FORUM

# DORA-ready und zukunftssicher

## Modernes IT Service Management für Banken

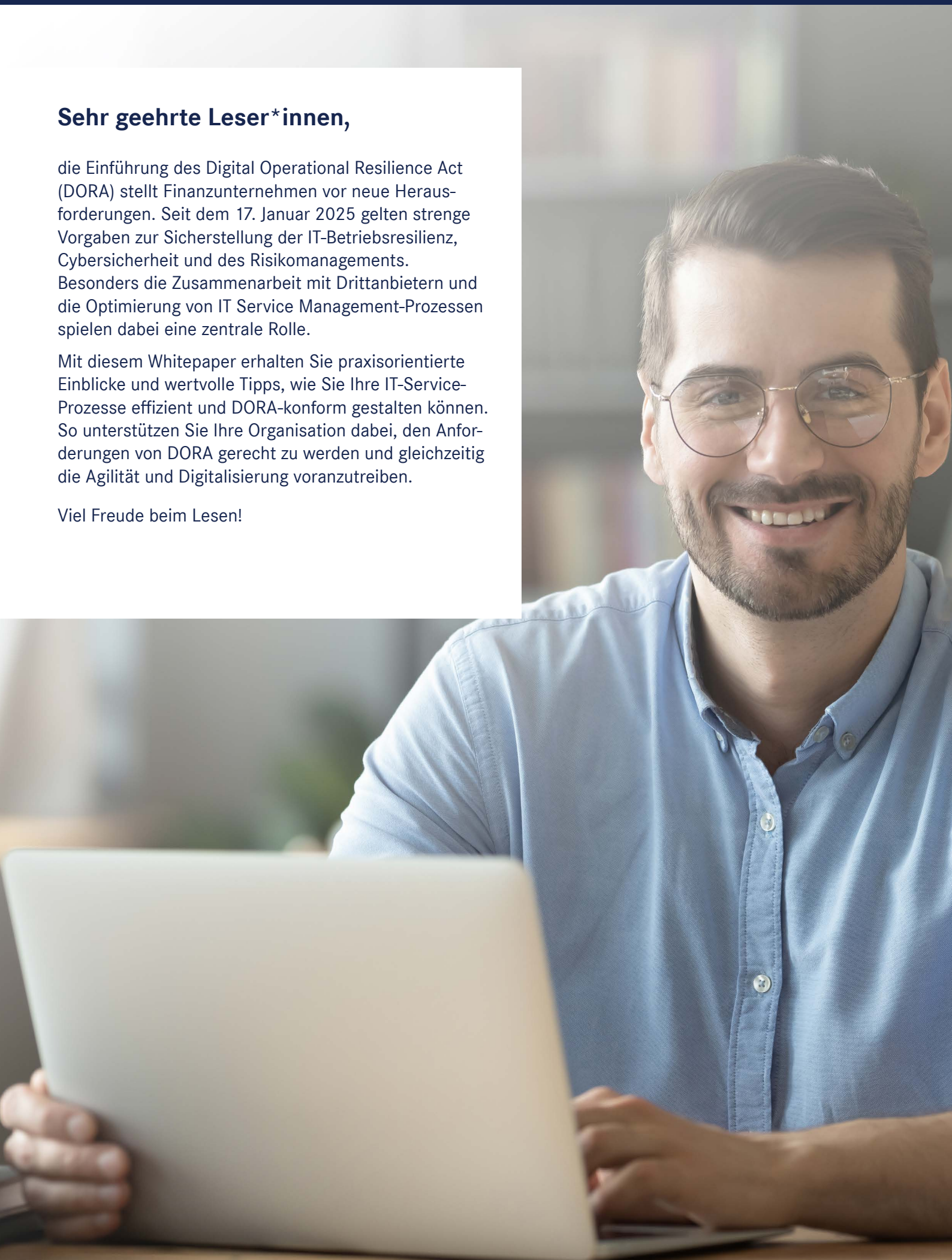
Seven Principles Mobility GmbH

## Sehr geehrte Leser*innen,

die Einführung des Digital Operational Resilience Act (DORA) stellt Finanzunternehmen vor neue Herausforderungen. Seit dem 17. Januar 2025 gelten strenge Vorgaben zur Sicherstellung der IT-Betriebsresilienz, Cybersicherheit und des Risikomanagements. Besonders die Zusammenarbeit mit Drittanbietern und die Optimierung von IT Service Management-Prozessen spielen dabei eine zentrale Rolle.

Mit diesem Whitepaper erhalten Sie praxisorientierte Einblicke und wertvolle Tipps, wie Sie Ihre IT-Service-Prozesse effizient und DORA-konform gestalten können. So unterstützen Sie Ihre Organisation dabei, den Anforderungen von DORA gerecht zu werden und gleichzeitig die Agilität und Digitalisierung voranzutreiben.

Viel Freude beim Lesen!



WHITEPAPER

# DORA-ready und zukunftssicher:

## Modernes **IT Service Management** für Banken und Versicherungen

Erfahren Sie, wie modernes IT Service Management die Anforderungen des Digital Operational Resilience Act (DORA) erfüllt und Finanz-IT widerstandsfähiger macht – mit praktischen Tipps aus der Sicht eines IKT-Drittdienstleisters.

Mehr Informationen erhalten Sie hier: 7p-mobility.com

# Inhaltsverzeichnis

# Inhaltsverzeichnis – Checklisten

# 1 Über dieses Whitepaper

**DORA (Digital Operational Resilience Act) tritt ab 17. Januar 2025 mit EU-Gesetzes-Charakter in Kraft. Finanz- und Versicherungsunternehmen überarbeiten derzeit ihre internen Strukturen im Rahmen von „DORA-Projekten", um die Anforderungen DORA-konform umzusetzen.**

Ziele von DORA sind unter anderem die Einhaltung der Informationssicherheit, die Gewährleistung der Cybersicherheit und des gesamten Risikomanagement-Rahmens, die Resilienz der IT-Betriebsorganisation und das Management des Drittparteienrisikos.

Insbesondere die beiden letztgenannten Themen (Resilienz des IT-Betriebs und Zusammenarbeit mit Dienstleistern) erfordern eine Optimierung der IT Service Management-Prozesse und -Systeme sowie der operativen Werkzeuge.

Ein professionelles und modernes IT Service Management zeichnet sich dadurch aus, dass es

- die regulatorischen Anforderungen erfüllt,
- die zunehmende Agilität und Digitalisierung unterstützt und
- die Zusammenarbeit mit Service Providern standardisiert.

Dieses Whitepaper geht auf diese wichtigen Aspekte zur Optimierung Ihrer modernen IT Service Organisation ein und gibt wertvolle Praxistipps, die Banken, Finanzdienstleister und Versicherungen schon morgen im Rahmen ihrer DORA-Projekte umsetzen können.

Das Whitepaper richtet sich an CIOs, IT-Betriebsleiter, Leiter IT Operations, IT-Service-Prozessverantwortliche und IT-Service-Delivery-Verantwortliche, die ihre IT-Service-Prozesse und -Systeme DORA-konform aufstellen.

# 2 Mehr als Compliance: Wie DORA die IT-Landschaft im Finanzsektor transformiert

## 2.1 Anforderungen an die digitale Resilienz

Stabile und sichere IT-Systeme sind ein entscheidender Erfolgsfaktor in der digitalisierten Finanzbranche. Der Digital Operational Resilience Act (DORA) der EU setzt klare Vorgaben, um Finanzinstitute vor Betriebsstörungen und Cyberangriffen zu schützen und ihre Geschäftsprozesse auch in Krisensituationen aufrechterhalten zu können. DORA geht weit über den Schutz einzelner Unternehmen hinaus: Ziel ist es, die Widerstandsfähigkeit des gesamten EU-Finanzmarktes umfassend zu stärken. Erreicht wird dies durch die Einführung detaillierter Vorschriften in den Regulatory Technical Standards (RTS) und Implementing Technical Standards (ITS). Diese zwingen Finanzinstitute nicht nur zu strategischen und operativen Anpassungen, sondern auch zur Steuerung und Zusammenarbeit mit Drittdienstleistern und verändern ihre IT-Landschaften grundlegend.

## 2.2 Der Beitrag von IT Service Management zur DORA-Konformität

Ein wesentlicher Baustein zur Erfüllung der DORA-Anforderungen ist das IT Service Management (ITSM). ITSM bietet den methodischen Rahmen für das systematische Management von IT-Services und unterstützt Finanzunternehmen dabei, ihre IT-Prozesse an die sich ständig ändernden regulatorischen und geschäftlichen Anforderungen anzupassen. Mit einem etablierten ITSM-Framework wie ITIL können Unternehmen ihre IT-Prozesse standardisieren und kontinuierlich verbessern. Damit wird eine stabile Basis für die Erfüllung der DORA-Anforderungen geschaffen.

Der Einsatz eines ausgereiften ITSM-Systems ermöglicht die Steuerung der gesamten Leistungskette und ein effektives Management der Service Level Agreements (SLAs), damit auch IKT-Drittanbieter die hohen DORA-Anforderungen erfüllen. Ein gut implementiertes ITSM bietet Unternehmen somit nicht nur einen methodischen Rahmen zur Compliance, sondern auch die Basis für ein umfassendes Risikomanagement, das alle internen und externen Risiken erfasst und managt.

## 2.3 DORA im Detail: Die 6 wichtigsten Schwerpunkte

DORA umfasst eine Vielzahl von Bereichen zur Sicherstellung einer ganzheitlichen Resilienz. Der Fokus liegt auf den folgenden sechs Schwerpunkten:

**1. IKT-Risikomanagement**

**Kapitel II, Artikel 5 bis 16**

Dieses Kapitel legt den grundlegenden Rahmen für das IKT-Risikomanagement fest und definiert die Verantwortlichkeiten der Unternehmen.

**2. Behandlung, Klassifizierung und Berichterstattung IKT-bezogener Vorfälle**

**Kapitel III, Artikel 17 bis 23**

Hier geht es um die Behandlung, Klassifizierung und Meldung von IKT-bezogenen Vorfällen. Unternehmen müssen Vorfälle erkennen, bewerten und entsprechend handeln.

**3. Testen der digitalen operationellen Resilienz einschließlich Threat Led Penetration Testing (TLPT)**

**Kapitel IV, Artikel 24 bis 27**

Dieses Kapitel befasst sich mit der Überprüfung der digitalen Widerstandsfähigkeit, einschließlich der Durchführung von Penetrationstests, um Schwachstellen aufzudecken.

**4. Management des IKT-Drittparteienrisikos**

**Kapitel V, Abschnitt I, Artikel 28 bis 30**

Unternehmen müssen ihre externen Dienstleister genau unter die Lupe nehmen, um potenzielle Risiken zu erkennen und zu minimieren.

**5. Überwachungsrahmen für kritische IKT-Drittdienstleister**

**Kapitel V, Abschnitt II, Artikel 31 bis 44**

Wichtige IT-Dienstleister werden besonders genau beobachtet, um sicherzustellen, dass sie hohe Sicherheitsstandards einhalten und Störungen schnell beheben können.

**6. Vereinbarungen über den Austausch von Informationen sowie Cyberkrisen- und Notfallübungen**

**Kapitel VI, Artikel 44 und Artikel Kapitel VII, Artikel 49**

Zielt darauf ab, die Zusammenarbeit und den Informationsaustausch zwischen Finanzinstituten und zur Aufsicht (z. B. BaFin) zu stärken.

## 2.4 Neue Anforderungen an die Unternehmensführung

Die DORA-Verordnung bringt eine neue Ernsthaftigkeit in den Finanzsektor. Sie stellt Anforderungen auf allen Unternehmensebenen und führt neue Mechanismen für Verantwortlichkeit und Transparenz ein:

**_ Persönliche Haftung der Geschäftsleitung**
Die Geschäftsleitung ist persönlich für die Einhaltung der DORA-Vorschriften verantwortlich und kann diese Verantwortung nicht delegieren.

**_ Reputationsrisiko**
Verstöße gegen DORA werden auf der Website der Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) veröffentlicht und können zu erheblichen Reputationsschäden führen.

**_ DOR-Strategie (Digital Operational Resilience-Strategie)**
Jedes Unternehmen muss eine spezifische DOR-Strategie entwickeln, die in die Geschäfts- und IT-Strategie integriert ist und die langfristige Sicherheit des Unternehmens gewährleistet.

**_ Dienstleisterauswahl und Vertragsgestaltung**
Die Auswahl und Steuerung externer Dienstleister wird komplexer. Die Verantwortung für die gesamte Dienstleistungskette bleibt beim auslagernden Unternehmen.

**_ Testverfahren**
Umfassende Tests auf allen strategischen und operativen Ebenen werden zur Praxis und die nachweisliche Umsetzung wird notwendig.

**_ Umgang mit Vorfällen**
Datenschutz- und Sicherheitsvorfälle werden neu integriert. Der Prozess orientiert sich an der Kritikalität und Bedeutung der betroffenen Geschäftsfunktionen und wird durch DORA geregelt.

## 2.5 Die Rolle des Asset Managements im DORA-konformen IT Service Management

DORA erfordert eine lückenlose Nachvollziehbarkeit und Kontrolle aller IT-Assets, da Finanzinstitute jederzeit in der Lage sein müssen, den Status und die Verfügbarkeit kritischer Assets zu überwachen. Der Service Asset und Configuration Management Prozess muss daher so angepasst werden, dass eine detaillierte Configuration Management Database (CMDB) geführt wird, die jederzeit einen vollständigen Überblick über alle IT-Ressourcen bietet. Darüber hinaus müssen Änderungen an den Assets und Konfigurationen genau dokumentiert und die möglichen Auswirkungen auf die Ausfallsicherheit bewertet werden. Ziel ist es, die Transparenz über die IT-Assets zu erhöhen, um Risiken frühzeitig zu erkennen und im Störungsfall schnell reagieren zu können.

## 2.6 DORA als Chance zur Modernisierung

Die Einführung von DORA ist nicht nur eine regulatorische Herausforderung, sondern bietet Unternehmen auch Chancen zur Modernisierung ihrer IT-Landschaften. Viele Unternehmen hatten bisher nur begrenzte Ressourcen, um ihre IT-Prozesse zu modernisieren. Mit DORA erhalten sie nun sowohl Handlungsdruck als auch Handlungsmöglichkeiten, um ihre digitale Resilienz auf ein neues Niveau zu bringen. Die Modernisierung von Prozessen, Systemen und Integrationen führt langfristig nicht nur zu einer höheren Compliance, sondern auch zu einer nachhaltigen Verbesserung der Effizienz und Sicherheit der gesamten IT-Landschaft.
Durch die gezielte Anpassung und Nutzung von ITSM können Unternehmen somit nicht nur die DORA-Konformität erreichen, sondern auch die Chance nutzen, ihre IT-Organisation strategisch weiterzuentwickeln.

# 3 Historisch gewachsene Prozesse und Systeme treffen auf regulatorische Anforderungen

Viele Finanz- und Versicherungsunternehmen stehen vor der Herausforderung, ihre historisch gewachsenen IT-Strukturen an die DORA-Anforderungen anzupassen. Häufig haben diese Systeme und Prozesse nicht den notwendigen Reifegrad, um eine stabile Basis für die Umsetzung der neuen regulatorischen Anforderungen zu bieten. Hier ist eine grundlegende Modernisierung zur Erfüllung der Anforderungen an Sicherheit und Resilienz und zur Beseitigung bestehender Schwachstellen erforderlich.

**Typische Schwachstellen im Kontext der DORA-Implementierung**

Finanzinstitute und Versicherer sehen sich häufig mit den folgenden Herausforderungen konfrontiert:

- Unvollständige Definition des Informationsverbundes
- Fehlende Digital Operational Resilience-Strategie (DOR-Strategie)
- Outsourcing kann nicht auf kritische und wichtige Funktionen abgebildet werden
- Bestehende IKT-Dienstleister erfüllen DORA-Anforderungen nicht
- Fehlender Notfallplan für bestehende IT-Dienstleister
- Veraltete und inhomogene Prozesse und Systeme
- Geringe Transparenz und Steuerbarkeit von Dienstleistern
- Abhängigkeit von Dienstleisterprozessen und -tools
- Veraltete ITSM-Systeme
- Niedrige Prozessreife
- Lückenhafte Dokumentation
- Isoliertes Asset Management ohne Integration der CMDB
- Fehlende Versionierung im Identity und Access Management

## Handlungsempfehlungen für eine nachhaltige DORA-Umsetzung

In diesem Whitepaper erfahren Sie, welche strategischen Schritte Sie mit Ihrer IT-Abteilung und dem Auslagerungsmanagement priorisieren sollten, um den Grundstein für eine stabile und DORA-konforme IT-Landschaft zu legen. Setzen Sie gezielte Maßnahmen in Ihrem IT-Betrieb zur schnellen Behebung von Schwachstellen und zur Schaffung einer langfristig belastbaren IT-Infrastruktur um.

# 4 7P – Ihr Partner für DORA-Compliance:
## Expertise, auf die Sie bauen können

Als IKT-Drittdienstleister, der sich bereits seit mehreren Jahren auf die Anforderungen von DORA vorbereitet hat, wissen wir genau, worauf es für Ihr Unternehmen ankommt!

Wir sind mit den regulatorischen DORA-Anforderungen der Finanz- und Versicherungsbranche bestens vertraut und verankern diese bereits proaktiv in unserer eigenen internen Service-Organisation.

Unsere Kunden aus der Finanz- und Versicherungsbranche profitieren dadurch von etablierten und erprobten Strukturen sowie effizienten Zusammenarbeitsmodellen.

So können sie viele Punkte der DORA-Compliance schnell und unkompliziert umsetzen und die Umsetzung der regulatorischen Anforderungen souverän meistern.

Ihr Weg zur DORA-Konformität beginnt hier.
Erfahren Sie, wie eine Partnerschaft mit uns als IKT-Dienstleister Ihre IT zukunftssicher macht.

Kontaktieren Sie uns noch heute!

Mit Experten sprechen →

WELL DONE Zertifizierungsgesellschaft mbH DIN EN ISO 9001:2015

FOX CERTIFICATION ISO 27001 CERTIFIED CERTIFIED ZN-2022-21 valid until 11/25/25

# 5 Welche Anforderungen stellt DORA an ein modernes ITSM?

Der Digital Operational Resilience Act stellt spezifische Anforderungen an die IT-Systeme und -Prozesse von Finanzunternehmen. Diese Anforderungen gehen weit über die klassischen Sicherheitsstandards hinaus und verlangen von IT-Organisationen ein höheres Maß an Proaktivität und Effizienz, insbesondere in den Bereichen Operational Resilience, Krisenmanagement und Reporting. Ein modernes IT Service Management muss daher so strukturiert und angepasst sein, dass es den DORA-Anforderungen gerecht wird.

Eine der Kernanforderungen von DORA ist die Gewährleistung der Widerstandsfähigkeit der IT-Systeme im operativen Betrieb. Die IT-Systeme müssen so gestaltet sein, dass sie im Rahmen der IKT-Geschäftsfortführung auch unter erhöhter Belastung oder nach einem Vorfall funktionsfähig bleiben und die kritischen Geschäftsprozesse weiterhin unterstützen. Dabei muss das ITSM in der Lage sein, nicht nur reaktiv auf Ausfälle zu reagieren, sondern auch präventive Maßnahmen zu ergreifen. Das beinhaltet die Implementierung zuverlässiger Verfahren zur kontinuierlichen Überwachung der Systemintegrität und Verfügbarkeit der IT-Services.

Darüber hinaus muss ein modernes ITSM über eine umfassende Risiko- und Schwachstellenbewertung verfügen. Diese muss laufend aktualisiert und in die ITSM-Prozesse integriert werden. Nur so können Schwachstellen frühzeitig erkannt und entsprechende Gegenmaßnahmen eingeleitet werden. DORA fordert explizit, dass Unternehmen regelmäßig potenzielle Risiken für ihre IT-Systeme analysieren und entsprechende Präventivmaßnahmen in ihre operativen Prozesse integrieren. Dabei geht es nicht nur um technologische Risiken, sondern auch um operationelle Schwachstellen, die durch unzureichende IT-Prozesse oder mangelnde Anpassung an neue Bedrohungsszenarien entstehen können.

Insbesondere bei Sicherheitsvorfällen oder Systemausfällen verlangt DORA von den Unternehmen eine detaillierte und umfassende Dokumentation aller IT-relevanten Prozesse und Ereignisse. Diese Berichte müssen nicht nur für den internen Gebrauch, sondern bei Bedarf auch zur Vorlage bei Aufsichtsbehörden zur Verfügung stehen. Dementsprechend muss ein modernes ITSM in der Lage sein, umfassende Protokolle und Berichte zu generieren, die einerseits den Betriebszustand eines Systems widerspiegeln, andererseits aber auch die Reaktionsgeschwindigkeit und Effizienz der getroffenen Maßnahmen nachweisen.

ITSM darf nicht isoliert betrachtet werden, sondern muss eng mit den allgemeinen Geschäftsstrategien und -prozessen verknüpft sein. Das bedeutet, dass IT Service Management auch eine Schlüsselrolle im Krisen- und Notfallmanagement spielen muss. Unternehmen müssen dafür Sorge tragen, dass ihre ITSM-Prozesse klare Eskalationswege und eine enge Verzahnung mit dem allgemeinen Krisenmanagement haben. Im Falle eines IT-Notfalls muss sofort klar sein, welche Maßnahmen zu ergreifen sind, wer für welche Maßnahmen verantwortlich ist und wie schnell die Wiederherstellung des Betriebs möglich ist.

Nicht zuletzt fordert DORA, dass moderne ITSM-Systeme flexibel und skalierbar sein müssen, um sich dynamischen Veränderungen und neuen Anforderungen anpassen zu können. Angesichts des schnellen technologischen Wandels und der sich ständig ändernden Bedrohungslage müssen ITSM-Lösungen modular aufgebaut und erweiterbar sein. Auf diese Weise ist eine schnelle Reaktion auf neue regulatorische Anforderungen oder Bedrohungen möglich, ohne dass eine Überarbeitung der gesamten Systemarchitektur erforderlich ist.

DORA erfordert ein modernes ITSM in Finanzunternehmen, das auf Prävention, proaktive Überwachung und umfassende Dokumentation setzt. Ein flexibles, integriertes und skalierbares ITSM ist der Schlüssel, um die betriebliche Ausfallsicherheit zu gewährleisten, Risiken frühzeitig zu erkennen und im Krisenfall effizient und nachweisbar zu handeln.

# 6 Was ist ein modernes IT Service Management?

„Modern“ ist ein vielschichtiger Begriff, der Raum für Interpretationen lässt. Zahlreiche Anbieter von IT Service Management Systemen bezeichnen ihre Lösungen als modern, sobald sie KI-Funktionen und Automatisierungsoptionen integriert haben. Unsere Definition eines wirklich modernen IT Service Management geht jedoch weit darüber hinaus.

Ein modernes ITSM sollte folgende Kriterien erfüllen:

- **Regulatorische Konformität:** Abdeckung aller relevanten Anforderungen wie DORA, NIS-2, BAIT, MaRisk und Datenschutzrichtlinien.
- **Agile Arbeitsweisen:** Unterstützung von Methoden wie Scrum oder Kanban zur schnellen Anpassung an veränderte Geschäftsanforderungen.
- **Integrierte Werkzeuge und Prozesse:** Berücksichtigung aller angrenzenden Systeme und Prozesse, um eine nahtlose End-to-End-Leistungserbringung zu ermöglichen.
- **Risikoorientierung:** Integration von Risikomanagement-Ansätzen, um IT-Risiken proaktiv zu identifizieren und zu managen.
- **Enterprise Service Management (ESM):** Ausweitung der ITSM-Prozesse auf andere Unternehmensbereiche wie HR, Facility Management oder Einkauf.
- **Umsetzung der IT- und Digital Operational Resilience (DOR)-Strategie:** Unterstützung der strategischen Unternehmensziele durch konsistente und belastbare IT-Prozesse.
- **IT Service Continuity Management (ITSCM):** Systematischer Ansatz, um die kontinuierliche Verfügbarkeit von IT-Diensten sicherzustellen und die Auswirkungen von Störungen auf die Geschäftsprozesse zu minimieren.
- **Datenschutz und IT-Sicherheit:** Vollständige Erfüllung der Datenschutzanforderungen und Schutz aller sensiblen Daten.
- **Nachhaltigkeit („Green IT“) in der Praxis:** Einsatz ressourcenschonender Technologien und Maßnahmen für einen nachhaltigen IT-Betrieb.
- **Einsatz neuster Technologien, Automatisierung und KI:** Für eine anwenderfreundliche und effiziente Bedienung und für einen nachhaltigen, risikoorientierten Betrieb.
- **Anwenderfreundlichkeit:** Intuitive Bedienung und hohe Akzeptanz bei den Anwendern.
- **Effektives Lieferantenmanagement:** Transparente Steuerung und Überwachung der Zusammenarbeit mit Service Providern.

## Technologie als Werkzeug, Strategie als Schlüssel

Der Einsatz von KI und ein hoher Automatisierungsgrad sind zweifelsfrei Kernelemente, aber ein modernes ITSM geht noch einen Schritt weiter. Es setzt auf eine enge Verzahnung von Technologien, Prozessen und Governance-Strukturen, um langfristig Mehrwert zu schaffen.

IT-Service-Management leicht gemacht: Ihr Leitfaden für effektive IT-Services →

## 6.1 Hoher Automatisierungsgrad im IT Service Management: Effizienzsteigerung und Schutz vor menschlichen Fehlern

Automatisierte Prozesse reduzieren das Risiko von Fehlkonfigurationen und Datenlöschungen, steigern die Effizienz und fördern die Compliance. Sie stellen korrekte und zeitnahe Datenberichte sicher, ermöglichen schnellere Reaktionen auf Sicherheitsvorfälle und unterstützen datenbasierte Entscheidungen durch die Analyse von Prozessdaten. So können Unternehmen die Effizienz ihrer IT-Prozesse steigern, die Sicherheit erhöhen und DORA-konform handeln.

Beispiele für den sinnvollen Einsatz von Automatisierung auch in Ihrem IT-Betrieb:

- **Provisionierung von IT-Ressourcen**
  Die Automatisierung der Bereitstellung von IT-Ressourcen wie Servern, Speicherplatz und Netzwerkressourcen kann die Bereitstellungszeit erheblich verkürzen und manuelle Fehler reduzieren. Automatisierungstools ermöglichen eine schnelle und konsistente Bereitstellung, was zur Effizienzsteigerung und Kostensenkung beiträgt.
- **Softwarebereitstellung**
  Die automatisierte Installation und Konfiguration von Software beschleunigt die Bereitstellung neuer Anwendungen und gewährleistet die Konsistenz von Softwareumgebungen. Mit Hilfe von Automatisierungswerkzeugen können Unternehmen sicherstellen, dass Software-Updates und Patches rechtzeitig und korrekt installiert werden.
- **IT-Monitoring und Alerting**
  Automatisierte Monitoring- und Alerting-Tools überwachen IT-Systeme kontinuierlich und melden auftretende Probleme direkt an die Administratoren. Dadurch können Probleme schnell erkannt und behoben werden, was die Verfügbarkeit und Zuverlässigkeit der IT-Services erhöhen.
- **Sicherheits-Patching und Updates**
  Das automatische Anwenden von Sicherheits-Patches und -Updates schützt IT-Systeme vor bekannten Sicherheitslücken. Automatisierte Prozesse sorgen dafür, dass Patches regelmäßig und zeitnah eingespielt werden und erhöhen damit das Sicherheitsniveau der IT-Infrastruktur.
- **Datensicherung und -wiederherstellung**
  Automatisierte Datensicherungs- und Wiederherstellungsprozesse bieten Schutz vor Datenverlust. Durch regelmäßige, automatisierte Backups können Unternehmen die Verfügbarkeit wichtiger Daten und deren schnelle Wiederherstellung nach einem Ausfall absichern.
- **Problemmeldung per E-Mail**
  Automatisierungstools können eingehende E-Mails analysieren und auf Basis der gemeldeten Probleme automatisch IT-Tickets erstellen. Das spart Zeit und stellt sicher, dass Probleme schnellstmöglich bearbeitet werden.

- **Ereignisgesteuerte Ticket-Erstellung**
  Durch die Überwachung von IT-Systemen und die automatische Erstellung von IT-Tickets bei bestimmten Ereignissen können Unternehmen proaktiv auf Probleme reagieren. Dies verhindert die Eskalation von Problemen und trägt zur Stabilität der IT-Systeme bei.
- **Self-Service-Portal**
  Ein Self-Service-Portal ermöglicht es den Mitarbeitenden, IT-Probleme selbst zu melden, Standardanfragen zu platzieren und den Status ihrer Tickets zu verfolgen. Das reduziert den Bedarf an manueller Unterstützung durch den IT-Helpdesk, erhöht die Effizienz des IT-Supports, reduziert menschliche Fehler in der Umsetzung und schafft maximale Transparenz über Aktionen, die Assets betreffen.
- **Automatische Ticket-Eskalation**
  Tickets mit hoher Priorität oder langer Bearbeitungszeit können automatisch eskaliert werden, um sicherzustellen, dass sie schnellstmöglich gelöst werden. Das Ergebnis ist eine Verbesserung der Reaktionszeit bei kritischen Störungen und eine Minimierung von deren Auswirkungen.
- **Automatisierte Benachrichtigungen**
  Automatisierte Benachrichtigungen informieren Anwender und IT-Mitarbeitende per E-Mail, SMS oder Chatbot über wichtige Ereignisse im Zusammenhang mit IT-Tickets. Damit wird die Transparenz erhöht. Gleichzeitig können sich alle Beteiligten kontinuierlich über den aktuellen Stand des Tickets informieren.
- **Automatisierte Berichte und Analysen**
  Automatisierungstools können Berichte und Analysen über die Leistung des IT-Supports generieren. Diese Berichte helfen, Verbesserungspotenziale zu identifizieren und die Effizienz der IT-Prozesse zu steigern.
- **Automatische Zuweisung von Tickets**
  IT-Tickets können automatisch den zuständigen Mitarbeitenden oder Teams zugewiesen werden, basierend auf der Art des Problems, der Priorität und anderen Kriterien. So können Probleme schnell von den richtigen Experten bearbeitet werden.
- **Automatische Updates**
  Die Benutzer können den Status ihrer Tickets in Echtzeit über ein Benutzerhilfe-Portal verfolgen. Automatische Updates informieren zusätzlich über den Bearbeitungsfortschritt und halten alle Beteiligten auf dem neuesten Stand.
- **Integration von Wissensdatenbanken**
  Durch die Integration von Wissensdatenbanken in das User Help Portal können Benutzer auf Lösungen für häufig auftretende Probleme zugreifen. Der Bedarf an IT-Support wird reduziert und die Problemlösung beschleunigt.

Durch die Erhöhung des Automatisierungsgrades können Unternehmen die Effizienz ihrer IT-Prozesse steigern, die Sicherheit erhöhen und die Compliance mit DORA sicherstellen. Automatisierte Prozesse ermöglichen es, Routineaufgaben zu reduzieren und sich auf wertschöpfende Tätigkeiten zu konzentrieren, was letztlich zu einer Verbesserung der gesamten IT-Infrastruktur beiträgt.

## 6.2 AIOps – Die Zukunft des modernen IT-Betriebs

AIOps (Artificial Intelligence for IT Operations) ist eine fortschrittliche Technologie, die auf den Einsatz von künstlicher Intelligenz (KI) und maschinellem Lernen (ML) zur Automatisierung und Optimierung der Verwaltung und Überwachung komplexer IT-Infrastrukturen spezialisiert ist. Dabei handelt es sich nicht um ein einzelnes Tool, sondern um ein integriertes System, das verschiedene Technologien miteinander kombiniert. Auf diese Weise werden datengestützte Entscheidungen ermöglicht, der menschliche Arbeitsaufwand reduziert und ein proaktiver IT-Betrieb sichergestellt.

## 6.2.1 Wie AIOps den IT-Betrieb unterstützt

Herkömmliche IT-Betriebsmodelle stoßen bei der Verarbeitung und Analyse großer Datenmengen häufig an ihre Grenzen. Hier setzt AIOps an, indem es durch den Einsatz von Big Data, Predictive Analytics und Natural Language Processing (NLP) eine Vielzahl von IT-Daten in Echtzeit analysiert und daraus Erkenntnisse ableitet. Dadurch können Unternehmen Ausfälle vorhersagen, Fehlermuster erkennen und Wartungsmaßnahmen proaktiv steuern.

Im Wesentlichen bietet AIOps folgende Vorteile:

- **Reduktion menschlicher Aufwände**
  Manuelle Tätigkeiten wie das Durchsuchen von Log-Dateien oder die manuelle Analyse von Vorfällen werden durch Automatisierung ersetzt. Dadurch bleibt den IT-Teams mehr Zeit für strategische Aufgaben.
- **Früherkennung von Anomalien**
  Mit Hilfe der Anomalieerkennung können potenzielle Probleme identifiziert werden, bevor sie zu Ausfällen führen. Das Ergebnis ist die Minimierung von Ausfallzeiten und die Verbesserung der Verfügbarkeit von Diensten.
- **Vorhersage von Ausfällen und Engpässen**
  AIOps nutzt Prognosemodelle, um Trends zu analysieren und zukünftige Probleme wie Kapazitätsengpässe oder Systemausfälle vorherzusagen.
- **Korrelationsanalyse**
  Die Verknüpfung und Analyse von Ereignissen und Systemmeldungen aus unterschiedlichen Quellen hilft, Root-Cause-Analysen schneller durchzuführen und komplexe Zusammenhänge innerhalb der IT-Infrastruktur besser zu verstehen.
- **Automatisierte Entscheidungsfindung**
  Durch den Einsatz von NLP-Technologie und KI-Modellen kann AIOps bei wiederkehrenden Ereignissen automatisch geeignete Lösungsmaßnahmen vorschlagen oder umsetzen.

## 6.2.2 AIOps als Schlüsseltechnologie zur Umsetzung von DORA

Im Rahmen der Umsetzung des Digital Operational Resilience Act ist AIOps ein wertvolles Werkzeug, um die strengen Anforderungen an Resilienz und Compliance zu erfüllen. Mit seiner Fähigkeit, große Datenmengen zu verarbeiten und komplexe Risikobewertungen durchzuführen, unterstützt AIOps Unternehmen im Finanzsektor dabei, ihre IT-Infrastruktur widerstandsfähiger zu machen und den Anforderungen eines stark regulierten Umfelds gerecht zu werden.

## 6.3 ITIL v3 vs ITIL v4: Ist ein Upgrade auf v4 nötig mit Blick auf DORA?

Mit dem Inkrafttreten des Digital Operational Resilience Act stehen viele Finanzunternehmen vor der Frage, ob ihre bestehenden ITIL v3-Prozesse noch ausreichen, um die Anforderungen zu erfüllen, oder ob ein Upgrade auf ITIL v4 notwendig ist. Beide Versionen des ITIL-Frameworks bieten bewährte Best Practices für das IT-Service-Management, jedoch weist ITIL v4 einige wesentliche Unterschiede auf, die im Kontext von DORA besonders relevant sein können.

Ein signifikanter Unterschied zwischen ITIL v3 und v4 ist der verstärkte Fokus auf Agilität, Flexibilität und die Integration neuer Technologien in ITIL v4. DORA fordert von Finanzunternehmen eine höhere operative Belastbarkeit und die Fähigkeit, schnell auf Störungen und Bedrohungen zu reagieren. ITIL v4 unterstützt diese Anforderungen durch die Betonung agiler Methoden und eine stärkere Verknüpfung mit DevOps und Continuous Delivery (CD) Ansätzen. Im Gegensatz zu ITIL v3, das stärker prozessorientiert und auf Best Practices fokussiert ist, fördert ITIL v4 einen adaptiven Ansatz im IT Service Management und ermöglicht eine schnellere Reaktionsfähigkeit auf regulatorische und betriebliche Veränderungen. Insbesondere im Rahmen von DORA ist das von Vorteil, da Unternehmen flexibler auf neue Bedrohungen oder regulatorische Anforderungen reagieren müssen.

Darüber hinaus legt ITIL v4 einen deutlich stärkeren Fokus auf Wertschöpfung und ganzheitliches Service Management. Während sich ITIL v3 primär auf die Optimierung einzelner IT-Prozesse konzentriert, betrachtet ITIL v4 das gesamte Ökosystem der IT-Services und deren Beitrag zur Wertschöpfung im Unternehmen. Denn die Verordnung zielt neben der technischen Belastbarkeit auch auf die Art und Weise ab, wie die IT-Services kontinuierlich die betriebliche Stabilität und Sicherheit des Unternehmens sicherstellen. ITIL v4 integriert Stakeholder-orientierte Praktiken und bietet eine klarere Verbindung zwischen IT und Geschäftsanforderungen, was entscheidend für die Erfüllung der DORA-Anforderungen ist.

DORA stellt strenge Anforderungen an IT-Risikoüberwachung und -management sowie an die Schaffung robuster Governance-Strukturen. In diesem Zusammenhang bietet ITIL v4 eine erweiterte Grundlage, indem es ein klares Rahmenwerk für Governance, Risk und Compliance (GRC) bereitstellt, das Unternehmen bei der Erfüllung der DORA-Anforderungen unterstützt. Während ITIL v3 diese Themen ebenfalls adressiert, ist ITIL v4 deutlich umfassender und bietet spezifische Werkzeuge und Methoden, um Governance und Risikomanagement effizienter zu gestalten.

Die Integration neuer Technologien wie Automatisierung, künstliche Intelligenz und maschinelles Lernen, die im modernen IT Service Management zunehmend an Bedeutung gewinnen, ist ein weiterer Vorteil von ITIL v4. DORA erfordert eine proaktive Überwachung und die Automatisierung von Prozessen, um die Ausfallsicherheit der IT zu gewährleisten und Berichtsanforderungen zu erfüllen. ITIL v4 berücksichtigt diese technologischen Fortschritte und bietet Best Practices, wie Unternehmen diese Technologien in ihre ITSM-Prozesse integrieren können. ITIL v3 bietet weniger klare Richtlinien für die Integration dieser modernen Technologien und Ansätze, was die Erfüllung der DORA-Anforderungen erschwert.

Im Hinblick auf DORA wird daher ein Upgrade auf ITIL v4 empfohlen. Während ITIL v3 ein solides Fundament bietet, ist ITIL v4 besser auf die von DORA in den Vordergrund gestellten Anforderungen an Flexibilität, Governance, Technologieintegration und Wertschöpfung ausgerichtet. Unternehmen, die ITIL v4 implementieren, können ihre IT Service Management Prozesse besser an neue regulatorische und betriebliche Anforderungen anpassen und so ihre IT-Betriebsresilienz und Compliance stärken.

# 7 Anwendung des Proportionalitätsprinzips: Verhältnismäßigkeit als Chance und Herausforderung

Das Proportionalitätsprinzip ist bei der Umsetzung von Maßnahmen ein zweischneidiges Schwert: Einerseits bietet es Flexibilität, um Maßnahmen effizient auf das spezifische Risikoprofil eines Unternehmens zuzuschneiden, andererseits stellt es auch eine Herausforderung dar. Ziel ist es, die Maßnahmen so zu gestalten, dass sie den individuellen Bedürfnissen (angelehnt an das Risikoprofil) der Bank, Versicherung oder des Finanzdienstleisters entsprechen und gleichzeitig die regulatorischen Anforderungen erfüllen. Die Kunst besteht darin, eine Balance zwischen Wirtschaftlichkeit, Kosteneffizienz und Effektivität zu finden.

Dabei gibt es zentrale Themenfelder, die unabhängig von der Unternehmensgröße zu berücksichtigen sind. Die konkrete Ausgestaltung der Maßnahmen hängt jedoch stark von den Grundsätzen der Proportionalität ab. Ein kleineres Finanzinstitut wird andere Ressourcen und Prioritäten setzen als eine global agierende Bank. Entscheidend ist daher, das Proportionalitätsprinzip nicht als starre Vorgabe, sondern als Leitfaden für eine sinnvolle Priorisierung von Maßnahmen zu nutzen.

## 7.1 Leitfragen für die Anwendung des Proportionalitätsprinzips

Bei der Beurteilung, wie das Proportionalitätsgebot auf die eigenen Geschäftsaktivitäten anzuwenden ist, müssen Finanzdienstleister eine Vielzahl von Faktoren berücksichtigen. Diese Faktoren sind eng miteinander verknüpft und müssen in ihrer Gesamtheit betrachtet werden, um eine angemessene und verhältnismäßige Umsetzung zu gewährleisten.

- ☐ **Unternehmensbezogene Faktoren**
- ☐ **Risikobezogene Faktoren**
- ☐ **Rechtsrahmen und regulatorische Anforderungen**
- ☐ **Branchenstandards und Best Practices**
- ☐ **Kundenanforderungen und Erwartungen**
- ☐ **Kosten-Nutzen-Abwägung**

**Unternehmensbezogene Faktoren**

- **Größe und Komplexität des Unternehmens:** Größere und komplexere Institute unterliegen in der Regel höheren Anforderungen.
- **Geschäftsmodell und angebotene Dienstleistungen:** Die Art der angebotenen Dienstleistungen und die damit verbundenen Risiken beeinflussen die Anforderungen an die digitale operative Resilienz.
- **Risikoprofil:** Das individuelle Risikoprofil des Unternehmens, einschließlich der Art, der Häufigkeit und der Schwere potenzieller Risiken, ist ein entscheidender Faktor.
- **IT-Infrastruktur:** Die Komplexität und die Reife der IT-Infrastruktur bestimmen den Umfang der erforderlichen Maßnahmen.
- **Auslagerung von IT-Dienstleistungen:** Der Grad der Auslagerung von IT-Dienstleistungen an externe Dienstleister beeinflusst die Anforderungen an die Überwachung und Steuerung dieser Dienstleister.

**Risikobezogene Faktoren**

- **Art und Schwere potenzieller Risiken:** Es ist zu unterscheiden zwischen allgemeinen Risiken (z. B. Cyberangriffe) und spezifischen Risiken (z. B. Ausfälle von kritischen Systemen).
- **Eintrittswahrscheinlichkeit:** Die Wahrscheinlichkeit des Eintretens eines Risikos beeinflusst die Priorität der Maßnahmen.
- **Auswirkungen eines Risikos:** Die potenziellen Auswirkungen eines Risikos auf die Geschäftstätigkeit und die Kunden bestimmen den Umfang der erforderlichen Maßnahmen.

**Rechtsrahmen und regulatorische Anforderungen**

- **DORA:** Die konkreten Anforderungen des Digital Operational Resilience Act müssen berücksichtigt werden.
- **Weitere relevante Gesetze und Vorschriften:** Neben DORA sind auch andere Gesetze und Vorschriften relevant, z. B. die Datenschutz-Grundverordnung (DSGVO).
- **Nationale und internationale Standards:** Internationale Standards wie ISO 27001 können als Orientierung dienen.

**Branchenstandards und Best Practices**

- **Branchenübliche Verfahren:** Die in der Branche üblichen Verfahren und Best Practices können als Orientierung dienen.
- **Erfahrungen anderer Unternehmen:** Der Austausch mit anderen Unternehmen kann wertvolle Erkenntnisse liefern.

**Kundenanforderungen und Erwartungen**

- **Kundenerwartungen:** Die Erwartungen der Kunden an die Sicherheit und Verfügbarkeit von digitalen Dienstleistungen müssen berücksichtigt werden.
- **Regulierungsbehörden:** Die Erwartungen der Regulierungsbehörden an die Transparenz und Rechenschaftspflicht der Unternehmen müssen erfüllt werden.

**Kosten-Nutzen-Abwägung**

- **Kosten der Umsetzung:** Die Kosten für die Umsetzung der Maßnahmen müssen gegen den Nutzen abgewogen werden.
- **Risikotoleranz:** Die Risikotoleranz des Unternehmens beeinflusst die Höhe der Investitionen in die digitale operative Resilienz.

Die Beantwortung dieser Fragen hilft Ihnen, Ihre Handlungsfelder klar zu definieren und sicherzustellen, dass die getroffenen Maßnahmen nicht nur regulatorisch konform, sondern auch optimal auf Ihre organisatorischen Gegebenheiten abgestimmt sind. Proportionalität bedeutet nicht, überall maximale Maßnahmen umzusetzen, sondern gezielt in die Bereiche zu investieren, die den größten Mehrwert für die Sicherheit und Stabilität Ihres Unternehmens bieten. Nutzen Sie das Prinzip der Proportionalität als Chance, Ihre IT-Ressourcen sinnvoll einzusetzen und gleichzeitig Ihre digitale Resilienz strategisch zu stärken.

# 8 ITSM – Prozessreifegrad-Check

Ein Prozessreifegradcheck ist eine systematische Bewertung zur Feststellung des aktuellen Zustands eines Prozesses im Unternehmen. Dabei wird der Prozess anhand definierter Kriterien und Standards auf seine Effizienz, Effektivität und Übereinstimmung mit den Unternehmenszielen und regulatorischen Anforderungen untersucht.

## 8.1 Unsere 8 Punkte-Checkliste für Ihren Prozessreifegrad-Check

- ☐ **1. Definition und Dokumentation**
- ☐ **2. Risikoorientierung in den Prozessschritten**
- ☐ **3. Verantwortlichkeiten**
- ☐ **4. Standardisierung und Automatisierung**
- ☐ **5. Integration**
- ☐ **6. Messbarkeit und Kontrolle**
- ☐ **7. Verbesserung**
- ☐ **8. Konformität**

**1. Definition und Dokumentation:**
Ist der Prozess, einschließlich Scope, Ziel und Owner eindeutig definiert?

- Scope-Definition: Welchen Umfang fasst der Prozess (organisatorisch, funktional, fachlich, strukturell)?
- Zielformulierung: Was ist das angestrebte Endergebnis des Prozesses? Wozu dient der Prozess?
- Prozessowner: Wer (Rolle und Name) ist für den Prozess, seine Dokumentation und die Überwachung der Prozessschritte und -ergebnisse verantwortlich?
- Sind Prozess, Rollenbeschreibungen, Prozessschritte und Arbeitsanweisungen strukturiert dokumentiert und wird diese Dokumentation regelmäßig überprüft?
- Finden regelmäßige Mitarbeiterschulungen und Awareness-Programme statt?
- Ist der Prozess kategorisiert? Eine Unterscheidung in Kernprozesse, Unterstützungsprozesse, Managementprozesse ist eine hilfreiche Einteilung.

**Kernprozesse**: Diese Prozesse sind direkt an der Wertschöpfung beteiligt und tragen unmittelbar zum Unternehmenserfolg bei. Sie bilden den Kern des Unternehmens und umfassen beispielsweise die Produktion, den Vertrieb oder die Erbringung von Dienstleistungen.

**Unterstützungsprozesse**: Sie dienen der Unterstützung der Kernprozesse und stellen deren reibungslosen Ablauf sicher. Dazu gehören zum Beispiel Personal, Finanzen, IT oder Einkauf.

**Managementprozesse**: Hierunter fallen Prozesse zur Steuerung und Überwachung des gesamten Unternehmens. Dazu gehören strategische Planung, Budgetierung, Qualitätsmanagement und vieles mehr.

**2. Risikoorientierung in den Prozessschritten:**

Spiegeln die einzelnen Prozessschritte das erforderliche Risikobewusstsein wieder?

- Was ist die jeweils definierte Voraussetzung für das Auslösen jedes Prozessschrittes?
- Was ist die Aktivität und der Inhalt jedes Prozessschrittes?
- Was ist das Ziel jedes Prozessschrittes?
- Berücksichtigen die Prozessschritte das Risikoprofil des Unternehmens?
- Berücksichtigt der Prozess die Klassifizierung kritischer und wichtiger Funktionen, die durch den Prozess behandelt werden?
- Wird in den Freigabe-/Genehmigungsstufen eine Risikoeinschätzung verlangt?
- Erfordern Freigaben ein Vier-Augen-Prinzip?
- Wird bei der Bearbeitung auf die betroffenen und involvierten Assets Bezug genommen?

**3. Verantwortlichkeiten:**

Ist für jeden Prozessschritt klar ersichtlich, wer was zu tun hat?

- Gibt es einheitliche Rollenbeschreibungen, in denen Aktivitäten, Verantwortlichkeiten und Kompetenzen aufgeführt sind?
- Ist das Rollenmodell im Tooling hinterlegt?
- Welche Rollen sind an den einzelnen Prozessschritten beteiligt?
- Gibt es eine nachvollziehbare Übersicht, welcher Mitarbeiter zu welchem Zeitpunkt welche Rolle innehatte?
- Wurde das RACI-Modell verwendet und Aufgaben, Kompetenzen und Verantwortlichkeiten in einer Matrix definiert?

**4. Standardisierung und Automatisierung:**

Folgt der Prozess einem gängigen Vorgehensmodell?

- Auf welchem Vorgehensmodell basiert der Prozess?
- Wie stark ist die Abweichung von den veröffentlichen Best Practices?
- Gibt es eine einheitliche, prozessübergreifende Definition von Fachbegriffen und ein Glossar?
- Wie nah am operativen Geschäft sind die Arbeitsanweisungen geschrieben und wo sind sie abgelegt?
- Gibt es eine Automatisierungsrichtlinie, die Leitplanken zur Automatisierung festlegt?
- Welche Arbeitsschritte sind automatisiert? Wurde der Prozess aufgrund der Automatisierung verändert oder manuelle Schritte in automatische Übergänge umgewandelt?
- Wie hoch ist der Automatisierungsgrad?
- Wie gut wird die Benutzerfreundlichkeit durch die Automatisierung unterstützt?
- Gewährleistet die Automatisierung die Datenqualität?
- Sichert die Automatisierung die Einhaltung regulatorischer Anforderungen?

**5. Integration:**
Wie ist der Prozess in andere Prozesse integriert?

- Gibt es eine klare Scope-Abgrenzung der involvierten Prozesse und keine fachlichen Überschneidungen?
- Sind die Übergänge zwischen den Prozessen eindeutig geregelt?
- Ist der Informationsfluss zwischen den Prozessen klar geregelt?
- Stimmen die Rollenbeschreibungen beider Prozesse überein und sind die Verantwortlichkeiten aufeinander abgestimmt?
- Findet eine Verankerung zwischen Vorfallerkennung und Meldewesen statt?
- Ist das Asset Management ausreichend in die Prozesse integriert?
- Ist das Risiko Management stark genug in die Prozesse integriert?

**6.Messbarkeit und Kontrolle:**
Findet eine systematische und datenbasierte Überwachung der Prozesseinhaltung und -qualität statt?

- Welche relevanten Kennzahlen (KPIs) sind definiert?
- Werden Kennzahlen systematisch erfasst und überwacht?
- Sind diese Messgrößen SMART (Specific Measurable Achievable Reasonable Time-Bound) definiert?
- Gibt es Kontrollmechanismen zur Qualitätssicherung?

**7. Verbesserung:**
Werden kontinuierliche Prozessverbesserungen angestrebt?

- Ist der Qualitätsmanagementprozess im Prozessmanagement verankert?
- Ist der kontinuierliche Verbesserungsprozess in die operativen Abläufe integriert und/oder zentral gemanagt?
- Gibt es einen Prozess, der die definierten Kennzahlen regelmäßig überprüft, Maßnahmen ableitet und diese überwacht?
- Gibt es einen Prozess, der den Ablauf regelmäßig auf Einhaltung überprüft, Maßnahmen ableitet und diese überwacht?
- Wie umfangreich ist die Berichterstattung über das Qualitätsmanagement der Prozesse?

**8. Konformität:**
Entspricht der Prozess den gesetzlichen und regulatorischen Anforderungen?

- Ist das erforderliche Risikobewusstsein in den Prozessen verankert?
- Sind die notwendigen Elemente des strukturierten Risikomanagements, des Testprogramms und Meldewesens in den Prozessen verankert?
- Ist das interne Kontrollsystem in den Prozessen verankert?
- Gibt es ein Mapping der regulatorischen Anforderungen auf die Prozesselemente?
- Sind die Prozesse ausreichend formuliert und dokumentiert, so dass sie den notwendigen Rahmen für die Steuerung des Dienstleisters bilden?

## 8.2 Exkurs: Welche Modelle werden häufig eingesetzt?

- **Capability Maturity Model Integration (CMMI):**
  Ein weit verbreitetes Modell zur Bewertung der Reife von Prozessen in der Softwareentwicklung und anderen Bereichen.
- **ITIL (Information Technology Infrastructure Library):**
  Ein Rahmenwerk für IT Service Management, das standardisierte Richtlinien und Best Practices zur Orientierung bietet.
- **ISO 9001:**
  Eine internationale Norm für Qualitätsmanagementsysteme, die Anforderungen an Prozesse stellt.
- **Prozess Audit:**
  Michael Hammer, 2007 -> https://hbr.org/resources/pdfs/hbr-articles/2007/04/hammer-assessing-worksheet.pdf
- **Gartner:**
  Das 6-Phasen Business Process Maturity Modell
- **ISO/IEC 15504-5 oder SPICE**
  **(Software Process Improvement and Capability Determination):**
  Internationale ISO-Norm, ursprünglich mit Schwerpunkt Softwareentwicklung, zur Durchführung von Assessments (Bewertungen) von Geschäftsprozessen.
- **BOOTSTRAP-Projekt:**
  Das Projekt wurde von der Europäischen Kommission ins Leben gerufen, um eine fortschrittliche Methode zur Prozessbewertung zu entwickeln.

## 8.3 Stufenmodell basierend auf CMMI

### Reifegrad 5 (Optimizing)

Die Organisation ist bestrebt, ihre Prozesse kontinuierlich zu verbessern und zu innovieren. Es gibt eine Kultur der Verbesserung und des Lernens.

### Reifegrad 4 (Quantitativ Managed)

Prozesse werden quantitativ gemessen und kontrolliert. Die Organisation kann die Leistung ihrer Prozesse besser vorhersagen und steuern.

### Reifegrad 3 (Defined)

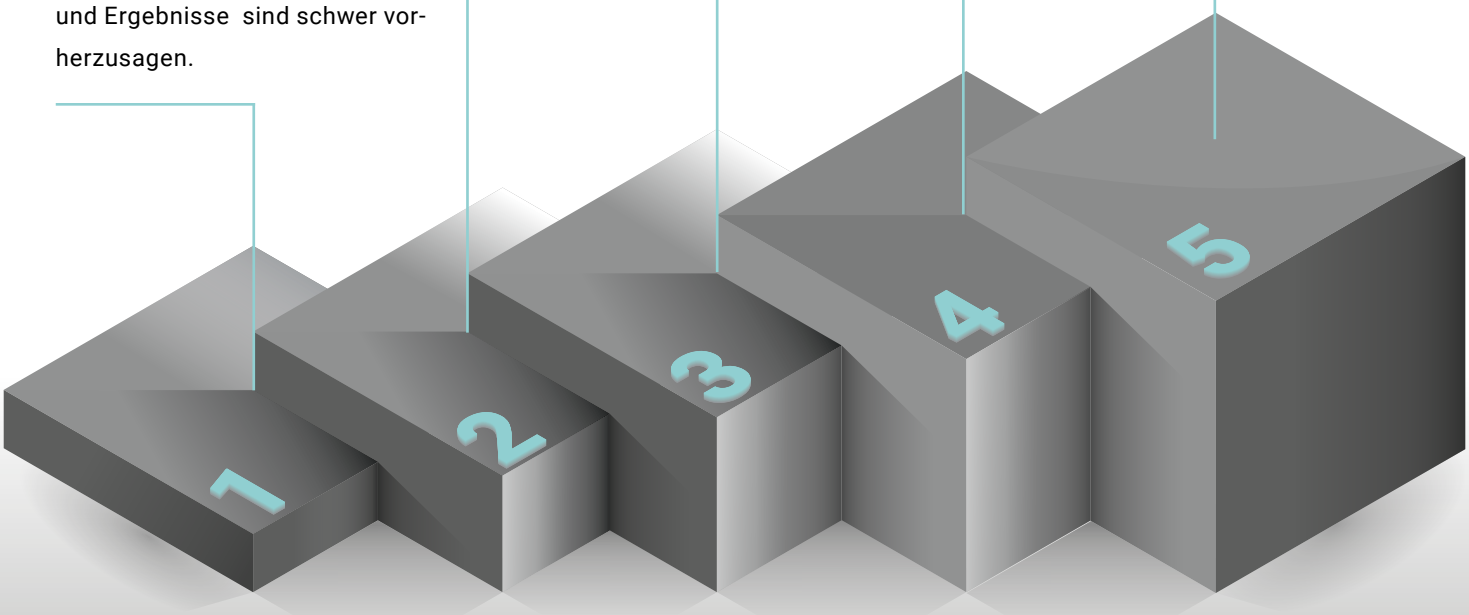
Prozesse sind standardisiert und dokumentiert. Die Organisation hat eine klare Vorstellung davon, wie Prozesse ablaufen sollen.

### Reifegrad 2 (Managed)

Grundlegende Prozesse werden eingeführt und verwaltet. Projekte werden geplant und verfolgt, um eine gewisse Kontrolle zu gewährleisten.

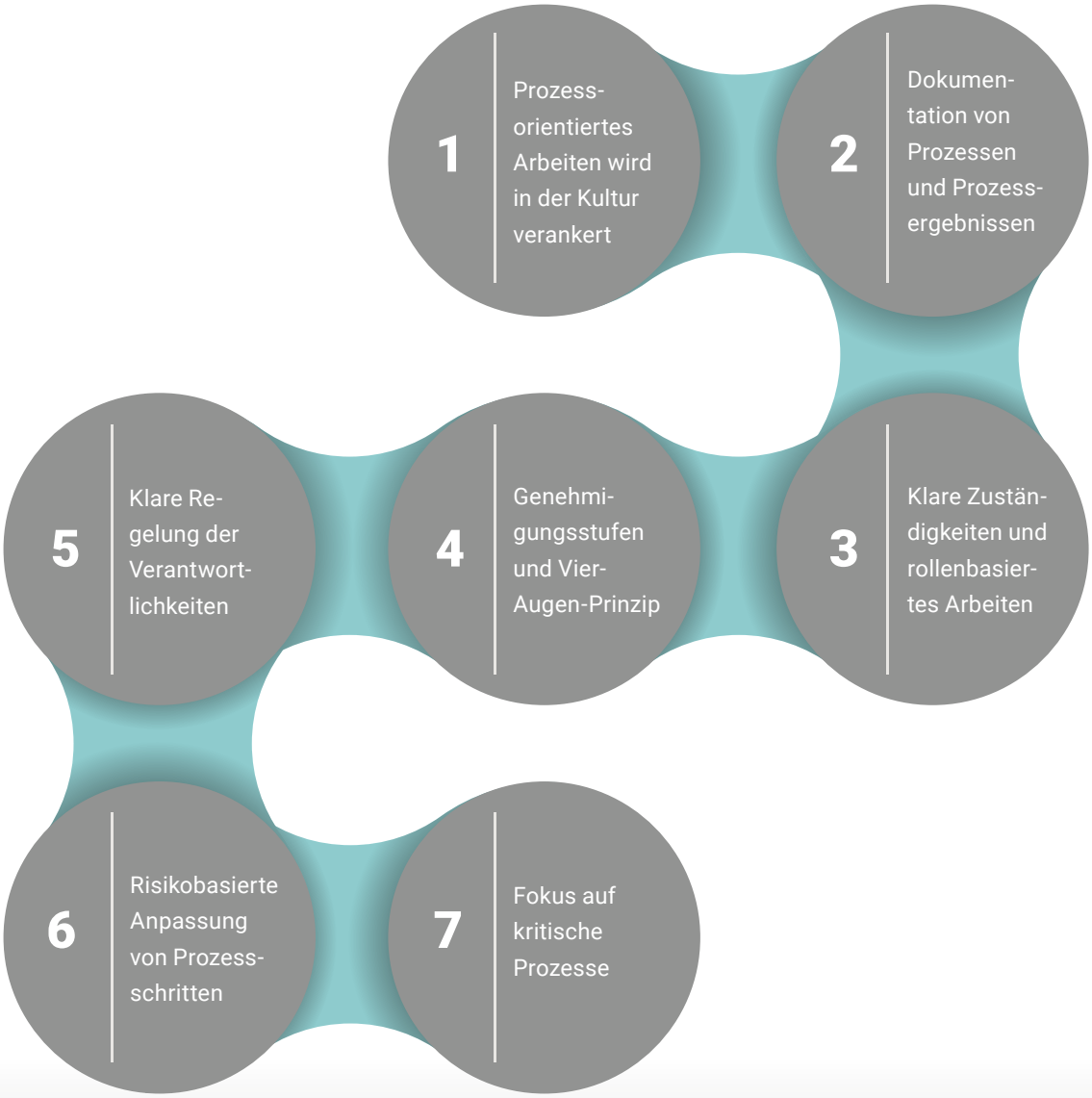
### Reifegrad 1 (Initial)

Die Organisation befindet sich am Anfang der Prozessverbesserung. Prozesse sind oft unstrukturiert und Ergebnisse sind schwer vorherzusagen.



# 9 Umsetzungsleitfaden zur Erhöhung des IT-Prozessreifegrads

DORA legt großen Wert auf die Fähigkeit von Finanzinstituten, ihre IT-Prozesse widerstandsfähig und effizient zu gestalten, um Risiken zu minimieren und die Kontinuität des Geschäftsbetriebs zu gewährleisten. Die Erhöhung der IT-Prozessreife spielt eine Schlüsselrolle bei der Erfüllung der DORA-Anforderungen, da sie dazu beiträgt, Prozesse zu standardisieren, Verantwortlichkeiten klar zu definieren und die gesamte IT-Infrastruktur zu optimieren. Im Folgenden werden die wesentlichen Aspekte zur Erhöhung der IT-Prozessreife erläutert.



## 9.1 Prozessorientiertes Arbeiten wird in der Kultur verankert

Eine prozessorientierte Unternehmenskultur unterstützt die Kommunikation intern und mit externen Partnern. Das Denken in Rollen, klare Zuständigkeiten und geregelte Verantwortungsübergänge sind wesentliche Elemente für eine reibungslose Zusammenarbeit. Die grundsätzlich konsequente Einhaltung von Prozessen erleichtert den Umgang mit Auffälligkeiten bei Audits und die Optimierung von Prozessen und Abläufen. Bei Prozessoptimierungen sollten alle Stakeholder sowie Dienstleister proaktiv eingebunden werden, um alle Dimensionen des Optimierungspotenzials auszuschöpfen.

## 9.2 Dokumentation von Prozessen und Prozessergebnissen

Eine umfassende und verständliche Prozessdokumentation im IT-Prozessmanagement hilft nicht nur, den Prozessablauf zu verstehen und zu optimieren, sondern dient auch als Grundlage für Schulungen und Kommunikation. Eine gute Dokumentation ist zudem wichtig für die Auditierbarkeit und die Einhaltung von Compliance-Anforderungen. Die Dokumentation kann als Nachweis für die Einhaltung der DORA-Anforderungen dienen, insbesondere im Hinblick auf das Risikomanagement und die Zusammenarbeit mit externen IKT-Dienstleistern. Eine vollständige und genaue Dokumentation der einzelnen Prozessschritte ist eine wesentliche Voraussetzung für die Durchführung von Audits und Kontrollen. Sie trägt zu einer erhöhten Transparenz der Prozesse bei und ermöglicht das Erkennen von Schwachstellen und Verbesserungspotenzialen.

Auch bei der Fehlerursachenanalyse und -vermeidung spielt die Dokumentation eine zentrale Rolle. Sie erleichtert die Identifikation von Fehlerursachen im Prozess und kann als Grundlage für die Entwicklung von Prozessverbesserungen dienen. Eine gute Dokumentation trägt dazu bei, dass sich Fehler nicht wiederholen. Darüber hinaus unterstützt sie den Prozessablauf, indem sie die Effizienz steigert, Missverständnisse minimiert und das Onboarding neuer Mitarbeitender erleichtert. Neue Mitarbeitende können mit Hilfe der Dokumentation den Prozess schneller und einfacher verstehen und in die Arbeit integriert werden.

## 9.3 Klare Zuständigkeiten und rollenbasiertes Arbeiten

Für eine optimale Prozessgestaltung ist eine klare Aufgabenverteilung unerlässlich. Durch die Einführung von Rollenmodellen, in denen jeder Prozessschritt einer bestimmten Rolle zugeordnet wird, schaffen wir Transparenz und Verantwortlichkeit.

Die konkrete Benennung der Rolleninhaber stellt sicher, dass jeder weiß, was von ihm erwartet wird und wer im Bedarfsfall als Ansprechpartner zur Verfügung steht. Diese klare Struktur minimiert Fehlerquellen und erhöht die Effizienz unserer Arbeitsabläufe.

## 9.4 Genehmigungsstufen und Vier-Augen-Prinzip

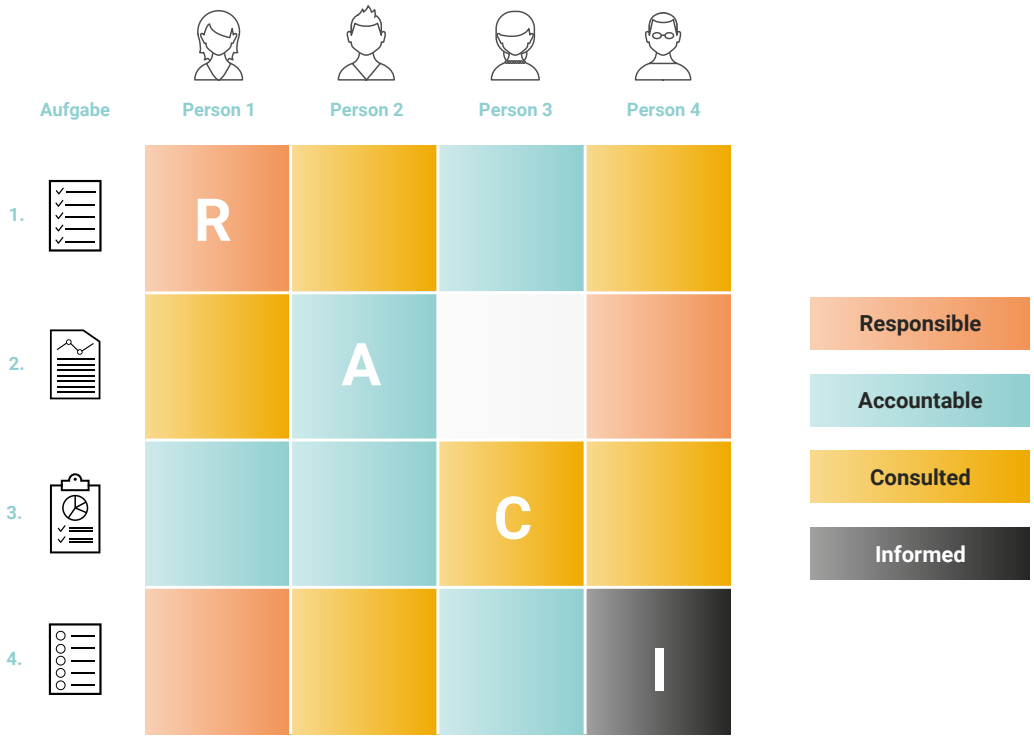
Freigabestufen und das Vier-Augen-Prinzip tragen entscheidend zur Sicherheit und Integrität der IT-Prozesse bei. Durch klar definierte Freigaberichtlinien wird sichergestellt, dass wichtige Entscheidungen nicht von Einzelpersonen, sondern von zwei verschiedenen Personen mit den notwendigen Kompetenzen getroffen werden. Diese Richtlinien sollten auch im ITSM-Tool als Voraussetzung dokumentiert werden, was die Sicherheit erhöht, die Kontrolle verbessert und Transparenz schafft.

Die im ITSM-System dokumentierten Genehmigungsschritte gewinnen insbesondere durch den DORA-Ansatz an Bedeutung, da sie sicherstellen, dass Änderungen an IT-Systemen und deren Konfigurationen nur nach sorgfältiger Prüfung und Auswirkungsanalyse freigegeben werden. Auch wenn der Einsatz von Automatisierung auf den ersten Blick vielversprechend erscheint, kann eine automatisierte Freigabe nur auf Basis zuvor sorgfältig definierter Kriterien erfolgen.

## 9.5 Klare Regelung der Verantwortlichkeiten

Die klare Definition von Verantwortlichkeiten ist ein weiterer grundlegender Bestandteil eines professionellen ITSM. Ein klares und eindeutiges Rollenmodell, in dem die Verantwortlichkeiten, Kompetenzen und Tätigkeiten der einzelnen Rollen geregelt sind, ist Voraussetzung für die eindeutige Kenntnis und Benennung des zuständigen Ansprechpartners bzw. Verantwortlichen für jeden Prozessschritt.

Zu diesem Zweck hat sich eine RACI-Matrix bewährt, in der die Verantwortlichkeiten klar geregelt sind.




**R (Responsible)** = Ausführender eines Prozessschritts
(es muss mindestens einen, kann aber auch mehrere geben)
**A (Accountable)** = Stellt sicher, dass der Prozessschritt ausgeführt wird
(es muss und kann nur einen geben)
**C (Consulted)** = Kann beratend hinzugezogen werden
**I (Informed)** = Sollte informiert werden

### Wichtig

DORA erfordert nicht nur eine klare Aufteilung von Verantwortlichkeiten in Rollen, sondern vielmehr noch in Rollen-Inhaber, d. h. konkrete Personen, die zu einem bestimmten Zeitpunkt (z. B. wenn eine Genehmigung erteilt oder ein Change ausgerollt wurde) eine Rolle innehatten.

## 9.6 Risikobasierte Anpassung von Prozessschritten

Bei der Modernisierung der ITSM-Prozesse im Rahmen von DORA ist ein hohes Risikobewusstsein unabdingbar, um potenzielle Bedrohungen und Schwachstellen frühzeitig zu erkennen und effektiv zu managen. DORA legt großen Wert auf die Resilienz und Sicherheit der IT-Infrastruktur, um die Kontinuität der Geschäftsprozesse zu wahren.

Durch ein ausgeprägtes Risikobewusstsein können Unternehmen proaktiv Maßnahmen zur Risikominderung implementieren und die Robustheit und Ausfallsicherheit aller IT-Services erreichen. Dazu gehören die regelmäßige Bewertung und Überwachung von Risiken, die Schulung der Mitarbeiter im Umgang mit Risiken und die Integration des Risikomanagements in alle ITSM-Prozesse.

Ein hohes Risikobewusstsein trägt dazu bei, dass Änderungen und neue Implementierungen sorgfältig geprüft werden, um negative Auswirkungen auf die IT-Sicherheit und Betriebsstabilität zu vermeiden. Es fördert eine Kultur der Wachsamkeit und Verantwortung, die notwendig ist, um den hohen Anforderungen von DORA gerecht zu werden und die digitale Resilienz des Unternehmens zu stärken.

Sie möchten das Risikobewusstsein in Ihrem Unternehmen stärken?
Erfahren Sie hier, wie Sie das operativ umsetzen können.

**1. Risikobewusstsein in die Unternehmenskultur integrieren:**

- **Schulungen und Weiterbildung:** Bieten Sie Ihren Mitarbeitern regelmäßige Schulungen und Weiterbildungen zum Thema Risikomanagement an.
- **Kommunikation:** Fördern Sie eine offene Kommunikationskultur, in der Mitarbeiter ihre Bedenken und Beobachtungen zu potenziellen Risiken äußern können.
- **Vorbildfunktion des Managements:** Führungskräfte sollten durch ihr eigenes Verhalten ein Vorbild in Bezug auf Risikobewusstsein sein.

**2. Hoher Prozessreifegrad und kontinuierliche Verbesserung:**

- Implementierung von **Best Practices und Standards** wie ITIL v4 zur Standardisierung und kontinuierlich Verbesserung der ITSM Prozesse.
- Einführung eines **Reifegradmodells** zur regelmäßigen Bewertung und Weiterentwicklung der ITSM-Prozesse.
- Etablierung eines integrierten und auch zentralen **kontinuierlichen Verbesserungsprozesses** zur regelmäßigen Optimierung der Prozesse.

**3. Hohes Risikobewusstsein und Sicherheitsverständnis:**

- Implementierung eines Risikomanagementprozesses, der Risiken identifiziert, bewertet und mitigiert.
- Schulung der Mitarbeiter im Risikomanagement und Sensibilisierung für potenzielle IT-Risiken.
- Risikoabwägung in Entscheidungsfällen, die dafür sorgt, dass Freigaben eine Risikobetrachtung einbeziehen.
- Etablierung von Sicherheitsüberprüfungen und -tests zur Erkennung potenzieller Schwachstellen.

**4. Genehmigungsstufen:**

- Einführung eines **mehrstufigen Genehmigungsprozesses** für Änderungen, damit alle Änderungen gründlich geprüft und genehmigt werden.
- Automatisierung des Genehmigungsprozesses mit **Workflow-Management-Tools**, um Effizienz und Nachverfolgbarkeit zu erhöhen.
- **Dokumentation von Genehmigungen** und Entscheidungsprozessen, um Nachvollziehbarkeit zu unterstützen.

**5. Transparenz und Historisierung:**

- Implementierung von Systemen zur **lückenlosen Dokumentation** und Historisierung aller Änderungen und Vorfälle.
- **Regelmäßige Audits und Reviews** zur Erhöhung der Transparenz und Verantwortlichkeit innerhalb der ITSM-Prozesse.
- **Einsatz von Versionierungstools** und Datenbanken für eine vollständige Nachverfolgbarkeit und Historie.

**6. Automatisierung:**

- **Robotic Process Automation:** Einsatz von Automatisierungstools zur Reduzierung manueller Aufgaben und zur Verbesserung der Effizienz und Erhöhung der Sicherheit.
- **Künstliche Intelligenz:** Der Einsatz von KI kann zur automatischen Erkennung von Anomalien und zur Vorhersage von Problemen beitragen.

## 9.7 Fokus auf kritische Prozesse

Die DORA-Anforderungen zwingen Finanzinstitute zu einer gezielten Anpassung ihrer bestehenden IT Service Management Prozesse im Hinblick auf eine höhere operative Resilienz und stärkere Kontrollmechanismen.

DORA legt besonderen Wert auf die Robustheit und Stabilität von IT-Systemen, weshalb spezifische ITSM-Prozesse in Bezug auf Service Levels, Assets, Incident-, Change- und Event-Management optimiert werden müssen, um den regulatorischen Anforderungen gerecht zu werden.

### 9.7.1 Service Level Management

Im Vertrag zum Beispiel mit dem IT-Dienstleister (Service Level Agreement) sollte detailliert festgelegt werden, welche IT-Services in welchem Umfang erbracht werden und welche Service Levels zu erfüllen sind. Service Levels sind die Qualitätsanforderungen und müssen nicht nur messbar formuliert werden, sondern auch nachweislich gemessen werden.

Dazu gehören die Verfügbarkeit der Services (z. B. während der Geschäftszeiten oder 24/7), die Wiederherstellungszeit nach einem Ausfall je nach Priorität (z. B. 1 Stunde bei Priorität 1) und die maximale Reaktionszeit bei Störungen (z. B. 15 Minuten bei Priorität 1). Darüber hinaus sollten messbare Key Performance Indicators (KPIs) definiert werden, um die Leistung des Dienstleisters zu bewerten. Regelmäßige Berichte über erreichte KPIs und aufgetretene Probleme sind ebenfalls notwendig, um Transparenz und Nachvollziehbarkeit zu gewährleisten.

Die regelmäßige Überprüfung und Anpassung der Service Levels ist notwendig, um auf veränderte Anforderungen zu reagieren und die Konformität mit DORA sicherzustellen. Ein kontinuierlicher Review-Prozess trägt zur Verbesserung und Anpassung der Services bei, so dass diese stets den aktuellen regulatorischen und geschäftlichen Anforderungen entsprechen.

**Klare Definition der Services und Leistungsversprechen**
Eine klare Definition und verständliche Beschreibung der angebotenen Services ist eine Hauptaufgabe des Service Level Management (SLM). Diese Definitionen sollten den Bezug der Services zu den Geschäftsprozessen sowie deren funktionalen und technischen Umfang beinhalten. Nachvollziehbare und eindeutige Leistungsversprechen gegenüber dem Kunden sind notwendig, um Missverständnisse zu vermeiden und Erwartungen zu steuern. Darüber hinaus ermöglichen sie die Ableitung relevanter Leistungsindikatoren und erforderlicher Maßnahmen.

**Bezug zu kritischen und wichtigen Funktionen**
DORA fordert Finanzinstitute auf, ihre kritischen und wichtigen Funktionen zu identifizieren und die IKT-Leistungen, die diese Funktionen unterstützen oder ganzheitlich erbringen, sorgfältig zu verwalten. Kritische Funktionen sind solche, deren Ausfall zu erheblichen finanziellen Verlusten, Reputationsschäden oder zum Ausfall des gesamten Systems führen kann. Wichtige Funktionen haben einen erheblichen Einfluss auf den Geschäftsbetrieb, auch wenn sie nicht kritisch sind. IT-Services müssen entsprechend ihrer Kritikalität überprüft werden, um eine hohe Verfügbarkeit und strenge Service Level Agreements zu gewährleisten. Diese SLAs definieren genau die Verfügbarkeit, die Wiederherstellungszeit und die maximale Ausfallzeit und leisten damit einen wichtigen Beitrag zur operationalen betrieblichen Resilienz.

## 9.7.2 Service Asset Management

Asset Management ist mit der Einführung von DORA besonders relevant geworden, da es weit mehr als nur eine Inventarliste darstellt. Es ist ein integraler Bestandteil der IT-Resilienz und -Sicherheit. Für eine ganzheitliche Sicht auf die IT-Infrastruktur muss das Asset Management in alle IT- und Geschäftsprozesse integriert werden. Es bietet vollständige Transparenz über alle eingesetzten IT-Assets, was für die Einhaltung von DORA-Anforderungen unerlässlich ist. Durch Automatisierung können Asset-Management-Prozesse effizienter gestaltet und Fehler minimiert werden. Automatisierte Systeme helfen dabei, aktuelle Daten zu pflegen und schnell auf Änderungen zu reagieren.

Ein effektives Asset Management ermöglicht eine schnelle und präzise Impact-Analyse bei Sicherheitsvorfällen, um die betroffenen Systeme und deren Kritikalität zu identifizieren. Die Verwaltung von End-of-Life (EOL)-Daten für alle Assets stellt sicher, dass veraltete Systeme rechtzeitig ersetzt werden und kein Sicherheitsrisiko darstellen. Jedes Asset sollte einen klar definierten Owner haben, der für die Verwaltung und Sicherheit des Assets verantwortlich ist.

Zusätzlich zur Compliance, die sicherstellt, dass alle Assets den regulatorischen Anforderungen entsprechen, spielt das Sicherheitsmanagement eine zentrale Rolle im Schutz der Assets vor unbefugtem Zugriff und Bedrohungen. Regelmäßige Wartung und Support der Assets gewährleisten deren Verfügbarkeit und Leistungsfähigkeit. Durch diesen umfassenden Ansatz wird das Asset Management zu einem zentralen Element der digitalen operationalen Resilienz, das die Sicherheit und Kontinuität der IT-Services unterstützt und die Einhaltung der DORA-Anforderungen absichert.

Das IKT-Risikomanagement zielt darauf ab, alle Informationen und IKT-Assets vor Risiken, Schäden und unbefugtem Zugriff zu schützen. Dazu gehören die Identifizierung von IKT-Risiken, die Bewertung von Cyber-Bedrohungen und Schwachstellen sowie die jährliche Überprüfung von Risikoszenarien. IKT-Systeme müssen stets auf dem neuesten Stand und technologisch belastbar sein, um Spitzenbelastungen und neue Technologien bewältigen zu können. Bei wesentlichen Änderungen der Infrastruktur oder der Prozesse ist eine Risikobewertung erforderlich.

Erweiterte Anforderungen umfassen Richtlinien für das Management von IKT-Assets, einschließlich der Bewertung der Kritikalität und des Zugangsmanagements. Es gibt Sicherheitsrichtlinien für den Schutz von Daten und Vermögenswerten, einschließlich Verschlüsselung und kryptografischer Kontrollen. Business Continuity Management und IT Service Continuity Management umfassen Reaktions- und Wiederherstellungspläne.

Ein aktuelles Inventar der IKT-Assets einschließlich Lebenszyklus, Klassifizierung und Abhängigkeiten ist erforderlich. Zusätzlich muss ein Verzeichnis aller Zertifikate und Zertifikatsspeicher geführt werden. Zur Wahrung der digitalen Resilienz sind risikobasierte Testpläne, Schwachstellenbewertungen, Penetrationstests und Dienstleisteraudits erforderlich. IKT-Systeme müssen kontinuierlich überwacht und protokolliert werden, und es muss eine strikte Trennung zwischen Produktions- und Testumgebungen bestehen. Die IKT-Umgebung sollte gut strukturiert sein, mit Netzwerksegmentierung und Isolationsmöglichkeiten im Falle eines Cyber-Angriffs.

Bei der Zusammenarbeit mit IT-Providern sollten Sie künftig auf mehrere Aspekte achten, um die Prozesse zu optimieren und den Anforderungen von DORA gerecht zu werden. Fördern Sie ein gemeinsames Verständnis für die Bedeutung von IT-Sicherheit und Resilienz sowohl innerhalb Ihres Unternehmens als auch bei Ihren Dienstleistern. Verpflichten Sie Ihre Partner, Ihre eigenen Prozesse zu nutzen, oder definieren Sie klare Übergänge zwischen den Prozessen. Schaffen Sie Transparenz über die Prozesse beim Dienstleister, um eine reibungslose Zusammenarbeit zu gewährleisten. Stellen Sie sicher, dass Verantwortlichkeiten klar definiert und Übergänge zwischen verschiedenen Rollen und Aufgaben eindeutig geregelt sind. Rollenbasiertes Arbeiten hilft, Verantwortlichkeiten zu klären und die Effizienz zu steigern. Implementieren Sie mehrstufige Genehmigungsprozesse, damit alle Änderungen und wichtigen Entscheidungen gründlich geprüft und genehmigt werden. Führen Sie eine strikte Dokumentationspflicht für jeden Schritt ein, um die Nachvollziehbarkeit und Transparenz zu erhöhen. Verbessern Sie Ihr Asset Management, indem Sie ein umfassendes und aktuelles Inventar aller IT-Assets führen. Das umfasst die Klassifizierung der Assets, die Verwaltung von Lebenszyklen und die Sicherstellung der Integrität und Sicherheit der Assets. Durch die Umsetzung dieser Maßnahmen können Sie die Zusammenarbeit mit Ihren IT-Providern effizienter und sicherer gestalten, was zur Erfüllung der DORA-Anforderungen beiträgt.

### 9.7.3 Incident Management

Der Incident Management Prozess ist aus DORA-Sicht besonders wichtig, da IT-Störungen und Sicherheitsvorfälle schnell und effizient erkannt, gemeldet und behoben werden müssen. Das ist entscheidend, um die Kontinuität der Geschäftsprozesse zu gewährleisten und potenzielle Schäden zu minimieren.

DORA verlangt von Finanzinstituten eine besonders schnelle und effiziente Reaktion auf Sicherheitsvorfälle und IT-Störungen. Daher muss der Incident Management Prozess so angepasst werden, dass Vorfälle entsprechend ihrer Kritikalität priorisiert und schnell eskaliert werden. Es müssen automatisierte Systeme eingeführt werden, die Vorfälle frühzeitig erkennen und sofortige Gegenmaßnahmen einleiten, damit der Schaden so gering wie möglich gehalten wird. Ziel des Incident Managements ist die schnelle Erkennung und Bearbeitung von Vorfällen, um Ausfallzeiten zu minimieren und die Betriebsfähigkeit auch in Krisensituationen sicherzustellen.

Bei der Anpassung des Prozesses ist es wichtig, klare Meldewege und Verantwortlichkeiten zu definieren, regelmäßige Mitarbeiterschulungen durchzuführen und alle Vorfälle zu dokumentieren und zu analysieren. Darüber hinaus sollten regelmäßige Tests und Simulationen durchgeführt werden, die die Wirksamkeit des Prozesses überprüfen und diesen kontinuierlich verbessern.

### 9.7.4 Change Enablement

Change Enablement stellt einen weiteren Kernprozess von DORA dar, der Änderungen an IT-Systemen kontrolliert und ohne negative Auswirkungen auf die betriebliche Stabilität und Sicherheit umsetzt. Jede geplante Änderung muss durch einen Risikomanagementprozess bewertet werden, damit keine negativen Auswirkungen auf die Kontinuität oder Sicherheit der IT-Dienste entstehen. Ein stärker formalisiertes Change Advisory Board (CAB) kann bei der Einhaltung der DORA-Anforderungen helfen, indem es die Bewertung und Genehmigung von Änderungen strukturiert und überwacht. Auf diese Weise werden alle Änderungen sorgfältig geprüft und kontrolliert implementiert, um die betriebliche Belastbarkeit und Sicherheit der IT-Infrastruktur zu gewährleisten.

Bei der Anpassung des Prozesses ist es wichtig, klare Kriterien für die Risikobewertung festzulegen, regelmäßige Schulungen für das CAB und die beteiligten Mitarbeiter durchzuführen und die Dokumentation und Nachverfolgung aller Änderungen zu garantieren. Darüber hinaus sollten automatisierte Tools eingesetzt werden, um den Änderungsprozess zu unterstützen und die Transparenz zu erhöhen. Regelmäßige Audits und Reviews des Change Enablement Prozesses helfen, kontinuierliche Verbesserungen zu identifizieren und umzusetzen.

### 9.7.5 Event Management

Im Hinblick auf die Überwachung und Reaktion auf kritische IT-Ereignisse ist eine Stärkung des Event Management Prozesses erforderlich. Der Einsatz proaktiver Überwachungssysteme, die potenziell kritische Ereignisse automatisch erkennen und eskalieren können, bevor sie zu größeren Problemen führen, ist notwendig. Die Systeme müssen so konfiguriert sein, dass sie insbesondere bei sicherheitsrelevanten oder systemkritischen Ereignissen automatisch Alarm auslösen und entsprechende Maßnahmen einleiten. Auf diese Weise soll eine frühzeitige Erkennung und präventive Reaktion auf kritische Ereignisse ermöglicht werden, um die Stabilität der IT zu erhalten und Ausfälle zu minimieren.

## 9.7.6 IT Service Continuity Management

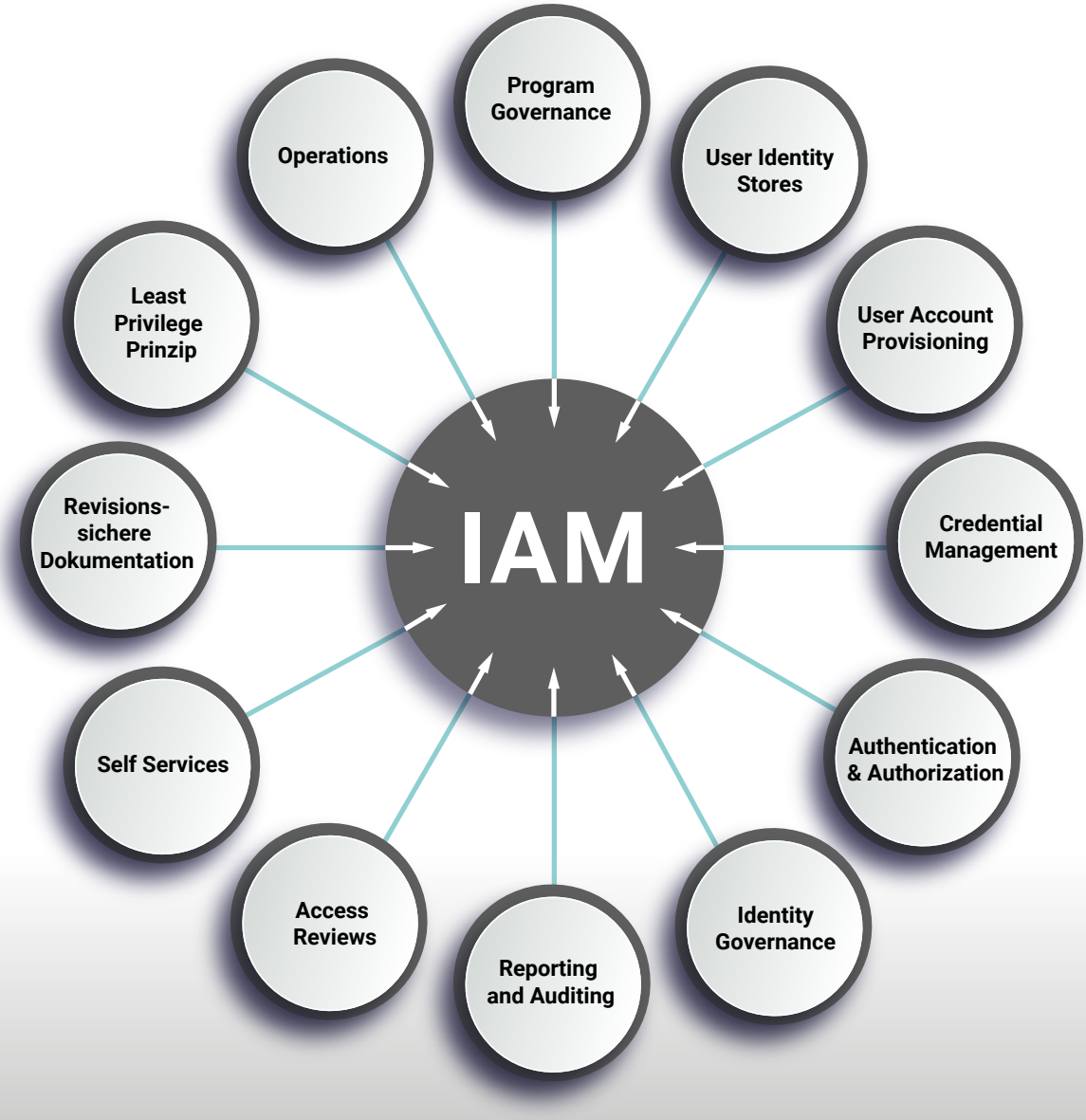
IT Service Continuity ist für DORA von besonderer Bedeutung, da es die Verfügbarkeit kritischer IT-Dienste auch im Falle von Störungen oder Krisen aufrechterhält. Das ist entscheidend für die Betriebsfähigkeit und Kontinuität der Geschäftsprozesse, was wiederum die Unternehmensresilienz stärkt. DORA legt großen Wert auf die Fähigkeit von Finanzinstituten, schnell auf IT-Störungen zu reagieren und den Betrieb ohne signifikante Unterbrechungen fortzusetzen. Ein robustes IT Service Continuity Management umfasst die Entwicklung und regelmäßige Aktualisierung von Notfall- und Wiederherstellungsplänen, die Durchführung von Business Impact Analysen (BIA) und die Implementierung von Maßnahmen zur Risikominderung. Regelmäßige Tests und Simulationen dieser Pläne stellen sicher, dass das Unternehmen auf verschiedene Szenarien vorbereitet ist und schnell reagieren kann. So können mögliche Schäden minimiert und die Kunden weiterhin zuverlässig bedient werden.

# 10 Tooling: DORA-Konformität beim Einsatz moderner Werkzeuge

Neben angepassten Prozessen und Strategien ist der Einsatz moderner Werkzeuge (Tooling) entscheidend für die Erfüllung der DORA-Anforderungen. Um die DORA-Konformität zu erfüllen, müssen diese Werkzeuge nicht nur eine umfassende Überwachung und Steuerung ermöglichen, sondern auch in der Lage sein, Berichte zu erstellen und Bedrohungen frühzeitig zu erkennen.

DORA-Compliance hängt stark von der Fähigkeit ab, Automatisierung, Transparenz und Sicherheitskontrollen in alle Aspekte der IT Service Management Prozesse zu integrieren. Moderne Werkzeuge bieten die notwendige Unterstützung, um diese Anforderungen zu erfüllen und gleichzeitig Effizienz und Sicherheit zu wahren.

## 10.1 Identity and Access Management (IAM)



Im Hinblick auf die Kontrolle von Identitäten und Zugriffsrechten stellt DORA sehr hohe Anforderungen. Finanzinstitute müssen dafür sorgen, dass nur berechtigte Personen Zugang zu sensiblen Daten und kritischen IT-Systemen haben. Unbefugte Zugriffe oder der Missbrauch von Berechtigungen können die Ausfallsicherheit erheblich gefährden.

Moderne IAM-Systeme bieten erweiterte Funktionen zur Verwaltung und Überwachung von Benutzerzugriffen. Dazu gehören Multi-Faktor-Authentifizierung (MFA), rollenbasierte Zugriffskontrollen und detaillierte Audit-Trails, die alle Aktionen im Zusammenhang mit Zugriffsrechten dokumentieren. Ein effektives IAM-Tool muss in der Lage sein, potenzielle Missbrauchsfälle zu erkennen und Zugriffe in Echtzeit zu überwachen, insbesondere bei privilegierten Benutzerkonten.

Ebenso wichtig ist die Sicherstellung der Segregation of Duties (SoD), um Interessenkonflikte und Betrug zu verhindern. Zudem müssen regelmäßige Überprüfungen der angelegten Benutzerkonten durchgeführt werden, wobei DORA vorschreibt, dass diese mindestens zweimal jährlich erfolgen müssen. Für eine lückenlose Nachvollziehbarkeit ist außerdem eine historische Dokumentation der vergebenen Benutzer und Berechtigungen erforderlich.

Angestrebt wird, den Zugriff auf kritische Systeme zu kontrollieren, das Risiko kompromittierter Benutzerkonten zu minimieren und detaillierte Berichte für Aufsichtsbehörden bereitzustellen.

## 10.2 Configuration Management Database (CMDB)

Finanzinstitute müssen den Status ihrer IT-Systeme, Konfigurationen und Abhängigkeiten jederzeit nachvollziehen können. Jede Abweichung oder Änderung kann die IT-Resilienz gefährden, weshalb eine lückenlose Nachverfolgung notwendig ist. Asset Management als reine Verwaltung ist nicht mehr zeitgemäß. Eine Configuration Management Database bildet die Grundlage für das Asset Management, indem sie Abhängigkeiten zwischen Assets und Informationen herstellt.

Moderne CMDB-Tools erfassen und überwachen alle IT-Ressourcen und deren Konfigurationen in Echtzeit. Sie ermöglichen die Nachverfolgung von Änderungen an Assets und liefern Reports über den aktuellen Zustand der IT-Umgebung. Die Integration mit Änderungsmanagementsystemen ermöglicht die Überwachung und Analyse von Änderungen, um ungeplante oder risikobehaftete Änderungen zu vermeiden. Transparenz über Softwarestände und ggf. bekannte Schwachstellen sowie Patching ist ebenso wichtig wie Transparenz über vorhandene (ggf. auch unerwünschte) Systeme.

Eine Risikoabschätzung bei Changes ist notwendig, um potenzielle Auswirkungen auf die IT-Resilienz zu bewerten. Lifecyclemanagement stellt sicher, dass alle IT-Assets während ihres gesamten Lebenszyklus überwacht und verwaltet werden. Je nach Suite können automatisiertes Patching, Schwachstellenscans und andere Funktionen integriert werden, um die Sicherheit und Effizienz zu erhöhen.

Auf diese Weise soll eine vollständige Transparenz und Kontrolle über die gesamte IT-Infrastruktur erreicht werden, um Risiken durch unkontrollierte Änderungen zu minimieren und eine schnelle Wiederherstellung im Störungsfall zu ermöglichen.

## 10.3 IT Service Management

ITSM-Plattformen sind zentrale Werkzeuge für das Management von IT-Prozessen. Sie müssen Incidents, Service Requests, Changes und Problems verwalten und deren Status überwachen können. Darüber hinaus müssen Finanzinstitute gemäß DORA in der Lage sein, Audits und Berichte über ihre ITSM-Aktivitäten zur Wahrung der Compliance zu erstellen.

Moderne ITSM-Plattformen bieten umfassende Funktionen für das Management von IT-Services, einschließlich Incident-, Change- und Problem-Management. Für eine schnelle und konsistente Bearbeitung von Incidents und Changes sollten diese Plattformen Workflows automatisieren können. Gleichzeitig sollten sie über integrierte Berichts- und Überwachungsfunktionen verfügen, um Compliance-Anforderungen zu erfüllen und regelmäßige Audits zu unterstützen. Einige ITSM-Tools bieten auch KI-gestützte Analysen, die Vorfälle vorhersagen und automatisch entsprechende Maßnahmen einleiten können.

Ebenfalls wichtig ist die Auditierfähigkeit, die durch Auditlogs und die Unveränderbarkeit von Daten gegeben sein muss. Zur Überwachung der Performance und Einhaltung der Service Level Agreements ist auch das Reporting von SLAs und KPIs für Tickets ausschlaggebend. Lückenlose Dokumentation, Approvals und Testing sind im Sinne der Nachvollziehbarkeit und Qualität der Prozesse erforderlich.

Durch die Integration in die Prozesse, einschließlich Risikoanalyse und Fallback-Szenarien, ist eine Vorbereitung auf unvorhergesehene Ereignisse möglich. Best Practice ist, dass der Dienstleister mit dem Kundensystem arbeitet; wenn dies nicht möglich ist, sollte eine Ticketkopplung zum System des Dienstleisters erfolgen.

ITSM soll die zentrale Steuerung aller ITSM-Prozesse ermöglichen, Routineaufgaben automatisieren und Berichtsanforderungen erfüllen, damit die Einhaltung von DORA eingehalten und die Servicequalität verbessert werden kann.

## 10.4 CI/CD Pipelines

Um die betriebliche Ausfallsicherheit zu gewährleisten, verlangt DORA, dass jede Einführung von Software oder Änderungen an IT-Systemen genau überwacht und kontrolliert werden. Unkontrollierte oder fehlerhafte Software-Deployments können zu Ausfallzeiten und Sicherheitslücken führen. Moderne Tools für die Continuous Integration und Continuous Deployment/Delivery automatisieren den Prozess der Softwareintegration und -bereitstellung, wobei jede neue Version strengen Tests unterzogen wird, bevor sie in die Produktionsumgebung gelangt. Diese Werkzeuge bieten eine enge Integration mit Test- und Sicherheitswerkzeugen, damit jede Softwareänderung sowohl funktional als auch sicher ist. Durch die Implementierung von automatisierten Rollbacks können fehlerhafte Änderungen schnell rückgängig gemacht werden, was die betriebliche Ausfallsicherheit weiter erhöht.

Automatisierung erhöht die Transparenz und reduziert die Fehlerwahrscheinlichkeit bei manuellen Tätigkeiten. Durch automatisiertes Scanning und Testing kann insbesondere bei Individualentwicklungen Sicherheit und Integrität schon beim Check-In geprüft werden. Eine Automatisierung selbst mit gängigen Tools wie Puppet oder Ansible reduziert Fehler und beschleunigt die Verfahren. Darüber hinaus kann die notwendige Dokumentation direkt erstellt werden.

Das Ziel ist die schnelle und sichere Bereitstellung neuer Software-Releases und die Minimierung von Risiken durch kontinuierliche Überwachung und Automatisierung der Testverfahren. ITSM-Plattformen sollen die zentrale Steuerung aller ITSM-Prozesse ermöglichen, Routineaufgaben automatisieren und Berichtsanforderungen erfüllen, um die Einhaltung von DORA zu unterstützen und die Servicequalität zu verbessern.

Der Einsatz von CI/CD-Pipelines soll die frühzeitige Erkennung von Sicherheitsbedrohungen, die schnelle Reaktion auf Vorfälle und die Bereitstellung umfassender Berichte zur Dokumentation und Sicherstellung der Einhaltung von DORA unterstützen.

## 10.5 Security Information and Event Management (SIEM)

DORA betont die Notwendigkeit einer kontinuierlichen Überwachung und einer schnellen Reaktion auf sicherheitsrelevante Vorfälle. Finanzinstitute müssen in der Lage sein, IT-Sicherheitsvorfälle in Echtzeit zu überwachen und sofort zu reagieren, um Betriebsunterbrechungen zu minimieren. Um Bedrohungen in Echtzeit zu erkennen, sammeln und analysieren moderne SIEM-Systeme Sicherheitsdaten aus der gesamten IT-Infrastruktur. Zur Identifizierung von Anomalien, die auf Sicherheitsvorfälle hindeuten könnten, nutzen diese Systeme künstliche Intelligenz und maschinelles Lernen. SIEM-Tools sind in der Lage, Alarme auszulösen, automatisch Gegenmaßnahmen einzuleiten und detaillierte Berichte über Vorfälle zu erstellen. Sie sind auch für forensische Analyse und Nachverfolgung von Vorfällen ausschlaggebend, um die gesetzlichen Berichtspflichten von DORA zu erfüllen.

SIEM-Systeme gewinnen zunehmend an Bedeutung, da sie zur Anomalieerkennung sowohl im Bereich der Sicherheit als auch im laufenden Betrieb beitragen, insbesondere in Kombination mit dem bestehenden Monitoring. Eine Baseline-Definition hilft, Abweichungen schnell zu erkennen und Transparenz über den Zustand der IT-Infrastruktur herzustellen. Die Unveränderbarkeit von Logfiles durch einen Collector wahrt die Integrität der Daten. Klare Eskalationsstrategien bei Anomalien, Security Incidents und Meldepflichten ermöglichen eine schnelle und effektive Reaktion.

# 11 Checklisten für die Zusammenarbeit mit IKT-Drittdienstleistern

Die Zusammenarbeit mit IKT-Dienstleistern muss regelmäßig und strukturiert überprüft werden, um sicherzustellen, dass die Servicequalität hoch bleibt, Risiken minimiert werden und alle gesetzlichen und vertraglichen Anforderungen kontinuierlich erfüllt werden.

- ☐ **Scope Management**
- ☐ **Communication Management**
- ☐ **Compliance Management**
- ☐ **Performance Management**
- ☐ **Resilience Management**

## 11.1 Scope Management

- Sind die Services klar definiert mit Scope, Owner und Verbindung zu betroffenen und unterstützten Geschäftsprozessen?
- Ist in den Service Definitionen ersichtlich, ob sie kritische und wichtige Funktionen unterstützen?
- Sind die Schnittstellen zwischen verschiedenen Services klar definiert?
- Sind die Verantwortlichkeiten klar strukturiert?
- Sind alle Stakeholder an der Definition des Serviceumfangs beteiligt?
- Gibt es eine klare Abgrenzung der Services im Hinblick auf interne und externe Abhängigkeiten?
- Wie werden Änderungen des Leistungsumfangs gesteuert und dokumentiert?
- Wurden Service Level Agreements (SLAs) definiert und entsprechen diese den Kundenanforderungen?
- Existiert ein Eskalationsplan für den Fall, dass SLAs nicht eingehalten werden können?

## 11.2 Communication Management

- Sind die Rollen und Verantwortlichkeiten aller Beteiligten definiert?
- Ist eine Kommunikationsmatrix definiert?
- Welche Tools werden zur Unterstützung der Kommunikation eingesetzt?
- Gibt es definierte Berichtsformate und Kommunikationswege?
- Finden regelmäßige Abstimmungsgespräche statt?
- Gibt es eine Kommunikationsrichtlinie für Krisensituationen?
- Wie wird sichergestellt, dass alle Stakeholder stets auf dem aktuellen Stand sind?
- Werden Kommunikations- und Eskalationsprozesse regelmäßig getestet?
- Existiert ein Feedback-Mechanismus zur kontinuierlichen Verbesserung der Kommunikation?
- Sind Kommunikationsrichtlinien für externe Partner definiert?

## 11.3 Compliance Management

- Welche regulatorischen Anforderungen sind relevant und werden berücksichtigt?
- Gibt es einen Compliance-Verantwortlichen?
- Sind alle Compliance-Standards dokumentiert und in die Prozesse integriert?
- Werden regelmäßig Überprüfungsreports erstellt und überprüft?
- Gibt es einen Eskalationsprozess bei Verstößen?
- Wurde eine vollständige Compliance-Risikobewertung durchgeführt?
- Existieren interne Audits, um die Einhaltung der Compliance regelmäßig zu überprüfen?
- Wie werden neue regulatorische Anforderungen erkannt und integriert?
- Werden die Compliance-Anforderungen mit Dienstleistern und Drittanbietern abgestimmt?
- Existieren Richtlinien für den Umgang mit Datenverstößen und deren Meldung?

## 11.4 Performance Management

- Sind alle wichtigen KPIs definiert und werden diese regelmäßig gemessen?
- Gibt es konkrete Ziele und Schwellenwerte für die KPIs?
- Werden die Leistungen anhand dieser KPIs regelmäßig bewertet?
- Besteht ein transparenter Verrechnungsmechanismus?
- Werden die Ergebnisse für eine kontinuierliche Verbesserung genutzt?
- Gibt es ein Tool zur automatisierten Erfassung und Analyse der KPIs?
- Werden die KPIs regelmäßig mit den Geschäftszielen abgestimmt?
- Wie wird die Performance der Dienstleister und Drittanbieter überwacht?
- Existiert ein Benchmarking-Prozess für die Leistungsbewertung?
- Gibt es einen Berichtskalender, der die regelmäßige Verfügbarkeit der Leistungsberichte sicherstellt?

## 11.5 Resilience Management

- Findet eine regelmäßige Business Impact Analysis (BIA) statt?
- Wie werden die Maßnahmen aus der BIA getrackt?
- Gibt es Pläne für Desaster Recovery und Business Continuity?
- Werden die Pläne regelmäßig getestet und aktualisiert?
- Welche Mechanismen zur proaktiven Fehlererkennung sind vorhanden?
- Werden alle Systeme kontinuierlich auf Anomalien überwacht?
- Gibt es eine Strategie zur schnellen Wiederherstellung nach Ausfällen?
- Sind alle relevanten Bedrohungen für die IT-Infrastruktur identifiziert und bewertet?
- Werden die Notfallpläne regelmäßig mit den aktuellen Bedrohungsszenarien abgeglichen?
- Gibt es Prozesse zur Priorisierung kritischer Systeme und Daten?
- Existieren Redundanz- und Failover-Mechanismen für alle kritischen Systeme?
- Wie wird die Wirksamkeit der Resilienzmaßnahmen überprüft?
- Werden Mitarbeiter regelmäßig zu Resilienz- und Notfallplänen geschult?
- Existiert eine automatisierte Überwachung zur Erkennung von Anomalien und Angriffen?

Praxisanleitung für Finanzunternehmen: DORA-Checklisten für effektive Nutzung von IKT-Drittdienstleistungen →

# 12 Vorteile für Ihre Due Diligence mit 7P einem DORA-konformen Dienstleister

**Standort und Leistungserbringung**

- Hauptsitz in Deutschland (Köln), keine Subdienstleister
- Optional: Leistungserbringung aus europäischen Ländern mit hohem CPI (z. B. Portugal)

**Zertifizierungen**

- ISO 27001: Informationssicherheits-Managementsystem
- ISO 9001: Qualitätsmanagement-System

**Risikomanagement**

- Integriertes Managementsystem, IKS gemäß ISAE 3402 Typ 2
- Auditsicheres Reporting, Interne Revision
- Konformität mit MaRisk, BAIT und DORA
- Regelmäßige DORA- und Datenschutzschulungen
- Prüf- und Auditrecht für Auftraggeber

**Skalierbarkeit und Zusammenarbeit**

- Breites Leistungsportfolio, Multivendor-Strategie
- ITIL-basierte Standards (ITIL v3, ITIL v4, SAFe, Prince2)
- Kontinuierlicher Verbesserungsprozess mit KPI's

**ESG-Bewusstsein**

- Ethische Verantwortung Compliance, Datenschutz, Sensibilisierung
- Soziale Verantwortung: Diversity, Sicherheitschecks, Karrieremöglichkeiten
- Umweltschutz: Green IT, Energieeinsparung durch Flächenoptimierung

Ihr Weg zur DORA-Konformität beginnt hier.
Erfahren Sie, wie eine Partnerschaft mit uns als IKT-Dienstleister Ihre IT zukunftssicher macht.
Kontaktieren Sie uns noch heute!

Mit Experten sprechen →

# 13 Fazit und Handlungsempfehlungen für eine erfolgreiche Umsetzung der DORA-Anforderungen

DORA verpflichtet Finanz- und Versicherungsunternehmen, ihre Dienstleister und Verträge kritisch zu prüfen, neu zu bewerten und anzupassen, insbesondere im Hinblick auf diejenigen Dienstleister, die kritische und wichtige Funktionen unterstützen. Nicht alle IT-Dienstleister können oder möchten die hohen Anforderungen von DORA vollständig erfüllen. Als DORA-konformer Partner kennen wir die spezifischen Herausforderungen und unterstützen Sie dabei, die regulatorischen Vorgaben zuverlässig umzusetzen. In diesem Zusammenhang ist es entscheidend, den passenden Partner sowohl auf vertraglicher als auch strategischer Ebene zu wählen und zugleich die operative Zusammenarbeit durch gezielte Prozess- und Tool-Optimierungen DORA-konform zu gestalten.

Empfehlungen für eine erfolgreiche Umsetzung:

- **Strategische Partnerschaften für Resilienz:** Die Wahl eines zuverlässigen Partners mit DORA-konformer Expertise und ITSM-Fachwissen ist entscheidend. Ein erfahrener Anbieter wie 7P unterstützt Finanzunternehmen dabei, die regulatorischen Anforderungen zu erfüllen und zugleich Innovationspotenziale auszuschöpfen.
- **Prozessreife und kontinuierliche Optimierung:** DORA-konformes IT Service Management verlangt einen hohen Reifegrad. Der Einsatz moderner Frameworks wie ITIL v4 und die kontinuierliche Verbesserung durch regelmäßige Risikoanalysen und Audits stellen die notwendige Prozessqualität und Dokumentation sicher.
- **Tool-Integration und Automatisierung:** Eine konsistente und leistungsfähige Tool-Landschaft, die durch Automatisierung und AIOps gestützt wird, erleichtert die Erfüllung der DORA-Anforderungen und schafft zugleich neue Effizienzvorteile. Insbesondere CMDB und Asset Management sollten als zentrale Elemente der IT-Resilienz angesehen und kontinuierlich gepflegt werden.
- **Transparenz und Nachvollziehbarkeit:** Die Einhaltung von DORA erfordert eine umfassende Nachvollziehbarkeit sämtlicher IT-Prozesse. Dazu gehören die Integration eines ITSM-Systems, das detaillierte Berichte und Audit-Logs erstellt, und die Implementierung einer SIEM-Lösung zur Echtzeit-Überwachung und proaktiven Incident-Erkennung.

Insgesamt zeigt das Whitepaper, dass DORA-konformes IT Service Management eine ganzheitliche Betrachtung und punktuelle Modernisierung der IT-Infrastruktur erfordert, um regulatorische Anforderungen zu erfüllen und zugleich einen strategischen Vorteil zu erlangen.

Die SEVEN PRINCIPLES steht als Partner bereit, um Ihr Unternehmen bei der Erreichung dieser Ziele zu unterstützen.

## 13.1 Wie wir Sie unterstützen können

- **CMDB-Aufbau, -Integration und -Modernisierung:** Wir unterstützen Sie beim Aufbau einer modernen und leistungsfähigen Configuration Management Database, um Ihre IT-Risiken besser managen zu können.

  Mehr zu CMDB →

- **Asset Management as a Service:** Neben dem Aufbau und Betrieb Ihrer CMDB integrieren wir diese in ein ganzheitliches Asset Management aus prozessualer und technischer Sicht.
- **IT Service Management as a Service:** Im Rahmen des Betriebs und der Modernisierung Ihrer ITSM-Suite unterstützen wir Sie dabei, den Reifegrad Ihrer Prozesse kontinuierlich zu erhöhen und in Ihrer Tool-Landschaft abzubilden.
- **Toolharmonisierung:** In historisch gewachsenen IT-Umgebungen existieren häufig eine Vielzahl an Tools und Werkzeugen. Sind alle diese Tools zweckorientiert und aus Sicht des Lizenzmanagements optimal eingesetzt oder finden wir Optimierungspotenzial? Starten Sie gemeinsam mit uns ein Analyseprojekt und wir zeigen Ihnen die Optimierungsmöglichkeiten auf.
- **Prozessoptimierung mit der Atlassian Toolsuite:** Viele Unternehmen setzen bei der Abbildung ihrer Prozesse auf Produkte von Atlassian. Mit 7P haben Sie einen erfahrenen Partner an Ihrer Seite, der Sie bei der Implementierung, Modernisierung, der Weiterentwicklung und dem Betrieb Ihrer Atlassian-Lösungen unterstützt.

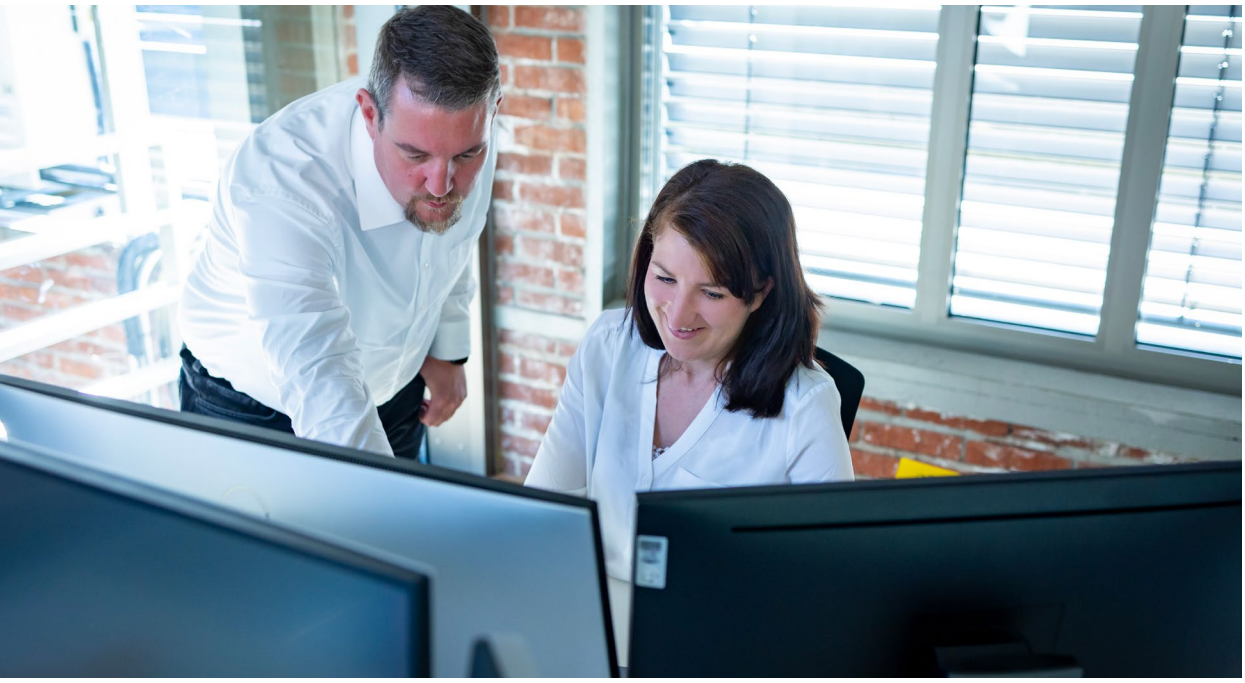
  Mehr zu Atlassian Toolsuite →

- **KI-gestützter IT-Betrieb (AIOps):** Wir unterstützen Sie beim Einsatz von Künstlicher Intelligenz, um Ihre IT-Prozesse zu automatisieren und die Ausfallsicherheit zu erhöhen.

  Mehr zu AiOps →

Wir achten auf eine ausgewogene Balance zwischen individueller Anpassung und dem Einsatz erprobter Standards, um Ihnen ein effizientes und skalierbares Bedienkonzept zu bieten. Unsere Expertinnen und Experten verfügen über fundierte Erfahrung im Umgang mit den Tools, eine hohe Prozessaffinität und umfassende Kenntnisse der regulatorischen Anforderungen einschließlich der BaFin.

# Setzen Sie auf 7P als zuverlässigen Partner



Wir stellen Ihnen ein maßgeschneidertes Team aus erfahrenen Prozessberater:innen, Business Engineers, Technical Engineers und DevOps-Spezialist:innen zur Seite. Gemeinsam entwickeln wir Lösungen, die Ihre spezifischen Anforderungen optimal in Ihrer Prozess- und Systemlandschaft umsetzen.

Kontaktieren Sie uns noch heute, um Ihre individuellen Bedarfe zu besprechen und die nächsten Schritte zu planen.

Kontakt aufnehmen →

**Mehr Informationen erhalten Sie hier:**

**7p-mobility.com**

**mobility@7p-group.com**

## Praxiswissen für Ihren Erfolg im Job

Erfahren Sie in unseren Weiterbildungen praktisches und aktuelles Know-how zu unterschiedlichen Themen der Kredit- und Bonitätsanalyse sowie Kreditvergabe und Finanzierung.
Jetzt informieren.

### e-Learning – Klicken und Lernen

Das FORUM Institut bietet mit hochwertigen e-Learning-Programmen eine flexible Weiterbildungsform. Entscheiden Sie selbst, wann und wo Sie lernen.
Jetzt testen.

### Inhouse-Seminare – Maßgeschneiderte Lösungen

Alle unsere Seminare eignen sich auch hervorragend als Inhouse-Training.
Jetzt individuelles Angebot anfordern.

FORUM · Institut für Management GmbH • Postfach 10 50 60 • 69040 Heidelberg • Germany
Telefon: +49 6221 500-500 • Fax: +49 6221 500-555 • www.forum-institut.de