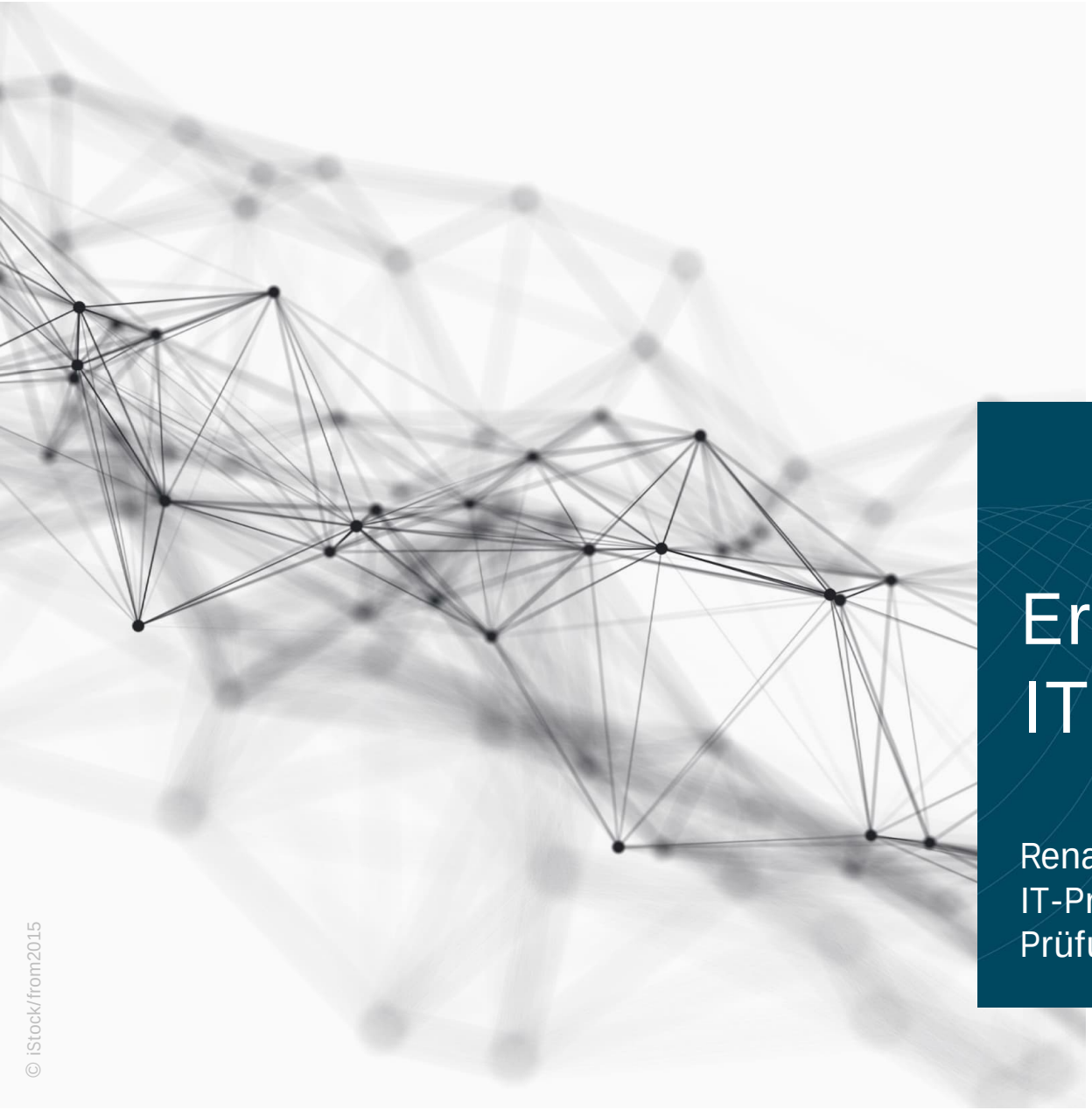

BaFin

Bundesanstalt für
Finanzdienstleistungsaufsicht

Erkenntnisse aus IT-Prüfungen

Renate Essler, Referat GIT 4
IT-Prüfungen und
Prüfungsunterstützung

Agenda

- Prüfungsorganisation
- Kategorisierung der Feststellungen
- Darstellung der Prüfungsgebiete

Prüfungsorganisation

3 - 4

Wochen durchschnittliche Prüfungsdauer, teilweise vor Ort und per Videokonferenz

5 - 8

IT-Prüfer typischerweise an Prüfung beteiligt

100%

Abdeckung der VAIT-Kapitel sowie des (IT-)Notfallmanagements

Kategorisierung der Prüfungsfeststellungen

	Kategorie F1	Kategorie F2	Kategorie F3	Kategorie F4
Bezeichnung	Geringfügig	Mittelschwer	Gewichtig	Schwerwiegend
Auswirkung für das Unternehmen	Geringes Risiko eines Schadens	Mittleres Risiko eines Schadens	Hohes Risiko eines Schadens	Sehr hohes Risiko eines Schadens und aufsichtlicher Handlungsbedarf
Beginn der Mängelbeseitigung	In überschaubarem Zeitrahmen	Zeitnah	Umgehend	Unverzüglich
Unzureichende Mängelbeseitigung	Hochstufung auf F2	Hochstufung auf F3	Hochstufung auf F4	Einzelfallbezogene Maßnahmen

IT-Strategie

Schweregrad der Feststellungen	▪ F1 – F2 ▪ F3 nur in extremen Ausnahmefällen
Wesentliche Mängel	▪ Keine IT-Strategie vorhanden ▪ Keine offizielle Verabschiedung der IT-Strategie durch den Vorstand ▪ Strategie hat den Charakter einer Präsentation, nicht den eines Strategiedokuments ▪ Keine überprüfbaren Ziele ▪ Mindestinhalte werden nicht abgedeckt ▪ Die Ausgliederung von Dienstleistungen wird nicht berücksichtigt. ▪ Fehlende Vorlage/Erörterung mit dem Aufsichtsorgan

IT-Governance

Schweregrad der Feststellungen	▪ F1 – F3 ▪ Große Bandbreite, da Governance-Sachverhalte zum Teil in anderen VAIT-Kapiteln beanstandet und bei der IT-Governance dann als Folgefehler angesehen werden.
Wesentliche Mängel	▪ Fehlende Richtlinien, Prozessbeschreibungen, Arbeitsanweisungen etc. ▪ Veraltete oder längere Zeit nicht überprüfte Dokumente ▪ Uneinheitliche Begriffsdefinitionen und Dokumentenbezeichnungen ▪ Keine IT-Governance-Pyramide vorhanden ▪ Unübersichtliche Wikis/Sharepoints/Intranetseiten ▪ Verweis auf nicht mehr aktuelle Versionsstände von Regelungen

Informationsrisikomanagement

Schweregrad der Feststellungen	▪ F1 – F4 ▪ Fast die Hälfte wurde mit F4 bewertet.
Wesentliche Mängel	▪ Fehlende, lückenhafte oder veraltete Übersicht über den eigenen Informationsverbund → keine ausreichende Berücksichtigung aller risikorelevanten IT-Assets im Risikomanagement ▪ Keine Übersicht über die aus Risikosicht kritischen IT-Assets aufgrund fehlender bzw. unzureichender Schutzbedarfsbestimmung ▪ Keine Festlegung der Soll-Maßnahmen auf Basis der Schutzbedarfe → nur wenig zielgerichtete Risikosteuerung ▪ Auf sinnvolle Sicherheitsmaßnahmen wird verzichtet, ohne das daraus resultierende Risiko zu analysieren. ▪ Das Risiko aus nicht oder nur unvollständig umgesetzten Soll-Maßnahmen sowie das verbleibende Restrisiko werden nicht analysiert.

Informationssicherheitsmanagement

Schweregrad der Feststellungen	▪ F1 – F4
Wesentliche Mängel	▪ Wichtige Bereiche von den Sicherheitsrichtlinien nicht abgedeckt ▪ Unzureichende Detaillierung der Sicherheitsrichtlinien ▪ IT-Schwachstellenmanagement fehlt oder ist unzureichend. ▪ Keine oder unzureichende Erkennung und Bearbeitung von IT-Sicherheitsvorfällen ▪ Personelle Ausstattung des Informationssicherheitsbeauftragten unzureichend

Automatisierte Erkennung von Sicherheitsvorfällen (Security Incident & Event Management - SIEM)

Schweregrad der Feststellungen	▪ F4 (unter Berücksichtigung von Maßnahmen auch F3)
Wesentliche Mängel	▪ Fehlende bzw. unzureichende Grundkonzeption des SIEM ▪ Fehlende Anbindung wichtiger Systeme ▪ Keine bzw. unzureichende Integritätssicherung der Protokolldaten in den Quellsystemen ▪ Fehlende Übersicht über die regulären Datenvolumina/Datenflüsse → ungewöhnliche Aktivitäten auf ungewöhnlichen Kanälen können nicht erkannt werden ▪ Keine bzw. unzureichende Überwachung kritischer Dateien und Verzeichnisse

Berechtigungsmanagement

Schweregrad der Feststellungen	▪ F3 – F4
Wesentliche Mängel	▪ Fehlende, unvollständige oder veraltete Berechtigungskonzepte für wesentliche Anwendungen oder Infrastrukturkomponenten ▪ Keine oder mangelhafte Wahrung der Funktionstrennung auf Ebene der Benutzerberechtigungen ▪ Keine auswertbare Dokumentation der genehmigten Berechtigungen → Soll-Zustand der IT-Systeme nicht zu ermitteln ▪ Keine angemessenen Prozesse zur Rezertifizierung von Benutzerberechtigungen, insbesondere fehlender Abgleich vergebener Rechte mit Berechtigungskonzepten ▪ Mangelhafte Ausgestaltung der Prozesse zur Rechtevergabe einschließlich der Überwachung/Protokollierung privilegierter Benutzer ▪ Unzureichende Überwachung von kritischen Berechtigungen (zum Beispiel Administratoren- oder Notfallkennungen) → zum Teil unzureichende Automatisierung gängiger Aufgaben

IT-Projekte, Anwendungsentwicklung

Schweregrad der Feststellungen	▪ F2 – F4
Wesentliche Mängel	▪ Fehlende bzw. unzureichende prozessuale Vorgaben sowie Überwachung der Vorgaben ▪ Keine Festlegung von produktionsverhindernden Abnahmekriterien ▪ Unzureichende Nachvollziehbarkeit des Test- und Freigabeprozesses anhand von Stichproben ▪ Keine bzw. unzureichende Zuordnung von Anforderungen mit den zugehörigen Tests ▪ Zu geringe Testabdeckung aufgrund unzureichender Testautomatisierung ▪ Keine Nachvollziehbarkeit des Tests der geforderten Systemleistung

Individuelle Datenverarbeitung (IDV)

Schweregrad der Feststellungen	▪ F3 – F4
Wesentliche Mängel	▪ Begriffsdefinition von IDV zu eng gefasst ▪ Fehlende bzw. zu generische Vorgaben zum Umgang mit IDV ▪ Fehlendes bzw. unvollständiges IDV-Register ▪ Keine Klassifikation der IDV-Anwendungen in Abhängigkeit ihres Risikos ▪ Zum Teil mehr als 400 IDV-Anwendungen im Einsatz → angemessene Qualitätssicherung fraglich

IT-Betrieb

Schweregrad der Feststellungen	▪ F1 – F3
Wesentliche Mängel	▪ Fehlende bzw. sich nicht an der Kritikalität der Daten orientierende Wiederherstellungstests ▪ Fehlende oder unzureichende technische (Mindest-)Anforderungen an die Rechenzentren ▪ Zu geringer Abstand der Rechenzentren → gleichzeitiger Ausfall beider Rechenzentren durch dasselbe Großereignis möglich

Ausgliederung von IT-Dienstleistungen

Schweregrad der Feststellungen	▪ F3 - F4
Wesentliche Mängel	▪ Fehlende bzw. inhaltlich unzureichende Risikoanalysen im Vorfeld der Ausgliederung (gilt auch für den sonstigen Fremdbezug von IT-Dienstleistungen) ▪ Keine vollständige Übersicht über die Ausgliederung von IT-Dienstleistungen und deren Weiterverlagerung ▪ Einstufung und Bewertung von Risiken wurden zum Teil ohne konkrete Prozessbeschreibung oder Bewertungskriterien vorgenommen. ▪ Unzureichende Ausgliederungsüberwachung ▪ Keine oder nur unzureichende Überlegungen zu Exit- oder Alternativ-Strategien für den Fall eines Ausfalls/der Kündigung eines IT-Dienstleisters → Keine IT-spezifischen Mängel, aber in dieser Schwere im IT-Umfeld tendenziell eher anzutreffen als in anderen ausgegliederten Bereichen

Notfallmanagement / IT-Notfallmanagement

Schweregrad der Feststellungen	▪ F3
Wesentliche Mängel	▪ Nur die zeitkritischsten Prozesse werden als relevant für die Notfallplanung angesehen → keine Notfallpläne für kurzfristig entbehrliche aber langfristig unverzichtbare Prozesse vorhanden ▪ Konsistenzabgleich der Wiederanlaufzeiten mit den Verfügbarkeitsanforderungen aus dem Informationsrisikomanagement fehlt. ▪ Der Ausfall von Personen mit unverzichtbaren Spezialkenntnissen wird nicht oder nur unzureichend betrachtet. ▪ Teilweise unzureichende Konsolidierung und Plausibilitätsüberprüfung der im Rahmen der Analysen abgefragten Rückmeldungen ▪ Der vollständige Transfer der gesamten Rechenleistung auf ein einziges Rechenzentrum wird nicht oder nur unzureichend getestet. ▪ Unzureichende Überprüfung, über welchen Zeitraum der Geschäftsbetrieb mit nur einem Rechenzentrum aufrecht erhalten werden kann.

Gesamt-Prüfungsurteil (ohne Nachschauprüfungen)

Die Anforderungen der VAIT sind

Nicht vollständig erfüllt	Nur teilweise erfüllt	Nicht erfüllt
10%	50%	40%

Renate Essler
Referat GIT 4
IT-Prüfungen und Prüfungsunterstützung
Telefon: +49(0)228 4108-2440
E-Mail: renate.essler@bafin.de

Bildnachweis: pixabay.com/geralt