BFMT

www.bfmt.net

AUDIT · TAX · ADVISORY

IT-Outsourcing
ISAE 3402

®2025 BFMT Gruppe

IT-Outsourcing und ISAE 3402

Standards für die Finanzdienstleistungsbranche

In der heutigen digitalisierten Finanzwelt wird IT-Outsourcing zunehmend zur strategischen Notwendigkeit. Mit der Auslagerung von IT-Diensten entstehen jedoch komplexe Anforderungen an Sicherheit, Compliance und Governance.

ISAE 3402 (International Standard on Assurance Engagements) hat sich als internationaler Prüfungsstandard etabliert, der speziell für Dienstleistungsorganisationen konzipiert wurde. Er bietet einen strukturierten Rahmen zur Bewertung und Dokumentation interner Kontrollen bei ausgelagerten Prozessen.

Diese Präsentation vermittelt einen umfassenden Überblick über die Bedeutung von IT-Standards und Prüfungen im Kontext von Outsourcing-Beziehungen und erklärt, warum diese für Finanzdienstleister unverzichtbar geworden sind.

IT-Standards und Zertifizierungen Überblick

1 ISAE 3402

International etablierter Standard für die Prüfung interner Kontrollen bei Dienstleistern. Fokussiert auf die Zuverlässigkeit der Kontrollen, die für die Finanzberichterstattung des Auftraggebers relevant sind. Besonders relevant für Banken und Versicherungen.

2 ISAE 3000

Flexible Prüfungsmethodik für alle Arten von Non-Financial Assurance. Deckt Bereiche ab, die über finanzielle Aspekte hinausgehen, wie Nachhaltigkeit, Datenschutz oder spezifische regulatorische Anforderungen.

3 SOC 1/2/3

US-amerikanische Standards: SOC 1 entspricht ISAE 3402, SOC 2 fokussiert auf Sicherheit, Verfügbarkeit und Vertraulichkeit, während SOC 3 eine vereinfachte Version für öffentliche Kommunikation darstellt.

4 ISO 27001

Internationaler Standard für Informationssicherheits-Managementsysteme (ISMS). Bietet einen systematischen Ansatz zum Management vertraulicher Informationen und berücksichtigt Menschen, Prozesse und IT-Systeme.

IT-Outsourcing: Gründe & Herausforderungen

Vorteile des IT-Outsourcings

- Signifikante Kostenreduktion durch Skaleneffekte und Spezialisierung
- Verbesserte Skalierbarkeit bei schwankenden Geschäftsanforderungen
- Fokussierung auf Kernkompetenzen und strategische Initiativen
- Zugang zu Spezialwissen und neuesten Technologien
- Erhöhte Flexibilität bei sich ändernden Marktbedingungen

Regulatorische Herausforderungen

- KWG §25b: Strenge Anforderungen an die Auslagerung von Aktivitäten
- MaRisk AT 9: Risikomanagement bei ausgelagerten Aktivitäten
- BAIT: Bankaufsichtliche Anforderungen an die IT
- DORA: Digital Operational Resilience Act der EU
- Haftungsfragen bei Compliance-Verstößen und Datenschutzproblemen

ISAE 3402 als Lösung für IT-Dienstleister

1

Typ 1 Prüfung

Stichtagsbezogene Prüfung der Angemessenheit des Kontrolldesigns. Bewertet, ob Kontrollen theoretisch geeignet sind, die definierten Kontrollziele zu erreichen, ohne deren Wirksamkeit über einen Zeitraum zu testen.

2

Typ 2 Prüfung

Umfassendere Prüfung, die zusätzlich die Wirksamkeit der Kontrollen über einen definierten Zeitraum (meist 6-12 Monate) testet. Bietet höhere Sicherheit für Kunden und wird von den meisten Finanzinstituten bevorzugt.

3

Bestandteile eines Reports

Enthält Beschreibung des internen Kontrollsystems (IKS), detailliertes Kontrollset mit Prüfungsergebnissen, Management Assertion (Verantwortungserklärung) sowie ein unabhängiges Prüfungsurteil durch Wirtschaftsprüfer.

4

Vorteile für IT-Dienstleister

Wettbewerbsvorteil durch nachgewiesene Kontrollstandards, Reduzierung redundanter Kundenaudits, Verbesserung interner Prozesse sowie Aufbau von Vertrauen bei Kunden aus regulierten Branchen.

Praxisbeispiel: ISAE 3402-Implementierung

Vorbereitungsphase

Ein mittelständischer IT-Dienstleister für Banken startete mit einem Gap-Assessment.
Dabei wurden bestehende Kontrollen erfasst, dokumentiert und mit den Anforderungen des ISAE 3402 abgeglichen.
Erhebliche Lücken wurden im Bereich Change Management und Zugriffskontrollen identifiziert.

Implementierungsphase

Über sechs Monate wurden die Kontrollumgebung optimiert, Prozesse neu definiert und Mitarbeiter geschult.
Ein dediziertes Projektteam arbeitete eng mit externen Beratern zusammen, um ein robustes internes Kontrollsystem (IKS) zu etablieren.

Prüfungsphase

Nach einer dreimonatigen Stabilisierungsphase begann eine renommierte Wirtschafts-prüfungsgesellschaft mit der Typ 1-Prüfung.
Im Folgejahr erfolgte die umfassendere Typ 2-Prüfung mit über 250 Stichproben aus verschiedenen Kontrollbereichen.

Ergebnisse

Der Dienstleister konnte die Anzahl der Kundenaudits um 70% reduzieren und drei Neukunden aus dem Bankensektor gewinnen.
Die internen Prozesse wurden effizienter und die Dokumentationsqualität signifikant verbessert.

Alternative Prüfstandards im Vergleich

Standard	Fokus	Zielgruppe	Besonderheiten
ISAE 3402	Interne Kontrollen mit Einfluss auf Finanzberichterstattung	Finanzdienstleister, Outsourcing-Anbieter	International anerkannt, spezifisch für Dienstleister
ISAE 3000	Nicht-finanzielle Kontrollen, Compliance	Diverses Spektrum an Dienstleistern	Flexibler Rahmen für unterschiedliche Prüfungen
SOC 2	Sicherheit, Verfügbarkeit, Vertraulichkeit	Cloud-Provider, SaaS-Anbieter	Besonders relevant für US-Geschäft
ISO 27001	Informationssicherheit	Alle Branchen	Zertifizierung statt Prüfungsbericht
FINMA-RS	Regulatorische Anforderungen für Schweizer Finanzmarkt	Schweizer Finanzinstitute	Länderspezifische Vorgaben

Die Wahl des passenden Standards hängt maßgeblich von den regulatorischen Anforderungen der Kunden, dem geografischen Fokus und der Art der ausgelagerten Dienstleistungen ab. Viele IT-Dienstleister implementieren mehrere Standards parallel, um verschiedene Kundenanforderungen abzudecken.

Fazit & Best Practices für IT-Dienstleister

Strategie entwickeln

Ermitteln Sie den passenden Standard basierend auf Ihrer Kundenbasis und Wachstumsstrategie

Kontinuierlich verbessern

Nutzen Sie Prüfungsergebnisse für Prozessoptimierungen

Gap-Analyse durchführen

Identifizieren Sie Lücken zwischen bestehenden Kontrollen und Anforderungen

Kontrollen implementieren

Setzen Sie fehlende Kontrollen um und optimieren Sie bestehende Prozesse

Prüfung durchführen

Arbeiten Sie mit qualifizierten Wirtschaftsprüfern zusammen

ISAE 3402 hat sich als De-facto-Standard für IT-Dienstleister von Finanzinstituten etabliert.
Die Implementierung erfordert zwar erhebliche Ressourcen, bietet jedoch entscheidende Wettbewerbsvorteile und reduziert langfristig den Prüfungsaufwand.

Vielen Dank für Ihre Aufmerksamkeit!

Dr. Martin Trost
Dipl.-Math-oec. WP/StB

https://bfmt.net

+49 (0)9942 - 94951 - 0

info@bfmt.net

BFMT Audit GmbH | Flurstraße 9 | 94234 Viechtach | Deutschland