

S16 E-COMMERCE

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 doelen van ISACA[®] is algemeen toepasbare normen te propageren om aan haar visie voldoen. De ontwikkeling en verspreiding van de IS-auditnormen vormen een belangrijk onderdeel van de professionele bijdrage van ISACA aan de auditwereld. Het framework van de IS-auditnormen geeft op verschillende niveaus ondersteuning:

- **Normen** zijn verplichte vereisten voor IS-audit en –rapportering. Zij informeren:
 - IS-auditors over het minimale prestatieniveau dat vereist is om te voldoen aan de professionele verantwoordelijkheden zoals omschreven in de ISACA Code of Professional Ethics.
 - Het management en andere betrokken partijen over verwachtingen vanuit de beroepsgroep in verband met het werk van IS-auditors.
 - Houders van het predikaat Certified Information System Auditor[™] (CISA[®]) over de vereisten. Wanneer niet aan deze normen wordt voldaan, kan de Raad van Bestuur van ISACA of een bevoegde commissie van ISACA een onderzoek instellen naar het gedrag van de CISA-houder, hetgeen uiteindelijk tot disciplinaire maatregelen 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** geven voorbeelden van procedures 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, maar stellen geen eisen. Het doel van de IS-auditprocedures is meer informatie te verschaffen over hoe aan de IS-auditnormen kan worden voldaan.

Control Objectives for Information and related Technology (CobIT[®]) is een kader voor IT-governance en een ondersteunend hulpmiddel waarmee managers het gat tussen beheersvereisten, technische zaken en bedrijfsrisico's kunnen overbruggen. CobIT maakt duidelijke beleidsontwikkeling en goede methoden voor IT-beheersing binnen een hele organisatie mogelijk. Het legt de nadruk op het naleven van regelgeving, helpt organisaties meer uit IT te halen, maakt afstemming mogelijk en vereenvoudigt de toepassing van de concepten van het CobIT-kader.

CobIT is bedoeld voor gebruik door het bedrijfs- en IT-management, alsmede door IS-auditors. Het helpt de bedrijfsdoelstellingen te begrijpen en de beste werkmethode en aanbevelingen over te brengen binnen een algemeen geaccepteerd en erkend kader. CobIT kan worden gedownload van de website van ISACA: www.isaca.org/cobit. Zoals beschreven in het CobIT-kader, wordt elk van de volgende producten en/of elementen ondersteund door een IT-beheersproces:

- **Beheersdoelstellingen:** algemene richtlijnen voor minimale goede beheersing in verband met IT-processen.
- **Richtlijnen voor het management:** richtlijnen voor het bepalen en verbeteren van de prestaties van IT-processen, met behulp van maturiteitsmodellen, RACI-diagrammen (Responsible, Accountable, Consulted and/or Informed), doelstellingen en criteria. Zij bieden een managementgericht kader voor een permanente en preventieve zelfevaluatie van de beheersing (control self-assessment), die specifiek is toegespitst op:
 - prestatiemeting
 - IT-beheersprofilering
 - bewustwording
 - benchmarking.
- **CobIT Control Practices:** risico- en waarderingsrichtlijnen en een implementatiegids voor de beheersdoelstellingen.
- **IT Assurance Guide:** richtlijnen voor elk controledomein om inzicht te verwerven, elke controlemaatregel te evalueren, de conformiteit te beoordelen en het risico te staven als aan de controlemaatregel niet wordt voldaan.

Een **Woordenlijst** van de gebruikte terminologie vindt u op de website van ISACA op www.isaca.org/glossary. De woorden audit en beoordeling worden onderling uitwisselbaar gebruikt in IS-normen, -richtlijnen en -procedures.

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. De publicatie mag niet worden beschouwd als inclusief eventuele eigen procedures en tests of exclusief andere procedures en tests die redelijkerwijze bedoeld zijn om dezelfde resultaten te behalen. Bij het bepalen van de geschiktheid van een bepaalde procedure of test, moet de controlespecialist zijn/haar eigen professionele inzicht toepassen op de specifieke controleomstandigheden van de betreffende systemen of IT-omgeving.

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 document is 1 december 2007 uitgebracht.

S16 E-commerce

Inleiding

- 01 De ISACA-normen bevatten de verplichte basisprincipes en essentiële procedures, aangeduid in vetdruk (zwarte letters), samen met aanverwante richtlijnen.
- 02 Het doel van deze ISACA-norm is normen op te stellen en richtlijnen te geven in verband met het beoordelen van e-commerce-omgevingen.

Normen

- 03 De IS-auditor moet bij het beoordelen van e-commerce-omgevingen de van toepassing zijnde beheersmaatregelen evalueren en de risico's bepalen, om zeker te stellen dat e-commercetransacties voldoende worden beheerst.**

Opmerkingen

- 04 E-commerce is gedefinieerd als de processen waarmee organisaties elektronisch handel drijven met hun klanten, leveranciers en andere externe partners, waarbij gebruik wordt gemaakt van internet als ondersteunende technologie. Dit omvat dus zowel e-commercemodellen voor handel tussen bedrijven (B2B of business-to-business) als voor handel met particulieren (B2C of business-to-consumer).
- 05 De IS-auditor moet een toepasselijke risico-evaluatietechniek of aanpak gebruiken bij het opstellen van het algemene IS-auditplan, waarin e-commerce-omgevingen zijn opgenomen.
- 06 De IS-auditor moet het gebruik van gegevensanalysetechnieken overwegen, waaronder het gebruik van doorlopende borging (continuous assurance), waarmee IS-auditoren doorlopend de betrouwbaarheid van het systeem kunnen volgen en via de computer selectief auditbewijs kunnen verzamelen bij het beoordelen van e-commerce-activiteiten.
- 07 Het vaardigheids- en kennisniveau dat vereist is voor het begrijpen van de implicaties van e-commerce op beheersmaatregelen en risicobeheersing, is afhankelijk van de complexiteit van de e-commerce-activiteiten van de organisatie.
- 08 De IS-auditor moet voordat aan de audit wordt begonnen de aard en het belang begrijpen van de bedrijfsprocessen die door de e-commercetoepassing worden ondersteund, zodat de resultaten in de juiste context kunnen worden beoordeeld.
- 09 Voor meer informatie over e-commerce raadpleegt u de volgende richtlijnen:
- Richtlijn G21 Enterprise Resource Planning (ERP) Systems Review
 - Richtlijn G22 Business-to-consumer (B2C) E-commerce Review
 - Richtlijn G24 Internet Banking
 - Richtlijn G25 Review of Virtual Private Networks (VPN)
 - Richtlijn G33 General Considerations on the Use of the Internet
 - Procedure P6 Firewalls
 - COBIT-kader en controledoelstellingen

Geldigheidsdatum

- 10 Deze ISACA-norm geldt voor IS-audits vanaf 1 februari 2008.

2007-2008 Raad van Bestuur ISACA

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

© 2007 ISACA. Alle rechten voorbehouden.

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