WHITEPAPER

# Reporting nach ISAE 3402 als **Lösung für die Steuerung von IT-Dienstleistern** in der Finanzdienstleistung

Mehr Informationen erhalten Sie hier:

**7p-group.com**

## INHALT



# Einleitung

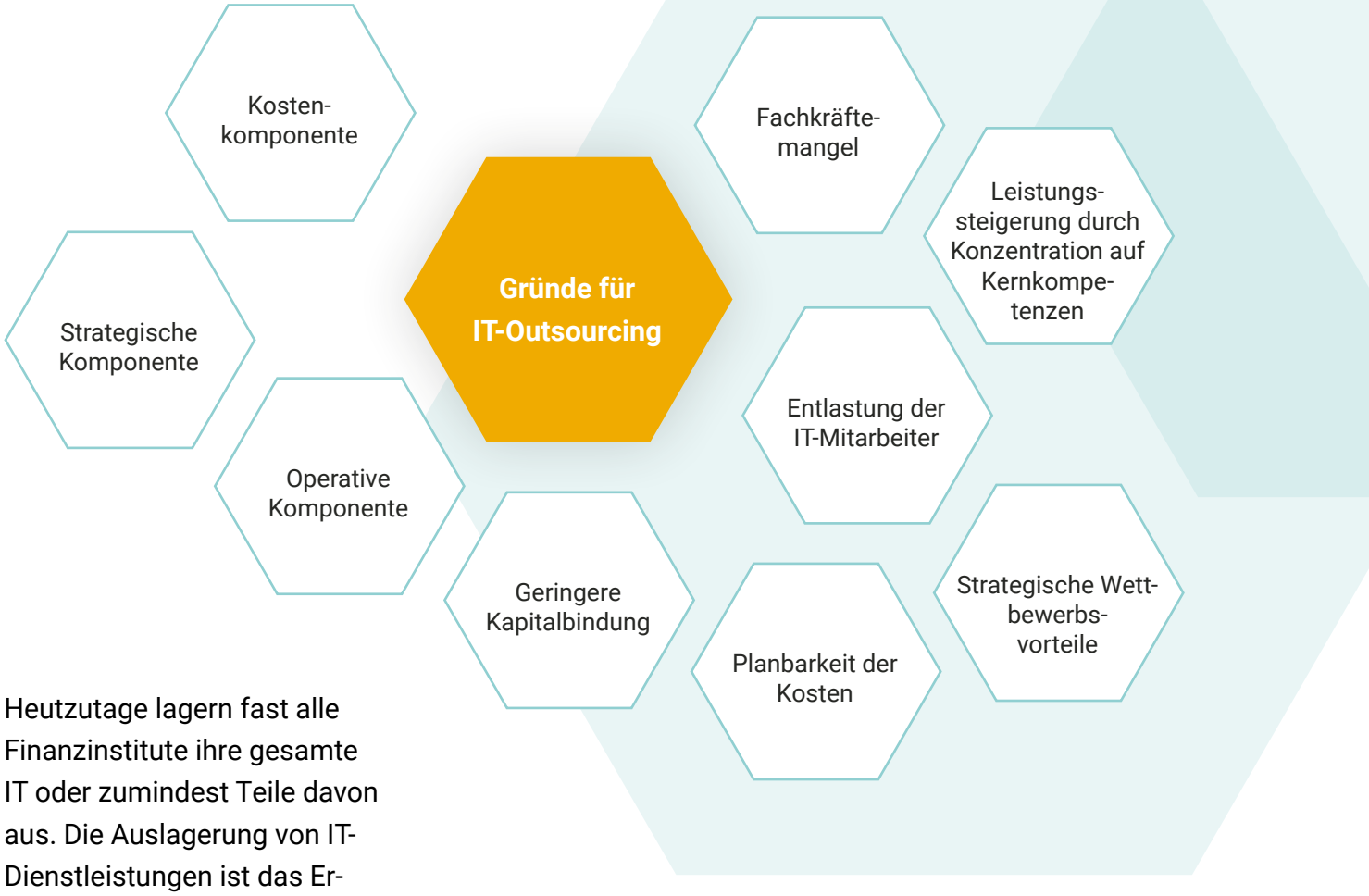
Die Auslagerung von IT-Dienstleistungen ist heutzutage für viele Unternehmen eine gängige Praxis. Diese Praxis bringt jedoch auch Herausforderungen mit sich, insbesondere in regulierten Umgebungen, in denen die Einhaltung von regulatorischen Vorschriften von entscheidender Bedeutung ist. Dieses Whitepaper bietet in diesem Kontext einen umfassenden Überblick über die Herausforderungen und Lösungen im Zusammenhang mit der Steuerung von IT-Dienstleistern.

Wir beginnen mit einer Diskussion über die Motivation, IT-Leistungen auszulagern und wie Unternehmen regulatorische Anforderungen sicherstellen können. Anschließend stellen wir den Reporting Standard ISAE 3402 als Lösungsansatz vor und gehen auf die verschiedenen Bestandteile eines Reportings nach ISAE 3402 ein, einschließlich des internen Kontrollsystems, des passenden Kontrollsets und der Management Assertion.

Zur Veranschaulichung der praktischen Anwendung dieser Konzepte präsentieren wir zwei Fallstudien. Die erste Fallstudie beschreibt die Transformation zu einer durch ISAE 3402 Reporting gesteuerten IT-Service Organisation. Die zweite Fallstudie stellt ein Kontrollset vor, das von 7P in einem konkreten Umfeld eingesetzt wird.

Wir hoffen, dass dieses Whitepaper Ihnen wertvolle Einblicke und praktische Anleitungen bietet, um Ihre Herausforderungen im regulierten Umfeld bei der Steuerung Ihrer IT-Dienstleister zu meistern.

# 1. Gründe für die **Auslagerung von IT**




Heutzutage lagern fast alle Finanzinstitute ihre gesamte IT oder zumindest Teile davon aus. Die Auslagerung von IT-Dienstleistungen ist das Ergebnis einer sorgfältigen Abwägung verschiedener Faktoren. Es ist eine strategische Entscheidung, die es den Instituten ermöglicht, ihre Ressourcen effizienter zu nutzen, ihre Geschäftsprozesse zu optimieren und letztendlich ihren Kunden einen besseren Service zu bieten. Die Gründe für die Entscheidung eines Finanzinstituts, seine IT auszulagern, sind vielfältig und oft eine Kombination aus mehreren Überlegungen:

1. **Kostenkomponente**
   IT-Outsourcing kann dazu beitragen, die Kosten zu senken. Insbesondere für mittlere und kleine Unternehmen kann es schwierig sein, ihre IT dauerhaft zu beschäftigen. Durch bedarfsorientiertes Outsourcing wird die Effizienz gesteigert und die Ausgaben auf das Notwendige reduziert, wodurch langfristig gesenkt werden.

2. **Strategische Komponente**
   Die Pflege der IT-Infrastruktur oder die Entwicklung von Applikationen benötigen ein hohes Fachwissen, um effizient umgesetzt werden zu können. Gleichzeitig darf das Kerngeschäft nicht vernachlässigt werden. Gezieltes Outsourcing kann hier für die nötige Entlastung sorgen.

3. **Operative Komponente**
   Die Abrechnungen durch den Dienstleister ermöglichen eine transparente Kostenbetrachtung. Auf schwankenden Volumen kann flexibel durch zügigen Aufbau und Abbau von Kapazitäten reagiert werden.

4. **Geringere Kapitalbindung**
   Für IT-Unternehmen, insbesondere kleinere, kann die Auslagerung von IT-Services eine sinnvolle Möglichkeit sein, um die Kapitalbindung zu reduzieren. Im Rahmen von IT-Outsourcing können Kosten für den Aufbau und Betrieb der Infrastruktur, Technik, Räumlichkeiten oder Personal eingespart werden.

5. **Planbarkeit der Kosten**
   Die Kosten für das IT-Outsourcing sind vertraglich geregelt. Standardisierte Arbeitsabläufe und die Protokollierung erledigter Aufgaben sorgen für eine hohe Kostentransparenz und -kontrolle.

6. **Strategische Wettbewerbsvorteile**
   Durch IT-Outsourcing können Unternehmen strategische Wettbewerbsvorteile aufbauen und erhalten.

7. **Entlastung der IT-Mitarbeiter**
   IT-Outsourcing kann dazu beitragen, die IT-Mitarbeiter zu entlasten und ihnen die Möglichkeit geben, sich auf andere Aufgaben zu fokussieren.

8. **Leistungssteigerung durch Konzentration auf Kernkompetenzen**
   Unternehmen können sich auf ihre Kernkompetenzen konzentrieren und die Qualität der eingekauften Leistungen verbessern.

9. **Fachkräftemangel**
   Die Unternehmen versuchen, neue Mitarbeiter anzulocken und ihre bestehenden IT-Fachkräfte langfristig zu binden, indem sie flexible Arbeitszeitmodelle, Home-Office-Angebote oder kostengünstige Kita-Plätze anbieten. Wenn diese Maßnahmen nicht ausreichen, entstehen Lücken, die im Unternehmen häufig nicht zu schließen sind.

# 2. Wie kann man die **regulatorischen Anforderungen sicherstellen?**

Ungeachtet der spezifischen Beweggründe jedes Finanzinstituts für die Auslagerung oder Teilauslagerung seiner IT, ist unbestreitbar, dass diese Praxis zu einem unverzichtbaren Element in der Geschäftsstrategie vieler Institute geworden ist. Die Gründe hierfür mögen vielfältig und nachvollziehbar sein, doch sie bringen in der Umsetzung stets erhebliche Herausforderungen, wenn nicht sogar Hürden mit sich:

## Die Gewährleistung der **Einhaltung regulatorischer Anforderungen**

Häufig verbirgt sich hinter dem IT-Outsourcing zudem eine ganze Kette von IT-Dienstleistern, was die Komplexität der Herausforderungen entsprechend potenziert.

In den letzten Jahren haben sich die Anforderungen an IT-Auslagerungen für Finanzinstitute stetig erhöht. Dieser Trend ist vor allem auf die zunehmende Komplexität und erhöhte Vernetzung zurückzuführen. Die regulatorischen Anforderungen aus dem Kreditwesengesetz (KWG), den Mindestanforderungen an das Risikomanagement (MaRisk), der Bankaufsichtlichen Anforderungen an die IT (BAIT) sowie dem Digital Operational Resilience Act (DORA) müssen eingehalten werden. Diese Vorschriften erfordern, dass Finanzinstitute ihre IT-Strukturen und -Prozesse kontinuierlich anpassen und weiterentwickeln müssen, um den steigenden Anforderungen gerecht zu werden. Dies hat das IT-Outsourcing zu einem zentralen und herausfordernden Aspekt der Geschäftsstrategie von Finanzinstituten gemacht.

## Anforderung aus **KWG**

Die Bundesaufsicht für Finanzen (BaFin) legt mit dem Kreditwesengesetz (KWG) Anforderungen an das IT-Outsourcing fest. Gemäß § 25a KWG müssen Institute, die IT-Dienstleistungen auslagern, sicherstellen, dass die Auslagerung keine negativen Auswirkungen auf die Kontrollmöglichkeiten der internen Revision hat und die Auslagerung die Einhaltung aufsichtsrechtlicher Anforderungen nicht beeinträchtigt.

## Anforderung aus **MaRisk**

Die Mindestanforderungen an das IT-Outsourcing sind in den „Mindestanforderungen an das Risikomanagement“ (MaRisk) der BaFin festgelegt. Diese Anforderungen umfassen Aspekte wie die sorgfältige Auswahl und Steuerung der Dienstleister, die Sicherstellung der Auslagerungsfähigkeit, die Einhaltung aufsichtsrechtlicher Anforderungen und die Sicherstellung eines jederzeitigen Zugriffs auf die ausgelagerten Daten.

## Anforderung aus **BAIT**

Die "Bankaufsichtlichen Anforderungen an die IT" (BAIT) legen spezifische Anforderungen für Finanzinstitute an das IT-Outsourcing fest. Diese Anforderungen umfassen Aspekte wie die sorgfältige Auswahl und Steuerung der Dienstleister, die Sicherstellung der Auslagerungsfähigkeit, die Einhaltung aufsichtsrechtlicher Anforderungen und die Sicherstellung eines jederzeitigen Zugriffs auf die ausgelagerten Daten.

# Anforderung aus **DORA**

Die neueste regulatorische Anforderung stammt aus dem „Digital Operational Resilience Act“ (DORA). Es handelt sich um eine Verordnung der Europäischen Union, die eine finanzsektorweite Regulierung für die Themen Cybersicherheit, IKT-Risiken und digitale operationale Resilienz schafft. Ziel ist es, den europäischen Finanzmarkt gegenüber Cyberrisiken und Vorfällen der Informations- und Kommunikationstechnologie (IKT) zu stärken. Die Anforderungen des DORA an IT-Outsourcing umfassen neben anderen Themen zwei wesentliche Punkte in Bezug auf IT-Dienstleister:

- **Etablierung eines Rahmenwerks für das IKT-Risikomanagement:**
  Dies beinhaltet die Implementierung von Prozessen und Kontrollen zur Identifizierung, Bewertung, Steuerung und Überwachung von IKT-Risiken.

- **Management des IKT-Drittparteienrisikos:**
  Dies erfordert die Implementierung von Prozessen zur Identifizierung und Steuerung von Risiken, die mit der Nutzung von IKT-Dienstleistungen von Drittanbietern verbunden sind, sowie die Gestaltung von Sub-Outsourcing-Arrangements.

Alle diese regulatorischen Anforderungen zielen darauf ab, die Risiken im Zusammenhang mit IT-Auslagerungen zu managen und die Sicherheit und Stabilität des Finanzsystems zu gewährleisten. Finanzinstitute müssen diese Anforderungen verstehen und einhalten, um regulatorischen Sanktionen zu entgehen und das Vertrauen ihrer Kunden zu wahren.

Die Herausforderung besteht darin, sicherzustellen und nachzuweisen, dass die regulatorischen Anforderungen auch bei ausgelagerten IT-Dienstleistungen lückenlos erfüllt werden. Dies erfordert die Einhaltung dieser Anforderungen entlang der gesamten Servicekette. Der International Standard on Assurance Engagements (ISAE) hat mit ISAE 3402 einen international anerkannten Standard für ein Reporting zwischen Dienstleistern und auslagernden Instituten geschaffen. Dieser Standard beantwortet genau diese Fragestellung.

# 3. **ISAE 3402** als Lösungsansatz

Der international anerkannte Reporting-Standard ISAE 3402 dient der umfassenden Überwachung und Kontrolle von Dienstleistern. Der deutsche Prüfungsstandard des Instituts der Wirtschaftsprüfer in Deutschland IDW PS 951 beschäftigt sich inhaltlich mit derselben Thematik.

Beide Standards haben das Ziel, die Qualität und Sicherheit von ausgelagerten Dienstleistungen zu gewährleisten. Sie beinhalten die Standardisierung der Prüfung des internen Kontrollsystems bei Dienstleistungsunternehmen. Die Inhalte der beiden Standards unterscheiden sich nur geringfügig und können vereinfachend gleichgesetzt werden.

## 3.1 **Einführung in das Reporting** nach ISAE 3402

Der Standard ISAE 3402 definiert ein standardisiertes Berichtsverfahren zur Prüfung des internen Kontrollsystems bei Dienstleistungsunternehmen. Er kann als Nachweis der Abbildung regulatorischer Anforderungen in der Finanzberichterstattung dienen. Der Standard unterscheidet zwischen zwei Arten von Prüfungen:

**Typ 1 Prüfung**
Bei einer Typ 1 Prüfung wird lediglich das Kontrolldesign und die Implementierung der Kontrollen geprüft, ohne dass die definierten Kontrollmaßnahmen durch Stichproben auf ihre Wirksamkeit hin untersucht werden.

**Typ 2 Prüfung**
Zusätzlich zur Prüfung des Designs und der Implementierung wird die tatsächliche Ausführung und damit die Wirksamkeit der Kontrollen über einen definierten Zeitraum geprüft und entsprechend berichtet.

## 3.2 Bestandteile eines Reportings nach ISAE 3402

Der ISAE 3402 Report beschreibt eine umfassende und detaillierte Darstellung des internen Kontrollsystems (IKS) eines Dienstleisters. Er wird in Zusammenarbeit mit einem akkreditierten Prüfer erstellt und dient als Nachweis für die Einhaltung regulatorischer Anforderungen. Der Bericht ist ein umfassendes Dokument, das aus mehreren Modulen besteht:

**Beschreibung des internen Kontrollsystems des Dienstleisters (IKS)**
In diesem Abschnitt wird das dienstleistungsbezogene interne Kontrollsystem des Dienstleisters detailliert beschrieben. Hierbei werden die Kontrollumgebung, die Risikobewertung, die Kontrollaktivitäten, die Informations- und Kommunikationssysteme sowie das Monitoring dargestellt.

**Beschreibung der Kontrollen des Dienstleisters (Kontrollset)**
An dieser Stelle werden die spezifischen Kontrollen dargestellt, die üblicherweise zwischen dem Finanzinstitut und dem Dienstleister abgestimmt wurden. Diese Aufstellung nennt sich „Kontrollset“ und bildet die Grundlage für die Prüfung durch akkreditierte Prüfer. Es ist wichtig, dass das Kontrollset klar und präzise formuliert ist, um Missverständnisse zu vermeiden.

**Prüfungsbericht**
Dieser Bericht wird von dem akkreditierten Prüfer erstellt. Er sollte detailliert auf die einzelnen Kontrollziele, die Kontrollen sowie die durch die Prüfung aufgedeckten Feststellungen eingehen. Der Bericht sollte auch die Methodik und das Vorgehen der Prüfung darlegen. Die Prüfungsinhalte unterscheiden sich je nach Prüfungstyp (Typ 1/Typ 2).

**Management Assertion – Erklärung der gesetzlichen Vertreter über die Angemessenheit des IKS**
In dieser Erklärung bestätigen die gesetzlichen Vertreter des Dienstleisters, dass das interne Kontrollsystem angemessen und wirksam ist. Sie übernehmen damit die Verantwortung für das Design, die Implementierung und die Wirksamkeit des internen Kontrollsystems.

## 3.2.1 Das Interne **Kontrollsystem als zentraler Bestandteil**

Das Interne Kontrollsystem (IKS) ist in den bankenaufsichtsrechtlichen Anforderungen im Ursprung in MaRisk AT1 verankert. Dort wird gefordert, dass ein internen Kontrollsystem Regelungen zur Aufbau- und Ablauforganisation, Risikosteuerungs- und Controllingprozesse, Prozesse sowie Funktionen für Risikocontrolling sowie Compliance beinhalten soll.

Aus Sicht eines IT-Dienstleisters für Finanzinstitute wird die genaue Ausgestaltung unter anderem in MaRisk AT 4.3 und 4.4 beschrieben:

**Auf- und Ablauforganisation**
Bei Ausgestaltung der Auf- und Ablauforganisation ist die Unvereinbarkeit von Tätigkeiten sicherzustellen, sofern diese Interessenskonflikte beinhalten könnten. Prozesse und die damit verbundenen Aufgaben, Kompetenzen, Verantwortlichkeiten, Kontrollen und Kommunikationswege müssen klar definiert und aufeinander abgestimmt sein. Berechtigungen und Kompetenzen müssen nach dem Sparsamkeitsgrundsatz (Need-to-know-Prinzip) vergeben und bei Bedarf zeitnah angepasst werden.
Eine regelmäßige und anlassbezogene Überprüfung von IT-Berechtigungen, Zeichnungsberechtigungen und sonstigen eingeräumten Kompetenzen ist sicherzustellen.

**Risikosteuerungs- und Controllingprozesse**
Bei der Umsetzung der Risikosteuerungs- und Controllingprozesse ist sicherzustellen, dass Risiken erkannt, dargestellt, begrenzt und überwacht werden. Die Prozesse müssen eine regelmäßige oder gegebenenfalls eine ad-hoc Berichterstattung an die Geschäftsleitung und das Aufsichtsorgan gewährleisten. Im Sinne einer kontinuierlichen Verbesserung sind die eingesetzten Prozesse, Methoden und Verfahren regelmäßig zu überprüfen, zu überwachen und anzupassen.

**Compliance-Funktion**
Die Compliance-Funktion eines Instituts, ist dafür verantwortlich, Risiken aus der Nichteinhaltung rechtlicher Regelungen und Vorgaben zu begegnen. Sie muss wirksame Verfahren zur Einhaltung dieser Regelungen implementieren und die Geschäftsleitung dabei unterstützen und beraten. Sie ist grundsätzlich der Geschäftsleitung unterstellt und berichtspflichtig. Es muss ein Compliance-Beauftragter benannt werden, dem ausreichende Befugnisse eingeräumt werden und der uneingeschränkt Zugang zu allen erforderlichen Informationen hat. Eine jährliche und anlassbezogene Berichterstattung an die Geschäftsleitung ist vorgeschrieben.

## 3.2.2 Das passende **Kontrollset zum internen Kontrollsystem**

Die Gestaltung des Kontrollsets eines ISAE 3402-Berichts kann stark variieren und ist maßgeblich von den zu erreichenden Kontrollzielen abhängig. Dabei spielen die Art der erbrachten Dienstleistung, die spezifische Branche und die individuellen Risiken des Dienstleistungsunternehmens eine entscheidende Rolle bei der Ausgestaltung des Kontrollsets. Es ist von zentraler Bedeutung, dass das Kontrollset in enger Abstimmung zwischen dem Dienstleister und dem Auftraggeber festgelegt wird, um sicherzustellen, dass es den spezifischen Anforderungen und Risiken beider Parteien gerecht wird. Es ist zwar nicht zwingend vorgeschrieben, aber durchaus üblich, dass die Kontrollsets eines ISAE 3402-Berichts auf der Grundlage von Normen und Best-Practice-Modellen erstellt werden. Diese bewährten Modelle bieten eine solide Basis und können individuell durch spezifischere Kontrollen ergänzt werden, um den einzigartigen Anforderungen jedes Unternehmens gerecht zu werden. Als Grundlage könnten beispielsweise folgende Modelle dienen:

- **COSO-Modell** (Committee of Sponsoring Organizations of the Treadway Commission): Das COSO-Modell ist ein umfassendes Rahmenwerk für interne Kontrollsysteme, das Unternehmen dabei unterstützt, ihre Geschäftsprozesse effektiv zu steuern und Risiken zu managen. Das Modell umfasst fünf Komponenten: Internes Kontrollumfeld, Risikobewertung, Kontrollaktivitäten, Information und Kommunikation sowie Überwachung.

- **COBIT** (Control Objectives for Information and Related Technologies): COBIT ist ein Rahmenwerk zur IT-Governance und zum IT-Management. Es wurde vom ISACA (Information Systems Audit and Control Association) entwickelt und ist ein international anerkanntes

Standardwerk. COBIT bietet einen strukturierten Ansatz für die Steuerung der IT eines Unternehmens. Es hilft dabei, die IT an die Geschäftsziele des Unternehmens auszurichten und sicherzustellen, dass die IT-Ressourcen effektiv und effizient genutzt werden.

- **ISO 27001:** ISO 27001 ist ein weltweit anerkannter Standard, der die Kriterien für ein Informationssicherheitsmanagementsystem (ISMS) festlegt und Unternehmen dabei unterstützt, ihre Informationen sicher zu verwalten und zu schützen. Er wurde von der International Organization for Standardization (ISO) entwickelt und ist auf alle Organisationen anwendbar, unabhängig von Größe, Branche oder geografischer Lage.

- **BAIT:** Die “Bankaufsichtlichen Anforderungen an die IT” (BAIT) sind regulatorische Vorgaben, die von der Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) herausgegeben werden und die Erwartungen der Aufsicht an die IT-Sicherheit in Kreditinstituten klar definieren.

- **VAIT:** Die “Versicherungsaufsichtlichen Anforderungen an die IT” (VAIT) sind regulatorische Vorgaben der Bundesanstalt für Finanzdienstleistungsaufsicht VAIT: (BaFin), die die Erwartungen der Aufsicht an die IT-Sicherheit in Versicherungsunternehmen klar definieren.

- **Unternehmensinterne Risiko-Kontroll-Matrizen:** Diese können ebenfalls zum Aufbau des Kontrollsets eines internen Kontrollsystems genutzt werden.

### 3.2.3 Die Management Assertion als **Bekenntnis zum internen Kontrollsystem**

Das Management des Dienstleisters muss eine Erklärung darüber abgeben, dass das IKS angemessen dargestellt ist bzw. die internen Kontrollen während des Prüfungszeitraums implementiert und im Falle einer Prüfung gemäß Typ II wirksam waren, um die vordefinierten Kontrollziele zu erreichen.

Die Management Assertion ist ein zentraler Bestandteil eines ISAE 3402-Berichts. Sie stellt eine schriftliche Erklärung des Managements des Dienstleistungsunternehmens dar. In dieser Erklärung bestätigt das Management die angemessene Darstellung und das Design der Kontrollen (in einem Typ-1-Bericht) oder die angemessene Darstellung, das Design und die betriebliche Wirksamkeit der Kontrollen (in einem Typ-2-Bericht).

Die Management Assertion dient dazu, den Risiken entgegenzuwirken, die sich aus der Nichteinhaltung rechtlicher Regelungen und Vorgaben ergeben können. Sie ist ein wichtiger Schritt zur Gewährleistung der Einhaltung der im Kontext geltenden wesentlichen rechtlichen Regelungen und Vorgaben.

Die Management Assertion ist auch ein Zeichen für die Verantwortung des Managements für die internen Kontrollen des Dienstleistungsunternehmens. Sie zeigt, dass das Management die Bedeutung der internen Kontrollen anerkennt und sich dafür einsetzt, dass diese Kontrollen effektiv sind und ordnungsgemäß funktionieren. Sie gewährleistet, dass das Management des Dienstleistungsunternehmens seine Verantwortung für die internen Kontrollen ernst nimmt. Dadurch wird das Vertrauen der Kunden in das Dienstleistungsunternehmen gestärkt und die Kundenbeziehung verbessert.

# 4. Case Study Teil 1: **Transformation zu einer** durch ISAE 3402 Reporting **gesteuerten IT-Service Organisation**

Als langjähriger Partner der Mercedes-Benz Bank AG hat 7P einen Transformationsprozess für IT-Dienstleistungen aufgesetzt und erfolgreich durchgeführt. Dieser Prozess hat Managed Services Leistungen entwickelt, die heute eine umfassende Abdeckung der bankenaufsichtsrechtlichen Anforderungen bieten. Ein wesentlicher Meilenstein war die Einführung eines MaRisk-konformen internen Kontrollsystems verbunden mit einem Reporting nach ISAE 3402. Die Erfolgsgeschichte lässt sich in verschiedene Stufen gliedern:

**Stufe 1**

**Konsolidierung der Kompetenzen**
Als Generalunternehmer übernahm 7P Freelancer und Subdienstleister vertraglich, um eine Konsolidierung zu erreichen. Der Fokus lag auf der Bündelung der Expertise, Erfüllung der Anforderungen zur Vermeidung von Scheinselbständigkeit von Beratern und der vertragsseitigen Konsolidierung.

**Stufe 2**

**Aufbau eines Service Centers**
Die Leistungserbringung wurde räumlich vom Kunden weg verlagert und von Einzelberatung zu Service-Teams transformiert. Dazu wurden SLAs und Leistungsscheine etabliert. Die Schnittstelle zwischen Kunde und 7P wurde operativ auf geregelte Service Management Prozeduren umgestellt.

**Stufe 3**

**Reifegraderhöhung Managed Services**
Die eigene Fertigungstiefe wurde optimiert und die Vertragsrisiken durch Reduktion von Sub-Auslagerungen reduziert. Der Reifegrad der Leistungsscheine wurde erhöht. In dieser Stufe lag der Fokus auf Skalierung, um das erfolgreiche Wachstum des Kunden zu begleiten.

**Aufbau eines internen Kontrollsystems für die Managed Services**

Bei 7P wurde ein internes Kontrollsystem entwickelt und implementiert, das die spezifischen Belange der Kundenumgebung abbildet. Dadurch wurde die Grundlage für ein Reporting nach ISAE 3402 geschaffen.

Stufe 4

**Einführung eines ISAE 3402 Reportings**

Es wurde ein ISAE Reporting eingeführt und das Kontrollset an ISO 27001 angepasst. Der Fokus lag auf der Reifegraderhöhung durch Vermeidung vieler Einzelaudits und der Effizienzsteigerung durch standardisierte Berichterstattung.

Stufe 5

Stufe 6

**Ausweitung des Kontrollsets im ISAE 3402 Reporting**

Das Kontrollset im ISAE Reporting wurde erweitert und ein ausführlicheres, branchenspezifischeres Kontrollset auf Basis von BAIT wurde eingeführt. Das Risikomanagement wurde durch die Erweiterung der Innenrevision um die MA-Risk Konformität ergänzt. Der Fokus lag auf einer maßgeschneiderten Schnittstelle zum Kunden.

**Ausweitung des Kontrollsets zur Abdeckung von DORA**

7P arbeitet daran, das Kontrollset zur Abdeckung der aktuellen Anforderungen von DORA (Digital Operational Resilience Act) auszuweiten.

Stufe 7

Diese Transformation zeigt, wie man mit einem koordinierten Vorgehensmodell hochgradig maßgeschneiderte IT-Services erbringen kann unter Berücksichtigung der Einhaltung von strengen regulatorischen Anforderungen. Wir sind stolz darauf, was wir für unseren Kunden, die Mercedes-Benz Bank AG, erreicht haben und freuen uns die Erfolgsgeschichte weiter mit begleiten zu können.

# 5. **Checkliste** zur Selbsteinschätzung des **Reifegrads einer IT-Dienstleistungsumgebung**

Die folgende Checkliste dient als Leitfaden zur Selbstbewertung des Reifegrads einer IT-Dienstleistungsumgebung, unabhängig davon, ob die IT-Serviceerbringung intern oder extern betrieben wird. Sie deckt verschiedene Aspekte ab, von der IT-Strategie und Governance bis hin zum Risiko- und Qualitätsmanagement. Durch strukturiertes Durcharbeiten dieser Checkliste können Stärken und Schwächen in der Service-Organisation identifiziert werden. So lassen sich Aspekte erkennen, die möglicherweise Verbesserungen erfordern. Ein hoher Reifegrad bildet das Fundament für eine IT-Auslagerung, die durch ein ISAE 3402 Reporting gesteuert und überwacht wird.

Diese Checkliste ist nicht erschöpfend, eignet sich jedoch sehr gut für eine erste Selbsteinschätzung. Sie soll dabei helfen, einen objektiven Überblick über den aktuellen Stand Ihrer IT-Dienstleistungsumgebung zu gewinnen und einen Fahrplan für zukünftige Verbesserungen zu erstellen. Viel Erfolg bei der Bewertung!

### 1. IT-Strategie

- Ist Ihre IT-Strategie klar definiert und mit der Unternehmensstrategie abgestimmt?
- Werden regelmäßige Überprüfungen und Anpassungen der IT-Strategie durchgeführt? Findet diese Überarbeitung durch einen geregelten Prozess statt?

### 2. IT-Governance

- Sind Verantwortlichkeiten und Zuständigkeiten in der IT-Organisation eindeutig festgelegt, schriftlich dokumentiert und transparent abgelegt?
- Werden IT-Prozesse regelmäßig überwacht und optimiert?

### 3. Allgemeine Aufbau- und Ablauforganisation

- Sind die IT-Prozesse definiert und transparent dokumentiert?
- Gibt es eindeutige Kommunikations- und Eskalationswege?

## 4. Informationsrisikomanagement

- Wird das Informationsrisiko regelmäßig bewertet, dokumentiert und gesteuert?
- Gibt es einen Prozess zur Identifikation und Behandlung von Informationsrisiken?

## 5. Informationssicherheitsmanagement

- Ist ein Informationssicherheitsmanagementsystem (ISMS) implementiert?
- Werden Informationssicherheitsziele definiert und überwacht?

## 6. Operative Informationssicherheit

- Sind Sicherheitsrichtlinien und -verfahren implementiert? Werden diese eingehalten?
- Werden regelmäßige Sicherheitsüberprüfungen durchgeführt?

## 7. Identitäts- und Rechtemanagement

- Gibt es einen Prozess zur Verwaltung von Benutzeridentitäten und Zugriffsrechten?
- Werden Zugriffsrechte regelmäßig überprüft und angepasst?

## 8. IT-Betrieb

- Sind die IT-Systeme stabil und zuverlässig?
- Werden regelmäßige Datensicherungen durchgeführt und getestet?

## 9. IT-Projekte, Anwendungsentwicklung

- Gibt es einen standardisierten Prozess für IT-Projekte und Anwendungsentwicklung?
- Werden IT-Projekte regelmäßig überwacht und gesteuert?

## 10. Auslagerungen und sonstiger Fremdbezug von IT-Dienstleistungen

- Werden Sub-Auslagerungen von IT-Dienstleistungen sorgfältig geplant und gesteuert?
- Gibt es detaillierte, messbare und auswertbare Vereinbarungen mit externen IT-Dienstleistern?

## 11. IT-Notfallmanagement

- Gibt es einen IT-Notfallplan?
- Werden regelmäßige Tests und Übungen des IT-Notfallplans durchgeführt?

## 12. Compliance

- Werden gesetzliche und regulatorische Anforderungen erfüllt?
- Gibt es einen Prozess zur Identifikation und Behandlung von Compliance-Risiken?

## 13. Datenschutz

- Werden personenbezogene Daten geschützt und Datenschutzbestimmungen eingehalten?
- Gibt es einen Datenschutzbeauftragten?

## 14. Risiko Management

- Gibt es einen Risikomanagementprozess?
- Werden Risiken regelmäßig bewertet und gesteuert?

## 15. KPI-Reporting

- Werden IT-Kennzahlen definiert und regelmäßig berichtet?
- Werden IT-Kennzahlen zur Steuerung und Verbesserung der IT genutzt?

## 16. Qualitätsmanagement

- Gibt es einen Qualitätsmanagementprozess?
- Werden Qualitätsziele definiert und überwacht?

# 6. 7P als **Transformationspartner**

Die Case Study zeigt, dass ein sinnvoller Einsatz eines ISAE 3402 Reportings einen hohen Reifegrad einer Dienstleistungsorganisation erfordert. Beispielsweise müssen Aspekte wie Auf- und Ablauforganisation, IT-Governance, Compliance oder Informationssicherheit mit einem hohen Reifegrad abgebildet sein, um ein entsprechendes ISAE 3402 Reporting zu ermöglichen. Oft sind die Voraussetzungen nur teilweise und in völlig unterschiedlichem Reifegrad erfüllt. Es ist sinnvoll, sich bei einer Transformation von einem erfahrenen Dienstleister unterstützen zu lassen, der den benötigten Reifegrad mitbringt.

**Haben Sie ähnliche Herausforderungen? Kontaktieren Sie uns als Spezialist für maßgeschneiderte IT-Services im hochregulierten Umfeld. In einem unverbindlichen Gespräch können wir evaluieren ob und wie wir Ihnen weiterhelfen können.**

SPRECHEN SIE MIT UNSEREN EXPERTEN →

# 7. Case Study Teil 2:
# Das eingesetzte Kontroll-Set von 7P

Im Folgenden geben wir Einblick in ein konkretes Kontrollset, dass wir bei 7P für einen Kunden im Einsatz haben. Für diese spezielle Kundenumgebung haben wir uns entschlossen das Kontrollset gemäß dem Standard BAIT auszurichten und an die spezifischen Anforderungen anzupassen. Wie bereits erwähnt, müssen Kontrollsets an Kundenanforderungen angepasst werden und sind somit nicht einfach kopierbar.

Dieses im Folgenden dargestellte spezifische Kontrollset besteht aus mehreren Untergruppen, die jeweils Aspekte der IT-Sicherheit und des Managements abdecken.

- Das Change Management bezieht sich auf die Prozesse, zur effektiven Verwaltung von Änderungen.
- Der logische Zugriff bezieht sich auf Kontrollen, die den Zugriff auf Informationssysteme regeln.
- Das Monitoring bezieht sich auf die Überwachung von Systemen und Prozessen.
- Das Incident Management bezieht sich auf die Prozesse zur Reaktion auf Sicherheitsvorfälle.
- Das Request Management bezieht sich auf die Verwaltung von Anfragen innerhalb des Unternehmens.
- Die Datensicherung bezieht sich auf die Prozesse und Technologien zur Sicherung von Daten.
- Das Notfallmanagement bezieht sich auf die Pläne und Prozesse zur Bewältigung von Notfällen.
- Die IT-Sicherheitsvorfälle beziehen sich auf die Verwaltung und Reaktion auf IT-Sicherheitsvorfälle.
- Das Datenschutzmanagement System umfasst Systeme und Prozesse zur Gewährleistung des Datenschutzes.
- Die Sicherheitskonzeption und das Sicherheitsmonitoring beziehen sich auf die Planung und Überwachung von Sicherheitsmaßnahmen.

Das Business Continuity Management bezieht sich auf die Strategien zur Sicherstellung der Geschäftskontinuität.

Jede dieser Untergruppen trägt zur Aufrechterhaltung der Integrität, Vertraulichkeit und Verfügbarkeit von Unternehmensinformationen und -systemen bei.

In den folgenden Abschnitten werden wir jede dieser Untergruppen im Detail darstellen.

## Kontrollen zur **Prüfung des Change Managements**

| Kontrolle | Kontrollziel |
|---|---|
| 1. | Anträge zur Änderung von IT-Systemen sind in geordneter Art und Weise aufzunehmen, zu dokumentieren, unter Berücksichtigung möglicher Umsetzungsrisiken zu bewerten, zu priorisieren, zu genehmigen sowie koordiniert und sicher umzusetzen (BAIT.49). Alle notwendigen Aufgaben sollten gemäß den Vorgaben geplant werden. |
| 2. | Im Rahmen der Anwendungsentwicklung ist die Anwendung übersichtlich und für sachkundige Dritte nachvollziehbar zu dokumentieren (BAIT.40).<br>Insbesondere:<br>_ Ein Versionsmanagement des Programmquellcodes ist implementiert und der Prozess wird eingehalten.<br>_ Es gibt eine aktuelle System-/Entwicklungsdokumentation. |
| 3. | Nach Produktivsetzung der Anwendung sind mögliche Abweichungen vom Regelbetrieb zu überwachen, deren Ursachen zu untersuchen und ggf. Maßnahmen zur Nachbesserung einzuleiten. |
| 4. | Die Komponenten der IT-Systeme und ihre Beziehungen zueinander müssen angemessen verwaltet werden.<br>Die erfassten Bestandsangaben sind regelmäßig und anlassbezogen zu aktualisieren. |
| 5. | Anträge zur Änderung von IT-Systemen sind in geordneter Art und Weise aufzunehmen, zu dokumentieren, unter Berücksichtigung möglicher Umsetzungsrisiken zu bewerten, zu priorisieren, zu genehmigen sowie koordiniert und sicher umzusetzen (BAIT.49). Alle notwendigen Aufgaben sollten gemäß den Vorgaben geplant werden. |

# Kontrollen zur **Prüfung des Logischen Zugriffs**

| Kontrolle | Kontrollziel |
|---|---|
| 1. | Nicht personalisierte IT-Berechtigungen müssen jederzeit eindeutig einer handelnden Person zugeordnet werden können, vorzugsweise automatisiert. Abweichungen in begründeten Ausnahmefällen sind zu genehmigen und zu dokumentieren (BAIT.25).<br>Insbesondere folgende Punkte sind im Berechtigungsmanagement zu berücksichtigen:<br>_ Es werden geeignete Verfahren für nicht personalisierte Benutzer definiert und umgesetzt, die die Anforderung, die Zuteilung und den Widerruf des Zugangsrechts abdecken.<br>_ Nicht personalisierte Benutzer sind gegen manuelles Login geschützt oder es wird sichergestellt, dass jederzeit reproduziert werden kann, von wem der nicht personalisierte Benutzer benutzt wurde. |
| 2. | Die Verfahren zur Einrichtung, Änderung, Deaktivierung oder Löschung von IT-Berechtigungen für Benutzer haben durch Genehmigungs- und Kontrollprozesse sicherzustellen, dass die Vorgaben des IT-Berechtigungskonzepts eingehalten werden. Dabei ist die fachlich verantwortliche Stelle angemessen einzubinden, damit sie ihrer fachlichen Verantwortung nachkommen kann. |
| 3. | Die Einrichtung, Änderung, Deaktivierung und Löschung von IT-Berechtigungen sowie die Rezertifizierung sind nachvollziehbar und auswertbar zu dokumentieren. |
| 4. | Durch begleitende technisch-organisatorische Maßnahmen ist einer Umgehung der Vorgaben der Berechtigungskonzepte vorzubeugen (BAIT.30). |
| 5. | Nicht personalisierte IT-Berechtigungen müssen jederzeit eindeutig einer handelnden Person zugeordnet werden können, vorzugsweise automatisiert. Abweichungen in begründeten Ausnahmefällen sind zu genehmigen und zu dokumentieren (BAIT.25).<br>Insbesondere sind folgende Punkte im Berechtigungsmanagement zu berücksichtigen:<br>_ Es werden geeignete Verfahren für nicht personalisierte Benutzer definiert und umgesetzt, die die Anforderung, die Zuteilung und den Widerruf des Zugangsrechts abdecken.<br>_ Nicht personalisierte Benutzer sind gegen manuelles Login geschützt oder es wird sichergestellt, dass jederzeit reproduziert werden kann, von wem der nicht personalisierte Benutzer benutzt wurde. |

# Kontrollen zur **Prüfung des Monitorings**

| Kontrolle | Kontrollziel |
|---|---|
| 1. | Die Meldungen über ungeplante Abweichungen vom Regelbetrieb (Störungen) und deren Ursachen sind in geeigneter Weise zu erfassen, zu bewerten, insbesondere hinsichtlich möglicherweise resultierender Risiken zu priorisieren und entsprechend festgelegten Kriterien zu eskalieren. Bearbeitung, Ursachenanalyse und Lösungsfindung inkl. Nachverfolgung sind zu dokumentieren. Ein geordneter Prozess zur Analyse möglicher Korrelationen von Störungen und deren Ursachen muss vorhanden sein. Der Bearbeitungsstand offener Meldungen über Störungen, wie auch die Angemessenheit der Bewertung und Priorisierung, ist zu überwachen und zu steuern. Ebenso sollten geeignete Kriterien für die Information der Geschäftsleitung über Störungen festgelegt werden (BAIT.50). Insbesondere werden:<br>_ IT-Systeme und/oder IT-Infrastruktur(-komponenten) überwacht. Protokolle sind verfügbar, um die Rekonstruktion zu ermöglichen und Störungen oder Leistungsprobleme zu überprüfen.<br>_ geplante Aufträge (Skripte, Chargen usw.) überwacht. Es ist geregelt, wie bei Fehlfunktionen/Jobabbrüchen vorgegangen werden soll. |
| 2. | Nach Produktivsetzung der Anwendung sind mögliche Abweichungen vom Regelbetrieb zu überwachen, deren Ursachen zu untersuchen und ggf. Maßnahmen zur Nachbesserung zu veranlassen. |

# Kontrollen zur **Prüfung des Incident Managements**

| Kontrolle | Kontrollziel |
| --- | --- |
| 1. | Die Meldungen über ungeplante Abweichungen vom Regelbetrieb (Störungen) und deren Ursachen sind in geeigneter Weise zu erfassen, zu bewerten, insbesondere hinsichtlich möglicherweise resultierender Risiken zu priorisieren und entsprechend festgelegten Kriterien zu eskalieren. Bearbeitung, Ursachenanalyse und Lösungsfindung inkl. Nachverfolgung sind zu dokumentieren. Ein geordneter Prozess zur Analyse möglicher Korrelationen von Störungen und deren Ursachen muss vorhanden sein. Der Bearbeitungsstand offener Meldungen über Störungen, wie auch die Angemessenheit der Bewertung und Priorisierung, ist zu überwachen und zu steuern. Ebenso sollten geeignete Kriterien für die Information der Geschäftsleitung über Störungen festgelegt werden (BAIT.50).<br>Insbesondere werden:<br>_ IT-Systeme und / oder IT-Infrastruktur (Komponenten) überwacht. Protokolle sind verfügbar, um die Rekonstruktion zu ermöglichen und Störungen oder Leistungsprobleme zu überprüfen.<br>_ geplante Aufträge (Skripte, Chargen usw.) überwacht. Es ist geregelt, wie bei Fehlfunktionen/Jobabbrüchen vorgegangen werden soll. |

## Kontrollen zur **Prüfung des Request Managements**

| Kontrolle | Kontrollziel |
|---|---|
| 1. | Die Meldungen über Anfragen der Nutzer sind in geeigneter Weise zu erfassen und zu bewerten. Die Bearbeitung und Lösungen inklusive Nachverfolgung sind zu dokumentieren. Der Bearbeitungsstand offener Meldungen über Anfragen ist zu überwachen und zu steuern. |

## Kontrollen zur **Prüfung der Datensicherung**

| Kontrolle | Kontrollziel |
|---|---|
| 1. | Die Backups sind vollständig durchgeführt. Abgebrochene Backups werden entdeckt und angemessene Maßnahmen eingeleitet. |

## Kontrollen zur **Prüfung des Notfallmanagements**

| Kontrolle | Kontrollziel |
|---|---|
| 1. | Für Notfälle in zeitkritischen Aktivitäten und Prozessen ist Vorsorge zu treffen (Notfallkonzept). Die im Notfallkonzept festgelegten Maßnahmen müssen dazu geeignet sein, das Ausmaß möglicher Schäden zu reduzieren. Die Wirksamkeit und Angemessenheit des Notfallkonzeptes ist regelmäßig durch Notfalltests zu überprüfen. Die Ergebnisse der Notfalltests sind den jeweiligen Verantwortlichen mitzuteilen. Im Fall der Auslagerung von zeitkritischen Aktivitäten und Prozessen haben das auslagernde Institut und das Auslagerungsunternehmen über aufeinander abgestimmte Notfallkonzepte zu verfügen. Insbesondere wird das Disaster Recovery regelmäßig getestet. |

## Kontrollen zur **Prüfung zum Umgang mit IT-Sicherheitsvorfällen**

| | Kontrolle | Kontrollziel |
|---|---|---|
| 1. | | Nach einem Informationssicherheitsvorfall sind die Auswirkungen auf die Informations-sicherheit zu analysieren und angemessene Nachsorgemaßnahmen zu veranlassen. |

## Kontrollen zur **Prüfung des Datenschutzmanagement Systems**

| | Kontrolle | Kontrollziel |
|---|---|---|
| 1. | | Für die eingesetzten Subdienstleister sind angemessene Auftragsdatenverarbeitungsvereinbarungen (ADV-Vereinbarungen) geschlossen. |
| 2. | | Ein Datenschutzbeauftragter ist bestellt, der regelmäßig Datenschutzberichte erstellt und kommuniziert. Das Unternehmen verfügt über Prozesse und Vorgaben hinsichtlich der Identifikation und der internen Meldung von Datenschutzvorfällen bzw. -verstößen. Außerdem wurde ein Maßregelungsprozess während der Beschäftigung bei Informationssicherheitsverstößen eingerichtet. Es sind Prozesse und Vorgaben zur externen Meldung (an die Behörden und an den Kunden) von Datenschutzverstößen implementiert. Bei den Mitarbeitern wird durch geeignete Maßnahmen ein hinreichendes Level an Awareness bezüglich Datenschutzanforderungen,-vorgaben und -prozessen erzielt. |
| 3. | | Die Büroräume verfügen über einen dem Schutzbedarf angemessenen Zutrittsschutz. Die in den Büroräumen befindliche Ausstattung ist angemessen gesichert. |
| 4. | | Sofern unterjährig interne oder externe Prüfungen hinsichtlich der Umsetzung von EU-DSGVO-Anforderungen durchgeführt wurden: Das Management hat die Auditergebnisse anerkannt und für identifizierte Defizite wurden Maßnahmen definiert. |

# Kontrollen zur **Prüfung der Sicherheitskonzeption und des Sicherheitsmonitorings**

| Kontrolle | Kontrollziel |
|---|---|
| 1. | Es besteht ein aktuell gültiger Satz an Informations-sicherheitsrichtlinien. Die Mitarbeiter werden hierüber angemessen informiert.<br>Ein aktuelles Sicherheitskonzept liegt vor. Ein unabhängiger Informationssicherheitsbeauftragter ist bestellt und in der Organisation angemessen eingeordnet. Es werden Informationssicherheitsreportings an die Geschäftsleitung in angemessener Frequenz durchgeführt. |
| 2. | Vor der Anstellung eines neuen Mitarbeiters bzw. vor einem Abteilungswechsel, werden unter Berücksichtigung der geltenden Vorschriften und Gesetze als auch basierend auf den Anforderungen der Aufgaben und der Funktionen entsprechende Überprüfungen durchgeführt.<br>Siehe auch Kontrolle in Personalsicherheit. |
| 3. | Im Fall des Verstoßes gegen Sicherheitsvorgaben sind Prozesse und Vorgaben hinsichtlich der Durchführung disziplinarischer Maßnahmen implementiert. |
| 4. | Der Abschluss einer Vertraulichkeits- oder Geheimhaltungsvereinbarungen muss dann erfolgen, sobald Informationen mit Vertraulichkeit „hoch“ ausgetauscht werden. |
| 5. | IT-Risiken werden identifiziert, bewertet und überwacht. |
| 6. | Sub-Outsourcings beim Dienstanbieter werden identifiziert. Die Überwachungen und Steuerung von Sub-Outsourcings werden sichergestellt. |
| 7. | Die Personalsicherheit wird allgemein und unabhängig einer zeitlichen Zuordnung zum Beschäftigungsstatus eines Mitarbeiters gewährleistet. |

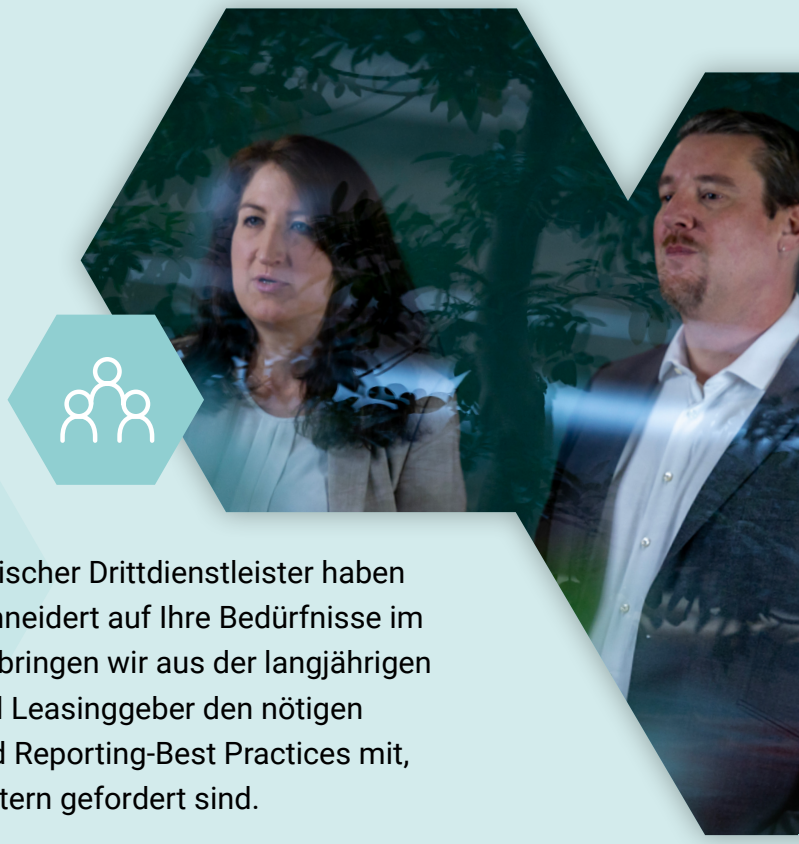
| Kontrolle | Kontrollziel |
| --- | --- |
| 8. | Neue Mitarbeiter sind für die vorgesehenen Rollen und Aufgaben geeignet und verstehen diese. |
| 9. | Beschäftigungs- und Vertragsbedingungen stellen sicher, dass die Informations-sicherheitsziele des Kunden sowie die damit einhergehenden Verantwortlichkeiten klar benannt werden. |
| 10. | Während der Beschäftigung ist sicher-gestellt, dass sich Auftragnehmer ihren Verantwortlichkeiten in der Informationssicherheit bewusst sind und diesen nachkommen. |
| 11. | Es ist sichergestellt, dass nach Beendigung oder bei Änderung der Beschäftigung dem Mitarbeiter der Zugang zu nicht mehr relevanten Informationen entzogen wird. |
| 12. | Sicherheitsüberprüfungen von Personal erfüllen alle relevanten Anforderungen. |
| 13. | Neue Mitarbeiter sind für die vorgesehenen Rollen und Aufgaben geeignet und verstehen diese. |
| 14. | Unbefugte Einsichtnahme ist verhindert. |
| 15. | Unbefugten ist der Zutritt zu Gebäuden und Räumlichkeiten verwehrt. Der physische Zugang zu den vorhandenen Assets darf nur für berechtigte Personen möglich sein |
| 16. | Zielsetzung ist die Ableitung von angemessenen Schutzmaßnahmen. Diese sind notwendig, um Informationssicherheits- und Datenschutzrisiken zu steuern. |
| 17. | Informationen werden nur nach Freigabe durch den Kunden veröffentlicht. |

# Kontrollen zur **Prüfung des Business Continuity Managements**

| Kontrolle | Kontrollziel |
|---|---|
| 1. | BCM* / ITSCM** Leitlinie ist definiert und Geschäftsführungs-verantwortung liegt vor. Prozesse für BCM/ITSCM sind etabliert. BCM/ITSCM Management Bericht für Geschäftsführung liegt vor. |
| 2. | BCM/ITSCM Leitlinie wird regelmäßig aktualisiert und geprüft. |
| 3. | BCM/ITSCM Aufbauorganisation, Rollen, Stellenbeschreibungen und zuständiger Notfallmanager/Business Continuity Manager sind definiert. Für alle BCM/ITSCM Rollen sind qualifizierte Personen benannt. BCM/ITSCM wird jährlich auf Angemessenheit geprüft und Aktualisierungen umgesetzt. |
| 4. | Ausreichende Ressourcenplanung für BCM/ITSCM liegt vor und Schnittstellen zu BCM/ITSCM sind festgestellt. |
| 5. | Schulungs- und Sensibilisierungsprogramm für BCM/ITSCM liegt vor. |
| 6. | Für den IT-Betrieb ist ein Notfallplan (Business Continuity Plan) zu erstellen, der die Fortführung der IT-Betriebsprozesse bei einem Nicht-IT-Ausfallszenario (bspw. Ausfall Standort, Ausfall Personal, Ausfall Dienstleister) sicherstellt. |

* BCM: Business Continuity
** ITSCM: IT- Service-Continuity-Management

# 8. **7P – Ihr Partner** für anspruchsvolle **IT-Anforderungen** in regulierten Umgebungen



7P ist der perfekte Partner für Sie: Als mittelständischer Drittdienstleister haben wir die optimale Größe, um flexibel und maßgeschneidert auf Ihre Bedürfnisse im regulierten Umfeld einzugehen – und gleichzeitig bringen wir aus der langjährigen Zusammenarbeit mit Banken, Versicherungen und Leasinggeber den nötigen Risikomanagementrahmen und die Strukturen und Reporting-Best Practices mit, die für die Zusammenarbeit mit IKT-Drittdienstleistern gefordert sind.

Mit unseren **450 Experten** bieten wir individuelle Managed IT Services, Softwareentwicklung mit und ohne mobile Frontends und strategische und operative Begleitung im Rahmen Ihrer agilen Transformation.

Unsere **Fachkenntnisse im Compliance-Umfeld** umfassen DORA, MaRisk (BAIT, VAIT, XAIT) und wir sind ISO27001 und ISO9001 zertifiziert.

Ein internes **Kontrollsystem und Reporting nach ISAE 3402** garantieren Qualität und Transparenz.

Durch den Einsatz von KI-Tools überwachen und sichern wir unsere Services proaktiv. Mit einer 100%-igen Tochtergesellschaft in Portugal operieren wir mittlerweile auch im Mixed-Modell aus dem EU-Rechtsraum, was uns ermöglicht, auf einen größeren Expertenpool zuzugreifen und trotzdem die etablierten Standards zu gewährleisten.

Wählen Sie 7P, um für sich einen IKT-Drittdienstleister an Board zu holen, der operative Erfahrung hat in der Zusammenarbeit mit BaFin-regulierten Instituten und mit dem Sie bestens aufgestellt sind, um auch künftig auch unter strengsten Anforderungen, die Leistungserbringung in Ihrer IT auszulagern, um eigene Ressourcen für andere wichtige Geschäftsvorhaben einzubringen.

Kontaktieren Sie uns, um zu erfahren, wie eine Zusammenarbeit aussehen kann.

**Zögern Sie nicht, uns zu kontaktieren, um mehr darüber zu erfahren, wie wir Ihnen helfen können, Ihre IT-Herausforderungen zu meistern. Wir freuen uns darauf, mit Ihnen zusammenzuarbeiten!**

SPRECHEN SIE MIT UNSEREN EXPERTEN →

# Sie möchten mehr erfahren

sowie praktische Tipps und Beispiele erhalten?

**7p-group.com**

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

WELL DONE Zertifizierungsgesellschaft mbH
DIN EN ISO 9001:2015

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