IT-Prüfungsstandard 1203 –Durchführung und Überwachung

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 1203 – Durchführung und Überwachung

Aussagen

1203.1 **IT-Prüfer müssen ihre Arbeit in Übereinstimmung mit dem genehmigten IT-Prüfungsplan durchführen, um erkannte Risiken abzudecken, und den vereinbarten Umfang einhalten.**

1203.2 **IT-Prüfer müssen diejenigen IT-Prüfungsmitarbeiter beaufsichtigen, die ihrer Aufsichtspflicht unterstehen, um die Prüfziele zu erreichen und die geltenden Prüfungsstandards einzuhalten.**

1203.3 **IT-Prüfer dürfen nur Aufgaben übernehmen, die ihren Kenntnissen und Fähigkeiten entsprechen oder bei denen davon ausgegangen werden kann, dass die Fähigkeiten im Verlauf der Beauftragung erlangt oder die Aufgaben mit entsprechender Aufsicht erfolgreich durchgeführt werden können.**

1203.4 **IT-Prüfer müssen ausreichende und angemessene Nachweise für das Erreichen der Prüfungsziele beschaffen. Die Prüfungsfeststellungen und Schlussfolgerungen müssen durch entsprechende Analyse und Interpretation dieser Nachweise gestützt werden.**

1203.5 **IT-Prüfer müssen den Prüfungsablauf dokumentieren, indem sie die Prüfungstätigkeiten und die Prüfungsnachweise beschreiben, auf denen die Feststellungen und Schlussfolgerungen beruhen.**

1203.6 **IT-Prüfer müssen Feststellungen treffen und entsprechende Schlussfolgerungen daraus ableiten.**

Wichtige Aspekte

IT-Prüfer sollten:

- Teammitglieder anhand deren Fähigkeiten und Erfahrungen in Übereinstimmung mit den Auftragsanforderungen festlegen.
- das IT-Prüfungsteam wo erforderlich um externe Ressourcen erweitern und sicherstellen, dass deren Arbeit ordnungsgemäß überwacht wird.
- die Funktionen und Verantwortlichkeiten der einzelnen Mitglieder des IT-Prüfungsteams im Verlauf des gesamten Auftrags steuern und hierbei mindestens Folgendes berücksichtigen:
  - Ausführende und überprüfende Funktionen
  - Verantwortlichkeit für die Entwicklung der Methodik und Vorgehensweise
  - Erstellung des Prüfungsprogramms
  - Durchführung der Aufgaben
  - Umgang mit auftretenden Fragen und Problemen
  - Dokumentation und Abstimmung der Feststellungen
  - Schreiben des Berichts
- jede durchgeführte Arbeit eines Teammitglieds von einem geeigneten anderen Teammitglied überprüfen lassen.
- die besten Prüfnachweise verwenden, die verfügbar sind. Sie sollten der Bedeutung des Prüfungsziels sowie dem Zeit- und Arbeitsaufwand für die Beschaffung entsprechen.

Wichtige Aspekte

Fortsetzung

- zusätzliche Nachweise beschaffen, wenn die vorliegenden Nachweise in fachlicher Hinsicht nicht geeignet sind, um eine Aussage zu treffen oder die Feststellungen und Schlussfolgerungen zu untermauern.
- anhand vordefinierter, dokumentierter und genehmigter Verfahren die im Rahmen der Beauftragung durchgeführten Aufgaben organisieren und dokumentieren.
- folgende Elemente in die Dokumentation aufnehmen:
  - Prüfungsziele und -umfang, Prüfungsprogramm, durchgeführte Prüfungsschritte, eingeholte Nachweise, Feststellungen, Schlussfolgerungen und Empfehlungen
  - Ausreichende Details, anhand derer ein sachverständiger, informierter Dritter die im Rahmen des Auftrags durchgeführten Arbeiten nachvollziehen und zum selben Ergebnis gelangen kann
  - Angaben zu den ausführenden Personen und ihren Rollen bei der Erstellung und Überprüfung der Dokumentation
  - Datum der Erstellung und Überprüfung der Dokumentation
- von der zu prüfenden Einheit schriftliche Darstellungen zu kritischen Bereichen des Auftrags, aufgetretenen Problemen und deren Lösung sowie getroffenen Aussagenbeschaffen.
- sicherstellen, dass die Darstellungen der zu prüfenden Einheit unterschrieben und mit einem Datum versehen wurden, um die Übernahme der Verantwortung in Bezug auf den Auftrag zu bestätigen.
- in den Arbeitspapieren jegliche schriftlichen oder mündlichen Darstellungen dokumentieren und aufbewahren, die sie im Rahmen der Durchführung des Auftrags erhalten haben.

Verknüpfung zu den Standards und Richtlinien

Typ	**Bezeichnung**
Standard	1005 – Berufsübliche Sorgfalt
Standard	1205 – Nachweise
Standard	1401 – Berichterstattung
Richtlinie	2202 – Risikoorientierte Planung

Zeitpunkt des Inkrafttretens

Dieser ISACA-Standard gilt für alle IT-Prüfungen und Aufträge, die nach dem 1. November 2013 beginnen.