

Het gespecialiseerde karakter van een audit van een informatiesysteem (IS) en de capaciteiten die vereist zijn om een dergelijke audit uit te voeren, vereisen normen die specifiek van toepassing zijn op IS-audits. Een van de doelstellingen van de Information Systems Audit and Control Association® (ISACA®) is algemeen aanvaarde normen te geven die overeenkomen met aan haar visie. De ontwikkeling en verspreiding van de IS-auditnormen vormen de bijdrage van ISACA aan de auditwereld. De IS-auditnormen zijn er op verschillende niveaus:

- **Normen** zijn verplichte vereisten voor IS-audit en –rapportering. Zij informeren:
 - IS-auditors over de minimale vereisten zoals omschreven in de professionele ethische code van ISACA.
 - Het management en andere betrokken partijen over verwachtingen in verband met het werk van IS-auditors.
 - Houders van het predikaat Certified Information System Auditor® (CISA®) over de vereisten bij het uitvoeren van audits. (Wanneer deze normen niet worden nageleefd, kan de Raad van Bestuur van ISACA of een bevoegde commissie van ISACA een onderzoek instellen naar het gedrag van de CISA-houder, wat uiteindelijk tot een disciplinaire maatregel kan leiden.)
- **Richtlijnen** geven instructies voor de toepassing van de IS-auditnormen. De IS-auditor moet hier rekening mee houden bij het bepalen hoe de normen kunnen worden geïmplementeerd. Hij moet zijn professioneel inzicht gebruiken bij de toepassing hiervan, en eventuele afwijkingen verantwoorden. Het doel van de IS-auditrichtlijnen is extra informatie te verschaffen over hoe aan de IS-auditnormen kan worden voldaan.
- **Procedures** zijn voorbeelden die een IS-auditor kan volgen tijdens een auditopdracht. De procedures geven de richting aan hoe aan de normen kan worden voldaan tijdens de uitvoering van een IS-audit. Het doel van de IS-auditprocedures is meer informatie te verschaffen over hoe aan de IS-auditnormen kan worden voldaan.

CobIT® hulpmiddelen moeten worden gebruikt als richtlijnen. Het CobIT *Framework* stelt: “Het management van de onderneming is verantwoordelijk voor alle assets van de onderneming. Om deze verantwoordelijkheid te kunnen nemen moet het management een passend intern controlesysteem invoeren.” CobIT biedt een uitgebreid geheel van controlemiddelen en –technieken voor het beheer van informatiesystemen.

Zoals beschreven in het CobIT *Framework*, wordt elk van de volgende elementen ondersteund door een IT managementproces. CobIT is bedoeld voor gebruik door het bedrijfs- en IT-management, alsook door IS-auditors. Het helpt de bedrijfsdoelstellingen te begrijpen, de best practice duidelijk te maken en aanbevelingen te doen rond een algemeen geaccepteerde en erkende normenkader. CobIT omvat:

- **Controledoelstellingen** – Hoog gestelde en gedetailleerde algemene verklaringen
- **Auditvoorbeelden** – Praktische voorbeelden hoe controledoelstellingen worden gehaald.
- **Auditrichtlijnen** – Richtlijnen voor elk controledomein om inzicht te verwerven, elke controle te evalueren, de conformiteit te beoordelen en het risico te staven als aan de controles niet voldaan wordt
- **Managementrichtlijnen** – Richtlijnen om de prestatie van het IT-proces te beoordelen en te verbeteren, door middel van maturiteitsmodellen, metrische gegevens en kritische succesfactoren. Zij bieden een managementgericht kader voor een permanente en preventieve zelfevaluatie van de controle, die specifiek is toegespitst op:
 - **Prestatiemeting** – Hoe goed ondersteunt de IT-afdeling de bedrijfsvoering? De managementrichtlijnen kunnen worden gebruikt om workshops over zelfevaluatie te ondersteunen, ze kunnen ook worden gebruikt om de implementatie te ondersteunen van permanente controle- en verbeteringsprocedures in het kader van een IT governance programma.
 - **IT controleprofilering** – Welke IT-processen zijn belangrijk? Welke zijn de cruciale succesfactoren voor de controle?
 - **Bewustzijn** – Wat zijn de risico's dat de doelstellingen niet worden gehaald?
 - **Benchmarking** – Wat doen de anderen? Hoe kunnen resultaten worden gemeten en vergeleken? De managementrichtlijnen geven typisch metrische gegevens die het mogelijk maken de IT-prestatie te evalueren in bedrijfstermen. De voornaamste doelindicatoren specificeren en meten resultaten van IT-processen. De voornaamste prestatie-indicatoren evalueren hoe goed de processen presteren. Maturiteitsmodellen en maturiteitsattributen zorgen voor competentie-evaluatie en benchmarking. Ze helpen het management de controlecompetentie te meten, tekortkomingen op te sporen en verbeteringsstrategieën vast te stellen.

Een **Woordenlijst** van de gebruikte terminologie vindt u op de website van ISACA op www.isaca.org/glossary. De woorden audit en controle worden door elkaar gebruikt.

Afwijzing van aansprakelijkheid: ISACA heeft deze richtlijnen opgesteld. Aan deze richtlijnen dient minimaal te worden voldaan. Ze zijn omschreven in de professionele ethische code van ISACA. ISACA beweert op geen enkele wijze dat gebruik van dit product een geslaagd resultaat garandeert. Bij het bepalen van de geschiktheid van een bepaalde procedure of test, moet de controlespecialist zijn/haar eigen professionele inzicht gebruiken.

De Raad van Bestuur van ISACA voert een ruim overleg in de voorbereiding van de IS-auditnormen, -richtlijnen en –procedures. Alvorens documenten te publiceren, publiceert de Normencommissie internationaal ontwerpversies hiervan zodat het grote publiek zijn opmerkingen kan geven. De Normencommissie kijkt ook uit naar mensen met een bijzonder expertise in of belangstelling voor het onderwerp, met het oog op consultatie indien nodig. De Normencommissie werkt met een permanent ontwikkelingsprogramma en is blij met elke inbreng van ISACA-leden en andere geïnteresseerde partijen. Suggesties zijn welkom via e-mail (standards@isaca.org), fax (+1 847 253 1443) of per post (adres achteraan dit document) naar ISACA International Headquarters, ter attentie van de directeur voor onderzoeksnormen en academische relaties. Dit materiaal werd gepubliceerd op 15 oktober 2004.

Audithandvest S1

Inleiding

- 01 De ISACA-normen bevatten basisprincipes en essentiële procedures, hier vet gedrukt, die verplicht zijn, samen met aanverwante richtlijnen.
- 02 Het doel van deze IS-auditnorm is richtlijnen te geven met betrekking tot het audithandvest dat wordt gebruikt tijdens het auditproces.

Norm

- 01 **Het doel, de verantwoordelijkheid, de bevoegdheid en aansprakelijkheid van de auditfunctie moet duidelijk worden toegelicht in een audithandvest of contractbrief.**
- 02 **Het audithandvest of de contractbrief moet op passend niveau binnen de organisatie(s) worden besproken en goedgekeurd.**

Opmerking

- 05 Voor de audit van een intern informatiesysteem, moet een audithandvest worden opgesteld voor doorlopende activiteiten. Het audithandvest moet jaarlijks worden herzien, of vaker als verantwoordelijkheden zijn veranderd. De interne IS-auditor kan een contractbrief gebruiken om de betrokkenheid bij specifieke audit- of niet-auditopdracht te verduidelijken of te bevestigen. Voor een externe IS-audit moet normaal een contractbrief worden opgesteld voor elke audit- of niet-auditopdracht.
- 06 Het audithandvest of de contractbrief moeten voldoende gedetailleerd zijn om het doel, de verantwoordelijkheid en beperkingen van de auditfunctie of auditopdracht duidelijk te maken.
- 07 Het audithandvest of de contractbrief moeten regelmatig worden herzien om te garanderen dat het doel en de aansprakelijkheid goed zijn omschreven.
- 08 Voor meer informatie over het opstellen van een audithandvest of contractbrief wordt verwezen naar de volgende richtlijnen:
- IS Auditrichtlijn G5, Audithandvest
 - COBIT *Framework*, Controledoelstelling M4

Geldigheidsdatum

- 09 Deze ISACA-norm is geldig voor alle audits van informatiesystemen vanaf 1 januari 2005.

Normcommissie 2004-2005 Information Systems Audit and Control Association

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

© Copyright 2004
Information Systems Audit and Control Association
3701 Algonquin Road, Suite 1010
Rolling Meadows, IL 60008 USA
Telefoon: +1.847.253.1545
Fax: +1.847.253.1443
E-mail: standards@isaca.org
Website: www.isaca.org