IT-Prüfungsstandard 1401 – Berichterstattung

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).

Aussagen

1401.1 **IT-Prüfer müssen einen Bericht erstellen, um die Ergebnisse beim Abschluss des Auftrags zu kommunizieren, darunter:**

- **Benennen der geprüften Organisation, der vorgesehenen Empfänger sowie jeglicher Inhalts- und Verbreitungsbeschränkungen**
- **Umfang, Ziele und Betrachtungszeitraum des Auftrags sowie Art, Zeitraum und Umfang der durchgeführten Arbeiten**
- **Feststellungen, Schlussfolgerungen und Empfehlungen**
- **Alle Einschränkungen oder Beschränkungen des Prüfungsumfangs, denen der IT-Prüfer hinsichtlich des Auftrags unterliegt**
- **Unterschrift, Datum und Verteiler in Übereinstimmung mit den Bestimmungen der Audit Charter oder der Auftragsvereinbarung**

1401.2 **IT-Prüfer müssen sicherstellen, dass die Feststellungen im Prüfbericht durch ausreichende und geeignete Nachweise belegt sind.**

Kernaspekte

IT-Prüfer sollten:

- von der zu prüfenden Einheit relevante schriftliche Darstellungen beschaffen, in denen wichtige Bereiche des Auftrags, aufgetretene Probleme und deren Lösungen sowie die von der zu prüfenden Einheit getroffenen Aussagen ausführlich aufgeführt werden.
- sicherstellen, dass die Darstellungen der zu prüfenden Einheit unterschrieben und datiert wurden, um die Anerkennung der Verantwortung der zu prüfenden Einheit im Rahmen des Auftrags festzuhalten.
- jegliche schriftliche oder mündliche Darstellungen in den Arbeitspapieren festhalten, die sie im Rahmen der Durchführung des Auftrags erhalten haben. Für Bestätigungsaufträge müssen Erklärungen der zu prüfenden Einheit schriftlich beschafft werden, um potenzielle Missverständnisse auszuschließen.
- die Form und den Inhalt des Berichts so anpassen, dass dieser dem durchgeführten Auftragstyp entspricht, z. B.:
  - Prüfung (direkt oder als Teil eines Bestätigungsauftrags)
  - Gutachten oder Untersuchungen (direkt oder als Teil eines Bestätigungsauftrags)
  - Prüfungshandlungen gemäß Vereinbarung
- die wesentlichen Mängel oder bedeutsamen Schwachstellen sowie deren Auswirkung auf das Erreichen der Auftragsziele im Bericht beschreiben.
- den Berichtsentwurf mit den jeweils verantwortlichen Führungskräften vor der Fertigstellung und Freigabe besprechen und, sofern angemessen, deren Rückmeldung zu den Feststellungen, Schlussfolgerungen und Empfehlungen in die endgültige Fassung des Berichts aufnehmen.
- bedeutsame Schwachstellen und wesentliche Mängel des Kontrollumfelds an die Leitungs- und Aufsichtsorgane und, sofern relevant, Aufsichtsbehörden kommunizieren. Im Bericht ist offenzulegen, dass diese Kontrollschwächen kommuniziert wurden.
- im endgültigen Bericht auf weitere gesonderte Berichte verweisen.
- die Führungskräfte der zu prüfenden Einheit auf Kontrollmängel hinweisen, die zwar nicht bedeutsam, jedoch mehr als vernachlässigbar sind. In solchen Fällen sollten die Leitungs- und Aufsichtsorgane oder die zuständigen Aufsichtsbehörden

darauf hingewiesen werden, dass die Führungskräfte der zu prüfenden Einheit über solche Mängel des Internen Kontrollsystems informiert wurden.
- die bei der Durchführung des Auftrags verwendeten Berufsgrundlagen benennen und gegebenenfalls das Abweichen von diesen Berufsgrundlagen kommunizieren.

Begriffe

Begriff	Definition
Relevante Informationen	In Bezug auf Kontrollen erfährt der Prüfer Aussagekräftiges über die Durchführung der zu Grunde liegenden Kontrollen oder Kontrollkomponenten. Informationen, welche die Durchführung von Kontrollen direkt bestätigen, sind besonders relevant. Auch Informationen, die sich indirekt auf die Durchführung von Kontrollen beziehen, können relevant sein, jedoch weniger als direkte Informationen. Wir verweisen dazu auf die COBIT 5-Informationsqualitätsziele
Zuverlässige Informationen	Genaue, verifizierbare Informationen, die aus einer objektiven Quelle stammen. Wir verweisen dazu auf die COBIT 5-Informationsqualitätsziele
Ausreichende Informationen	Informationen sind ausreichend, wenn Prüfer daraus eine begründete Schlussfolgerung ziehen können. Damit Informationen ausreichend sein können, müssen Informationen zunächst geeignet sein. Wir verweisen dazu auf die COBIT 5-Informationsqualitätsziele
Geeignete Informationen	Relevante (d. h. für den vorgesehenen Zweck geeignete), zuverlässige (d. h. genaue, verifizierbare und von einer objektiven Quelle stammende) und rechtzeitige (d. h. in einem angemessenen Zeitrahmen erstellte und verwendete) Informationen. Wir verweisen dazu auf die COBIT 5-Informationsqualitätsziele
Rechtzeitige Informationen	Informationen, die in einem Zeitraum erstellt und verwendet werden, der es ermöglicht, Kontrollschwächen zu verhindern oder zu erkennen, bevor diese für eine Organisation wesentlich werden. Wir verweisen dazu auf die COBIT 5-Informationsqualitätsziele

Verknüpfung zu den Standards und Richtlinien

Typ	Bezeichnung
Richtlinie	2401 – Berichterstattung

Zeitpunkt des Inkrafttretens

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

