

IS-AUDITNORM

ONREGELMATIGE EN ONRECHTMATIGE HANDELINGEN

DOCUMENT S9

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 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 geaccepteerd en erkend 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 toegespit 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 is uitgegeven op 1 juli 2005.

Onregelmatige en onrechtmatige handelingen S9

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 ISACA-normen is richtlijnen op te stellen en te geven verband houdend met onregelmatige en onrechtmatige handelingen waarop de IS-auditor moet letten tijdens het auditproces.

Normen

- 03 **Bij het plannen en uitvoeren van de audit moet de IS-auditor letten op het risico van onregelmatige en onrechtmatige handelingen.**
- 04 **De IS-auditor moet gedurende de audit een professionele, kritische houding aanhouden en rekening houden met de mogelijkheid dat er belangrijke onjuistheden kunnen bestaan in verband met onregelmatige en onrechtmatige handelingen . Dit onafhankelijk van zijn inschatting op de kans op onregelmatigheden en illegale handelingen.**
- 05 **De IS-auditor moet zich op de hoogte stellen van de organisatie en haar omgeving, inclusief de interne controles.**
- 06 **De IS-auditor moet voldoende en adequaat auditbewijs verzamelen om vast te stellen of het management of anderen binnen de organisatie kennis hebben van werkelijke, veronderstelde of beweerde onregelmatigheden of illegale handelingen.**
- 07 **Bij het uitvoeren van het auditprocedures voor het verkrijgen van inzicht in de organisatie en de omgeving hiervan, moet de IS-auditor rekening houden met ongewone en onverwachte relaties. deze kunnen wijzen op een verhoogd risico van relevante onjuistheden samenhangend met onregelmatige en onrechtmatige handelingen.**
- 08 **De IS-auditor moet procedures ontwerpen en doorlopen waarmee wordt getest hoe groot risico's zijn dat het management interne controles omzeilt.**
- 09 **Als de IS-auditor een onjuistheid ontdekt, moet hij bepalen of deze wijst op een onregelmatigheid of een illegale handeling. Vervolgens moet de IS-auditor de implicaties overwegen in relatie tot de overige aspecten van de audit en speciaal tot de informatieverstrekking door het management.**
- 10 **De IS-auditor moet ten minste jaarlijks schriftelijke informatie van het management verkrijgen. Deze moet:**
 - **de verantwoordelijkheid voor het ontwerp en de implementatie van interne controles ter voorkoming van onregelmatige en onrechtmatige handelingen bevatten,**
 - **de IS-auditor inzicht geven in de resultaten van de risico's van het bestaan van relevante onjuistheden door onregelmatige of onrechtmatige handelingen,**
 - **de IS-auditor op de hoogte stellen van kennis van onregelmatige of onrechtmatige handelingen die van invloed zijn op de organisatie in relatie tot:**
 - **het management,**
 - **werknemers met significante rollen in de interne controle;**
 - **de IS-auditor op de hoogte stellen van kennis van beschuldigingen van onregelmatige of onrechtmatige handelingen, of verwachte onregelmatige of onrechtmatige handelingen, die van invloed zijn op de organisatie, zoals gemeld door werknemers, vroegere werknemers, controleurs en anderen.**
- 11 **Als de IS-auditor een significante onregelmatige of onrechtmatige handeling heeft aangetroffen, of informatie verkrijgt dat een significante onregelmatige of onrechtmatige handeling kan bestaan, moet hij dit tijdig doorgeven aan het daarvoor verantwoordelijke managementniveau.**
- 12 **Als de IS-auditor een significante onregelmatige of onrechtmatige handeling heeft aangetroffen waarbij het management of werknemers zijn betrokken met een significante rol in de interne controle, moet hij dit tijdig doorgeven aan degenen die met governance zijn belast.**
- 13 **De IS-auditor moet het daarvoor verantwoordelijke managementniveau op de hoogte stellen van significante zwakten in het ontwerp en de implementatie van interne controles, ter voorkoming en detectie van onregelmatige en onrechtmatige handelingen die de IS-auditor tijdens de audit tegengekomen kan zijn.**
- 14 **Als de IS-auditor vanwege een relevante onjuistheid of onrechtmatige handeling uitzonderlijke omstandigheden tegenkomt, die van invloed zijn op het voortzetten van de audit, moet de IS-auditor de wettelijke en beroepsmatige verantwoordelijkheden nemen die onder de gegeven omstandigheden van toepassing zijn. De IS-auditor is verplicht te rapporteren aan degenen waarmee hij de overeenkomst heeft aangegaan, of in sommige gevallen aan degenen die belast is met governance of aan regulerende autoriteiten, of overwegen zich uit de opdracht terug te trekken.**
- 15 **De IS-auditor moet alle communicatie met het management of degenen belast met governance, de regulerende autoriteiten of anderen vastleggen. Het betreft de plannings, resultaten, evaluaties en conclusies die betrekking hebben op significante onregelmatige en onrechtmatige handelingen.**

Opmerkingen

- 16 De IS-auditor moet de IS Auditing Guideline G19, Irregularities and Illegal Acts volgen voor definities van wat een onregelmatige of onrechtmatige handeling is.
- 17 De IS-auditor moet redelijke zekerheid verkrijgen dat er geen relevante onjuistheden zijn die zijn veroorzaakt door onregelmatigheden of onrechtmatigheden. Een IS-auditor kan geen absolute zekerheid verkrijgen, vanwege factoren als gebruik van eigen oordeel, het bereik van de testen en de inherente beperkingen van interne controles. Het auditbewijs dat tijdens een audit voor de IS-auditor beschikbaar is, moet overtuigend zijn. Er dient een deugdelijke grondslag te zijn.
- 18 Het risico op het niet detecteren van relevante onjuistheden door onrechtmatige handelingen is groter dan dat op het niet detecteren van relevante onjuistheden door onregelmatigheden of fouten, omdat onrechtmatige handelingen ingewikkelder kunnen zijn opgezet voor het verbergen van doelbewuste onjuistheden voor de IS-auditor.
- 19 Eerdere ervaringen met en kennis van de organisatie van de IS-auditor vergemakkelijkt de audit. Bij het verzamelen van informatie en het uitvoeren van auditprocedures mag van de IS-auditor niet worden verwacht dat deze eerdere ervaringen geheel negeert, maar mag wel een niveau van professionele scepsis worden verwacht. De IS-auditor mag zich niet tevreden stellen met een minder overtuigend auditbewijs op basis van de opvatting dat het management en degenen die met governance zijn belast eerlijk en integer zijn. De IS-auditor en het betrokken team moeten de gevoeligheid van de organisatie voor onregelmatige en onrechtmatige handelingen bespreken als onderdeel van het planningsproces en gedurende de hele audit.

- 20 Voor het evalueren van het risico op het bestaan van significante onregelmatige en onrechtmatige handelingen, moet de IS-auditor overwegen gebruik te maken van:
- eerdere kennis van en ervaring met de organisatie (inclusief ervaring met de eerlijkheid en integriteit van het management en degenen die met governance zijn belast),
 - informatie verkregen uit ondervraging van het management,
 - informatie van het management en de resultaten van interne controles,
 - overige betrouwbare informatie die tijdens de audit is verkregen,
 - inschatting door het management van het risico op onregelmatige en onrechtmatige handelingen en het proces van het management voor het identificeren van en reageren op deze risico's.
- 21 Voor meer informatie over onregelmatige en onrechtmatige handelingen wordt verwezen naar de volgende richtlijnen:
- IS Auditing Guideline G5, Audit Charter
 - COBIT Framework, control objective DS3, DS5, DS9, DS11 en PO6
 - Sarbanes-Oxley Act of 2002
 - Foreign Corrupt Practices Act 1977
 - Code Tabaksblad

Geldigheidsdatum

- 22 Deze ISACA-norm is geldig voor alle audits van informatiesystemen vanaf 1 september 2005.

Normcommissie 2004-2005 Information Systems Audit and Control Association

Voorzitter, Sergio Fleginsky, CISA	ICI Paints, 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	Tangerine Consulting, Italië
Christina Ledesma, CISA, CISM	Citibank NA Sucursal, Uruguay
Andrew MacLeod, CISA, CIA, FCPA, PCP	Brisbane City Council, Australië
V. Meera, CISA, CISM, ACS, CWA	Microsoft Corporation, USA
Ravi Muthukrishnan, CISA, CISM, FCA, ISCA	Ikanos Communications., India
Peter Niblett, CISA, CISM, CA, CIA, FCPA	WHK Day Neilson, Australië
John G. Ott, CISA, CPA	AmerisourceBergen, USA
Thomas Thompson, CISA	Ernst & Young, VAE

© Copyright 2005
 Information Systems Audit and Control Association
 3701 Algonquin Road, Suite 1010
 Rolling Meadows, IL 60008 USA
 Telefoonnummer: +1.847.253.1545
 Fax: +1.847.253.1443
 E-mail: standards@isaca.org
 Website: www.isaca.org