

IT-Prüfungsstandard 1004 – Hinreichende Durchführbarkeit

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 CISA 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).

ISACA 2012-2013 Professional Standards and Career Management Committee

Steven E. Sizemore, CISA, CIA, CGAP, Chairperson	Texas Health and Human Services Commission, USA
Christopher Nigel Cooper, CISM, CITP, FBCS, M.Inst.ISP	HP Enterprises Security Services, Großbritannien
Ronald E. Franke, CISA, CRISC, CFE, CIA, CICA	Myers and Stauffer LC, USA
MurariKalyanaramani, CISA, CISM, CRISC, CISSP, CBCP	British American Tobacco IT Services, Malaysia
Alisdair McKenzie, CISA, CISSP, ITCP	IS Assurance Services, Neuseeland
Katsumi Sakagawa, CISA, CRISC, PMP	JIEC Co. Ltd., Japan
Ian Sanderson, CISA, CRISC, FCA	NATO, Belgien
Timothy Smith, CISA, CISSP, CPA	LPL Financial, USA
Rodolfo Szuster, CISA, CA, CBA, CIA	Tarshop S.A., Argentinien

IT-Prüfungsstandard 1004 – Hinreichende Durchführbarkeit

Aussagen

- 1004.1** IT-Prüfer müssen hinreichend sicher sein, dass der Auftrag in Übereinstimmung mit den IT-Prüfungsstandards oder, sofern erforderlich, anderen geltenden Berufs- und Branchenstandards oder Bestimmungen abgeschlossen sowie zu einer qualifizierten Stellungnahme oder Schlussfolgerung führen kann.
- 1004.2** IT-Prüfer müssen hinreichend sicher sein, dass der Auftragsumfang eine Schlussfolgerung zum Untersuchungsgegenstand ermöglicht und mögliche Einschränkungen berücksichtigt.
- 1004.3** IT-Prüfer müssen hinreichend sicher sein, dass die Führungskräfte der Organisation ihre Verpflichtungen und Verantwortlichkeiten hinsichtlich der Bereitstellung der für das Durchführen des Auftrags erforderlichen geeigneten, relevanten und rechtzeitigen Informationen verstanden haben.
-

Wichtige Aspekte

IT-Prüfer sollten:

- IT-Prüfungen oder Aufträge nur durchführen, wenn die Arbeit erfolgreich und in Übereinstimmung mit den Berufsgrundlagen abgeschlossen werden kann.
 - IT-Prüfungen oder Aufträge nur durchführen, wenn der Untersuchungsgegenstand anhand geeigneter Kriterien bewertet werden kann.
 - den Umfang der IT-Prüfung oder des Auftrags hinterfragen, um sicherzustellen, dass der Auftrag eindeutig bestimmt ist und eine Schlussfolgerung über den Untersuchungsgegenstand ermöglicht.
 - jegliche Einschränkungen des durchzuführenden Auftrags einschließlich des Zugangs zu geeigneten, relevanten und rechtzeitigen Informationen ermitteln und adressieren.
 - prüfen, ob der Auftragsumfang ausreicht, um ein Prüferteil über den Untersuchungsgegenstand zu fällen. Einschränkungen des Umfangs können auftreten, wenn zur Auftragsdurchführung erforderliche Informationen nicht verfügbar sind, wenn der dem IT-Prüfer durch einen Prüfungsauftrag gegebene Zeitrahmen unzureichend ist oder wenn Führungskräfte versuchen, den Prüfungsumfang auf bestimmte Bereiche zu beschränken. In solchen Fällen können andere Auftragsarten in Erwägung gezogen werden, z. B. die Unterstützung der Prüfung von Abschlüssen oder Interner Kontrollen sowie das Prüfen der Einhaltung von Standards und Vorgehensweisen oder der Einhaltung von Vereinbarungen, Lizenzen, Gesetzen und Vorschriften.
-

Begriffe

Begriff	Definition
Prüferteil	<p>Förmliche Aussage eines IT-Prüfers, die den Auftragsumfang und die beim Erstellen des Berichts verwendeten Verfahren beschreibt und die angibt, ob die Feststellungen das Einhalten der Prüfkriterien untermauern oder nicht.</p> <p>Es gibt folgende Arten von Prüferteilen:</p> <ul style="list-style-type: none">• Uneingeschränkte Bestätigung– Stellt keine Abweichungen fest bzw. keine der festgestellten Abweichungen führen

IT-Prüfungsstandard 1004 – Hinreichende Durchführbarkeit

	<p>insgesamt zu einer bedeutsamen Schwachstelle</p> <ul style="list-style-type: none"> • Eingeschränkte Bestätigung– Stellt Abweichungen fest, die insgesamt eine bedeutsame Schwachstelle, jedoch keinen wesentlichen Mangel ergeben • Verweigerung der Bestätigung– Stellt eine oder mehrere bedeutsame Schwachstellen fest, die einen wesentlichen Mangel ergeben <p>Hinweis: Die Ablehnung einer Stellungnahme wird erklärt, wenn der Prüfer nicht in der Lage ist, zum Begründen einer Stellungnahme hinreichende und geeignete Prüfnachweise zu erlangen, oder wenn aufgrund mehrerer, eventuellverknüpfter Unsicherheiten und deren möglicher Gesamtwirkung keine Stellungnahme abgegeben werden kann.</p>
--	---

Verknüpfung
zu den
Richtlinien

	Typ	Bezeichnung
	Richtlinie	2004 – Hinreichende Durchführbarkeit

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