IT-Prüfungsstandard 1201 – Auftragsplanung

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

1201.1 Bei der Planung von IT-Prüfungen müssen IT-Prüfer folgende Punkte berücksichtigen:

- **Ziel(e), Umfang, Zeitrahmen und Arbeitsergebnisse**
- **Einhaltung der geltenden Gesetze und Prüfungsstandards**
- **Gegebenenfalls Verwendung eines risikobasierten Ansatzes**
- **Auftragsspezifische Themen**
- **Anforderungen an die Dokumentation und Berichterstattung**

1201.2 IT-Prüfer müssen einen Projektplan für IT-Prüfungen entwickeln und dokumentieren, der Folgendes darstellt:

- **Art des Auftrags, Ziele, Zeitrahmen und benötigte Ressourcen**
- **Zeitplan und Umfang der Prüfungshandlungen**

Wichtige Aspekte

IT-Prüfer sollten:

- sich mit der zu prüfenden Aktivität vertraut machen. Der Umfang der erforderlichen Kenntnisse sollte anhand der Art des Unternehmens, des Umfelds, der Risikobereiche und der Auftragsziele ermittelt werden.
- die von Regierungen oder Branchen veröffentlichten Gesetze, Bestimmungen, Vorschriften, Richtlinien und Verlautbarungen als Vorgabe oder Richtungsweisung in Bezug auf den Prüfungsgegenstand berücksichtigen.
- eine Risikobeurteilung durchführen, um angemessene Sicherheit zu erlangen, dass im Rahmen des Auftrags alle wesentlichen Aspekte Berücksichtigung finden. Darauf aufbauend können die Prüfstrategie, Wesentlichkeitsgrade und Ressourcenanforderungen erarbeitet werden.
- den Projektplan unter Verwendung geeigneter Projektmanagementverfahren erstellen, um zu gewährleisten, dass der zeitliche und finanzielle Rahmen eingehalten wird.
- auftragsspezifische Aspekte im Plan berücksichtigen wie z. B.:
  - Verfügbarkeit von Ressourcen mit entsprechendem Wissen, Fähigkeiten und Erfahrung
  - Auswahl von Hilfsmitteln für die Beschaffung von Prüfungsnachweisen, die Durchführung von Tests und das Vorbereiten/Zusammenfassen der Informationen für die Berichterstattung
  - Anzuwendende Bewertungskriterien
  - Anforderungen an die Berichterstattung und -verteilung
- den Projektplan für den IT-Prüfungsauftrag so dokumentieren, dass folgende Aspekte deutlich werden:
  - Ziel(e), Umfang und Zeitrahmen
  - Ressourcen
  - Rollen und Verantwortlichkeiten
  - Identifizierte Risikobereiche und deren Auswirkungen auf die Auftragsplanung
  - Zu verwendende Hilfsmittel und Methoden
  - Durchzuführende Interviews zur Aufnahme der Sachverhalte
  - Zu beschaffende relevante Informationen
  - Verfahren zum Verifizieren oder Validieren der erhaltenen Informationen und deren Verwendung als Nachweise
  - Annahmen im Hinblick auf den Ansatz, die Methodik, die Verfahren und die erwarteten Ergebnisse und Schlussfolgerungen
- den Auftrag zeitlich so einplanen, dass zeitliche Aspekte, Verfügbarkeiten und

Wichtige Aspekte Fortsetzung

andere Verpflichtungen sowie die Anforderungen des Managements und der zu prüfenden Einheit soweit wie möglich berücksichtigt werden

- den Projektplan im Verlauf der IT-Prüfung anpassen, um auf Sachverhalte, die sich im Rahmen der Auftragsbearbeitung ergeben, zu reagieren, z. B. auf weitere Risiken, falsche Annahmen oder Feststellungen aus bereits durchgeführten Prüfungshandlungen.
- bei internen Aufträgen:
  - der zu prüfenden Einheit die AuditCharter kommunizieren; sofern notwendig sollte hierbei ein Prüfungsauftrag oder ein vergleichbares Dokument verwendet werden, um die Durchführung bestimmter Aufträge klarzustellen bzw. zu begründen
  - der zu prüfenden Einheit den Prüfungsplan kommunizieren, so dass diese vollständig informiert ist und angemessenen Zugang zu den benötigten Personen, Dokumente und sonstigen Ressourcen bereitstellen kann
- bei externen Aufträgen:
  - für jede externe IT-Prüfung ein gesondertes Auftragsschreiben erstellen
  - für jede externe IT-Prüfung einen Projektplan erstellen. Der Plan sollte mindestens die Ziele und den Umfang der Beauftragung dokumentieren.

Verknüpfung zu den Richtlinien

Typ	Bezeichnung
Richtlinie	2201 – Auftragsplanung

Zeitpunkt des Inkrafttretens

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

