
- Definition von IKS-Kontrollen

Deliverables:

– Allgemeine Informationssicherheitsanforderungen

– Spezielle Sicherheitsanforderungen für SLAs und Lieferantenverträge für IKT-DL zur Unterstützung von kritischen und wichtigen Funktionen

Schnittstellen:

- Legal
- Informationssicherheits beauftragter
- IKS-Verantwortlicher
- Risk Management

Artefakte (beispielhaft):

Risiko-Assessment | Due Diligence | **Vertragsphase** | Dienstleister-steuerung | Vertrags-beendigung & Offboarding

Dienstleistersteuerung (1/3)

IKT Informationsregister

Aktivitäten:

- Etablierung eines IKT-Informationsregisters, in dem alle IKT-Dienstleister inkl. Bewertung & Ergebnis des Risk Assessments erfasst werden
- Aufgrund der detaillierten DORA Anforderungen an das Informationsregister wird eine tool-basierte Lösung empfohlen

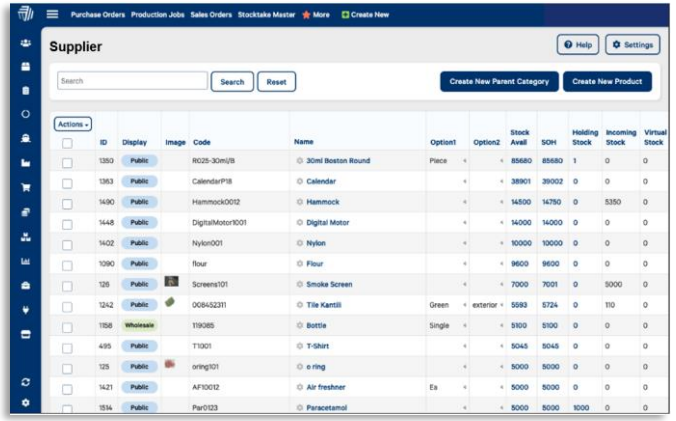
Deliverables:

– Die Anforderungen an die im Informationsregister zu erfassenden Datenpunkte und Informationen pro Dienstleister ist erstellt

Schnittstellen:

- Risiko Management
- Datenschutz

Artefakte (beispielhaft):



Risiko-Assessment → Due Diligence → Vertragsphase → **Dienstleister-steuerung** → Vertrags-beendigung & Offboarding

Dienstleistersteuerung (2/3)

Issue Management

Aktivitäten:

- Etablierung eines Prozesses für die Erstellung und den regelmäßigen Test von Ausstiegstrategien für kritische Dienstleister
- Definition und Testen von Notfall-Konzepten im Rahmen der BCM-Planung bei Ausfall eines Dienstleisters
- Notfallkonzepte für den Fall eines Sicherheitsvorfalls bei einer Third Party
- Definition von geeigneten Präventionsmaßnahmen

Deliverables:

– Prozess zum Issue Management von Third Parties ist etabliert

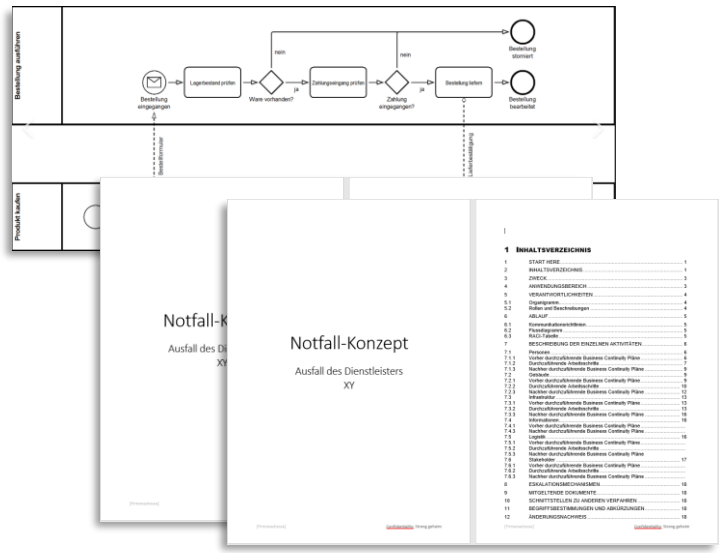
– Ausstiegsstrategien pro kritische Dienstleister sind definiert

– Notfall-Konzepte für Sicherheitsvorfälle bzw. Business Continuity mit entsprechenden Präventionsmaßnahmen ist definiert

Schnittstellen:

- Incident Management
- Business Continuity Management
- Informationssicherheits beauftragter

Artefakte (beispielhaft):



Risiko-Assessment | Due Diligence | Vertragsphase | **Dienstleister-steuerung** | Vertrags-beendigung & Offboarding

Dienstleistersteuerung (3/3)

Kontinuierliches Monitoring und Reporting

Aktivitäten:

- Definition der tourlichen Risikobewertung von bestehenden Lieferanten
- Definition von relevanten Third Party Risk KPIs
- Etablierung eines Monitoring-Prozesses für die SLA-/Vertragseinhaltung und Eskalations-Maßnahmen bei Nicht-Erfüllung durch den Dienstleister
- Etablierung eines Monitoring-Prozesses für die Einhaltung der Informationssicherheitsstandards und notwendige Prüfhandlungen in Abhängigkeit von der Kritikalitätseinstufung des Dienstleisters (zB. eigene Audits vs. Nimbusec-Ratings)
- Definition der Reportempfänger (Vorstand, Stakeholder, Behörden)
- Definition und Monitoring von IKS Kontrollen

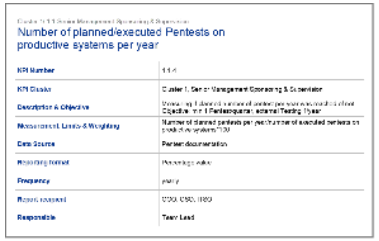
Deliverables:

– Monitoring- und Risikobewertungsprozesse ist etabliert
– KPIs zur Überwachung und Steuerung der Third Parties sowie die Reportempfänger sind definiert
– Meldepflichten an zB. Vorstand, Stakeholder, Behörden sind definiert

Schnittstellen:

- Risiko Management
- Informationssicherheits beauftragter
- Datenschutz
- IKS-Verantwortlicher
- Einkauf/Procurement

Artefakte (beispielhaft):



Risiko-Assessment | Due Diligence | Vertragsphase | **Dienstleister-steuerung** | Vertrags-beendigung & Offboarding

Vertragsbeendigung & Offboarding

Vertragsbeendigung & Offboarding

Aktivitäten:

- Etablierung eines Offboarding-Prozesses für Third Parties (inkl. Access Management und Rückgabe von Equipment)
- Regelmäßige Überprüfung und gegebenfalls Aktualisierung der erstellten Ausstiegsstrategien für kritische Dienstleister bzw. Evaluierung von Handlungsalternativen

Deliverables:

- Offboarding Prozess ist definiert
- Notwendige Schnittstellen zu anderen Abteilungen definiert

Schnittstellen:

- HR
- Facility Management
- IT-Support
- IAM
- Legal

Artefakte (beispielhaft):

Risiko-Assessment → Due Diligence → Vertragsphase → Dienstleister-steuerung → **Vertrags-beendigung & Offboarding**