IT-Prüfungsstandard 1207 – Unregelmäßigkeiten und gesetzeswidrige Handlungen

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

1207.1 **IT-Prüfer müssen bei der Durchführung des Auftrags das Risiko von Unregelmäßigkeiten und gesetzeswidrigen Handlungen berücksichtigen.**

1207.2 **IT-Prüfer müssen bei der Durchführung des Auftrags eine berufsübliche Skepsis walten lassen.**

1207.3 **IT-Prüfer müssen die entsprechenden Parteien rechtzeitig auf jegliche wesentliche Unregelmäßigkeiten oder gesetzeswidrige Handlungen hinweisen und diese dokumentieren.**

Wichtige Aspekte

IT-Prüfer sollten:

- das beim Planen und Durchführen des Auftrags bestehende Prüfungsrisiko auf ein annehmbares Niveau reduzieren, indem sie:
  - sich bewusst sind, dass wesentliche Fehler, Kontrollmängel und Falschaussagen aufgrund von Unregelmäßigkeiten oder gesetzeswidrigen Handlungen möglich sind und zwar unabhängig von deren Risikobewertung
  - versuchen, das Unternehmen und dessen Umgebung zu verstehen, einschließlich der internen Kontrollen, mit denen die für den Gegenstand, den Umfang und die Ziele des Auftrags relevanten Unregelmäßigkeiten und gesetzeswidrigen Handlungen vermieden oder erkannt werden sollen
  - ausreichende und angemessene Nachweise einholen, um festzustellen, ob Führungskräfte oder andere Personen im Unternehmen Kenntnis von tatsächlichen, vermuteten oder angeblichen Unregelmäßigkeiten und gesetzeswidrigen Handlungen haben
- bei der Durchführung der Prüfungshandlungenungewöhnliche oder unerwartete Beziehungen berücksichtigen, die darauf hindeuten können, dass ein Risiko von wesentlichen Fehlern, Kontrollschwächen oder Falschaussagen aufgrund von Unregelmäßigkeiten und gesetzeswidrigen Handlungen besteht
- Verfahren entwickeln und anwenden, mit denen die Angemessenheit der internen Kontrollen, mit denen Unregelmäßigkeiten und gesetzeswidrige Handlungen vermieden oder erkannt werden sollen, ebenso geprüft wird wie das Risiko, dass das Management diese Kontrollen umgeht,
- bewerten, ob erkannte Fehler, Kontrollschwächen oder Falschaussagen auf eine Unregelmäßigkeit oder gesetzeswidrige Handlung hinweisen. Wenn ein solcher Hinweis vorliegt, müssen die Auswirkungen auf andere Aspekte des Auftrags und insbesondere auf die Darstellungen des Managements berücksichtigt werden.
- mindestens einmal jährlich oder je nach Art des Auftrags auch öfter eine schriftliche Erklärung vom Management einholen, um:
  - die Verantwortung des Managements für die Entwicklung und Einführung interner Kontrollen zu bestätigen, durch die Unregelmäßigkeiten und gesetzeswidrige Handlungen verhindert und erkannt werden.
  - die relevanten Ergebnisse von Beurteilungen offenzulegen, die auf das Vorhandensein von Fehlern, Kontrollschwächen oder Falschaussagen aufgrund von Unregelmäßigkeiten oder gesetzeswidrigen Handlungen hinweisen.
  - die Kenntnis des Managements von unternehmensrelevanten Unregelmäßigkeiten oder gesetzeswidrigen Handlungen die

Wichtige Aspekte

Fortsetzung

Führungskräfte des Unternehmens und Mitarbeiter mit wichtiger Rolle bei den internen Kontrollen betreffen, offenzulegen.
- die Kenntnis des Managements von jeglichen vermuteten oder angeblichen, unternehmensrelevanten Unregelmäßigkeiten und gesetzeswidrigen Handlungen, die von aktuellen oder ehemaligen Mitarbeitern, Aufsichtsbehörden oder anderen Stellen gemeldet wurden, offenzulegen.

- rechtzeitig die folgenden Stellen verständigen:
  - Die entsprechende Managementebene über jegliche ermittelte oder erhaltene Information, die das Vorhandensein wesentlicher Unregelmäßigkeiten oder gesetzeswidriger Handlungen belegt
  - Die Leitungs- und Aufsichtsorgane über jegliche wesentlichen Unregelmäßigkeiten und gesetzeswidrigen Handlungen, die das Management oder Mitarbeiter mit wichtiger Rolle bei den internen Kontrollen betreffen
- die die Leitungs- und Aufsichtsebene auf jegliche, im Rahmen des Auftrags erkannten wesentlichen Mängel in Bezug auf Aufbau und Implementierung interner Kontrollen hinweisen, mit denen Unregelmäßigkeiten und gesetzeswidrige Handlungen vermieden oder erkannt werden sollen, auch wenn diese außerhalb des Auftragsumfangs liegen.
- die unter den Umständen geltenden rechtlichen und berufsüblichen Anforderungen an die Berichterstattung berücksichtigen.
- einen Rücktritt von der Beauftragung in Erwägung ziehen, wenn wesentliche Fehler, Kontrollschwächen, Falschaussagen oder gesetzeswidrige Handlungen die weitere Auftragsdurchführung beeinträchtigen.
- alle Mitteilungen, Pläne, Ergebnisse, Beurteilungen und Schlussfolgerungen in Bezug auf wesentliche Unregelmäßigkeiten oder gesetzeswidrige Handlungen, die dem Management, den für die Governance Verantwortlichen, den Aufsichtsbehörden und anderen mitgeteilt wurden, dokumentieren.

Begriffe

Begriff	Definition
Unregelmäßigkeit	Verstoß gegen eine festgelegte Managementrichtlinie oder aufsichtsrechtliche Anforderung. Hierbei kann es sich um absichtliche Falschaussagen, unvollständige Informationen über den zu prüfenden Bereich oder das Gesamtunternehmen, grobe Fahrlässigkeit oder unbeabsichtigte gesetzeswidrige Handlungen handeln.
Wesentliche Falschaussage	Eine versehentlich oder absichtlich unwahre Aussage, die sich nachweislich auf die Prüfung auswirkt.
Berufsübliche Skepsis	Eine Haltung, die die Prüfbefunde hinterfragt und kritisch bewertet. Quelle: American Institute of Certified Public Accountants (AICPA) AU 230.07

Verknüpfung zu den Standards und Richtlinien

Typ	Bezeichnung
Standard	1008 – Kriterien

Standard	1202 – Risikoorientierte Planung
Standard	1205 – Nachweise
Richtlinie	2206 – Hinzuziehung anderer Sachverständiger
Richtlinie	2207 – Unregelmäßigkeiten und gesetzeswidrige Handlungen

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

