IT-Prüfungsstandard 1202 – Risikoorientierte Planung

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

1202.1 Die IT-Revision muss einen geeigneten Risikobeurteilungsansatz und eine unterstützende Methodik anwenden, um den allgemeinen IT-Prüfungsplan zu entwickeln und die Prioritäten für die effiziente Zuweisung von IT-Prüfungsressourcen festzulegen.

1202.2 IT-Prüfer müssen bei der Planung einzelner Aufträge die für den zu prüfenden Bereich relevanten Risiken identifizieren und bewerten.

1202.3 IT-Prüfer müssen die Risiken des Prüfungsgegenstands, das Prüfungsrisiko sowie das sich daraus ergebende Gefahrenpotenzial für das Unternehmen berücksichtigen.

Wichtige Aspekte

Beim Planen der fortlaufenden Aktivitäten sollte die IT-Revision:

- mindestens jährlich eine Risikobeurteilung durchführen und dokumentieren, um die Entwicklung des IT-Prüfungsplans zu erleichtern.
- die strategischen Pläne und Ziele des Unternehmens sowie das Rahmenwerk und die Maßnahmen zum Risikomanagement bei der Risikobeurteilung berücksichtigen.
- die benötigten Ressourcen zur Erfüllung der Anforderungen des Auftrags für jeden Prüfungsauftragbestimmen und begründen.
- einen risikoorientierten Ansatz bei der Auswahl der maßgeblichen Prüffelder und Prüfungsgegenstände sowie bei der Entscheidung zur Gestaltung einzelner Prüfungen wählen.
- die Anerkennung der Risikobeurteilung seitens der Prüfungsbeteiligten sowie weiterer angemessener Interessensgruppen anstreben.
- die IT-Prüfungsaufgaben anhand der Risikobeurteilung priorisieren und planen.
- auf Grundlage der Risikobeurteilung einen Plan entwickeln, der:
  - als Rahmenwerk für die IT-Prüfungsaktivitäten dient
  - nicht IT-bezogene Prüfungsanforderungen und -aktivitäten berücksichtigt
  - mindestens jährlich von den mit der Aufsichtbeauftragten Stellen aktualisiert und genehmigt wird
  - die in der Audit Charter festgelegten Verantwortlichkeiten berücksichtigt

Beider Planung einzelner Aufträge sollten IT-Prüfer:

- die für den zu prüfenden Bereich relevanten Risiken ermitteln und bewerten
- für jeden Auftrag eine vorläufige Bewertung des für den zu prüfenden Bereichrelevanten Risikos vornehmen. Die Zielsetzungen jedes Auftrags sollten die Ergebnisse der vorläufigen Risikobeurteilung widerspiegeln.
- beider Ermittlung von Risikobereichen und beim Planen eines Auftrags vorangegangene Prüfungen, Nachschauen und Feststellungen einschließlich der Umsetzungsaktivitäten berücksichtigen. Auch sollte das übergreifende Risikobeurteilungsverfahren der Steuerungs- und Aufsichtsorgane berücksichtigt werden.
- bei der Planung und Durchführung der IT-Prüfungversuchen, das Prüfungsrisiko auf ein annehmbares Niveau zu reduzieren und die Prüfungsziele durch eine geeignete Bewertung des Prüfungsgegenstands und der zugeordneten Kontrollen zu erfüllen.
- beider Planung einer spezifischen IT-Prüfungshandlung beachten, dass eine

geringere Wesentlichkeitsgrenze mit konkreteren Erwartungen an die Prüfung und einem höheren Prüfungsrisikos einhergeht.
- das Risiko bei höherer Wesentlichkeit kompensieren, indem zusätzliche Sicherheit durch die Ausweitung der Kontrollprüfungen(geringeres Kontrollrisiko)und/oder die Ausweitung Substanzieller Prüfungshandlungen (geringeres Entdeckungsrisiko) erlangt wird.

Begriffe

Begriff	Definition
AuditCharter	• Ein Dokument, das von der Unternehmensleitung genehmigt ist und das den Zweck, die Kompetenzen und die Verantwortung einer internen Revisionsfunktion definiert.
Prüfungsrisiko	Das Risiko, aufgrund der Prüfungsergebnisse zu einer falschen Schlussfolgerung zu gelangen. Das Prüfungsrisiko besteht aus den folgenden drei Komponenten: • Kontrollrisiko • Entdeckungsrisiko • Inhärentes Risiko
Risiko des Prüfungsgegenstands	Das für den zu prüfenden Bereich relevante Risiko. • Geschäftsrisiko (Zahlungsfähigkeit der Kunden, Kreditwürdigkeit, Marktfaktoren usw.) • Vertragsrisiko (Haftung, Preis, Typ, Strafen usw.) • Länderrisiko (Politik, Umwelt, Sicherheit usw.) • Projektrisiko (Ressourcen, Fertigkeitsprofil, Methodik, Produktstabilität usw.) • Technologisches Risiko (Lösung, Architektur, Hard- und Software-Infrastruktur, Netzwerk, Lieferwege usw.) Siehe „Inhärentes Risiko“
Kontrollrisiko	Das Risiko eines wesentlichen Fehlers, der vom internen Kontrollsystem nicht rechtzeitig erkannt oder vermieden wird. (Siehe „Inhärentes Risiko“.)
Entdeckungsrisiko	Das Risiko, dass der IT-Prüfer mithilfe der substanziellen Prüfungshandlungen einen für sich genommenen oder in Kombination mit anderen Fehlern möglicherweise wesentlichen Fehler nicht erkennt. (Siehe „Prüfungsrisiko“).
Inhärentes Risiko	Das Risikoniveau oder -potenzial ohne Berücksichtigung der vom Management ergriffenen oder möglicherweise geplanten Aktionen (z. B. Implementieren von Kontrollen). Siehe „Kontrollrisiko“.
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.
Risikobeurteilung	Ein Prozess zum Ermitteln und Bewerten der Risiken und potenziellen Auswirkungen. Mit Risikobeurteilungen werden die Elemente oder Bereiche ermittelt, die für das Unternehmen die größten Risiken, Schwachstellen oder Risikopotenziale darstellen, damit diese in den jährlichen IT-Prüfungsplan aufgenommen werden können. Risikobeurteilungen werden zudem eingesetzt, um die Projektergebnis- und Projektnutzenrisiken zu steuern.
Substanzielle Prüfungshandlungen	Erlangen von Prüfungsnachweisen über Vollständigkeit, Richtigkeit oder Existenz von Aktivitäten oder Transaktionen im Verlauf des Prüfungszeitraums

Verknüpfung zu den Richtlinien

Typ	**Bezeichnung**
Richtlinie	2202 – Risikoorientierte Planung

Zeitpunkt des Inkrafttretens

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

