EXIN Information Security Management ISO/IEC 27001

EXPERT

Guide

Editie 201710

Inhoud

Algemeen

De module Information Security Management Expert based on ISO/IEC 27001 (ISMES) bestaat uit een schriftelijk en een mondeling examendeel.

Dit document beschrijft de opzet van het schriftelijke deel (praktijkwerkstuk), de opzet en duur van het mondeling examen en de procedure van het gehele examen. Het document bevat bovendien de beoordelingscriteria en een casus waarvan gebruik gemaakt kan worden voor het werkstuk.

Vertrouwelijkheid

De examinatoren hebben een Non Disclosure Agreement getekend met EXIN. De informatie in het werkstuk, de presentatie en het examengesprek wordt vertrouwelijk behandeld.

Opzet van het examen

De module Information Security Management Expert based on ISO/IEC 27001 (ISMES) bestaat uit twee gedeelten.
Het schriftelijk gedeelte, het praktijkwerkstuk, is het eerste onderdeel. Dit onderdeel moet met een voldoende (55% of meer) behaald zijn alvorens u het mondeling examen kunt afleggen.
Het mondeling gedeelte is het tweede onderdeel.

Schriftelijk gedeelte

Werkstuk

Het schriftelijk gedeelte betreft een praktijkwerkstuk van ongeveer 6000 woorden en een managementsamenvatting.

Idealiter is het praktijkwerkstuk in zijn geheel voor de module ISMES geschreven; bijvoorbeeld als logisch vervolg in een lopend traject of omdat de organisatie waar u werkzaam bent hier behoefte aan heeft. Ook in het laatste geval gelden de richtlijnen voor het start- en slothoofdstuk.

De inhoud van het praktijkwerkstuk dient gerelateerd te zijn aan uw werkcontext. De kern van het werkstuk kan een bestaand document zijn (over één van de exameneisen), op voorwaarde dat u daarvan de auteur of co-auteur bent, met voldoende inhoudelijke inbreng. In het starthoofdstuk dient uw rol duidelijk te zijn gemaakt.

Het werkstuk bevat een starthoofdstuk, een kern en een slothoofdstuk.

Onderdelen van het starthoofdstuk zijn onder andere:
- de aanleiding voor het tot stand komen van het betreffende document in de organisatie, met daaraan gerelateerd een vraag- en doelstelling;
- de rol van de kandidaat bij het tot stand komen van het document;
- de rol/status van het document in de organisatie.

De kern van het praktijkwerkstuk behandelt één van de exameneisen van ISMES naar keuze:

- Security Awareness-plan;
- Risicoanalyse;
- Veranderplan;
- ISMS-plan;
- Auditplan;
- Quickscan;
- Informatiebeveiligingsbeleid.

Onderdelen van het slothoofdstuk zijn onder andere:

- zorgvuldige reflecties op de verschillende onderdelen van het proces; hierin wordt het functioneren van de kandidaat zichtbaar; waar liep de kandidaat tegenaan, welke alternatieven waren er, welke keuzes werden gemaakt, wat kan een volgende keer beter, etc.;
- een terugkoppeling naar het starthoofdstuk, onder andere naar de vraag- en doelstelling.

Wanneer het voor u niet mogelijk is een praktijkwerkstuk te schrijven op basis van uw werkomgeving, kunt u in overleg met uw opleider een werkstuk schrijven op basis van de bijgevoegde casus. De casus is opgenomen aan het eind van deze Guide. In het geval van een werkstuk op basis van de casus dient u wel de eigen inbreng uit werkervaring en werkcontext duidelijk te maken. In het slothoofdstuk van het werkstuk kan dan worden aangegeven bij welke onderdelen is geput uit eigen ervaring, wat relevante overeenkomsten/verschillen zijn met de eigen werkcontext, wat de leerpunten van de casus zijn voor de eigen werkomgeving etc.

Het is sterk aanbevolen dat u het plan voor het werkstuk naar EXIN stuurt in een vroeg stadium om te laten controleren dat het aan de minimum eisen voldoet.

Met het werkstuk levert u in:

1. een managementsamenvatting van het werkstuk, die aan de volgende eisen voldoet:
   - de samenvatting omvat maximaal 2 kantjes
   - de samenvatting is gericht aan het managementteam
   - de samenvatting bevat een inleiding, een kern, een slot met de conclusies en aanbevelingen
2. een kort curriculum vitae, waaruit blijkt dat u minstens 2 jaar werkervaring heeft, op managementniveau, op het gebied van minstens 2 exameneisen.
3. de opleider voegt een verantwoording toe van de relatie tussen de gekozen exameneis en het werkstuk.

Beoordeling

Het werkstuk wordt door twee examinatoren beoordeeld. Het beoordelingsinstrument dat zij daarbij gebruiken is te vinden in bijlage 1 verderop in deze Guide.
Voordat u het mondeling examen gaat afleggen, dient het werkstuk met een voldoende (55% of meer) te zijn beoordeeld.
De feedback van de examinatoren op het werkstuk wordt ruim vóór het mondeling examen naar de opleider gestuurd.

Afhankelijk van het gekozen onderwerp, wordt één van de onderstaande tabellen gebruikt bij de beoordeling van het werkstuk.

Mondeling gedeelte

I Presentatie

Het examen begint met een presentatie van het werkstuk door de examenkandidaat. De presentatie wordt gegeven aan een managementteam met het doel het management te overtuigen en eventuele voorstellen aanvaard te krijgen. Hierbij wordt onder andere beoordeeld of de presentatie voldoende afgestemd is op het MT. Deze presentatie duurt (maximaal) 15 minuten.

II Examengesprek naar aanleiding van de presentatie

Het tweede deel van het mondeling examen bestaat uit een gesprek met de examinatoren over de presentatie. De examinatoren bevragen de kandidaat kritisch, als leden van een managementteam. Dit gesprek duurt 15 minuten.

III Examengesprek met betrekking tot de overige exameneisen

In het derde en laatste deel van het mondeling examen stellen de examinatoren vragen over de exameneisen die nog niet of onvoldoende aan bod zijn gekomen in de presentatie of in het examengesprek naar aanleiding van de presentatie. De examinatoren zijn hierbij niet meer in hun rol als managementteam. Er wordt getoetst of de kandidaat in staat is de inhoud van ISMES ook buiten de eigen werkcontext te plaatsen, verbanden te leggen tussen het werkstuk, de presentatie, de eigen werkcontext en recente ontwikkelingen in het vakgebied. Daarnaast kan getoetst worden of de kandidaat in staat is te reflecteren op het eigen handelen in relatie tot de inhoud. De kandidaat dient dus ook buiten de context van zijn/haar eigen functie of bedrijf inzicht te hebben in de onderwerpen die in de exameneisen staan. Dit laatste examengesprek duurt 25 minuten.

IV Beoordeling

Direct na het examen bepalen de examinatoren in onderling overleg het eindoordeel en stellen daarbij het eindcijfer vast. Dit duurt 25 minuten. Aansluitend delen de examinatoren het eindcijfer mondeling mee aan de examenkandidaat en lichten het eindoordeel toe. Dit duurt 10 minuten. Het hele examen neemt 90 minuten in beslag.

Procedure

In dit hoofdstuk staan de procedure en de regels die de examenkandidaat en de examinatoren in acht moeten nemen bij het mondeling examen ISMES.

Uiterlijk **acht weken** voor het mondeling examen is het werkstuk in **drievoud** ingeleverd bij EXIN samen met een managementsamenvatting.
De opleider heeft een verantwoording bijgevoegd voor de relatie tussen de gekozen exameneis en het werkstuk.
De kandidaat heeft een kort CV bijgevoegd waaruit blijkt dat hij/zij minstens 2 jaar werkervaring heeft, op managementniveau, op het gebied van minstens 2 exameneisen.

De examenzitting

- Bij de presentatie dient de examenkandidaat gebruik te maken van Powerpoint-dia's op een cd of een eigen laptop.
- Direct voorafgaande aan de presentatie worden twee setjes enkelzijdig bedrukte afdrukken van de presentatie aan de examinatoren verstrekt (1 dia per pagina).
- De presentatie start met:
    - Eén dia met de titel van de presentatie.
    - Eén dia met naam van de kandidaat, de functie, het bedrijf, en de aard van het bedrijf.
- De presentatie betreft het werkstuk, niet de biografie van de examenkandidaat of een beschrijving van het bedrijf waar de kandidaat werkt.
- Tijdens de presentatie kunnen de examinatoren alleen vragen stellen ter verheldering.
- Het gehele mondeling examen wordt vastgelegd met opnameapparatuur.
- Het is niet toegestaan de examinatoren te beïnvloeden met mededelingen over zakelijke of privéomstandigheden.

Bij het mondeling examen zijn de volgende personen aanwezig:
- de kandidaat
- twee examinatoren

De opleider/begeleider van de kandidaat kan het mondeling examen als toehoorder bijwonen, als de kandidaat hier mee instemt.

Tijdsduur

De gehele examensessie duurt maximaal 90 minuten, inclusief het verstrekken van de uitslag. De opbouw van het examen is als volgt:
- 15 minuten (maximaal) voor de presentatie;
- 15 minuten voor het gesprek over de presentatie;
- 25 minuten voor het examengesprek over de overige exameneisen;
- 25 minuten beoordelingsoverleg examinatoren;
- 10 minuten bespreking uitslag met de examenkandidaat.

Beoordeling

De examinatoren beoordelen de drie mondeling examenonderdelen aan de hand van drie beoordelingsinstrumenten (Tabel I, II en III). De examinatoren vullen tijdens het mondeling deze beoordelingsinstrumenten in. Na afloop van het examen verlaat de examenkandidaat het vertrek waar het examen is afgenomen. De examinatoren bepalen in onderling overleg het eindcijfer. Aansluitend delen de examinatoren dit cijfer aan de examenkandidaat mondeling mee en lichten hun eindoordeel toe.

Appendix 1: Beoordelingsinstrumenten

Security Awareness-plan

Naam kandidaat :
Kandidaatnummer :
Titel werkstuk :

Onderwerp dat moet zijn opgenomen	Beoordelingsaspecten	Score in punten	Toegekend
1. Inleiding, achtergrond, uitgangspunten	• Aanleiding • Scope (reikwijdte) • Vaststellen stakeholders	10	
2. Ontwerpen en plannen	• Samenstellen stuurgroep en projectorganisatie • Vastleggen taken, verantwoordelijkheden en bevoegdheden projectleden • Bepalen scope, doelstelling (eindsituatie, termijn) • Bepalen van slogan/logo • Bepalen strategie • Uitvoeren nul-meting • Vaststellen communicatiedoelstellingen per doelgroep • Bepalen doelgroepen en maken beschrijving van de kenmerken van de doelgroepen • Vaststellen kernboodschappen (bijv. 'juist wachtwoord gebruik', 'afsluiten van beeldscherm', etc.) • Opstellen projectplan	20	
3. Ontwikkeling	• Keuze en productie van communicatiemiddelen • Toetsing van de ontwikkelde communicatiemiddelen • Aanpassing communicatiemiddelen • Ontwikkelen draaiboek	20	
4. Uitvoering	• Communicatie van de visie • Uitvoering van het projectplan	30	
5. Evaluatie en continuering	• Meten van de effecten • Omzetten van projectactiviteiten in structurele activiteiten	10	
6. Taalgebruik en vormgeving	• Correct taalgebruik (spelling, grammatica, stijl) • Heldere structuur, passende lay-out	10	
TOTAAL		**100**	

Risicoanalyse

Naam kandidaat :
Kandidaatnummer :
Titel werkstuk :

Onderwerp dat moet zijn opgenomen	Beoordelingsaspecten	Score in punten	Toegekend

1. Inleiding, achtergrond, uitgangspunten	• Doel
	• Scope (reikwijdte)
	• Veranderingslogboek (versiebeheer)
	• Ondertekening:
	  ○ wie zijn de opstellers;
	  ○ wie zijn de respondenten;
	  ○ wie zijn de risico-eigenaren.
	• Gekozen werkvorm bij uitvoering (bijv. workshops of interviews)
	• Managementsamenvatting
		30	

2. Procesbeschrijving	• Beschrijving van het doorlopen proces	15	
3. Uitwerking	• Welke bedreigingen zijn in kaart gebracht en hoe • Resultaten van de doorlopen stappen • Eindconclusie • De te nemen maatregelen • Invoeringsplan (planning, prioritering, verantwoordelijkheden)	45	
4. Taalgebruik en vormgeving	• Correct taalgebruik (spelling, grammatica, stijl) • Heldere structuur, passende lay-out	10	
TOTAAL		**100**	

Veranderplan

Naam kandidaat :
Kandidaatnummer :
Titel werkstuk :

Onderwerp dat moet zijn opgenomen	Beoordelingsaspecten	Score in punten	Toegekend

1. Inleiding, achtergrond, uitgangspunten	• Doel
	• Scope (reikwijdte)
	• Veranderingslogboek (versiebeheer)
	• Ondertekening:
	  ○ wie zijn de opstellers;
	  ○ wie zijn de respondenten;
	  ○ wie accordeert.
	• De fasen die worden onderscheiden in de veranderaanpak (bijv. AURRA, J.P. Kotter)
	• De bereidheid tot veranderen
	• Belonen en straffen
	• Managementsamenvatting
		10	

2. Voorbereidingen en Organisatie	• Vaststellen van de dwingende noodzaak • Samenstelling van de stuurgroep • De keuze van sleutelfiguren (management, expertise, reputatie) • De visie waarheen het project moet leiden, de rode draad (moet in 5 minuten zijn uit te leggen) • Bepalen van de organisatiedelen die betrokken zijn bij de veranderingen • De rol van het management • De bijdrage per organisatiefunctie (afdeling)	40	
3. Uitvoering	• Communicatie van de visie • Afstemming van opleiding en training van medewerkers met ingevoerde maatregelen (kennis, hulpmiddelen, vaardigheden) • Plannen van de korte-termijn-winsten • Consolideren van de winst • Institutionaliseren van de nieuwe aanpak • Evaluatie	40	
4. Taalgebruik en vormgeving	• Correct taalgebruik (spelling, grammatica, stijl) • Heldere structuur, passende lay-out	10	
TOTAAL		**100**	

ISMS-plan

Naam kandidaat :
Kandidaatnummer :
Titel werkstuk :

Onderwerp dat moet zijn opgenomen	Beoordelingsaspecten	Score in punten	Toegekend
1. Beschrijving ISMS	• Werkingsgebied • Doel • Inleiding • Volledigheid beschrijving ISMS	20	
2. Proces ISMS	• Werking van het proces • Resultaten • Registraties	10	
3. Organisatie	• Beschrijving organisatie • Taken, bevoegdheden, verantwoordelijkheden • Rapportage	15	
4. Beschrijving inrichting	Beschrijf globaal 1 stappen: ○ beleid ○ organisatie ○ training & awareness ○ deelprocessen ISMS (bijvoorbeeld: risicoanalysemethode, Incident Handling) ○ Evaluatie ○ Rapportage 2 planning 3 evaluatie 4 rapportage	45	
5. Taalgebruik en vormgeving	• Correct taalgebruik (spelling, grammatica, stijl) • Heldere structuur, passende lay-out	10	
TOTAAL		**100**	

Auditplan

Naam kandidaat :
Kandidaatnummer :
Titel werkstuk :

Onderwerp dat moet zijn opgenomen	Beoordelingsaspecten	Score in punten	Toegekend
1. Voorwoord, inleiding, achtergrond, uitgangspunten e.d.	• Inleiding, werkingsgebied • Doel • Focus	20	
2. Basis van het plan	• Referenties, standaarden • Rapportage • Vertrouwelijkheid	30	
3. Uitvoering	• Uitvoeringsdetails • Verantwoordelijkheden • Rapportagedetails • Vertrouwelijkheid	40	
4. Taalgebruik en vormgeving	• Correct taalgebruik (spelling, grammatica, stijl) • Heldere structuur, passende lay-out	10	
TOTAAL		**100**	

Quickscan

Naam kandidaat :
Kandidaatnummer :
Titel werkstuk :

Onderwerp dat moet zijn opgenomen	Beoordelingsaspecten	Score in punten	Toegekend

1. Inleiding, achtergrond, uitgangspunten	• Doel
	• Scope (reikwijdte)
	• Veranderingslogboek (versiebeheer)
	• Ondertekening:
	  ○ wie zijn de opstellers;
	  ○ wie zijn de respondenten;
	  ○ wie accordeert.
	• Op welke vragenlijst is deze quickscan gebaseerd (bijv. Code voor Informatiebeveiliging)
	• Gekozen werkvorm bij uitvoering (bijv. workshops of interviews)
	• Managementsamenvatting
		30	

2. Procesbeschrijving	• Beschrijving van de doorlopen stappen	30	
3. Uitwerking	• Resultaten van de doorlopen stappen • Eindconclusie • Afhankelijk van de eindconclusie: ○ De te nemen maatregelen; • Invoeringsplan (planning, prioritering, verantwoordelijkheden).	30	
4. Taalgebruik en vormgeving	• Correct taalgebruik (spelling, grammatica, stijl) • Heldere structuur, passende lay-out	10	
TOTAAL		**100**	

Informatiebeveiligingsbeleid

Naam kandidaat :
Kandidaatnummer :
Titel werkstuk :

Onderwerp dat moet zijn opgenomen	Beoordelingsaspecten	Score in punten	Toegekend
1. Voorwoord, inleiding, achtergrond, uitgangspunten e.d.	• Motivatie, belang, prioriteit • Doel • Inleiding, werkingsgebied • Afstemming op niveau doelgroep	20	
2. Beleidsuitspraken	• Compleetheid • Realisme • Strategisch niveau	10	
3. Detailonderwerpen	• Organisatie • Verantwoordelijkheden • Incidentafhandeling • Continuïteit van informatiebeveiliging • Sancties • Bewustwording, opleiding • Rapportage, onderhoud beleid • Afwijkingen van het beleid • Back-up cycli • Informatiebeveiliging en leveranciers	50	
4. Uitwerking	• Ondersteuning bij uitvoering, details • Planning • Goedkeuring, ondertekening	10	
5. Taalgebruik en vormgeving	• Correct taalgebruik (spelling, grammatica, stijl) • Heldere structuur, passende lay-out	10	
TOTAAL		**100**	

Mondeling examen
De examinatoren baseren hun oordeel op de aantoonbare (werk)ervaring op managementniveau, het werkstuk, kennis en inzicht in het vakgebied en het vermogen van de examenkandidaat hierop te reflecteren. De examinatoren vinden het belangrijk dat de kandidaat laat zien wat hij of zij geleerd heeft tijdens en voorafgaand aan de module ISMES en wat zijn of haar visie is op het vakgebied. In dit hoofdstuk staan de beoordelingscriteria die gelden voor het mondeling examen ISMES.

I Presentatie
In tabel I leggen de examinatoren de score vast die u behaald heeft voor de presentatie. Dit is het eerste deel van het mondeling examen.

De kandidaat…	Score (punten)	
	max.	behaald
belicht het onderwerp voldoende en binnen de gestelde tijdsduur	10	
behandelt het onderwerp inhoudelijk correct	10	
behandelt het onderwerp op het juiste niveau en voor de juiste doelgroep	20	
brengt het onderwerp op overtuigende wijze en kan eigen standpunten motiveren	30	
zet zelf ingenomen standpunten begrijpelijk uiteen	30	
Totaal (max. 100 punten)	**100** **I**	

Tabel I: beoordeling presentatie

II Examengesprek naar aanleiding van presentatie

In tabel II leggen de examinatoren de score vast die u behaald heeft voor het examengesprek naar aanleiding van de presentatie. Dit is het tweede deel van het examen.

De kandidaat…	Score (punten)	
	max.	behaald
geeft inhoudelijk correcte antwoorden en motivatie van antwoorden	15	
motiveert en/of verdedigt standpunten op professionele wijze	15	
gaat professioneel om met vragen of opmerkingen van de examinatoren	20	
toont reflectievermogen ten aanzien van het eigen handelen in de werkcontext	25	
toont reflectievermogen ten aanzien van het eigen handelen tijdens presentatie en examengesprek	25	
Totaal (max. 100 punten)	**100** **II**	

Tabel II: beoordeling examengesprek naar aanleiding van presentatie

III Examengesprek over overige exameneisen

In tabel III leggen de examinatoren de score vast die u behaald heeft voor het examengesprek over de exameneisen die in de twee eerdere onderdelen nog niet aan bod zijn geweest. Dit is het laatste deel van het examen.

Exameneis	Max. punten	Mondeling Score
1. Organisatie van de informatiebeveiliging (opstellen ISMS) 1.1 De kandidaat kan het risicomanagementproces in relatie met het ISMS beargumenteren. 1.2 De kandidaat kan de rollen voor informatiebeveiliging definiëren. 1.3 De kandidaat kan een rapportagesysteem ten behoeve van het management inrichten en toepassen.	**20**	
2. Informatiebeveiligingsbeleid 2.1 De kandidaat kan meewerken aan het proces van het tot stand komen van het informatiebeveiligingsbeleid. 2.2 De kandidaat kan een informatiebeveiligingsbeleid opstellen, presenteren en uitdragen.	**10**	
3. Risicoanalyse 3.1 De kandidaat kan op basis van inzicht in de verschillende risicoanalysemethoden een methode kiezen en uitvoeren. 3.2 De kandidaat kan de resultaten van een risicoanalyse analyseren.	**10**	
4. Organisatieverandering en –ontwikkeling met betrekking tot Informatiebeveiliging 4.1 De kandidaat kan in een gegeven situatie een veranderplan op- of bijstellen. 4.2 De kandidaat kan in een gegeven situatie een awareness programma opstellen, communiceren, presenteren en uitvoeren.	**40**	
4.3De kandidaat kan in een gegeven situatie de veranderingen doorvoeren of dit proces begeleiden.		
5. Standaarden en normen 5.1 De kandidaat kan in een gegeven situatie een relevante standaard kiezen en hanteren. 5.2 De kandidaat kan in een gegeven situatie een normenkader of baselineconstructie implementeren.	**10**	
6. Audit en certificatie 6.1 De kandidaat kan de uitvoering van audits organiseren. 6.2 De kandidaat kan meewerken aan een managementbeoordeling van het ISMS.	**10**	
Totaal	**100** **III**	

Tabel III: beoordeling overige exameneisen

IV Eindbeoordeling ISMES

Na het examen verlaat u de ruimte en bepalen de examinatoren in onderling overleg hun eindoordeel. Hiervoor gebruiken zij tabel IV. Direct daarna geven zij u uitsluitsel en lichten het eindoordeel toe.

Onderdeel	Gewicht	Punten per examenonderdeel		Gewicht punten per onderdeel
Werkstuk	**10%**	**W**		
Mondeling				
I Presentatie	**20%**	**I**		
II Examengesprek naar aanleiding van presentatie	**20%**	**II**		
III Examengesprek overige exameneisen	**50%**	**III**		
	100%	**Totaal behaalde punten**		

Tabel IV: eindbeoordeling ISMES

Appendix 2: Casus Van Dijk-IT B.V.

De casus is optioneel en hoort bij het schriftelijk gedeelte.

Van Dijk-IT B.V.
Leidschendam

Company Profile
Van Dijk-IT B.V.[1] is een relatief klein adviesbureau (ca. 180 medewerkers) op het gebied van automatisering. Het bedrijf bestaat inmiddels ongeveer zestien jaar.
Door hun opdrachtgevers worden ze gewaardeerd om hun vermogen niet-alledaagse problemen te kunnen oplossen. Zo hebben ze demonstratieprojecten uitgevoerd om aan te tonen dat met Open Source software, volledige kantooromgevingen of complexe beveiligingsfunctionaliteit te realiseren is en dat met deze software online en mobiele applicaties gebouwd kunnen worden, waardoor organisaties gemakkelijker bereikbaar zijn voor hun klanten.

Opdrachtgevers zijn onder meer het Kadaster, een aantal Ministeries, een bank, verzekeringsmaatschappijen en ingenieursbureaus.

Van Dijk-IT is verdeeld in drie divisies die de verschillende activiteiten uitvoeren. De divisies worden beschouwd als business units met eigen winst/verliesverantwoordelijkheid.

- **Consultancy**: Business Consultants (25) – leveren adviesdiensten op het raakvlak van operatie en IT. Onderwerpen zijn bijvoorbeeld: organisatieanalyse, vertaling van businessprocessen naar webapplicaties, ondersteuning bij het opstellen van functionele eisen, in kaart brengen van de bedrijfsinformatiemiddelen en hun eigenaren, enz.
- **ITC**: IT consultants (60) – leveren adviesdiensten op het gebied van IT, softwareontwerp en –ontwikkeling, project management enz. Voorbeelden zijn: omzetten van functionele naar technische specificaties, configureren van de infrastructuurcomponenten, capaciteitsbeheer, opzetten van configuratiebeheer, inrichten van informatiebeveiliging, Netwerk Management, Service Management, enz.
- **SO**: Softwareontwikkeling (85): het ontwerpen, ontwikkelen en leveren van software. In voorkomende gevallen worden ook hardwarecomponenten en softwarepakketten geleverd zodat opdrachtgevers complete oplossingen ontvangen. Daarnaast wordt beheer op afstand uitgevoerd voor een beperkt aantal klanten.

Iedere divisie heeft een eigen administratieve staf die verantwoordelijk is voor personeelsbeleid (HRM), urenadministratie en facturering. Office management en 1e lijns systeembeheer is ook lokaal aanwezig.

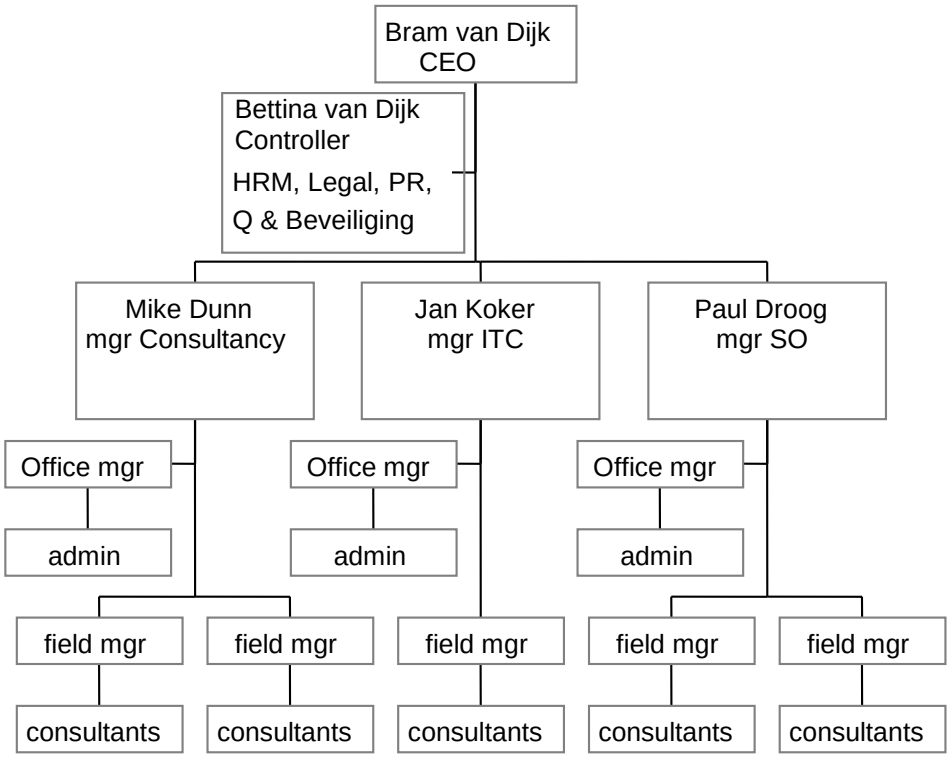
De centrale organisatie (10) omvat de Directie, juridische zaken, facilitair management (valt ICT ook onder), Interne Communicatie en Public Relations (PR), salarisadministratie, centrale personeelsadministratie, helpdesk en Quality & Security (Q&S).

Van Dijk-IT heeft een ISO 9001 kwaliteitscertificaat. Dat is verleend voor het uitvoeren van projecten in de ITC-divisie en voor beheer en ondersteuning op afstand in de SO-divisie.

Tijdens het certificeringstraject voor ISO 9001 is Bettina van Dijk (geen familie van Bram) als kwaliteitscoördinator (daar staat de 'Q' voor) aangesteld. Recentelijk (3 maanden geleden) heeft zij ook Beveiliging in haar portefeuille gekregen.

---

[1]) *Iedere gelijkenis met een bestaande organisatie of bedrijf berust op toeval, deze casus is in zijn geheel verzonnen.*



Figuur 1: Organisatie Van Dijk-IT B.V.

Kantooromgevingen
Van Dijk-IT/Consultancy is gevestigd in Leidschendam, Van Dijk-IT/ITC is gevestigd in Nieuwegein, terwijl Van Dijk-IT/SO kantoor houdt in Leusden. De directie en de centrale afdelingen werken vanuit het kantoor in Leidschendam.

Ieder kantoor heeft een bemande receptie (alleen tijdens kantooruren). In Nieuwegein en Leusden wordt regelmatig overgewerkt. ‘s Nachts zijn de panden op slot. Iedere vestiging heeft een alarmsysteem dat melding doet bij een lokale alarmcentrale.
Een half jaar geleden toonde rapportering aan dat het aantal valse alarmmeldingen stijgt; op dit moment is dat weer wat afgenomen. De alarmsystemen zijn inmiddels 5 tot 7 jaar oud. Het lijkt erop dat recentelijk vaker vergeten wordt de alarmsystemen
‘s avonds in te schakelen.

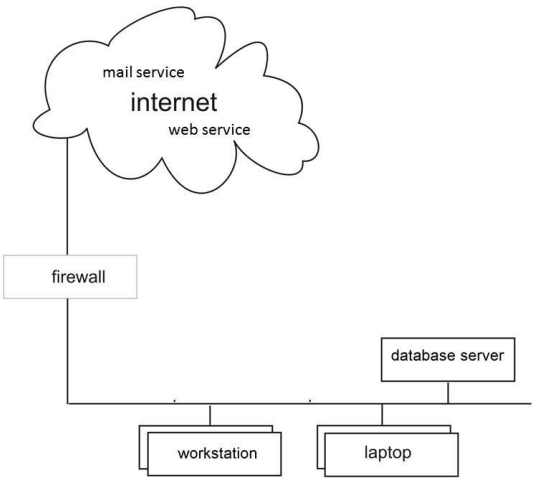
IT omgeving
Van Dijk-IT heeft een netwerk met verschillende merken hubs die gedurende de afgelopen jaren, toen de prijzen laag waren, door verschillende personeelsleden zijn aangeschaft. Er vindt relatief weinig verkeer tussen de vestigingen plaats. Verbinding tussen de vestigingen bestaat uit een trage en verouderde breedbandinternetverbinding.

In iedere vestiging staan fileservers voor opslag van rapporten en documenten (de Y-schijf). De meeste medewerkers hebben toegang tot hun eigen directory; een aantal (secretariaat, administratie) hebben ook toegang tot gezamenlijke directories.

In Leusden staat de aansluiting met internet, met Cisco firewall waarvoor een onderhoudscontract bestaat. Een router (vier jaar geleden geplaatst) verdeelt het verkeer tussen het interne netwerk en het Internet. De mail service en web services die worden gebruikt door Van Dijk zijn externe Clouddiensten.

De SO-consultant die de technische details had bepaald, is twee jaar geleden vertrokken. Omdat het systeem zonder problemen werkt, heeft niemand zich bekommerd om documentatie. Het is ook niet duidelijk wie verantwoordelijk is voor onderhoud.

De inhoud van de corporate website wordt bijgehouden door de mensen uit de PR-groep.



Figuur 2:Overzicht IT-infrastructuur

In Leusden staat t.b.v. SO een afzonderlijke LAN (twee servers, vijf werkstations, en extra hubs voor de laptops) om te experimenteren. Verder staan hier drie Linux-servers voor ontwikkeling en testen. Ook zijn een aantal werkstations met Linux-versies aanwezig.

De financiële administratie en de urenadministratie draaien centraal. Deze maken gebruik van een Oracle database met Internetapplicatie front end (Oracle applicatieserver). De applicaties zijn niet bereikbaar voor de vestigingsadministratie. Lokale informatie gaat per e-mail (Excel-sheet in bijlage, eens per maand) naar de centrale administratie. Daar wordt het omgezet in het juiste formaat en ingelezen in de databases.

Voor remote gebruik van intranet en voor het gebruik van webmail worden gebruikersnaam en wachtwoord gebruikt. Er gaan geluiden op om daarvoor een token te gaan gebruiken.

Medewerkers hebben allemaal een snelle internetverbinding thuis. Iedereen krijgt 30 Euro per maand als tegemoetkoming in de kosten van het zakelijk gebruik van de internetverbinding. Een paar medewerkers hebben een afgeschreven PC gekregen om te kunnen mailen.

Kantoorautomatisering (alle recente varianten van MS Office) draait lokaal op de werkstations en laptops.

De consultants zijn verdeeld volgens een expertisegroepen-structuur. Per EG is er een gezamenlijke directory voor de opslag en distributie van rapporten en andere documentatie.

Informatiebeveiliging
Tot nog toe is informatiebeveiliging niet structureel aan de orde geweest. Er zijn wat vragen gesteld over intranet en beveiliging, maar dat is snel weggeëbd. Het aantreden van Bettina van Dijk heeft tot nog toe geen effect gehad, maar zij is er ook nog maar heel kort. Wel wordt verwacht dat binnenkort allerlei procedures ingericht gaan worden. Dat zou kunnen betekenen dat de meer technisch onderlegde consultants en de mensen van SO een aantal van hun onderhands verkregen privileges kwijt zullen raken.

De kern van de beveiliging wordt gevormd door een gebruikersnaam-wachtwoordconstructie om toegang te krijgen tot het netwerk. Op basis van de gebruikersnaam wordt toegang verleend tot files en applicaties. Toegangsrechten worden toegekend via Active Directory (AD). Een aantal medewerkers wijzigt hun password regelmatig, maar het wordt niet afgedwongen.

Centraal wordt een back-up gemaakt van de databasefiles. Back-up van de mail en van de webcontent wordt door de externe Cloud serviceprovider uitgevoerd. Er bestaat een mogelijkheid om belangrijke files te bewaren op het netwerk, maar niet iedereen (eufemisme voor bijna niemand) maakt daar gebruik van. De documenten die door de administratie gebruikt worden staan wel allemaal op het netwerk.

In Leidschendam zijn te weinig kasten. Met name de financiële administratie klaagt over het niet kunnen opbergen van hun documenten. Zij hebben ook de contracten onder hun beheer.

Alleen in Leusden staat een shredder, een grote, waarin hele boeken vernietigd kunnen worden. Het apparaat is overgebleven na een vertrouwelijk project voor Defensie, net als de kluis waarin nu de originele cd's van het grootste deel van de aangeschafte software liggen.

Centraal is een abonnement met McAfee antivirussoftware afgesloten. Dat draait op de servers, de werkstations en op de laptops. Onderdeel van het inlogscript is dat gecheckt wordt welke versie van de antivirussoftware aanwezig is. Indien nodig wordt de meest recente versie geïnstalleerd. Helaas is het voor werkstation- en laptopgebruikers mogelijk de virusscanner uit te zetten. Daardoor start de PC een stuk sneller op.

Er zijn geen licenties voor cryptografische software.

Operationele processen
Over de bedrijfsprocessen van Van Dijk-IT wordt tamelijk simpel gedacht. Het bedrijf ziet drie processen als primair:

- Consultancy en projecten: het leveren van diensten volgens afgesloten overeenkomsten in drie vormen (detachering, consultancy of projecten tegen tijd en materiaalkosten, en projecten met een vaste prijs)
- Sales: het verkopen van diensten
- Facturatie: het verzenden en innen van facturen voor geleverde diensten.

Alle primaire processen zijn aanwezig in elk van de divisies.

Er is wel enig verschil in inzicht welke van de primaire processen de hoogste prioriteit heeft. Het leveren van diensten mag niet lang onderbroken worden. Verder blijkt dat sommige opdrachtgevers hun informatie als uiterst sensitief beschouwen met hoge concurrentiewaarde.
Het Salesproces kan indien nodig een week stilliggen, veel langer wordt ongemakkelijk. Het proces maakt voornamelijk gebruik van kantoorautomatiseringsfuncties. Gelukkig is veel informatie die in het Salesproces gebruikt wordt, verspreid aanwezig in agenda's en laptops.
Facturatie kent in de eerste week van de maand topdrukte. Onderbreking daarvan kost direct geld. De rest van de maand is dat minder belangrijk.

Daarnaast zijn er ondersteunende processen zoals:

- Consoliderende administratie (uren en financiën);
- Juridische zaken – contracten;
- Centrale personeelsadministratie;
- Salarisadministratie;
- Beheer van faciliteiten, waaronder het IT-park;
- Interne communicatie en PR;
- Enz.

Het Managementteam (directeur, managers en controller) vindt dat al deze processen rustig een langere periode onderbroken kunnen worden zonder risico voor de business. Wel moet er dan een oplossing gevonden worden voor de salarisbetalingen.

Reacties van managers op de vraag: Is informatiebeveiliging nodig?

Reactie van Bettina van Dijk (Q&B manager, Van Dijk-IT bv)
Er is drie maanden geleden een financiële audit uitgevoerd door de accountant. Daaruit blijkt dat er mogelijk volgend jaar geen goedkeurende verklaring komt, als de betrouwbaarheid van de geautomatiseerde informatieverwerking niet is verbeterd.
Er is hevige onrust uitgebroken in het Managementteam, wat ertoe heeft geleid dat 'Security' op mijn bord is gedeponeerd met de opmerkingen 'Doe er wat aan' en 'Als dat geld gaat kosten, laat het dan weten- maar niet teveel hoor'.

Van Dijk-IT heeft zich ontwikkeld van vier consultants die samen een bedrijfje gingen starten tot de club die het nu is. Omdat er altijd ruim voldoende opdrachten zijn geweest – regelmatig zijn zelfs externen ingehuurd van collega's – heeft de operatie steeds voorrang gekregen. Eigenlijk heerste er een wildwest-cultuur. We schoten op alles dat bewoog met alles wat we hadden. En het werkte ook nog.
Daarom is de infrastructuur ook een rommeltje. We weten niet meer precies wat we aan hardware en software in huis hebben. Aan licentiemanagement en beheer van de bedrijfsmiddelen is letterlijk nooit gedacht. Op het moment dat er iets nodig is, wordt het besteld. Dat geldt voor de hardware, dat geldt ook voor de software. De decentrale structuur werkt dit in de hand. Het kost handenvol geld, maar je hoeft tenminste niet na te denken.

De experts van SO weten gelukkig wat ze doen. Er zijn – zover ik weet – nooit grote problemen geweest. Geen inbraken en maar één of twee keer hebben we Internet even moeten afkoppelen omdat er teveel virussen binnen waren. We hebben daardoor maar een dag of twee aan mail verloren.

O ja, één van de consultants is een jaar geleden zijn laptop kwijtgeraakt, gestolen. Dat was wel vervelend. Er waren immers geen back-ups. Gelukkig is het meeste teruggevonden. Ik geloof niet dat de klant er iets van gemerkt heeft. Maar zeker weten doe ik dat niet. En back-ups maken ze nog steeds niet.

Helaas weet ik zelf niet zoveel van computerbeveiliging. Ik doe dit nog maar net. Er zijn ook weinig cursussen om zoiets snel op te pikken. Ik zou wel wat hulp kunnen gebruiken met het opzetten. Er zijn vragen genoeg, zoals:

- Waarmee moet ik beginnen?
- Wat hebben we al?
- Hoeveel maatregelen zijn nog nodig? En is dat dan voldoende?
- Wie is verantwoordelijk?
- Hoe kunnen we de medewerkers zover krijgen dat ze bijvoorbeeld regelmatig hun wachtwoord veranderen?
- Hoe krijg ik de managers zover dat ze hun medewerkers in beweging krijgen?

Reactie van Mike Dunn, mgr Consultancy
Informatiebeveiliging moet. Ik had gehoopt al iets van Bettina van Dijk gehoord te hebben. Al onze grote klanten hebben het over cyber security vanwege de vele recente grote cyber attacks. En daarbij zijn er zoveel eisen in wetten en regelgeving op dit gebied, die ook gelden voor sommige buitenlandse organisaties. Welke invloed heeft dit op onze klanten? En hoe moeten wij daarmee omgaan?

Kunnen we dat ook als dienst aan onze klanten verkopen? In de vorm van Risicomanagement of zo? Ik zal eens kijken of daar behoefte aan is. Ik heb wel wat relaties.

Informatiebeveiliging zal het werken toch niet moeilijker maken? Mijn adviseurs zijn geen automatiseerders. Het moet niet te moeilijk worden.

Anders nog iets?

Reactie van Paul Droog, mgr SO
Informatiebeveiliging zal best nodig zijn, maar daar hebben we nu even geen tijd voor. Het gaat toch allemaal goed. We zijn nog nooit in de krant gekomen. We zijn kennelijk best in staat om het allemaal binnenkamers te houden. Best veilig lijkt me.

Trouwens, kunnen we dan nog wel werken? Kunnen we dan nergens meer bij?

Waarom is dat nu ineens nodig? Het gaat toch allemaal goed? We hebben nooit grote problemen gehad. Afgezien dan van die laptop, dat was stom. Zo'n vent moet zoiets toch niet op z'n achterbank laten liggen. Vervelend dat die database van de klant erop stond. Goed dat we nog iemand bij de klant hadden zitten. Kon hij nog even een kopietje maken. Maar goed dat de klant niets gemerkt heeft; anders hadden we onze biezen kunnen pakken.
O ja, die disk crash van vorig jaar was slecht nieuws, vooral toen de back-up niet bruikbaar bleek. Moesten we toch maar wat vaker testen. Ik heb geen idee of daar nog wel eens naar gekeken is. Toch knap van dat bedrijf dat nog 72% van de data van die schijf heeft weten te peuteren. 't Heeft wat gekost, en het duurde langer dan leuk was, maar ja. Wat moet je anders.

Zie je wel, 't valt allemaal best mee. Iedereen heeft toch wel eens dat het netwerk plat ligt, of dat Windows stopt?

Opdracht bij de casus

Schrijf voor Van Dijk-IT bv een werkstuk over één van de volgende onderdelen van ISMES:

- Security Awareness-plan;
- Risicoanalyse;
- Veranderingsplan;
- ISMS-plan;
- Auditplan;
- Quickscan;
- Informatiebeveiligingsbeleid.

Contact EXIN

www.exin.com

YOUR ICT COMPETENCE PARTNER