

Die speziellen Eigenarten des Information Systems (IS) Auditing (IS-Prüfung) und die Kenntnisse, die zur Durchführung solcher Prüfungen erforderlich sind, erfordern die Erstellung spezieller Standards für IS-Prüfungen. Eines der Ziele der Information Systems Audit and Control Association® (ISACA®) ist es, die Entwicklung solcher global anwendbarer Standards zu fördern. Entwicklung und Verbreitung von IS Auditing Standards ist ein Hauptanliegen des Engagements der ISACA im Prüfungswesen. Die IS Auditing Standards umfassen Dokumente auf mehreren Ebenen:

- In den **Standards** sind obligatorische Anforderungen für IS-Prüfung und Berichtswesen definiert. Sie sollen
 - IS-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 Auditors®) 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 von IS-Prüfstandards. Der IS-Prüfer sollte sich bei der Durchsetzung 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 Einhaltung und Durchsetzung der IS Auditing Standards durch Bereitstellung weiterer Informationen unterstützen.
- Die **Verfahren** zeigen Beispiele dafür, welche Verfahren bei einer Prüfung vom IS-Prüfer angewendet werden können. Die Verfahren informieren darüber, wie bei der Durchführung von IS-Prüfungen den Standards entsprochen werden kann, sie stellen aber keine Mindestanforderungen dar. Vielmehr sollen die Verfahren Einhaltung und Durchsetzung der IS Auditing Standards durch Bereitstellung weiterer Informationen unterstützen.

Die **COBIT®** Ressourcen sollten als Leitfaden für gängige, generell akzeptierte Praktiken ("Best Practices") verwendet werden. Im **COBIT Framework** heißt es: "Es liegt in der Verantwortung der Geschäftsleitung, alle Vermögenswerte des Unternehmens zu schützen. Um dieser Verantwortung gerecht zu werden, und um die gesteckten Ziele zu erreichen, muss die Geschäftsleitung ein wirksames internes Kontrollsystem einführen." COBIT umfasst einen detaillierten Katalog an Kontrollen und Kontrollmechanismen für das IS-Management. Die Auswahl des für die jeweilige Prüfung am besten geeigneten COBIT-Materials hängt von der Wahl des spezifischen COBIT IT-Prozesses und den entsprechenden COBIT-Informationskriterien ab.

Jedes der folgenden Elemente ist gemäß dem **COBIT Framework** im IT Managementprozess organisiert. COBIT ist zur Verwendung durch Unternehmens- und IT-Management sowie durch IS-Prüfer vorgesehen. Seine Anwendung macht es möglich, Geschäftsziele zu verstehen und ermöglicht die Kommunikation von "Best Practices" und Empfehlungen auf der Grundlage eines allgemein verständlichen und fachlich anerkannten Standardwerks. COBIT umfasst:

- **Kontrollziele (Control Objectives)**—eine komplexe und detaillierte allgemein gültige Aufstellung der Mindestanforderungen an funktionierende Kontrollen
- **Kontrollpraktiken (Control Practices)**—praktische Verfahrensweisen und Anweisungen zur Einführung von Kontrollzielen
- **Revisionsrichtlinien (Audit Guidelines)**—Richtlinien für jeden Kontrollbereich darüber, wie man einen Einblick erhält, einzelne Kontrollen bewertet, die Einhaltung beurteilt und das Risiko ermisst, das mit der Unwirksamkeit von Kontrollen verbunden ist
- **Management-Richtlinien (Management Guidelines)**—Anweisungen, um die Leistung von IT-Prozessen abzuschätzen und zu verbessern, unter Berücksichtigung von Reifegradmodellen, Metriken und kritischen Erfolgsfaktoren Diese Richtlinien bieten einen managementorientierten Rahmen für die laufende und proaktive Selbstbewertung der Kontrollfunktion (Control Self-Assessment) mit besonderem Augenmerk auf:
 - **Leistungsbewertung (Performance Measurement)**—Wie gut unterstützt die IT-Funktion die Geschäftsvorgänge? Die Management Guidelines können für Self-Assessment Workshops eingesetzt werden, und sie können auch die Implementierung kontinuierlicher Überwachungs- und Verbesserungsverfahren im Rahmen eines IT-Governance-Schemas unterstützen.
 - **Profile der IT-Kontrollen (IT Control Profiling)**—Welche IT-Prozesse sind wichtig? Was sind die kritischen Erfolgsfaktoren für Kontrolle?
 - **Bewusstsein (Awareness)**—Wie groß ist das Risiko, die Ziele nicht zu erreichen?
 - **Benchmarking**—Wie verfahren die anderen? Wie können Ergebnisse gemessen und verglichen werden? Die Management Guidelines geben den Nutzern Beispielmetriken an die Hand, mit denen sie die IT-Performance in betrieblichen Größen darstellen können. Die Hauptziel-Indikatoren identifizieren und messen die Ergebnisse von IT-Prozessen und die Hauptperformance-Indikatoren bewerten, wie gut die Prozesse funktionieren, indem die Auslöser der Prozesse gemessen werden. Reifegradmerkmale helfen bei der Fähigkeitsbewertung und dem Benchmarking, wodurch die Unternehmensleitung in die Lage versetzt wird, die Kontrollfähigkeiten zu messen sowie Kontrolllücken und Verbesserungsstrategien zu identifizieren.

Ein vollständiges **Glossar** aller Begriffe finden Sie auf der ISACA Website unter www.isaca.org/glossary. Die Begriffe "Audit", "Review" und "Revision/Prüfung" sind austauschbar.

Hinweis: 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 Verfahren 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, auch 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 der Standardisierung 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 research@isaca.org, per Fax an +1.847.253.1443 oder per Post an die am Ende dieses Dokuments angegebene Anschrift). Dieses Dokument wurde am 15. Oktober 2004 erstellt.

Audit-Charta S1

Einführung

- 01 Die ISACA Standards enthalten obligatorische grundlegende Prinzipien und wichtige Verfahren (durch Fettdruck gekennzeichnet) sowie weitere Orientierungshilfen.
- 02 Dieser IS Prüfstandard soll als Orientierung bezüglich der Audit Charta dienen, die dem IS Prüfungsprozess zugrundeliegt.

Standard

- 03 Zweck, Verantwortungsbereiche, Autorität und Rechenschaftspflicht der IS-Prüffunktion bzw. der für die IS-Prüfung zugewiesenen Aufgaben müssen in einer Charta oder einem schriftlichen Auftrag festgehalten werden.**
- 04 Die Charta bzw. der Auftrag muss von einer angemessenen Führungsebene innerhalb der Organisation(en) genehmigt werden.**

Anmerkungen

- 05 Für interne IS-Revisionsstellen sollte eine Charta für die laufenden Aktivitäten erstellt werden. Diese Audit-Charta sollte mindestens einmal pro Jahr, bei sehr unterschiedlichen oder veränderten Verantwortungsbereichen auch öfter, überprüft und ggf. revidiert werden. Interne IS-Prüfer können ebenfalls Auftragsschreiben zur weiteren Klärung oder Bestätigung von spezifischen, im Rahmen der Revision oder außerhalb des Rahmens der Revision liegenden Aufgaben verwenden. Bei einer externen IS-Prüfung sollte normalerweise ein Auftragsschreiben für jeden Auftrag erstellt werden.
- 06 Die Charta bzw. der Auftrag müssen detailliert genug sein, so dass Zweck, Verantwortung und Einschränkungen der Prüffunktion oder Prüfaufgabe klar dargelegt sind.
- 07 Die Charta bzw. der Auftrag sollte regelmäßig überprüft und ggf. revidiert werden, um sicherzustellen, dass Zweck und Verantwortungsbereich dokumentiert worden sind.
- 08 Weitere Informationen zur Erstellung einer Audit-Charta oder eines Auftragsschreibens sind in folgenden Referenzen zu finden:
 - IS-Richtlinie G5, Audit-Charta
 - COBIT *Framework*, Kontrollziel M4

Zeitpunkt des Inkrafttretens

- 09 Dieser ISACA Standard gilt für alle IS-Prüfungen, die am oder nach dem 01.01.05 begonnen werden.

Information Systems Audit and Control Association 2004-2005 Standards Board

Chair, Sergio Fleginsky, CISA PricewaterhouseCoopers, Uruguay
Svein Aldal Aldal Consulting, Norwegen
John Beveridge, CISA, CISM, CFE, CGFM, CQA Office of the Massachusetts State Auditor, USA
Claudio Cilli, Ph.D., CISA, CISM, CIA, CISSP Value Partners, Italien
Christina Ledesma, CISA, CISM Citibank NA Sucursal, Uruguay
Andrew MacLeod, CISA, CIA, FCPA, MACS, PCP Brisbane City Council, Australien
V. Meera, CISA, CISM, ACS, CISSP, CWA Microsoft Corporation, USA
Ravi Muthukrishnan, CISA, CISM, FCA, ISCA NextLinx India Private Ltd., Indien
Peter Niblett, CISA, CISM, CA, CIA, FCPA WHK Day Neilson, Australien
John G. Ott, CISA, CPA Aetna Inc., USA
Thomas Thompson, CISA Ernst & Young, UAE

© Copyright 2004
Information Systems Audit and Control Association
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