IT-Prüfungsstandard 1205 – Nachweise

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 1205 – Nachweise

Aussagen

1205.1 IT-Prüfer müssen ausreichende und angemessene Nachweise einholen, um sinnvolle Schlussfolgerungen ziehen zu können, auf welche die Prüfungsergebnisse gestützt werden.

1205.2 IT-Prüfer müssen beurteilen, ob die eingeholten Nachweise ausreichend sind, um die Schlussfolgerungen zu untermauern und die Auftragsziele zu erreichen.

Wichtige Aspekte

Beim Durchführen eines Auftrags sollten IT-Prüfer:

- ausreichende und angemessene Nachweiseerlangen, darunter:
  - die durchgeführten Verfahren
  - die Ergebnisse der durchgeführten Verfahren
  - Quelldokumente (in elektronischer oder Papierform), Unterlagen und Belegmaterial, das in den Auftrag eingeflossen ist
  - Feststellungen und Ergebnisse des Auftrags
  - Nachweise, dass die Arbeitendurchgeführt wurden und geltenden Gesetzen, Bestimmungen und Richtlinienentsprechen
- eine Dokumentation anfertigen, die:
  - über einen bestimmten Zeitraum und in einem Format aufbewahrt wird und verfügbar ist, das den Richtlinien des Prüfungsunternehmens sowie relevanten berufsüblichen Standards, Gesetzen und Bestimmungen entspricht
  - bei der Bearbeitung und Aufbewahrung jederzeit vor nicht autorisierter Offenlegung oder Änderung geschützt ist
  - am Ende des Aufbewahrungszeitraums ordnungsgemäß entsorgt wird
- beim Erhalten von Nachweisen aus Kontrollprüfungen die Hinlänglichkeit der Nachweise zum Unterstützen des bewerteten Kontrollrisikoniveaus berücksichtigen.
- Nachweise angemessen identifizieren, referenzieren und katalogisieren.
- Eigenschaften der Nachweise wie Quelle, Art (z. B. schriftlich, mündlich, visuell, elektronisch) und Authentizität (z. B. digitale und manuelle Unterschriften, Stempel) bei der Beurteilung ihrer Zuverlässigkeit berücksichtigen.
- die wirtschaftlichste und schnellste Methode zur Erlangung der Nachweise berücksichtigen, um Auftragszielen und -risiken zu genügen. Schwierigkeiten oder Kosten stellen jedoch keinen gültigen Grund für das Auslassen einer erforderlichen Prüfungshandlung dar.
- das für das Zusammenstellen der Nachweise angemessene Verfahren in Abhängigkeit vom Untersuchungsgegenstandauswählen (d. h. Art, Zeitpunkt der Prüfung, professionelles Ermessen). Zu den für das Erbringen der Nachweise verwendeten Methoden gehören:
  - Befragung und Bestätigung
  - Erneute Durchführung
  - Erneute Berechnung
  - Berechnung
  - Analytische Verfahren
  - Überprüfung / Begehung / Einsichtnahme
  - Beobachtung
  - Andere allgemein akzeptierte Methoden

Wichtige Aspekte

Fortsetzung

- Quelle und Art von Informationen in Betracht ziehen, um deren Zuverlässigkeit sowie die Notwendigkeit einer weiteren Verifizierung zu beurteilen. Generell ist die Zuverlässigkeit von Nachweisen höher, wenn diese
  - in schriftlicher Form vorliegen, nicht in Form mündlichen Äußerungen
  - aus unabhängigen Quellen stammen
  - vom Prüfer zusammengestellt werden, nicht von der zu prüfenden Einheit
  - von einem unabhängigen Dritten beglaubigt werden
  - von einem unabhängigen Dritten aufbewahrt werden
  - das Ergebnis einer Überprüfung / Begehung / Einsichtnahme sind
  - das Ergebnis einer Beobachtung sind
- objektive und ausreichende Nachweise erbringen, sodass ein qualifizierter, unabhängiger Dritter in der Lage ist, alle Tests nachzuvollziehen und zu denselben Ergebnissen und Schlussfolgerungen zu gelangen.
- Nachweise erbringen, die der Wesentlichkeit des geprüften Gegenstands und den damit verbundenen Risiken entsprechen.
- hinreichend auf die Genauigkeit und Vollständigkeit der Informationen achten, wenn der IT-Prüfer vom Unternehmen erhaltene Informationen zum Durchführen von Prüfungshandlungen verwendet.
- alle Situationen offenlegen, in denen kein ausreichender Nachweis in Übereinstimmung mit der Kommunikation der Prüfungsergebnisse beschafft werden kann.
- die Nachweise vor nicht autorisiertem Zugriff und Änderungen schützen.
- die Prüfungsnachweise nach Abschluss der IT-Prüfung oder des Auftrags solange aufbewahren, wie dies durch die anwendbaren Gesetze, Bestimmungen und Richtlinien vorgeschrieben wird.

Begriffe

Begriff	Definition
Angemessene Nachweise	Der Qualitätsmaßstab für die Nachweise.
Ausreichende Nachweise	Der Quantitätsmaßstab für die Nachweise; belegt alle wesentlichen Fragen in Bezug auf Prüfungsziel und -umfang. Siehe „Nachweise“.

Verknüpfung zu den Richtlinien

Typ	Bezeichnung
Richtlinie	2205 – Nachweise

Zeitpunkt des Inkrafttretens

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

