Een audit approach voor logisch identiteits- en toegangsbeheer

Gebaseerd op COBIT en ISO17799:2005

Geert Huyck

Identiteits- en toegangsbeheer is een complex en belangrijk proces binnen een bedrijf dat de veiligheid van bedrijfsgegevens moet garanderen. Identiteits- en toegangsbeheer wordt binnen organisaties meer en meer beschouwd als één proces, bestaande uit tal van subprocessen die zich afspelen binnen verschillende departementen, gaande van ondersteunende processen zoals HR over IT tot de business zelf.

G. (Geert) Huyck MA is IT-audit specialist bij Fortis. Hij schreef dit artikel op persoonlijke titel.

Het geheel van deze bedrijfsprocessen en de onderliggende infrastructuur voor het aanmaken, onderhoud en gebruik van digitale identiteiten die toegangsrechten bepalen in elektronische omgevingen, wordt gezien als één proces dat men identiteits- en toegangsbeheer noemt. De noodzaak om bedrijfsgegevens te beschermen in combinatie met het toenemend aantal externe wetgevingen en regelgevingen (SOX, Basel II, HIPAA, …) die eisen stellen aan informatiebeveiliging, heeft ervoor gezorgd dat een degelijke controleomgeving nodig is. Die moet erop gericht zijn de risico's te beperken die zich kunnen voordoen bij het slecht functioneren van dit proces.

Belangrijke termen

Identiteitsbeheer

Identificatie en authenticatie is het proces om iemands identiteit te bewijzen en te bevestigen. In het kader van dit artikel gaat het daarbij om bewijs en bevestiging van de identiteit in elektronische omgevingen. Het is het proces waarin het systeem de identiteit of voorgedane identiteit van de gebruiker, en het bewijs dat nodig is om deze identiteit te bewijzen, valideert. Verschillende technieken kunnen gebruikt worden om de identiteit van een gebruiker te valideren. Deze technieken zijn gebaseerd op iets dat de gebruiker weet, iets dat hij in bezit heeft, iets dat hij is, of een combinatie van deze factoren. Identificatie en authenticatie zijn kritieke bouwstenen voor informatiebeveiliging. Ze zijn nodig voor de meeste types van toegangscontrole en voor het kunnen aantonen van iemands aansprakelijkheid. Aansprakelijkheid kan aangetoond worden als men er zeker van is dat alle activiteiten uitgevoerd op een systeem kunnen worden toegewezen aan een geïdentificeerd persoon. Identiteitsdiefstal kan voorkomen worden door het inrichten van formele identificatie- en authenticatieprocessen en het implementeren van beveiligde toepassingen voor het beheer.

Toegangsbeheer

Gebaseerd op de authenticiteit van een identiteit moet een toegangsbeheersysteem bepalen welke acties een bepaalde persoon kan uitvoeren. Toegangsbeheerregels bepalen welke gebruiker welke applicaties en/of gegevens mag raadplegen en welke acties hij op die gegevens kan uitvoeren. Toegangsbeheer moet gebaseerd worden op het 'minste rechten'-principe, dat wil zeggen dat de gebruiker enkel die rechten

krijgt die hij nodig heeft voor het uitvoeren van zijn functie. Dit principe wordt ook wel het 'nodig-om-te-weten'- en 'nodig-om-te-doen'-principe genoemd. De toegangsrechten van een individu moeten in lijn zijn met de organisatorische bevoegdheden van die gebruiker, waarbij functiescheidingen ook in de systeembevoegdheden tot uitdrukking komen. De nodige functiescheiding en dus ook scheiding van toegangsrechten moeten dus in acht genomen worden bij het bepalen van de toegangsrechten van een gebruiker.

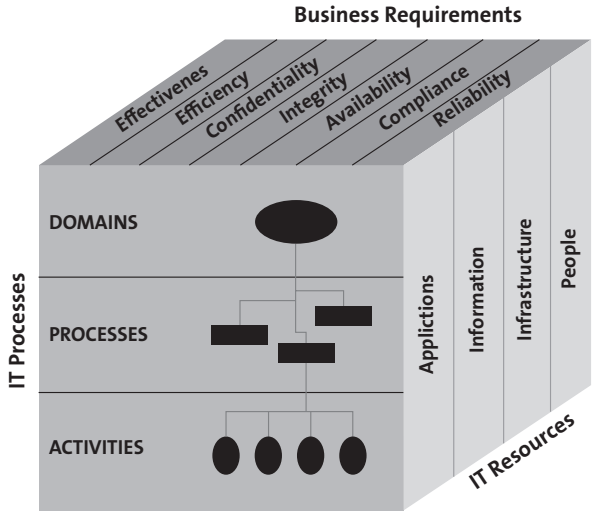
Doel en opzet van het artikel

Doel van het artikel is om te laten zien hoe op een gestructureerde en systematische manier een werkprogramma voor een audit van identiteits- en toegangsbeheer kan worden afgeleid, steunend op COBIT en gebruikmakend van de ISO-standaard 17799:2005 rond informatiebeveiliging. *Control Objectives for Information and related Technology* (COBIT) is een raamwerk voor het gestructureerd inrichten en beoordelen van een IT-omgeving. Hoewel voor elk van de 32 IT-processen gedefinieerd in COBIT 4.1 wel ergens een link zal kunnen worden gemaakt naar identiteits- en toegangsbeheer, proberen we in dit artikel de belangrijkste processen en controleobjectieven op een verantwoorde manier te bepalen om tot een goed werkprogramma voor identiteits- en toegangsbeheer te komen. Hiervoor hebben we twee strategieën gevolgd. Bij de eerste strategie zijn we uitgegaan van de ISO 17799:2005-standaard om tot een lijst van relevante COBIT-processen te komen. Bij de tweede strategie zijn we uitgegaan van een aantal bedrijfsdoelstellingen gedefinieerd in COBIT. Op basis van deze twee lijsten van COBIT-processen en rekening houdend met de nodige bedrijfsvereisten voor informatie en de IT-middelen, komen we zo tot een lijst van activiteiten, 'control practices' en 'assurance steps'. Dit leidt tot een werkprogramma voor het auditeren van identiteits- en toegangscontrole, dat als appendix aan het artikel is toegevoegd. Het voordeel van deze aanpak is dat alle belangrijke processen worden afgedekt, op een verantwoorde manier, om zo aan een compleet beeld rond identiteits- en toegangsbeheer te komen. De strategie vertrekkende van de ISO-standaard zorgt ervoor dat alle belangrijke COBIT-processen worden geselecteerd vertrekkend uit een algemeen aanvaard raamwerk rond informatiebeveiliging. Door vervolgens deze strategie te combineren met de strategie vertrekkende van de bedrijfsdoelstellingen, garanderen we dat zowel businessvereisten en algemeen aanvaarde praktijken rond informatiebeveiliging in acht worden genomen in het auditwerkprogramma.

Bedrijfsvereisten, IT-middelen en IT-processen

COBIT definieert de bedrijfsvereisten voor informatie als de 'informatiecriteria'. Voor elk van de 32 processen gedefinieerd door COBIT, is weergegeven in welke mate deze bijdragen tot deze bedrijfsvereisten.

Hetzelfde is gedaan voor de vier IT-middelen gedefinieerd door COBIT. In dit hoofdstuk zullen we de bedrijfsvereisten voor informatie en de IT-middelen selecteren die beïnvloed worden door een degelijk identiteits- en toegangsbeheerproces.



Bedrijfsvereisten

Om tegemoet te komen aan de bedrijfsdoelstellingen, moet informatie voldoen aan een aantal kwaliteitseisen die COBIT de 'Bedrijfsvereisten voor informatie' noemt. Gebaseerd op de ruimere kwaliteits- en beveiligingsvereisten zijn zeven afzonderlijke en zeker overlappende informatiecriteria gedefinieerd:

- **Effectiviteit** behandelt de relevantie van informatie voor het bedrijf en het bedrijfsproces en behandelt of deze informatie op een snelle, correcte en consistente vorm wordt afgeleverd.
- **Efficiëntie** behandelt het beschikbaar stellen van informatie voor een optimaal gebruik door gebruik te maken van IT-middelen.
- **Vertrouwelijkheid** behandelt de bescherming van gevoelige informatie tegen ongeautoriseerde toegang.
- **Integriteit** behandelt de correctheid en volledigheid van gegevens in overeenstemming met de bedrijfsverwachtingen.
- **Beschikbaarheid** behandelt het beschikbaar zijn van gegevens, nu en in de toekomst, indien deze nodig zijn voor een bepaald bedrijfsproces. Het behandelt ook het voorzien van de nodige systemen voor het bewaren van de gegevens en het tijdig beschikbaar stellen van de gegevens.
- **Compliance** behandelt dat bedrijfsprocessen in lijn zijn met wetgevingen, regelgevingen en contractuele overeenkomsten.
- **Betrouwbaarheid** behandelt dat de aangeleverde informatie aan het management of aan een proces volledig correct is voor het maken van de juiste beslissingen.

Een degelijk identiteits- en toegangsbeheerproces moet primair kijken naar de vertrouwelijkheid en integriteit, en secundair ook naar beschikbaarheid, compliance en betrouwbaarheid van gegevens.

Deze COBIT-informatiecriteria zullen, rekening houdend met hun relatieve belang, in acht worden genomen wanneer

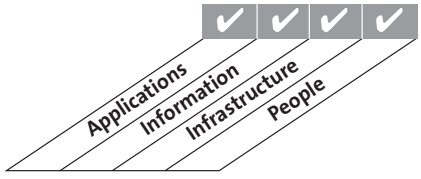
we later in dit artikel beschrijven hoe we de relevante COBIT-processen voor identiteits- en toegangsbeheer selecteren.

IT-middelen

COBIT definieert de volgende IT-middelen:

- **Toepassingen of applicaties** zijn geautomatiseerde gebruikerssystemen en geautomatiseerde procedures die informatie verwerken.
- **Informatie** is gegevens in al zijn vormen (voor, tijdens of na de verwerking door systemen) en bruikbaar voor het bedrijf.
- **Infrastructuur** is de technologie en de faciliteiten (databanken, netwerken, besturingssystemen) die toelaten dat applicaties gegevens verwerken.
- **Mensen** zijn het personeel die nodig zijn voor het plannen, organiseren, aanschaffen, implementeren, ondersteunen, opvolgen en evalueren van informaticasystemen en diensten. Deze kunnen zowel internen als externen zijn.

Identiteits- en toegangsbeheer kan beschreven worden als het proces om identiteit en toegangsrechten van **mensen** tot **informatie** te definiëren, gebruikmakende van de **toepassingen** en **infrastructuur** van de organisatie.
Voor identiteits- en toegangsbeheer zijn dus alle IT-middelen gedefinieerd door COBIT relevant.

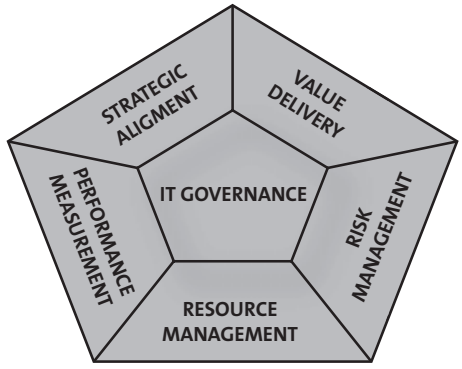


IT-processen

In de volgende paragrafen worden de relevante domeinen, COBIT-processen en activiteiten geselecteerd, startende vanuit de ISO-standaard rond informatiebeveiliging 17799:2005 en van de bedrijfsdoelstellingen gedefinieerd door COBIT.

IT bestuur: belang voor identiteits- en toegangsbeheer

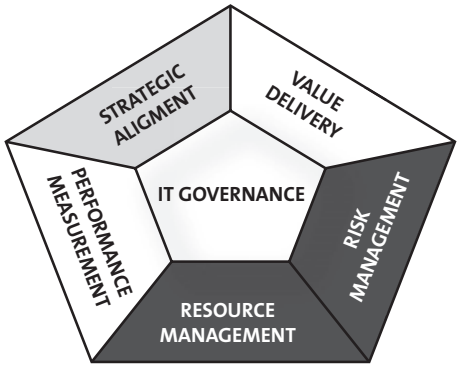
COBIT definieert vijf focus gebieden voor degelijk IT-bestuur:
'Strategic Alignment' focust op het zorgen voor overeenkomst en aansluiting tussen bedrijfsplannen en IT-plannen; definiëren, valideren en onderhouden van de toegevoegde waarde van IT en het afgestemd zijn van de werkwijze van IT op de werkwijze van het bedrijf.
'Value delivery' gaat over het verkrijgen van waardevoordeel gedurende de levenscyclus van applicaties. IT levert toegevoegde waarde aan het bedrijf door het optimaliseren van kosten en het bewijzen van de intrinsieke waarde van applicaties en IT-infrastructuur.
'Resource management' gaat over het optimaal investeren in, en het degelijke management van kritische IT-middelen zoals applicaties, informatie, infrastructuur en mensen. Het belangrijkste hierbij is het optimaal gebruik van kennis en de onderliggende infrastructuur.
'Risk management' veronderstelt risicobesef bij senior managers, een duidelijk begrip en voeling van het bedrijf met risico's die het loopt, verstand van de compliancebehoeften, een duidelijk inzicht in de verschillende risico's binnen de organisatie en managementverantwoordelijkheden binnen de organisatie om deze risico's te minimaliseren.
'Performance measurement' volgt de implementatie van de strategie op, het aantal projecten dat wordt afgerond, het gebruik van IT-middelen, de performantie van processen en diensten gebruik makend van bijvoorbeeld 'balanced scorecards' die strategie in meetbare acties en doelen omschrijft.



Voor identiteit en toegangsbeheer zijn volgende bestuursprincipes van primordiaal belang:
Resource management: Zoals beschreven in voorgaande paragraaf zijn alle vier de IT-middelen relevant voor identiteit en toegangsbeheer. Zoals gespecificeerd in de definitie is identiteits- en toegangsbeheer een proces om identiteit en toegangsrechten van mensen tot informatie te definiëren gebruikmakend van de organisatorische toepassingen en infrastructuur. Het beheer van IT-middelen wordt dus in grote mate beïnvloed door het identiteits- en toegangsbeheerproces.
Risk management: De implementatie van een betrouwbaar identiteits- en toegangsbeheerproces vergt volledige steun van het topmanagement. Het topmanagement moet de risico's van ongeautoriseerde toegang tot gegevens begrijpen en adresseren, en moet de compliancevereisten begrijpen die hun origine hebben in externe wetten en regelgeving. In die zin is identiteits- en toegangsbeheer een hele duidelijke maatregel waarmee het management uitdrukking kan geven aan risk response (integraal onderdeel van risk management).

Het is vanzelfsprekend ook heel belangrijk dat het identiteits- en toegangsbeheersysteem de bedrijfsstrategie onder-

steunt. We hebben er dan ook voor gekozen om dit mee op te nemen na resource management en risk management.



Gedetailleerde controleobjectieven voor identiteit en toegangsbeheer

Benadering beginnende van ISO 17799:2005

Een eerste benadering die werd gevolgd om tot een lijst van relevante COBIT-processen en controleobjectieven voor identiteits- en toegangsbeheer te komen, was om te starten vanuit de ISO 17799:2005-standaard. Deze standaard wordt erkend als de globale standaard rond informatiebeveiliging en is daarom een goed vertrekpunt.

ISO 17799:2005 *'Code of Practice for Information Security Management'* is een internationale standaard. Deze internationale standaard werd gepubliceerd door de International Standard Organisation (ISO) en de 'International Electro Technical Commission' (IEC), die samen een technisch comité oprichtten, namelijk ISO/IEC JTC 1. De historische bron voor de standaard was BS 7799-1, waarvan essentiële stukken werden overgenomen voor het schrijven en de ontwikkeling van 'ISO/IEC 17799:2005 *Information Technology - Code of Practice For Information Security Management'*.

De ISO 17799:2005-standaard bestaat uit 11 hoofdstukken rond beveiliging:

- beveiligingsbeleid;
- organiseren van informatiebeveiliging;
- activabeheer;
- beveiliging menselijke middelen;
- fysieke en omgevingbeveiliging;
- communicatie en verrichtingenbeheer;
- toegangscontrole;
- informaticasystemen: acquisitie, ontwikkeling en onderhoud;
- informatiebeveiliging: incidentenbeheer;
- bedrijfscontinuïteitbeheer;
- naleving.

Elk van deze beveiligingscategorieën bevat:

- een controleobjectief dat specificeert wat er moet bereikt worden;
- een of meerdere maatregelen die toegepast kunnen worden om het controleobjectief te bereiken.

Die maatregelen bevatten naast bijkomende informatie een implementatiebegeleiding die uitlegt hoe men kan voldoen aan het controleobjectief. Voor verdere detailinformatie verwijzen we hier kortheidshalve naar de ISO 17799:2005-standaard zelf.

Hoewel ISO 17799:2005 verschillende hoofdstukken bevat die relevante controleobjectieven voor identiteits- en toegangsbeheer bevatten, hebben we ons in dit artikel gefocust op het meest relevante hoofdstuk, namelijk hoofdstuk 11, 'Toegangscontrole'. Hoewel sommige aspecten in dit hoofdstuk niet 100 procent relevant zijn voor dit artikel, zoals '11.3.3 Clear desk and clear screen', zijn de meeste deelhoofdstukken van groot belang bij het bepalen van de controleobjectieven voor identiteits- en toegangsbeheer.

De hoofdcategorieën vermeld in hoofdstuk 11 van ISO 17799:2005 voor toegangscontrole zijn de volgende:

11.1 bedrijfsvereisten voor toegangscontrole;
11.2 toegangbeheer van de gebruiker;
11.3 verantwoordelijkheden van de gebruiker;
11.4 netwerktoegangscontrole;
11.5 besturingsysteemtoegangscontrole;
11.6 applicatie en informatietoegangscontrole;
11.7 mobiele computers en afstandswerken.

Ook elk van deze paragrafen bevat één of meerdere controleobjectieven, maatregelen om deze objectieven te realiseren, implementatie-instructies en aanvullende informatie. Wie een audit rond identiteits- en toegangsbeheer plant, kan hier veel achtergrondinformatie vinden.

Vervolgens gaan we voor alle controleobjectieven, zoals gedefinieerd in (hoofdstuk 11 van) de ISO 17799:2005, de overeenkomstige COBIT 4.1-controleobjectieven definiëren om zo tot een lijst van belangrijke COBIT-controleobjectieven te komen voor identiteits- en toegangsbeheer. We hebben als referentie het recent gepubliceerde document [ITGI01] van het IT Governance Institute (ITGI) gebruikt, dat in één van de paragrafen de informatievereisten van ISO 17799:2005 verbindt met relevante controleobjectieven rond informatiebeveiliging van COBIT. In feite hebben we, specifiek voor toegangscontrole, voor dit artikel de tegenovergestelde richting gevolgd.

Gebaseerd op deze verbindingen kunnen de volgende controleobjectieven van COBIT 4.1 worden geselecteerd die van belang zijn voor identiteits- en toegangsbeheer:

- PO2.1 Bedrijfsarchitectuur voor informatie.
- PO2.3 Gegevensclassificatieschema.
- PO3.4 Technologiestandaard.
- PO6.2 Bedrijfs-IT-risico en interne controleraamwerk.
- AI6.3 Onvoorziene veranderingen.
- DS5.2 IT-beveiligingsplan.
- DS5.3 Identiteitsbeheer.
- DS5.4 Gebruikersaccountbeheer.
- DS5.7 Beveiliging van technologie.
- DS5.10 Netwerkbeveiliging.

ISO 17799:2005	COBIT 4.1 controle objectieven
Bedrijfsvereisten voor toegangscontrole	
11.1.1 Toegangscontrolebeleid	PO2.1 Bedrijfsarchitectuur voor informatie PO2.3 Gegevens classificatieschema PO6.2 Bedrijf IT risico en interne controle raamwerk DS5.2 IT beveiligingsplan DS5.4 Gebruikers account beheer
Gebruikers toegang beheer	
11.2.1 Gebruikersregistratie	DS5.4 Gebruikers account beheer
11.2.2 Privilégebeheer	DS5.4 Gebruikers account beheer
11.2.3 Beheer van gebruikerpaswoorden	DS5.3 Identiteitsbeheer
11.2.4 Nakijken van toegangsrechten	DS5.4 Gebruikers account beheer
Gebruikers verantwoordelijkheden	
11.3.1 Paswoordgebruik	PO6.2 Bedrijf IT risico en interne controle raamwerk DS5.2 IT beveiligingsplan DS5.4 Gebruikers account beheer
11.3.2 Onveilig bewaard IT materiaal	DS5.7 Beveiliging van technologie PO6.2 Bedrijf IT risico en interne controle raamwerk
11.3.3 Nette bureau en blanco scherm beleid	PO6.2 Bedrijf IT risico en interne controle raamwerk DS5.7 Beveiliging van technologie
Netwerk toegangscontrole	
11.4.1 Beleid over het gebruik van netwerk diensten	DS5.3 Identiteitsbeheer DS5.10 Netwerkbeveiliging
11.4.2 Gebruiker authenticatie voor externe netwerken	DS5.11 Uitwisseling van gevoelige informatie
11.4.3 Materiaal identificatie in netwerken	DS5.7 Beveiliging van technologie DS5.10 Netwerkbeveiliging DS9.2 Identificatie en onderhoud configuratie
11.4.4 Buitenhuis diagnose en configuratie poortbeveiliging	DS5.7 Beveiliging van technologie DS5.10 Netwerkbeveiliging
11.4.5 Splitsing in netwerken	DS5.10 Netwerkbeveiliging
11.4.6 Netwerk connectie controle	DS5.10 Netwerkbeveiliging
11.4.7 Netwerk routering controle	DS5.10 Netwerkbeveiliging
Besturing systeem controles	
11.5.1 Beveiligde aanlog procedures	DS5.3 Identiteitsbeheer DS5.4 Gebruikers account beheer DS5.7 Beveiliging van technologie
11.5.2 Gebruikersidentificatie en authenticatie	DS5.3 Identiteitsbeheer
11.5.3 Paswoordbeheersysteem	DS5.4 Gebruikers account beheer DS5.3 Identiteitsbeheer
11.5.4 Gebruik van systeem programma's	AI6.3 Onvoorziene veranderingen DS5.7 Beveiliging van technologie
11.5.5 Voortijdige afsluiting sessies	DS5.3 Identiteitsbeheer DS5.7 Beveiliging van technologie
11.5.6 Beperking van de connectie tijd	DS5.3 Identiteitsbeheer DS5.7 Beveiliging van technologie
Applicatie en gegevens toegangscontrole	
11.6.1 Toegangbeperking tot informatie	DS5.3 Identiteitsbeheer DS5.4 Gebruikers account beheer
11.6.2 Afzondering sensitieve systemen	AI2.4 Applicatie beveiliging en beschikbaarheid DS5.7 Beveiliging van technologie DS5.10 Netwerkbeveiliging
Mobiele computers en werken van op afstand	
11.7.1 Mobiele computers en communicatie	PO6.2 Bedrijf IT risico en interne controle raamwerk DS5.7 Beveiliging van technologie
11.7.2 Werken van op afstand	PO3.4 Technologie standaard DS5.2 IT beveiliging plan DS5.7 Beveiliging van technologie PO6.2 Bedrijf IT risico en interne controle raamwerk

- DS5.11 Uitwisseling van gevoelige informatie
- DS9.2 Identificatie en onderhoud configuratie

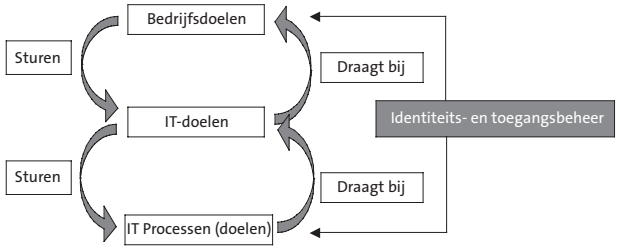
Dit komt neer op de volgende relevante COBIT-processen voor identiteits- en toegangsbeheer. Dit moet in twee richtingen geïnterpreteerd worden. Ten eerste zal het identiteits- en toegangsbeheer binnen een bedrijf een belangrijke input zijn voor deze processen; ten tweede zal de output van deze processen belangrijk zijn voor de manier waarop identiteits- en toegangsbeheer binnen een bedrijf wordt beheerd.

- PO2 Definieer de informatiearchitectuur.
- PO3 Bepaal de technologische richting.
- PO6 Communiceer de plannen van het bestuur en de richting welke ze uitgaan.
- AI6 Beheer de veranderingen.
- DS5 Verzeker de beveiliging van de systemen.
- DS9 Beheer de configuratie.

Benadering startende van de bedrijfsdoelstellingen

In het vorige hoofdstuk zijn we uitgegaan van de ISO 17799:2005-standaard om tot een lijst van de belangrijkste COBIT-processen te komen die bijdragen aan een betrouwbaar identiteits- en toegangsbeheer. In dit hoofdstuk kiezen we voor een andere invalshoek, en gaan we van de bedrijfsdoelstellingen uit om de belangrijkste COBIT-processen te selecteren. We hebben COBIT 4.1 gebruikt om tot onze selectie te komen.

We starten vanuit de veronderstelling dat we een degelijk identiteits- en toegangsbeheer zien als een IT-doel, dat helpt om de bedrijfsdoelstellingen te realiseren en dat ondersteund wordt door verschillende processen.



Bedrijfsdoelen kunnen volgens COBIT vanuit vier verschillende perspectieven bekeken worden. Deze vier perspectieven zijn dezelfde als die gebruikt worden in 'balanced scorecards'.

- financieel perspectief;
- klantperspectief;
- intern perspectief;
- leer- en groeiperspectief.

Waar vroeger enkel een financieel perspectief gebruikt werd om bedrijfsdoelen te bepalen en op basis daarvan vervolgens een bedrijfsstrategie op te stellen, gaan veel organisaties tegenwoordig breder te werk. Ook een aantal andere, niet financiële factoren speelt een rol bij het bepalen van de bedrijfsstrategie.

COBIT 4.1 beschrijft 17 bedrijfsdoelen. Als we deze 17 bedrijfsdoelen doorlopen, kunnen we op basis van gezond verstand er drie selecteren die een degelijk identiteits- en toegangsbeheerproces vereisen. We hebben voor deze drie gekozen aangezien we vinden dat de link hier het meest relevant is. Plaatsen we deze direct bij één van de vier perspectieven, dan komen we tot volgende lijst:

- Financieel perspectief
  - Beheers IT-gerelateerde bedrijfsrisico's
- Intern perspectief
  - Leef externe wetten en regelgevingen na
  - Leef interne beleidsnota's na

Deze drie bedrijfsdoelen op zich bepalen in grote mate de strategie die een bedrijf gaat volgen aangaande zijn identiteits- en toegangsbeheerproces. Sommige bedrijven verwerken veel confidentiële informatie en zijn onderworpen aan strikte regelgevingen aangaande beveiliging van informatie en gegevens, denk maar aan de financiële en farmaceutische industrie. Binnen andere bedrijven zal dit veel minder een rol spelen.

Als we deze drie bedrijfsdoelen vervolgens iets verder in detail gaan onderzoeken, kunnen we op basis van COBIT 4.1 de informatiecriteria voor deze bedrijfsdoelen afleiden. Dit verband is in de volgende opsomming aangegeven. Om de opsomming te vervolledigen, hebben we bij elk van de bedrijfsdoelen ook geprobeerd specifieke risico's te plaatsen, zonder de bedoeling compleet te zijn.

Beheers-IT-gerelateerde bedrijfsrisico's

- Dit bedrijfsdoel ondersteunt volgende COBIT informatiecriteria:
  - confidentialiteit;
  - integriteit;
  - beschikbaarheid.
- Het niet beschikken over een degelijk identiteits- en toegangsbeheerproces vergroot het risico op:
  - onthulling van confidentiële informatie;
  - gegevens zijn aangepast door een ongeautoriseerde partij;
  - gegevens zijn niet beschikbaar indien nodig.

Leef externe wetten en regelgevingen na

- Dit bedrijfsdoel ondersteunt volgende COBIT informatiecriteria:
  - confidentialiteit;
  - 'compliance'.
- Het niet naleven van de verschillende nieuwe wet- en regelgevingen (SOx, Basel II, HIPAA…) kan leiden tot financiële schade en/of imagoschade.

Leef interne beleidsnota's na

- Dit bedrijfsdoel ondersteunt volgende COBIT informatiecriteria:
  - confidentialiteit;
  - 'compliance'.

- Het niet naleven van interne beleidsnota's kan ertoe leiden dat binnen een bedrijf verschillende processen gevolgd worden, wat leidt tot inefficiëntie.

IT-doelen

Gebaseerd op de geselecteerde bedrijfsdoelen werden de volgende IT-doelen bepaald op basis van COBIT 4.1. Deze link is rechtstreeks uit COBIT 4.1 gehaald.

Beheers-IT-gerelateerde bedrijfsrisico's
- 2. Beantwoord aan bestuurseisen in lijn met de richting van de directie.
- 14. Verantwoordelijk zijn voor en beschermen van IT-middelen.
- 17. Bescherm het bereiken van IT-objectieven.
- 18. Maak de bedrijfsimpact duidelijk voor het falen van IT-objectieven en - middelen.
- 19. Voorzie dat confidentiële informatie niet kenbaar wordt gemaakt aan diegene die er geen toegang tot moeten hebben.
- 20. Voorzie dat geautomatiseerde bedrijfstransacties en uitwisseling van informatie op een te vertrouwen manier kunnen verlopen.
- 21. Voorzie dat IT-diensten en -infrastructuur degelijk kunnen weerstaan en herstellen van faling veroorzaakt door fouten, aanvallen of rampen.
- 22. Voorzie minimale bedrijfsimpact in het geval van onderbreking in diensten of veranderingen in de infrastructuur.

Leef externe wetten en regelgevingen na
- 2. Beantwoord aan bestuurseisen in lijn met de richting van de directie.
- 19. Voorzie dat confidentiële informatie niet kenbaar wordt gemaakt aan diegenen die er geen toegang tot moeten hebben.
- 20. Voorzie dat geautomatiseerde bedrijfstransacties en uitwisseling van informatie op een te vertrouwen manier kunnen verlopen.
- 21. Voorzie dat IT-diensten en -infrastructuur degelijk kunnen weerstaan en herstellen van faling veroorzaakt door fouten, aanvallen of rampen.
- 22. Voorzie minimale bedrijfsimpact in het geval van onderbreking in diensten of veranderingen in de infrastructuur.
- 26. Onderhoud de integriteit van informatie en de verwerkende infrastructuur.
- 27. Voorzie het naleven van wetten en regelgevingen.

Leef interne beleidsnota's na
- 2. Beantwoord aan bestuurseisen in lijn met de richting van de directie.
- 13. Voorzie degelijke performantie van applicaties en de technologische infrastructuur.

Processen

De belangrijkste informatiecriteria voor het bedrijf ondersteund door een degelijk identiteits- en toegangsbeheersysteem zijn (zie begin van dit artikel voor de uitwerking):
- confidentialiteit (P)
- integriteit (P)
- beschikbaarheid (S)
- 'compliance' (S)
- betrouwbaarheid (S)

Aangezien binnen de context van identiteits- en toegangsbeheer 'compliance'-vereisten en betrouwbaarheidsvereisten in grote mate afgedekt worden door confidentialiteit, integriteit en beschikbaarheid, gaan we hier op focussen.
Gebaseerd op de tabel in COBIT 4.1 die de IT-doelen verbindt met de IT-processen, hebben we die IT-doelen geselecteerd waarvoor de primaire bijdrage van de informatiecriteria focust op confidentialiteit, integriteit en beschikbaarheid. Als selectiecriteria hebben we gesteld dat er minstens twee primaire bijdragen moeten zijn. Dit levert de volgende tabel op:

		Confidentialiteit	Integriteit	Beschikbaarheid
14	Verantwoordelijk zijn voor en beschermen van IT-middelen.	P	P	P
18	Maak de bedrijfsimpact duidelijk voor het falen van IT-objectieven en -middelen.	P	P	P
19	Voorzie dat confidentiële informatie niet kenbaar wordt gemaakt aan diegenen die er geen toegang tot moeten hebben.	P	P	S
26	Onderhoud de integriteit van informatie en de verwerkende infrastructuur.		P	P

Indien we deze lijst combineren met de tabel in COBIT 4.1 die de IT-doelen verbindt met IT-processen, kunnen we nu die COBIT-processen selecteren die relevant zijn voor identiteits- en toegangsbeheer.
- 14. Verantwoordelijk zijn voor en beschermen van IT-middelen
  - PO9 Inschatten en beheersen van IT-risico's.
  - DS5 Voorzie systeembeveiliging.
  - DS9 Beheer de configuratie.
  - DS12 Beheer de fysische omgeving.
  - ME2 Monitor en evalueer interne controle.
- 18. Maak de bedrijfsimpact duidelijk voor het falen van IT-objectieven en -middelen
  - PO9 Inschatten en beheersen van IT-risico's.
- 19. Voorzie dat confidentiële informatie niet kenbaar wordt gemaakt aan diegenen die er geen toegang tot moeten hebben.
  - PO6 Communiceer de plannen van het bestuur en de richting welke ze uitgaan.

- DS5 Voorzie systeembeveiliging.
- DS11 Beheer de gegevens.
- DS12 Beheer de fysische omgeving.

• 26. Onderhoud de integriteit van informatie en de verwerkende infrastructuur
- AI6 Beheers de veranderingen.
- DS5 Voorzie systeembeveiliging.

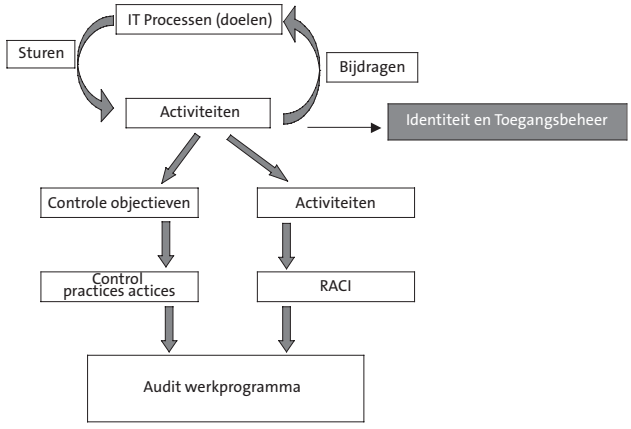
DS12 is uit de lijst gehouden aangezien we ons in dit artikel willen toeleggen op logische toegang en niet op fysische toegang.

Startend van de relevante bedrijfsdoelen gedefinieerd door COBIT geeft dit ons de volgende lijst van COBIT-processen die een betrouwbaar identiteits- en toegangsbeheer ondersteunen:

- PO6 Communiceer de plannen van het bestuur en de richten welke ze uitgaan.
- PO9 Inschatten en beheersen van IT-risico's.
- DS5 Voorzie systeembeveiliging.
- DS9 Beheer de configuratie.
- DS11 Beheer de gegevens.
- AI6 Beheers de veranderingen.
- ME2 Monitor en evalueer interne controle.

Control practices voor identiteits- en toegangsbeheer

Vervolgens kunnen we uit deze lijst van belangrijke processen voor identiteits- en toegangsbeheer een aantal zaken afleiden zoals schematisch hierna voorgesteld. In deze paragraaf zullen we starten van de geselecteerde COBIT-processen om tot een lijst van 'control practices' te komen die relevant zijn voor identiteits- en toegangsbeheer. Deze definiëren welke beheersmaatregelen nodig zijn voor een degelijk identiteits- en toegangbeheersysteem. Uiteindelijk komen we tot een werkprogramma voor het uitvoeren van een audit op het identiteits- en toegangsbeheerssysteem.



IT-processen

In de laatste twee paragrafen hebben we een lijst van COBIT-processen geselecteerd die relevant zijn voor identiteits- en toegangsbeheer op basis van twee verschillende benaderingen, namelijk (1) startende van de IS0 17799:2005-standaard en (2) startende van de bedrijfsdoelen relevant voor identiteits- en toegangscontrole. Als we deze twee resultaten combineren, komen we tot volgende lijst van processen die van belang zijn voor identiteits- en toegangscontrole. Processen die meerdere malen naar voor komen, hebben we onder het kopje 'heel belangrijk' geplaatst, processen die éénmaal naar voor komen, hebben we onder 'belangrijk' geplaatst:

Heel belangrijk:

- PO6 Communiceer de plannen van het bestuur en de richten welke ze uitgaan.
- AI6 Beheers de veranderingen.
- DS5 Voorzie systeembeveiliging.
- DS9 Beheer de configuratie.

Belangrijk:

- PO2 Definieer de informatiearchitectuur.
- PO3 Bepaal de technologische richting.
- PO9 Inschatten en beheersen van IT-risico's.
- DS11 Beheer de gegevens.
- ME2 Monitor en evalueer interne controle.

In de lijst van geselecteerde COBIT-processen hebben we vervolgens die COBIT-activiteiten geselecteerd die relevant zijn voor identiteits- en toegangsbeheer:

PO6 Communiceer de plannen van het bestuur en de richting welke ze uitgaan

- Creëer en onderhoud een IT-controleomgeving en -framework.
- Ontwikkel en onderhoud een IT-beleid.
- Communiceer over het IT-controleframework, IT-objectieven en IT-doelstellingen.

AI6 Beheers de veranderingen

- Ontwikkel en implementeer een proces om op consistente manier veranderingen te documenteren, te beoordelen en het belang in te schatten.
- Ontwikkel een proces om veranderingen autoriseren.

DS5 Verzeker de beveiliging van de systemen

- Definieer en onderhoud een IT-beveiligingsplan.
- Definieer en maak een identiteitsbeheersysteem operationeel.
- Controleer op potentiële en effectieve beveiligingsincidenten.
- Kijk regelmatig de gebruikersrechten en privileges na en valideer deze.
- Voer regelmatig beveiligingscontroles uit.

DS9 Beheer de configuratie

- Verifieer de configuratie.

PO2 Definieer de informatiearchitectuur

- Definieer en onderhoud een gegevensclassificatieschema.
- Voorzie gegevensverantwoordelijken van procedures en middelen voor het classificeren van gegevens.

PO3 Bepaal de technologische richting

- Creëer en onderhoud een plan voor de technologische infrastructuur.

PO9 Inschatten en beheersen van IT-risico's

- Identificeer gebeurtenissen die relevant zijn voor de objectieven.

DS11 Beheer gegevens, ME2 Monitor en evalueer interne controle

- *Ondanks dat deze processen identiteit en toegangsbeheer ondersteunen, zijn er geen activiteiten die direct verbonden zijn met dit proces.*

Gedetailleerde controleobjectieven -> Control practices

Gebaseerd op de geselecteerde activiteiten hebben we die controleobjectieven bepaald die relevant zijn voor identiteits- en toegangsbeheer. Voor elk controleobjectief werd het volgende gedefinieerd:

- Een uitleg waarom het controleobjectief relevant is voor identiteits- en toegangsbeheer.
- Control practices voor identiteits- en toegangsbeheer. Deze control practices zijn gebaseerd op de lijst gedefinieerd in COBIT 4.1. Hoewel meer control practices kunnen gegeven worden, hebben we ons gefocust op de belangrijkste. Voor de belangrijkste processen hebben we een maximum van drie control practices gespecificeerd. Voor de minder relevante processen voor identiteits- en toegangsbeheer hebben we er minder gedefinieerd.

Deze control practices kunnen nu helpen bij het definiëren van de 'assurance steps' (zoals dit tegenwoordig in COBIT 4.1 wordt genoemd) voor identiteits- en toegangsbeheer, om op die manier tot een werkprogramma te komen voor het uitvoeren van een audit in een organisatie. Dit auditwerkprogramma is in appendix bijgevoegd, aangezien het objectief van dit artikel primair was om de gehanteerde systematiek te verduidelijken om tot dit auditwerkprogramma te komen.

Appendix

Basisauditwerkprogramma: testen van het controleontwerp en de operationele effectiviteit van het identiteits- en toegangsbeheerssysteem.

Gebaseerd op de geïdentificeerde gedetailleerde controleobjectieven en control practices kunnen we de 'assurance steps' voor het auditwerkprogramma voor identiteits- en toegangsbeheer bepalen. Dit werkprogramma kan ook door de lezer worden afgeleid uit de 'assurance steps' van COBIT. In het werkprogramma hebben we de meer algemene controles die in COBIT worden gedefinieerd, aangepast, zodat deze direct toepasbaar zijn voor een audit op identiteits- en toegangsbeheer. De lezer kan bij het samenstellen van een gedetailleerd werkprogramma voor identiteits- en toegangsbeheer deze lijst gebruiken en op basis van COBIT een aantal specifieke controles toevoegen die belangrijk zijn binnen zijn bedrijf. Verder hebben we gerelateerde onderwerpen gegroepeerd om zo tot een uniform werkprogramma te komen. We hebben de volgende hoofdcategorieën gedefinieerd en daaronder de afgeleide gedetailleerde controleobjectieven genoemd.

Organisatie rond beveiliging
- PO6.1 IT-beleid en controleomgeving.
- PO6.3 Beheer van IT-beleidsnota's.
- PO6.4 Beleidsnota's, standaarden en procedures.
- PO6.5 Communicatie van IT-objectieven en richting.
- DS5.1 Beheer van IT-beveiliging.
- DS5.2 IT-beveiligingsplan.

Classificatie
- DS5.2 IT-Beveiligingsplan.
- PO2.3 Dataclassificatieschema.

Definitie van rollen en functionaliteiten
- PO6.4 Beleidsnota's, standaarden en procedures.
- DS5.1 Beheer van IT-beveiliging.

Gebruikersadministratie
- DS5.3 Identiteitsbeheer.
- DS5.4 Beheer van gebruikersaccounts.
- AI6.1 Wijziging standaarden en procedures.
- AI6.4 Opvolgen en rapporteren van de status van wijzigingen.

Technische implementatie
- DS9.3 Nazicht van de integriteit van de configuratie.
- PO3.1 Planning van de technologische richting.

Controle
- DS5.5 Testen, controle en opvolging van beveiliging.
- DS5.9 Voorkomen, detecteren en corrigeren van vijandige software.
- PO9.3 Identificatie van gebeurtenissen.

Organisatie rond beveiliging

PO6.1 IT-beleid en controleomgeving
- Controleer en bevestig dat er voldoende aandacht is bij het topmanagement voor identiteit en toegangsbeheer en dat hun aandacht ook binnen de organisatie duidelijk wordt gemaakt (nieuwsbrieven, e-mails, doorschemering in IT-visie …). Controleer dat identiteit en toegangsbeheer in lijn is met het bedrijf zijn algemene risico- en controleomgeving.
- Controleer of verantwoordelijkheden aan individuen zijn opgehangen.
- Bevestig het bestaan van beleidsnota's en richtlijnen ter ondersteuning van identiteit en toegangsbeheer binnen IT en het bedrijf.
- Controleer of er bewijzen zijn dat er regelmatig opleidingen gegeven worden rond de beleidsnota's en richtlijnen in verband met identiteit en toegangsbeheer.
- Controleer of er een proces bestaat om minstens jaarlijks de adequaatheid van de controleomgeving voor identiteit

en toegangsbeheer na te gaan binnen de veranderingen van het bedrijf.

PO6.3 Beheer van IT-beleidsnota's
- Controleer en bevestig dat er een hiërarchische set van beleidsnota's, standaarden en procedures gecreëerd is die overeenkomt met de strategie van IT, de strategie van het bedrijf en van de controleomgeving.
- Controleer en bevestig dat er beleidsnota's bestaan rond relevante onderdelen van identiteit en toegangsbeheer.
- Controleer en bevestig dat er een beleidsnota-aanpassingsproces bestaat dat er voor zorgt dat deze jaarlijks nagekeken en aangepast wordt, indien nodig.
- Controleer en definieer dat er procedures bestaan voor het nagaan of identiteit en toegangsbeheer interne en externe regelgevingen naleeft en dat die procedures de consequenties van het niet naleven van deze regelgevingen bevatten.
- Controleer en bevestig dat verantwoordelijkheden zijn gedefinieerd.
- Controleer dat alle elementen van het beleidsnotabeheersproces toegewezen zijn aan verantwoordelijke personen.

PO6.4 Beleidsnota's, standaarden en procedures
- Controleer en bevestig dat er een proces bestaat die de beleidsnota's omzet in hanteerbare standaarden en procedures.
- Controleer dat er voldoende opgeleid personeel beschikbaar is voor de uitrol van de beleidsnota's voor identiteit en toegangsbeheer.
- Controleer en bevestig dat beleidsnota's en procedures gekend zijn binnen het bedrijf.

PO6.5 Communicatie van IT-objectieven en richting
- Controleer en bevestig dat er managementprocessen zijn die er voor zorgen dat de objectieven en de richting van identiteit en toegangsbeheer regelmatig worden gecommuniceerd.
- Controleer met een representatief aantal dat de objectieven duidelijk gekend zijn binnen de organisatie.
- Controleer oude communicatieplannen of deze de nodige informatie rond identiteit en toegangsbeheer bevatten.

DS5.1 Beheer van IT-beveiliging
- Bepaal of er een identiteit en toegangsbeheercommissie bestaat. Er moet een nauwe samenwerking bestaan tussen deze commissie en de commissie informatiebeveiliging.
- Bepaal of er een vast proces bestaat die de belangrijkheid van projecten bepaalt en bepaalt welke subprojecten eerst worden uitgevoerd.
- Controleer en bevestig dat de beveiligingsnota's alle verantwoordelijkheden rond informatiebeveiliging omschrijven, inclusief deze rond identiteit en toegangsbeheer.
- Controleer en bevestig dat een gedetailleerde beveiligingsnota, standaarden en procedures bestaan.
- Controleer en bevestig dat een adequate organisatorische structuur en rapporteringlijn bestaan voor identiteit en toegangsbeheer in lijn met die voor beveiligingsbeleid.
- Controleer en bevestig dat een rapporteringlijn binnen het bedrijf bestaat dat het topmanagement inlicht over zaken rond identiteit en toegangsbeheer.

DS5.2 IT-beveiligingsplan
- Bepaal of de effectiviteit van het proces voor het verzamelen van de bedrijfsvereisten voor identiteit en toegangsbeheer voldoende is. Deze bedrijfvereisten moeten opgenomen worden in het globale beveiligingsplan.
- Bepaal of het plan van aanpak voor identiteit en toegangsbeheer regelmatig wordt aangepast aan de nieuwe bedrijfsvereisten. Bepaal ook of deze aanpassingen de nodige goedkeuringsprocessen hebben doorlopen.
- Bepaal of alle procedures rond identiteit en toegangsbeheer in overeenstemming blijven met het aangepaste beveiligingsplan. Dit omvat onder andere de aanpassingen rond configuratiemanagement (DS9).

Classificatie

DS5.2 IT Beveiligingsplan
- Controleer of Identiteit en toegangsbeheer volgende processen mee opneemt: IT tactische plannen (PO1), data classificatie (PO2), Technologische standaarden (PO3), beveiliging en controlenota's (PO6), risico beheer (PO9) en externe 'Compliance' vereisten (ME3).

PO2.3 Dataclassificatie schema
- Controleer het dataclassificatie schema en ga na dat alle relevante componenten worden vermeld. Het schema moet ook een overzicht geven van de risico's versus de kost die gepaard gaat met het voorkomen van dat risico.
- Controleer dat de beveiligingsclassificatie, die is meegegeven in het document, regelmatig wordt gecontroleerd op accuraatheid.

Definitie van rollen en functionaliteiten

PO6.4 Beleidsnota's, standaarden en procedures
- Controleer en bevestig dat er een proces bestaat om beleidsnota's en standaarden om te zetten in operationele procedures.
- Controleer en bevestig dat contracten in overeenstemming zijn met beleidsnota's. Ga na of het 'nodig-om-te-weten' en 'nodig-om-te-doen' principe expliciet mee is opgenomen en ga na of de consequenties van het niet naleven van de beleidsnota's zijn beschreven.
- Controleer en bevestig dat de gebruikers op de hoogte zijn beleidsnota's, standaarden en procedures. Ga na of de gebruikers dit ook formeel hebben moeten bevestigen.
- Controleer of er voldoende personeel met de nodige kennis aanwezig is voor de implementatie van de beleidsnota's, standaarden en procedures binnen het bedrijf.

DS5.1 Beheer van IT-beveiliging
- Controleer of een identiteit en toegangsbeheercommissie bestaat. Er moet een nauwe samenwerking bestaan tussen deze commissie en de commissie informatiebeveiliging.
- Controleer en bevestig dat de beleidsnota rond identiteit en toegangsbeheer de rollen en verantwoordelijkheden van iedereen bevat en duidelijk omschrijft.
- Controleer en bevestig dat een duidelijke organisatorische structuur en rapporteringlijn voor identiteit en toegangsbeheer bestaan.
- Controleer en bevestig dat een managementrapporteringmechanisme bestaat dat het topmanagement informeert over de status van identiteit en toegangsbeheer.

Gebruikersadministratie

DS5.3 Identiteitsbeheer
- Controleer dat de verschillende systemen vereisen dat gebruikers uniek identificeerbaar zijn. Controleer dat alle systemen identiteit en toegangsbeheer vereisen voor er toegang tot de systemen wordt gegeven.
- Als vooraf bepaalde en gedefinieerde rollen worden gebruikt om toegangsrechten te verschaffen, ga dan na dat deze rollen de nodige toegangsrechten verschaffen maar ook niet te veel. Aanpassingen van rollen moeten goedgekeurd worden via een standaardproces.
- Controleer of er voldoende controleprocessen zijn ingebouwd in de verschillende stadia die worden doorlopen bij het geven van logische toegang tot systemen. Dit zowel voor interne als externe gebruikers.

DS5.4 Beheer van gebruikersaccounts
- Controleer of er procedures bestaan voor het regelmatig nagaan en corrigeren van toegangsrechten tot systemen. Ga de operationele effectiviteit na.
- Bepaal of er voldoende procedures bestaan om toegangsrechten te controleren en te beheren volgens het bedrijf zijn beleidsnota's rond beveiliging. Ga de operationele effectiviteit van de procedures na en ga na dat deze overeenstemmen met legale vereisten.
- Controleer of systemen, applicaties en gegevens geclassificeerd zijn volgens niveaus van belang en risico. Controleer of proceseigenaars zijn gedefinieerd.
- Bepaal of de beleidsnota's, standaarden en procedures rond identiteit en toegangsbeheer op alle systemen, processen en gebruikers van toepassing zijn.

AI6.1 Wijziging van standaarden en procedures
- Controleer en bevestig dat er processen en procedures bestaan voor het behandelen van wijzigingen met betrekking tot identiteit en toegangsbeheer.
- Controleer en bevestig dat er een postimplementatieproces bestaat voor het nazicht van wijzigingen.

AI6.4 Opvolgen en rapporteren van de status van wijzigingen
- Controleer en bevestig dat er een proces en systeem bestaan die de gebruikers toelaat de status van hun wijzigingsaanvraag na te gaan.
- Controleer en bevestig dat een proces bestaat voor de opvolging en controle van wijzigingen.
- Controleer en bevestig dat wijzigingen tijdig worden uitgevoerd en dit op basis van hun prioriteit.

Technische implementatie

DS9.3 Nazicht van de integriteit van de configuratie
- Controleer en bevestig dat er een proces is dat voorziet in de regelmatige controle van de integriteit van de configuraties voor identiteit en toegangsbeheer.
- Controleer of vervallen toegangsrechten worden verwijderd.
- Controleer of toegangsrechten op de applicaties en infrastructuur up-to-date worden gehouden.

PO3.1 Planning van de technologische richting
- Controleer het proces en technisch platform voor identiteit en toegangsbeheer op sterkten, zwakten, mogelijkheden en bedreigingen (SZMB). Controleer of op basis van deze SZMB-analyse de processen en platformen worden aangepast. Continu verbeteringsproces.
- Bevestig op basis van interviews met de CIO en andere leden van het senior management dat er voldoende oog is voor risico's en dat deze risico's bepaald zijn door de bedrijfsstrategie.
- Controleer dat de huidige technische platformen adequaat en aanpasbaar zijn.

Controle

DS5.5 Testen, nazicht en opvolging van beveiliging
- Controleer en bevestig dat een overzicht bestaat van alle netwerkapparaten, diensten en applicaties en dat er een risicoscore aan elk is gegeven.
- Controleer dat alle kritische netwerkapparaten regelmatig op beveiligingsincidenten worden gecontroleerd. Dit omvat ook de technische platformen rond identiteit en toegangsbeheer.
- Controleer dat identiteit en toegangsbeheerfuncties en -processen geïntegreerd zijn met de organisatie haar projectbeheer om er zeker van te zijn dat identiteit en toegangsbeheer mee is genomen in de ontwikkeling-, ontwerp-, test- en implementatiefases.

DS5.9 Voorkomen, detecteren en corrigeren van vijandige software
- Controleer of de medewerkers rond identiteit en toegangsbeheer op de hoogte zijn van de beleidsnota's rond het voorkomen van vijandige software en hun verantwoordelijken ten opzichte van 'compliance'.
- Controleer dat de technische platformen voor identiteit en toegangsbeheer een antivirusprogramma hebben en dat deze up-to-date is.

- Controleer dat het technische platform voor het beheer van identiteit en toegangsbeheer de laatste nieuwe beveiliging-'patches' heeft.
- Controleer dat het technische platform voor de implementatie van identiteit en toegangsbeheer geen directe kwetsbaarheden vertoont.

PO9.3 Identificatie van gebeurtenissen
- Controleer en bevestig dat er een proces is dat voorziet in een regelmatige controle van de configuratiegegevens.
- Controleer dat afwijkingen van de beleidsnota rond identiteit en toegangsbeheer worden gemeld en gecorrigeerd.

Naast het auditwerkprogramma werd in mijn artikel in de losbladige gids *Audit & controle in de praktijk* (Kluwer Uitgevers) ook de 'RACI' ('Responsible', 'Accountable', 'Consulted' en 'Informed')-tabel opgesteld. Vervolgens werden doelen en metrieken voor identiteits- en toegangsbeheer opgesteld en een maturiteitsmodel gedefinieerd. Voor de volledige tekst en uitwerking verwijs ik graag naar de genoemde publicatie. ■

Literatuuroverzicht

- Cobit 4.0: Control Objectives, Management Guidelines, Maturity Models
- Cobit 4.1: Framework, Control Objectives, Management Guidelines, Maturity Models
- Cobit 4.1: IT assurance guide: Need for IT Governance and Assurance, The COBIT® Framework IT Assurance Approaches and How COBIT Supports IT Assurance Activities
- Cobit Online
- CISA manual
- Several documents from www.isaca.org and www.itgi.org ([ITGI01]Mapping between Cobit and ISO17799:2005)
- Course documents UAMS – Master in Computer Auditing
- Losbladige gids *Audit & controle in de praktijk* (Kluwer Uitgevers)
- ISO 17799:2005-standaard

dit is een zwart-wit pagina