–IT-Prüfungsstandard 1008 – Kriterien

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

1008.1 IT-Prüfer müssen Kriterien zur Beurteilung des Untersuchungsgegenstandesauswählen, die objektiv, vollständig, relevant, messbar, weithin anerkannt, maßgeblich sowie allen Lesern und Nutzern der Berichterstattung verständlich und zugänglich sind.

1008.2 IT-Prüfer müssen die Quellen der Kriterien berücksichtigen und diejenigen bevorzugt zu Grunde legen, die von relevanten und maßgeblichen Regulierungsinstanzen festgelegt wurden, bevor weniger maßgebliche Kriterien verwendet werden.

Wichtige Aspekte

IT-Prüfer sollten:

- die Auswahl der Kriterien sorgfältig prüfen und diese begründen können.
- anhand ihres Sachverstands sicherstellen, dass durch das Anwenden der Kriterien eine faire und objektive Meinung oder Schlussfolgerung erzielt werden kann, die zu keiner Irreführung des Lesers oder Nutzers führt. Es ist möglich, dass Führungskräfte der Organisation Kriterien bestimmen, die nicht alle Anforderungen erfüllen.
- beim Festlegen der Prüfungsanforderungen die Eignung und Verfügbarkeit von Kriterien berücksichtigen.
- wenn Kriterien nicht ohne weiteres verfügbar, unvollständig oder auslegungsfähig sind, der Berichterstattung eine Beschreibung und weitere Informationen hinzufügen, die sicherstellen, dass die Berichterstattung fair, objektiv und verständlich ist, und dass der Anwendungskontext der Kriterien in der Berichterstattung nachvollziehbar wird.

Die Eignung und Angemessenheit der Kriterien für die Beurteilung des Untersuchungsgegenstandes sollten anhand der folgenden fünf Kriterien bewertet werden:

- **Objektivität** – Die Kriterien sollten frei von Vorurteilen sein, die die Erkenntnisse und Schlussfolgerungen der Prüfer beeinflussen und entsprechend zu einer Irreführung des Nutzers der Berichterstattung führen können.
- **Vollständigkeit** – Die Kriterien sollten hinlänglich vollständig sein, damit alle Kriterien, die sich auf die Schlussfolgerungen des Prüfers über den Gegenstand auswirken können, ermittelt und beim Durchführen des Auftrags verwendet werden können.
- **Relevanz** –Die Kriterien sollten für den Untersuchungsgegenstand relevant sein und zu Feststellungen und Schlussfolgerungen beitragen, die die Zielsetzungen des Auftrags erfüllen.
- **Messbarkeit**– Die Kriterien sollten eine konsistente Bewertung des Untersuchungsgegenstands und das Entwickeln konsistenter Schlussfolgerungen ermöglichen, wenn diese von verschiedenen Prüfern unter vergleichbaren Bedingungen angewendet werden.
- **Verständlichkeit** – Die Kriterien sollten klar kommuniziert werden und keine erheblich abweichenden Interpretationen durch die vorgesehenen Nutzer zulassen.

Die Akzeptanz der Kriterien wird beeinflusst von der Verfügbarkeit der Kriterien für die Nutzer der Berichterstattung, sodass die Nutzer die Grundlage der Prüfung sowie die Bedeutung von Feststellungen und Schlussfolgerungen verstehen. Als Quellen

Wichtige Aspekte Fortsetzung

können berücksichtigt werden:

- **Anerkannte Quellen** – Die Kriterien sollten hinreichend breit anerkannt sein, damit deren Verwendung von den Nutzern nicht in Frage gestellt wird.
- **Quellen mit Vorgabecharakter** – Es sollten Kriterien angewendet werden, die den im jeweiligen Untersuchungsbereich vorhandenen Verlautbarungen mit Vorgabecharakter entsprechen und die sich für den Untersuchungsgegenstand eignen. Äußerungen mit Vorgabecharakter können beispielsweise von Fachverbänden, Branchenvereinigungen, Regierungen und Aufsichtsbehörden stammen.
- **Öffentlich zugängliche Quellen** – Die Kriterien sollten für die Nutzer der Berichterstattung verfügbar sein. Hierzu zählen beispielsweise Standards, die von Fachorganisationen für Rechnungslegung und Abschlussprüfung wie der ISACA, der International Federation of Accountants (IFAC) und anderen anerkannten Regierungsstellen oder Fachverbänden entwickelt wurden.
- **Allen Nutzern zugängliche Quellen** – Wenn die Kriterien nicht öffentlich zugänglich sind, sollten diese allen Nutzern in Form von Aussagenkommuniziert werden, die einen Teil der Berichterstattung bilden. Die Aussagen bestehen aus Stellungnahmen zum Untersuchungsgegenstand, die die Anforderungen für geeignete Kriterien erfüllen und daher als Prüfungsgrundlage zu Grunde gelegt werden können.

Zusätzlich zur Eignung und Verfügbarkeit sollte bei der Auswahl der IT-Prüfkriterien hinsichtlich der Verwendung und des potenziellen Adressatenkreises die jeweilige Quelle betrachtet werden. So eignen sich beispielsweise im Umgang mit Regierungsbehörden Kriterien am besten, die sich auf Aussagen beziehen, welche auf den Untersuchungsgegenstand betreffenden Gesetzen und Bestimmungen beruhen. In anderen Fällen sind möglicherweise die Kriterien von Branchen- oder Handelsverbänden relevant. Im Folgenden werden in der Reihenfolge der Berücksichtigung mögliche Quellen für Kriterien aufgeführt:

- **Von der ISACA aufgestellte Kriterien** – Hierbei handelt es sich um öffentlich verfügbare Kriterien und Standards, die einer Begutachtung durch Fachkollegen und einem gründlichen Überprüfungsprozess durch anerkannte internationale Experten für IT-Governance, -Kontrolle, -Sicherheit und -Prüfung unterzogen wurden.
- **Von anderen Expertengremien aufgestellte Kriterien** – Ähnlich wie die ISACA-Standards und -Kriterien sind diese für den Untersuchungsgegenstand relevant, wurden durch Experten entwickelt und sind einer Überprüfung durch die Fachwelt sowie durch Experten verschiedener Themengebiete unterzogen worden.
- **Auf Gesetzen und Vorschriften beruhende Kriterien** – Obwohl Gesetze und Vorschriften die Grundlage von Kriterien bilden können, muss bei deren Verwendung sorgfältig vorgegangen werden. Mitunter sind die Formulierungen komplex und haben eine besondere juristische Bedeutung. In vielen Fällen müssen die rechtlichen Anforderungen in Aussagenumformuliert werden. Zudem sind Stellungnahmen zur Gesetzgebung und deren Auslegung in der Regel Juristen vorbehalten.
- **Von Dritten aufgestellte Kriterien, die keinem anerkannten, definierten Abstimmungs- und Veröffentlichungsprozessunterliegen**– Diese umfassen relevante Kriterien, die von anderen Organisationen entwickelt wurden, die keinem

anerkannten definierten Abstimmungs- und Veröffentlichungsprozess und keiner öffentlichen Beratung und Diskussion unterlagen.

- **Speziell für eine IT-Prüfung oder einen Auftrag entwickelte Kriterien** –Obwohl speziell für eine IT-Prüfung oder einen Auftrag entwickelte Kriteriengeeignet sein können, muss sichergestellt werden, dass diese Kriterien den Eignungs- und Angemessenheitskriterien und hierbei insbesondere der Vollständigkeit, Messbarkeit und Objektivität entsprechen. Bei spezifisch für eine IT-Prüfung oder einen Auftrag entwickelten Kriterien handelt es sich um Aussagen.

Die Auswahl der Kriterien sollte mit Sorgfalt erfolgen. Wiewohl das Einhalten der lokalen Gesetze und Bestimmungen wichtig ist und als verbindliche Anforderung betrachtet werden muss, ist es gemeinhin anerkannt, dass viele IT-Prüfungen Bereiche wie z. B. die Änderungsverwaltung sowie die allgemeinen IT- und Zugriffskontrollen betreffen, die nicht von Gesetzen oder Vorschriften geregelt werden. Zudem haben verschiedene Branchen (wie z. B. die Kreditkartenbranche) verpflichtende Anforderungen aufgestellt, die eingehalten werden müssen. Wenn gesetzliche Anforderungen auf Prinzipien beruhen, sollte der Prüfer sicherstellen, dass die ausgewählten Kriterien den Auftragszielen entsprechen.

Im Verlauf der Auftragsdurchführung können zusätzliche Informationen dazu führen, dass bestimmte Kriterien für das Erreichen der Auftragsziele nicht mehr erforderlich sind. In diesem Fall sind weitere Arbeiten im Zusammenhang mit diesen Kriterien nicht erforderlich.

Begriffe

Begriff	Definition
Kriterien	Die zum Bewerten und Darstellen des Untersuchungsgegenstands verwendeten Standards und Maßstäbe, anhand derer ein IT-Prüfer den Untersuchungsgegenstand beurteilt. Kriterien sollten folgende Eigenschaften aufweisen: • Objektiv – Unvoreingenommen • Vollständig – Unter Einschluss aller zum Erreichen einer Schlussfolgerung erforderlichen Faktoren • Relevant – Mit Bezug zum Untersuchungsgegenstand • Messbar – Geeignet für konsistente Bewertungen In Bezug auf einen Prüfungsauftrag bezeichnet dies Maßstäbe, gegen die die schriftliche Erklärung der geprüften Führungskräfte zum Untersuchungsgegenstand bewertet werden kann. Der Prüfer kommt zu einer Schlussfolgerung hinsichtlich des Untersuchungsgegenstands, indem er auf geeignete Kriterien verweist.

Verknüpfung zu den Richtlinien

Typ	Bezeichnung
Richtlinie	2008 – Kriterien

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

