Prüfung dienstleistungsbezogener Kontrollsysteme

IT & Controls Assurance

Outsourcing ist insbesondere im Bereich der Informationstechnologie ein wachsender Trend. Nicht zuletzt aufgrund der immer stärker werdenden Komplexität von IT-Hardware, IT-Infrastrukturen und Anwendungen sowie steigenden Anforderungen an die IT-Sicherheit, nutzen immer mehr Unternehmen entsprechende Dienstleistungen (u. a. Infrastructure as a Service (IaaS), Managed Services, Software as a Service (SaaS) etc.) von externen und spezialisierten Dritten.

Aufgrund dieser Auslagerungsverhältnisse erlangt das interne Kontrollsystem der Outsourcingnehmer (dienstleistungsbezogenes Kontrollsystem) für die Beurteilung der Frage Bedeutung, ob sich aus der Ausgestaltung der Kontrollen mögliche Risiken ergeben, welche Einfluss auf die Rechnungslegung der Kunden haben können. In umgekehrter Betrachtungsweise kann ein zielführend implementiertes und entsprechend wirksames internes Kontrollsystem dem Kunden Sicherheit in Bezug auf eine ordnungsgemäße Umsetzung der ausgelagerten Services geben.

Aus diesen Gründen, inbesondere zum Nachweis wirksamer Kontrolltätigkeiten, lassen Outsourcingnehmer als Dienstleistungsunternehmen ihr internes Kontrollsystem von einem externen und unabhängigen Wirtschaftsprüfer prüfen.

Ein „must have“

Aufgrund der zunehmenden Bedeutung solcher Auslagerungsverhältnisse verlangen immer mehr Kunden von Dienstleistungsunternehmen einen Prüfbericht über das Kontrollsystem des Dienstleistungsunternehmens, um Sicherheit über die Prozesskontrollen zu erhalten.

Die Vorteile sind:

- Förderung der Reputation Ihres Unternehmens
- Unterstützung Ihrer Kunden und deren Prüfer bei der Erfüllung ihrer Prüfungspflichten
- Nachweis der Ausgestaltung und Implementierung eines Kontrollsystems auf der Grundlage eines anerkannten Kontroll-Rahmenkonzepts (z. B. Cobit, COSO)
- Unabhängige Bescheinigung des Kontrollumfeldes nach einem anerkannten Standard
- Weniger bzw. keine kundenindividuellen Prüfungen, da eine Verwertbarkeit der Prüfberichte gemäß der Standards gewährleistet.

Über uns

BDO zählt mit über 3.000 Mitarbeiterinnen und Mitarbeitern an 28 Offices zu den führenden Gesellschaften für Wirtschaftsprüfung und prüfungsnahe Dienstleistungen, Steuerberatung und wirtschaftsrechtliche Beratung sowie Advisory in Deutschland.
Die BDO AG Wirtschaftsprüfungsgesellschaft ist Gründungsmitglied von BDO International (1963), der mit heute über 115.000 Mitarbeiterinnen und Mitarbeitern in 166 Ländern einzigen weltweit tätigen Prüfungs- und Beratungsorganisation.

www.bdo.de

Kontaktieren Sie uns!

BDO AG
Wirtschaftsprüfungsgesellschaft

Markus Keil

Partner, IT & Controls Assurance
Tel.: +49 0711 34237-224
markus.keil@bdo.de

06/2024

Relevante Standards

In vielen Fällen richtet sich die Auswahl des richtigen Standards nach geographischen Kriterien: SSAE20 wird der für Dienstleistungsunternehmen mit Sitz und/oder Tätigkeiten in den USA anzuwendende Standard sein, während bei internationaler Serviceerbringung die internationalen Standards ISAE 3000 und ISAE 3402 relevant sein werden, welche sich im deutschen Standards PS 951 des IDW wiederfinden. Die Entscheidung, nach welchem Standard berichtet wird, erfolgt durch die Outsourcingnehmer oftmals in Abstimmung mit Ihrem Prüfer, welcher hier die notwendige Erfahrung in die Entscheidungsfindung einbringen kann.

ISAE 3402	ISAE 3000	SOC 1	SOC 2	IDW PS 951
Abschlussrelevante Themen (financial reporting) ▶ Kontrollen im Bereich der finanzrelevanten Geschäftsprozessverarbeitung ▶ unterstützende generelle IT-Kontrollen	Alles außer abschlussrelevante Themen; freie Wahl von Sachverhalt und Kriterien; es werden definierte Kriterienkataloge herangezogen (z.B. C5, DSGVO)	Nur abschlussrelevante Themen (financial reporting) ▶ Kontrollen im Bereich der finanzrelevanten Geschäftsprozessverarbeitung ▶ unterstützende generelle IT-Kontrollen	Vorgegebene Liste von Themen (Trust Criteria), die mit Kontrollen abzudecken sind ▶ Sicherheit (Security) ▶ Verfügbarkeit (Availablity) ▶ Vertraulichkeit (Confidentiality) ▶ Verarbeitungsintegrität (Processing Integrity) ▶ Datenschutz (Privacy)	Deutscher Standard des Instituts der Wirtschaftsprüfer (IDW) analog ISAE 3402

Beurteilung des ausgestaltungsgrades ihres Internen Kontrollsystems

Abhängig vom Ausgestaltungsgrad des Internen Kontrollsystems eines Dienstleistungsunternehmens kommen zwei Berichtstypen in Betracht:

Typ 1-Berichte über die Ausgestaltung des Kontrollsystems	Typ 2-Berichte über die Ausgestaltung des Kontrollsystems und deren Wirksamkeit
▶ Berichterstattung über die eingerichteten Kontrollen (bezogen auf einen Zeitpunkt)	▶ Berichterstattung über die Ausgestaltung des Kontrollsystems und die Prüfung der Wirksamkeit (i.d.R. für einen Zeitraum zwischen sechs und 12 Monaten)
▶ Betrachtung des Bestehens und der Ausgestaltung der Kontrollen – keine Untersuchung ihrer Wirksamkeit	▶ Unterscheidungskriterium: beinhaltet Prüfung der Wirksamkeit
▶ Verwendung nur zu Informationszwecken	▶ Stärkerer Schwerpunkt auf Prüfungsnachweisen
▶ Keine Verwendung durch andere Prüfer zur Erhöhung der Prüfungssichheit	▶ Erfordert höheren internen und externen Arbeitsaufwand
▶ Grundsätzlich durchgeführt im ersten Jahr, in dem das Dienstleistungsunternehmen eine Untersuchung durchführen lässt	▶ Möglichkeit der Verwendung durch andere Prüfer als Grundlage für die Reduktion ihrer Prüfungshandlungen beim Dienstleistungsunternehmen

Ein Typ 1 Bericht deckt die zu einem bestimmten Zeitpunkt implementiertenKontrollen ab und ist nur von eingeschränktem Nutzen, da er nicht die Wirksamkeit der eingerichteten Kontrollen prüft (Design-Prüfung).

Ein Typ 2 Bericht deckt die Ausgestaltung des Kontrollsystems und die Prüfung der Wirksamkeit der Kontrollen für eine Zeitperiode (i.d.R. zwischen sechs und 12 Monate) ab. Diese Berichtsform kann durch Kunden des Dienstleistungsunternehmens und deren Abschlussprüfer zur Gewinnung von Kontrollsicherheit im Rahmen einer Abschlussprüfung verwendet werden, da ein Typ 2 Bericht Prüfunghandlungen zur Beurteilung der Wirksamkeit von Kontrollen und die entsprechenden Prüfungsergebnisse enthält.

Der BDO Prüfungsansatz

Insbesondere bei Erstprüfungen hat sich unser stufenweiser Prüfungsansatz bewährt. Neben der Entwicklung eines internen Kontrollsystems (Kontrollmatrix sowie textuelle Beschreibung des internen Kontrollsystems) ist insbesondere der zu prüfende Scope bzw. Service zu berücksichtigen und abzugrenzen. Im Weiteren sind die aus Dienstleistersicht ergänzend zu erwartenden Kontrollen beim Outsourcinggeber zu definieren. Im Rahmen einer vorläufigen Beurteilung (Preliminary assessment) können die Voraussetzungen für eine spätere Prüfung aufgenommen und beurteilt werden, bevor die eigentliche Phase der Prüfungsdurchführung dann angegangen wird. Wir sind überzeugt davon, dass wir unseren Prüfungsansatz sowie unsere Erfahrungen in der Durchführung von Kontrollprüfungen bei Dienstleistungsunternehmen auch bei Ihnen unter Beweis stellen können.

BDO Prüfungsansatz