IT-Prüfungsstandard 1204 – Wesentlichkeit

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 1204 – Wesentlichkeit

Aussagen

1204.1 **IT-Prüfer müssen bei der Auftragsplanung potenzielle Kontrollschwächen oder das Fehlen von Kontrollen ebenso berücksichtigen wie die Frage, ob diese zu einer bedeutsamen Schwachstelle oder einem wesentlichen Mangel führen können.**

1204.2 **IT-Prüfer müssen die Wesentlichkeit und deren Auswirkung auf das Prüfungsrisiko beachten, wenn sie Art, Zeitpunkt und Umfang der Prüfungshandlungen festlegen.**

1204.3 **IT-Prüfer müssen berücksichtigen, dass der kumulative Effekt geringfügiger Kontrollschwächen oder -mängel und das Fehlen von Kontrollen zu einer bedeutsamen Schwachstelle oder einem wesentlichen Mangel führen kann.**

1204.4 **IT-Prüfer müssen Folgendes im Bericht offenlegen:**

- **Fehlende oder unwirksame Kontrollen**
- **Bedeutsamkeit von Kontrollschwächen**
- **Die Wahrscheinlichkeit, mit der diese Schwächen zu einer bedeutsamen Schwachstelle oder einem wesentlichen Mangel führen**

Wichtige Aspekte

Beim Durchführen eines Auftrags sollten IT-Prüfer:

- das Konzept der Wesentlichkeit anwenden für:
  - das Planen und Durchführen der Beauftragung
  - das Bewerten der Auswirkungen bestimmter Elemente, Prozesse, Kontrollen oder Fehler

Jegliche Schwachstelle, jeglicher Mangel oder jegliches Fehlen angemessener Richtlinien, Verfahren und Kontrollen sollten im Kontext der jeweiligen Auftragsumstände beurteilt werden.

- gegebenenfalls gesetzliche oder aufsichtsrechtliche Wesentlichkeitsdefinitionen berücksichtigen.
- zur Kenntnis nehmen, dass die Beurteilung von Wesentlichkeit und Prüfungsrisiko von Fall zu Fall variieren kann in Abhängigkeit von den jeweiligen Umständen und einer Änderung des Umfelds.
- versuchen, beim Planen und Durchführen des Auftrags das Prüfungsrisiko auf ein annehmbares Niveau zu reduzieren und dennoch die Zielsetzungen zu erreichen.
- bei der Festlegung von Art, Zeitrahmen und Umfang der Prüfungsverfahren die Wesentlichkeit berücksichtigen.
- das Prüfungsrisiko für Untersuchungsgegenstände mit einer höheren Wesentlichkeit verringern durch Ausweitung der Kontrollprüfungen (geringeres Kontrollrisiko) und/oder die Ausweitung substanzieller Prüfungshandlungen (geringeres Entdeckungsrisiko).
- die Auswirkungen von kompensierenden Kontrollen ebenso bewerten wie die Frage, ob diese wirksam sind, um zu bestimmen, ob eine Kontrollschwäche oder eine Kombination von Kontrollschwächen einen wesentlichen Mangel darstellt.
- beim Ermitteln der Wesentlichkeit den kumulativen Effekt mehrerer Fehler oder dem Versagen von Kontrollen berücksichtigen.
- nicht nur die Größe, sondern auch die Art von Kontrollschwächen sowie die jeweiligen Umstände bei deren Auftreten berücksichtigen, wenn deren Gesamtwirkung auf Prüfungsurteil oder -schlussfolgerung bewertet wird.

IT-Prüfungsstandard 1204 – Wesentlichkeit

Begriffe

Begriff	Definition
Prüfungsrisiko	Das Risiko, aufgrund der Prüfungsergebnisse zu einer falschen Schlussfolgerung zu gelangen. Das Prüfungsrisiko besteht aus den folgenden drei Komponenten: • Kontrollrisiko • Entdeckungsrisiko • Inhärentes Risiko
Wesentlicher Mangel	Eine Schwachstelle oder eine Kombination von Schwachstellen im Internen Kontrollsystem, die mit nennenswerter Wahrscheinlichkeit nach sich ziehen, dass ein wesentlicher Falschausweis nicht vermieden oder nicht rechtzeitig erkannt werden kann. Ein Mangel im Kontrollsystem gilt als wesentlich, wenn das Fehlen der Kontrolle verursacht, dass keine hinreichende Sicherheit über die Erreichung des Kontrollziels mehr möglich ist. Ein als wesentlich eingestufter Mangel bedeutet, dass: • Kontrollen nicht implementiert wurden und/oder diese nicht durchgeführt werden und/oder diese unzureichend sind. • eine Eskalation angebracht ist. Die Wesentlichkeit und das Prüfungsrisiko, das der IT-Prüfer für akzeptabel hält, stehen in einem umgekehrten Verhältnis zueinander, d.h., je größer die Wesentlichkeitsgrenze, desto geringer die Annehmbarkeit des Prüfungsrisikos und umgekehrt.
Wesentlichkeit	Ein Prüfungskonzept mit Bezug auf die Bedeutung eines Informationselements aufgrund der Auswirkungen auf die Funktionsfähigkeit der zu prüfenden Einheit. Ein Ausdruck der relativen Bedeutung oder Wichtigkeit eines bestimmten Gegenstands im Gesamtkontext des Unternehmens.

Verknüpfung zu den Standards und Richtlinien

Typ	Bezeichnung
Standard	1201 – Auftragsplanung
Standard	1202 – Risikoorientierte Planung
Standard	1207 – Unregelmäßigkeiten und gesetzeswidrige Handlungen
Standard	1401 –Berichterstattung
Richtlinie	2202 – Risikoorientierte Planung
Richtlinie	2204 – Wesentlichkeit

Zeitpunkt des Inkrafttretens

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