IT-Prüfungsstandard 1001 – AuditCharter

Die Besonderheiten einer Prüfung von Informationssystemen und die Kenntnisse, die zur Durchführung solcher Prüfungen erforderlich sind, erfordern spezifische Berufsgrundlagen für IT-Prüfungen. Das Entwickeln und Verbreiten von IT-Prüfungsstandards ist ein Hauptanliegen des Engagements der ISACA® im Prüfungswesen.

In den IT-Prüfungsstandards werden verpflichtende Anforderungen für IT-Prüfungen sowie die Berichterstattung definiert. Zudem informieren sie:

- IT-Prüfer über die Mindestanforderungen, die erfüllt werden müssen, um den berufsständischen Verpflichtungen gemäß des Ethik-Kodex der ISACA (ISACA Code of Professional Ethics for IS Auditors) zu entsprechen
- Führungskräfte und andere interessierte Stellen über die Erwartungen des Berufsstandes, die an die Arbeit von IT-Prüfern gestellt werden
- Inhaber des Certified Information Systems Auditor®- (CISA®-)Zertifikats über die mit diesem Titel verbundenen Anforderungen. Die Nichtbeachtung dieser Berufsgrundlagen kann zu einer Untersuchung des Verhaltens des CISAs durch das ISACA Board of Directors oder das zuständige Komitee und letztendlich zur Verhängung von Disziplinarmaßnahmen führen

IT-Prüfer sollen an geeigneter Stelle ihrer Arbeit eine Erklärung abgeben, dass der Auftrag in Übereinstimmung mit den IT-Prüfungsstandards der ISACA oder mit anderen geeigneten Berufsgrundlagen durchgeführt wurde.

Das ITAF™-Rahmenwerk für IT-Prüfer umfasst Richtlinien auf mehreren Ebenen:

- **Standards**, die in drei Kategorien eingeteilt sind:
  - Allgemeine Standards (1000er-Serie) – Dies sind die Prinzipien, nach denen IT-Prüfer arbeiten. Sie gelten für das Durchführen aller Aufträge und beschäftigen sich mit der Ethik, Unabhängigkeit, Objektivität und Sorgfaltspflicht der IT-Prüfer ebenso wie mit deren Wissen, Kompetenz und Fähigkeit. Die Angaben der Standards (**fett** gedruckt) sind verpflichtend.
  - Ausführungsstandards (1200er-Serie) – Diese beschäftigen sich mit der Durchführung des Prüfungsvorhabens hinsichtlich Planung und Beaufsichtigung, Definieren des Auftragsumfangs, Risiken, Wesentlichkeit, Ressourceneinsatz, Überwachung und Leitung der Aufträge, Prüfnachweisen sowie der Ausübung berufsüblicher Urteilsbildung und Sorgfalt.
  - Berichterstattungsstandards (1400er-Serie) – Diese behandeln Berichtstypen, Kommunikationswege und kommunizierte Informationen.
- **Richtlinien** unterstützen die Standards und sind ebenfalls in drei Kategorien eingeteilt:
  - Allgemeine Richtlinien (2000er-Serie)
  - Ausführungsrichtlinien (2200er-Serie)
  - Berichterstattungsrichtlinien (2400er-Serie)
- **Instrumente und Methoden**, die den IT-Prüfern weitere Anleitungen bereitstellen, z. B. Whitepaper, IT-Prüfprogramme sowie die COBIT® 5-Produktfamilie

Ein Onlineglossar der im ITAF verwendeten Begriffe finden Sie unter www.isaca.org/glossary.

Hinweis/Haftungsausschluss: Die ISACA beschreibt in diesem Dokument die Mindestanforderungen, die erforderlich sind, um der berufsständischen Verantwortung gemäß der im Ethik-Kodex der ISACA aufgeführten Anforderungen zu entsprechen. Die ISACA übernimmt keinerlei Gewähr, dass die Verwendung dieses Dokuments stets zu den gewünschten Ergebnissen führen wird. Die in diesem Dokument enthaltenen Informationen sollten nicht dahingehend ausgelegt werden, dass sie die ordnungsgemäßen Verfahren und Prüfmethoden abschließend darstellen und dass andere angemessene Verfahren und Prüfmethoden, mit denen dieselben Ergebnisse erzielt werden können, ausgeschlossen werden sollen. Bei der Überlegung, wie angemessen ein bestimmtes Verfahren oder eine Prüfmethode ist, sollten die Anwender sich vornehmlich auf ihre fachliche Kompetenz stützen und die spezifischen Umstände, die sich aus den Kontrollen des jeweiligen Systems oder der IT-Umgebung ergeben, berücksichtigen.

Das ISACA Professional Standards and Career Management Committee (PSCMC) verpflichtet sich bei der Erstellung von Standards und Leitlinien zu einer breiten Anhörung. Vor der Freigabe jedes Dokuments wird der Entwurf weltweit zur öffentlichen Kommentierung bereitgestellt. Zudem können Kommentare direkt an den Director of Professional Standards Development gerichtet werden: per E-Mail (standards@isaca.org), Fax (+1.847. 253.1443) oder auf dem Postweg (ISACA International Headquarters, 3701 Algonquin Road, Suite 1010, Rolling Meadows, IL 60008-3105, USA).

IT-Prüfungsstandard 1001 – AuditCharter

Aussagen

1001.1 Die IT-Revision muss ihre Organisation angemessen in einer AuditCharter dokumentieren, die Zweck, Verantwortungsbereich, Kompetenzen und Verantwortlichkeit bestimmt.

1001.2 Die IT-Revision muss die AuditCharter auf der angemessenen Organisationsebene abstimmen und genehmigen lassen.

Wichtige Aspekte

Die IT-Revision sollte:

- eine AuditCharter erstellen, welche die Aktivitäten der internen IT-Revision hinreichend detailliert definiert und die folgenden Punkte kommuniziert:
  - DieKompetenzen, den Zweck, die Verantwortlichkeiten und Beschränkungen der IT-Revision
  - Die Unabhängigkeit und Verantwortlichkeit der IT-Revision
  - Die Rollen und Verantwortlichkeiten der geprüften Stellen im Rahmen der Durchführung einer IT-Prüfung oder eines Bestätigungsauftrags
  - Berufsgrundlagen, die von den IT-Prüfern beim Durchführen einer IT-Prüfung oder eines Auftrags angewendet werden
- die AuditCharter mindestens jährlich, beim Wechsel von Verantwortlichkeiten auch öfter überprüfen.
- die AuditCharter falls erforderlich aktualisieren, um sicherzustellen, dass Zweck und Verantwortlichkeiten ordnungsgemäß dokumentiert waren und bleiben.
- die AuditCharter den zu prüfenden Stellenim Rahmen jeder IT-Prüfung oder jedes Auftrags formell kommunizieren.

Begriffe

Begriff	Definition
Bestätigungsauftrag	Eine objektive Untersuchung von Nachweisen zum Zweckder Beurteilungvon Risikomanagement-, Kontroll- oder Führungsprozessender Organisation. Hinweis zum Anwendungsbereich: Beispiele sind Finanz-, Programm-, Compliance- und Systemsicherheitsbeurteilungen.
AuditCharter	Ein Dokument, das von der Unternehmensleitung genehmigt ist und das den Zweck, die Kompetenzen und die Verantwortung einer internen Revisionsfunktion definiert. Die Charter sollte: • die Position der internen Revisionsfunktion in der Organisation bestimmen • den Zugriff auf die für die Durchführung der IT-Prüfungen und Aufträge erforderlichen Daten, Mitarbeiter und Infrastruktur autorisieren • den Tätigkeitsbereich der Revisionsfunktion festlegen
Auftrag	Ein Prüfungsvorhaben, eine Aufgabe oder Tätigkeit wie z. B. eine Prüfung, eine Selbstbeurteilung des Kontrollsystems, eine Betrugsermittlung oder ein Beratungsauftrag.

	Ein Auftrag kann mehrere Aufgaben oder Tätigkeitenzum Erreichen zusammengehöriger Zielsetzungen umfassen.
Unabhängigkeit	Das Fehlen von Bedingungen, die die Objektivität tatsächlich oder dem Anschein nach beeinträchtigen. Derartige Gefährdungen der Objektivität müssen auf Prüfer-, Auftrags-, Funktions- und Organisationsebene gehandhabt werden. Die Unabhängigkeit umfasst die persönliche Unvoreingenommenheit ebenso wie das unabhängige Auftreten.

Verknüpfung zu den Richtlinien

Typ	**Bezeichnung**
Richtlinie	2001 – AuditCharter

Zeitpunkt des Inkrafttretens

Dieser ISACA-Standard gilt für alle IT-Prüfungen und Aufträge, die ab dem 01. November 2013 beginnen.

