

S16 E-COMMERCE

Die Besonderheiten von Prüfungen der Informationstechnologie (IT-Prüfung) und die Kenntnisse, die zur Durchführung solcher Prüfungen erforderlich sind, erfordern die Erstellung spezieller Standards für IT-Prüfungen. Eines der Ziele der Information ISACA[®] ist es, die Entwicklung solcher global anwendbarer Standards zu fördern. Die Entwicklung und Verbreitung von IT-Prüfungsstandards ist ein Hauptanliegen des Engagements der ISACA im Prüfungswesen. Das Rahmenwerk für die IT-Prüfungsstandards umfasst Leitlinien auf mehreren Ebenen:

- In den **Standards** sind obligatorische Anforderungen für IT-Prüfungen und das Berichtswesen definiert. Sie sollen:
 - IT-Prüfer über die Mindestanforderungen informieren, die erfüllt werden müssen, um der professionellen Verantwortung gemäß dem Ethik-Kodex der ISACA (ISACA Code of Professional Ethics for IS Auditors) zu entsprechen
 - Führungskräfte und andere interessierte Stellen über die Erwartungen dieses Berufsstandes an Prüfer in Kenntnis setzen
 - Inhaber des CISA[®]-Zertifikats (Certified Information Systems Auditor™) über die mit diesem Titel verbundenen Anforderungen informieren. Die Nichtbeachtung dieser Standards kann zu einer Untersuchung des Verhaltens des CISA durch das ISACA Board of Directors oder das zuständige ISACA Committee und ggf. zur Verhängung von Disziplinarmaßnahmen führen.
- Die **Richtlinien** bieten Orientierung bei der Anwendung der IT-Prüfungsstandards. Der IT-Prüfer sollte sich bei der Umsetzung der Standards an diesen Richtlinien orientieren, er sollte seine fachliche Kompetenz bei ihrer Anwendung einsetzen, und er sollte in der Lage sein, Abweichungen von diesen Richtlinien zu begründen. Die Richtlinien sollen die Einhaltung und Durchsetzung der IT-Prüfungsstandards unterstützen.
- Die **Handlungsanweisungen** zeigen Beispiele dafür, welche Verfahren bei einer Prüfung vom IT-Prüfer angewendet werden können. Die Handlungsanweisungen geben Hinweise, wie bei der Durchführung von IT-Prüfungen die Standards eingehalten werden können, sie haben aber keinen verpflichtenden Charakter. Vielmehr sollen die Handlungsanweisungen die Einhaltung und Durchsetzung der IT-Prüfungsstandards weiter unterstützen.

COBIT[®] (Control Objectives for Information and related Technology) ist ein Framework zur IT-Governance und ermöglicht die Verbindung von Kontrollerfordernissen, technischen Anforderungen und geschäftlichen Risiken. Das COBIT Framework unterstützt die Erstellung klarer Vorgaben und stellt „Good Practice-Methoden“ für ein unternehmensweites internes IT-Kontrollsystem dar. Es konzentriert sich auf die Einhaltung gesetzlicher Anforderungen (Compliance), unterstützt Unternehmen dabei, die sich aus der IT ergebende Wertschöpfung zu steigern, unterstützt die Ausrichtung auf die Ziele und Strategie und vereinfacht die Umsetzung der im COBIT Framework enthaltenen Konzepte.

COBIT ist zur Verwendung durch Unternehmens- und IT-Management sowie durch IT-Prüfer vorgesehen. Seine Anwendung fördert das Verständnis geschäftlicher Ziele sowie die Kommunikation bewährter Methoden und Empfehlungen auf der Grundlage eines allgemein verständlichen und fachlich anerkannten Rahmenwerkes. COBIT steht auf der ISACA-Website (www.isaca.org/cobit) zum Download zur Verfügung. Jedes der folgenden relevanten Produkte und/oder Elemente ist gemäß dem COBIT Framework im IT-Managementprozess organisiert.

- **Control Objectives (Kontrollziele)** — Allgemein gültige Aufstellung der Mindestanforderungen an funktionierende Kontrollen in den IT-Prozessen
- **Management Guidelines (Management-Richtlinien)** — Vorgaben, um die Leistung von IT-Prozessen abzuschätzen und zu verbessern, Berücksichtigung von Reifegradmodellen, RACI-Diagrammen, Zielen und Metriken. Diese Richtlinien bieten einen managementorientierten Rahmen für die laufende und aktive Selbstbewertung der Kontrollfunktionen (Control Self-Assessment) mit besonderem Augenmerk auf:
 - Leistungsmessung
 - Profilierung der IT-Kontrollen
 - Bewusstseinsbildung
 - Festlegung von Benchmarks
- **COBIT Control Practices** — Aussagen zu Risiken und Nutzen sowie Hinweise zur Einführung der Control Objectives
- **IT Assurance Guide** — Vorgaben für jeden Kontrollbereich zur Schaffung eines Verständnisses, zur Bewertung der einzelnen Kontrollen, zur Beurteilung deren Einhaltung und zum Abschätzen des Risikos, das mit der Unwirksamkeit von Kontrollen verbunden ist

Ein vollständiges **Glossar** aller Begriffe finden Sie auf der ISACA Website unter www.isaca.org/glossary. Die Begriffe „Audit“, „Review“ und „Revision/Prüfung“ werden in den Standards, Richtlinien und Verfahren als Synonym genutzt.

Hinweis/Haftungsausschluss: Die ISACA hat in diesem Dokument die Mindestanforderungen dargelegt, die erforderlich sind, um der professionellen Verantwortung gemäß den im Ethik-Kodex der ISACA aufgeführten Anforderungen zu entsprechen. Die ISACA übernimmt keinerlei Gewähr, dass die Verwendung dieses Dokuments zu den gewünschten Ergebnissen führen wird. Die in diesem Dokument enthaltenen Informationen sollten auch nicht dahingehend ausgelegt werden, dass alle ordnungsgemäßen Verfahren und Prüfungen hierin enthalten sind, und dass alle anderen angemessenen Verfahren und Prüfungen, mit denen dieselben Ergebnisse erzielt werden können, hierin ausgeschlossen werden. Bei der Überlegung, wie angemessen ein bestimmtes Verfahren oder eine Prüfmethode ist, sollte der Anwender sich vornehmlich auf seine fachliche Kompetenz stützen und die spezifischen Umstände, die sich aus den Kontrollen des jeweiligen Systems oder der Systemumgebung ergeben, berücksichtigen.

Das ISACA Standards Board ist daran interessiert, die Entwicklung von Standards, Richtlinien und Handlungsanweisungen auf eine möglichst breite Basis zu stellen. Vor der Freigabe von Dokumenten veröffentlicht das Standards Board Entwürfe auf internationaler Ebene und bittet die Leserschaft um Kritik und Anregungen. Das Standards Board bemüht sich, wo dies erforderlich ist, um den Rat besonders qualifizierter oder interessierter Fachleute. Das Standards Board hat ein Programm zur fortlaufenden Verbesserung eingeführt. Hinweise von ISACA-Mitgliedern und anderen interessierten Personen oder Institutionen auf Bereiche, die einer Berücksichtigung im Rahmen von Standards, Richtlinien und Handlungsanweisungen bedürfen, sind stets willkommen. Richten Sie Ihre Vorschläge bitte an ISACA International Headquarters, zu Händen Director of Research Standards and Academic Relations (per E-Mail an standards@isaca.org, per Fax an +1.847.253.1443 oder per Post an die am Ende dieses Dokuments angegebene Anschrift). Dieses Dokument wurde am 1. Dezember 2007 veröffentlicht.

S16 E-Commerce

Einführung

- 01 Die ISACA Standards enthalten obligatorische grundlegende Prinzipien und wichtige Verfahren (durch Fettdruck gekennzeichnet) sowie weitere Orientierungshilfen.
- 02 Dieser IT-Prüfungsstandard soll Normen setzen und als Orientierung für die Prüfung von E-Commerce-Umgebungen dienen.

Standard

- 03 **Bei der Prüfung von E-Commerce-Umgebungen muss der IT-Prüfer die relevanten Kontrollen beurteilen und Risiken bewerten, um sicherzustellen, dass die E-Commerce-Transaktionen einem angemessenen Kontrollniveau unterliegen.**

Anmerkungen

- 04 E-Commerce wird definiert als der Prozess, in dessen Rahmen Organisationen auf elektronischem Wege mit ihren Kunden, Lieferanten und anderen externen Geschäftspartnern Geschäfte tätigen, wobei sie das Internet als Trägertechnologie nutzen. Dieser Begriff beinhaltet daher sowohl B2B- (Business-to-Business) als auch B2C-Modelle (Business-to-Consumer).
- 05 Der IT-Prüfer muss bei der Ausarbeitung des IT-Prüfungsplans eine angemessene Methode bzw. einen angemessenen Ansatz für die Risikobewertung verwenden, wobei dieser auch die E-Commerce-Umgebungen berücksichtigen muss.
- 06 Der IT-Prüfer sollte die Verwendung von Datenanalysemethoden in Erwägung ziehen, einschließlich der Verwendung eines Continuous Assurance-Verfahrens, das es IT-Prüfern ermöglicht, die Zuverlässigkeit eines Systems auf fortlaufender Basis zu überwachen und bei der Prüfung der E-Commerce-Aktivitäten zusätzliche selektive Prüfungsnachweise zu erhalten.
- 07 Die Kompetenzen und das Fachwissen, welches für das Verständnis der Auswirkungen von E-Commerce auf das Interne Kontrollsystem und die Implikationen für das Risikomanagement erforderlich sind, hängen in ihrem Grad und Umfang von der Komplexität der E-Commerce-Aktivitäten der jeweiligen Organisation ab.
- 08 Der IT-Prüfer muss vor Beginn der Prüfung Zweck und Relevanz der durch die E-Commerce-Anwendung unterstützten Geschäftsprozesse verstehen, so dass die Prüfungsergebnisse in einem korrekten Zusammenhang bewertet werden können.
- 09 Weitere Informationen zu E-Commerce sind in folgenden Referenzen zu finden:
 - Richtlinie G21, Prüfung von ERP-Systemen (Enterprise Resource Planning-Systemen)
 - Richtlinie G22, Prüfung des Business-to-Consumer-E-Commerce (B2C)
 - Richtlinie G24, Internetbanking
 - Richtlinie G25, Prüfung virtueller Privatnetze (VPN)
 - Richtlinie G33, Allgemeine Überlegungen zur Nutzung des Internets
 - Verfahren P6, Firewalls
 - COBIT Framework und Kontrollziele

Zeitpunkt des Inkrafttretens

- 10 Dieser ISACA Standard gilt für alle IT-Prüfungen, die am oder nach dem 01.02.08 begonnen werden.

2007-2008 ISACA Standards Board

Ravi Muthukrishnan, CISA, CISM, FCA, ISCA Capco IT Services India Private Limited, Indien
Brad David Chin, CISA, CPA Google Inc., USA
Sergio Fleginsky, CISA ICI Paints, Uruguay
Maria Gonzalez, CISA HomeLand Office, Spanien
John Ho Chi, CISA, CISM, CBCP, CFE Ernst & Young, Singapur
Andrew MacLeod, CISA, CIA, FCPA, MACS, PCP Brisbane City Council, Australien
John G. Ott, CISA, CPA AmerisourceBergen, USA
Jason Thompson, CISA, CIA KPMG LLP, USA
V. Meera, CISA, CISM, ACS, CISSP, CWA Microsoft Corp., USA

© 2007 ISACA. Alle Rechte vorbehalten.

ISACA
3701 Algonquin Road, Suite 1010
Rolling Meadows, IL 60008 USA
Tel: +1.847.253.1545
Fax: +1.847.253.1443
E-Mail: standards@isaca.org
Website: www.isaca.org