Starterkit Informatiebeveiliging

Colofon

Starterkit Informatiebeveiliging

SURFfoundation
PO Box 2290
NL-3500 GG Utrecht
T + 31 30 234 66 00
F + 31 30 233 29 60

info@surf.nl
www.surf.nl

Auteurs
Rene Ritzen (Universiteit Utrecht)
Mark Hoevers (IGI groep)

SURF is de ICT-samenwerkingsorganisatie van het hoger onderwijs en onderzoek (www.surf.nl).
Deze publicatie is digitaal beschikbaar via de website van SURFfoundation:
www.surffoundation.nl/publicaties

December 2010

SurfIBO

Het SURF Informatie Beveiligers Overleg is ingesteld door het programma SURF ICT en Bedrijfsvoering met als doelen het actief stimuleren van en richting geven aan informatiebeveiliging binnen het hoger onderwijs (universiteiten, hogescholen en universitair medische centra). Dat wordt bereikt door het bevorderen van de samenwerking tussen informatiebeveiligers en het leveren van praktisch bruikbare adviezen.

Voor meer informatie zie www.surfibo.nl

Inhoudsopgave

Samenvatting

Deze Starterkit Informatiebeveiliging heeft als doel de inrichting van informatiebeveiliging in een hoger onderwijsinstelling stap voor stap te begeleiden. Er wordt uitgegaan van een situatie dat er nog niet structureel aandacht aan informatiebeveiliging wordt gegeven en dat er geen bestuurlijk commitment en geen budget aanwezig is. Dat is de slechtst denkbare uitgangssituatie. Indien een instelling al iets aan de inrichting van informatiebeveiliging heeft gedaan kan het zijn dat de in deze starterkit beschreven fasen 1 en 2 sneller doorlopen kunnen worden.

Informatiebeveiliging bestrijkt een breed aandachtsgebied. Omdat niet alles tegelijk gerealiseerd kan worden is een fasering aangebracht.

Fase 1: inventarisatie huidige situatie
Het is belangrijk dat een informatiebeveiliger weet hoe de organisatie in elkaar zit, wat de primaire en ondersteunende bedrijfsprocessen zijn, welke informatiesystemen gebruikt worden om die bedrijfsprocessen te ondersteunen, wie verantwoordelijk is voor het beheer daarvan, et cetera. Fase 1 bestaat dan ook uit het voeren van (kennismakings)gesprekken met eigenaren en beheerders van bedrijfsprocessen, informatiesystemen, applicaties, e.d.

Als dat inzicht is verkregen (en gedocumenteerd), wordt in overleg met die eigenaren bekeken hoe kwetsbaar de bedrijfsprocessen zijn voor verstoringen in de ICT-voorziening: voor de belangrijkste applicaties wordt voor beschikbaarheid, integriteit en vertrouwelijkheid gescoord op een schaal van 1 (nog niets aan beveiliging gedaan) tot 3 (voldoende gedaan).

Daarnaast wordt geïdentificeerd voor welke onderdelen van informatiebeveiliging beleid en procedures bestaan. Denk hierbij onder meer aan de aanwezigheid van een goedgekeurd beleidsdocument, het hebben van een beveiligingsorganisatie waarin iedereen zijn of haar verantwoordelijkheden kent, een gebruiksreglement, een incident registratiesysteem, viruscontrole, etc. Meestal zijn er al technische voorzieningen op beveiligingsgebied getroffen zoals bijvoorbeeld het gebruik van viruscheckers, maar is de organisatie nog niet gerealiseerd en het beleid niet vastgesteld.

Fase 2: korte termijn verbeteringen en opstellen Plan van Aanpak
Om aan het bestuur aan te kunnen tonen dat het loont om structureel aandacht aan informatiebeveiliging te geven worden de meest lonende maatregelen doorgevoerd (laaghangend fruit). Deze zijn afgeleid uit de inventarisatie van kwetsbaarheden en de stand van zaken m.b.t. te nemen maatregelen.

In deze fase wordt ook een Plan van Aanpak voor de lange termijn opgesteld, waarin alle aspecten van informatiebeveiliging aan de orde komen. In dat plan komen projectvoorstellen te staan die de komende jaren uitgevoerd moeten worden. Denk hierbij een het opstellen van een baseline informatiebeveiliging, het inrichten van de informatiebeveiligingsorganisatie en maatregelen op het gebied van bedrijfscontinuïteit.

Fase 3: de dialoog met bestuurders
In deze fase is het belangrijk om commitment van het bestuur te krijgen.
Kan de informatiebeveiliger het bestuur overtuigen van het belang van structurele aandacht voor informatiebeveiliging? In principe zou dit moeten lukken op basis van de al eerder genomen maatregelen (laaghangend fruit) en de risicoverlaging die daarmee gerealiseerd is.

Het kan best zijn dat er meerdere gesprekken en presentaties nodig zijn om duidelijk te maken dat informatiebeveiliging helpt om de overall doelstellingen van de onderwijsinstelling te realiseren. Aandacht voor de Wet Bescherming Persoonsgegevens, aansprakelijkheidsclaims van opdrachtgevers, reputatieschade, het niet 'in control' zijn, zijn doorgaans zaken die tot inzicht kunnen leiden.

Uiteindelijk zal er commitment ontstaan en zullen middelen (menskracht en financiering) ter beschikking gesteld worden voor de uitvoering van het gepresenteerde Plan van Aanpak.

Fase 4: projectmatige uitvoering Plan van Aanpak
Het is belangrijk om informatiebeveiliging beheersbaar te maken. Daarvoor zal aangesloten moeten worden bij de budgetcyclus. Dus zal er naast het opstellen van beleid en het inrichten van een informatiebeveiligingsorganisatie waarin rollen en verantwoordelijkheden zijn beschreven, ook gewerkt moeten worden aan het inrichten van de Plan-Do-Check-Act-cyclus voor informatiebeveiliging. Dat geeft ook mogelijkheden om delen van het plan van aanpak in de jaarbegroting mee te nemen.

Verder zal er gewerkt moeten worden aan de inrichting van een risicomethodiek, het incident managementproces, het inrichten van een communicatie- en rapportagestructuur en de uitvoering van diverse deelprojecten uit het Plan van Aanpak.

Fase 5: beheer
Het is belangrijk periodiek de status van informatiebeveiliging in de instelling te monitoren en, bij geconstateerde tekortkomingen, maatregelen te treffen. Dit kan door het uitvoeren van nieuwe risicoanalyses, door het (laten) uitvoeren van audits, door het inhuren van een 'misteryman' die de vinger op de zere plekken legt, etc.

Onderdeel van beheer is ook de bevordering van bewustwording. Dat kan met trainingen via een intranetsite, posters en/of e-learning. Waar het om gaat is dat het beleid bekend wordt gemaakt en wordt gehandhaafd. Dit vergt de nodige aandacht. Mensen kennen de risico's onvoldoende en doen, soms uit behulpzaamheid, dingen die beter achterwege gelaten kunnen worden (social engineering) en daar moet op getraind worden.

Controle, naleving en sancties vormen het onvermijdelijke sluitstuk van een serieus informatiebeveiligingstraject. Interne en externe accountants kunnen daarbij behulpzaam zijn.

Tot slot
De starterkit geeft voor elke fase aan hoe de opstelling en instelling van de informatiebeveiliger het beste kan zijn en welke 'soft skills' hij of zij nodig heeft.

Een algemeen format voor een Plan van Aanpak en een projectformat zijn als bijlage opgenomen.

1 Inleiding

Bedrijven en instellingen zijn in hoge mate afhankelijk van ongestoorde en betrouwbare bedrijfsprocessen. Bij hogeronderwijsinstellingen geldt dit niet alleen voor de processen van bestuur en beheer maar uitdrukkelijk ook voor de primaire processen onderwijs en onderzoek. Informatiebeveiliging is een belangrijk middel om de risico's op verstoring van de bedrijfsprocessen te voorkomen of te beperken.

Informatiebeveiliging is een breed werkterrein dat zich richt op de Beschikbaarheid, Integriteit en Vertrouwelijkheid van informatie (BIV). Zeker bij hoger onderwijs instellingen kan dit een uitdaging zijn. Om onderwijs en onderzoek optimaal te laten gedijen wordt aan de ene kant de grootst mogelijke openheid gevraagd. Aan de andere kant is het noodzakelijk om informatie en informatiesystemen zodanig te beschermen dat de beschikbaarheid, integriteit en vertrouwelijkheid worden gewaarborgd.

Gelukkig ontstaat bij steeds meer instellingen het besef dat het noodzakelijk is om informatiebeveiliging serieus op te pakken. Veelal is de verantwoordelijkheid voor informatiebeveiliging belegd bij een ICT-afdeling of voelt deze zich hiervoor verantwoordelijk zonder bijbehorende bevoegdheden te hebben gekregen. Het komt in zo'n situatie vaak voor dat de verantwoordelijke persoon niet goed weet waar hij of zij moet beginnen en wat er allemaal gedaan moet worden om tot een verantwoord niveau van informatiebeveiliging te komen. Over het algemeen wordt geadviseerd om de Code voor Informatiebeveiliging te hanteren. Deze Code is een goede leidraad om het totale spectrum van informatiebeveiliging mee in te richten, maar is op een vrij hoog abstractieniveau geschreven, waardoor het lastig is om de vertaling te maken naar de praktijk van een hogeronderwijsinstelling.

1.1 Doelstelling

Deze starterkit informatiebeveiliging beoogt een handreiking te zijn voor de inrichting van informatie-beveiliging in de sector hoger onderwijs. In deze starterkit is de Code voor Informatiebeveiliging weliswaar leidend voor het totale landschap van informatiebeveiliging, maar er wordt zoveel mogelijk getracht om per onderdeel laagdrempelig te starten met als doel in relatief korte tijd zo veel mogelijk resultaat te boeken.

1.2 Overwegingen

Volgens de Code voor Informatiebeveiliging dienen we een heel palet aan maatregelen te treffen. De belangrijkste hoofdstukken van de Code betreffen:

1. Beveiligingsbeleid
2. Organisatie van de informatiebeveiliging
3. Beheer van bedrijfsmiddelen
4. Beveiliging van personeel
5. Fysieke beveiliging en beveiligingsomgeving
6. Beheer van communicatie en bedieningsprocessen
7. Toegangsbeveiliging
8. Verwerving, ontwikkeling & onderhoud van informatiesystemen
9. Beheer van informatiebeveiligingsincidenten
10. Bedrijfscontinuïteitsbeheer
11. Naleving

Bij een volwassen informatiebeveiliging dienen al deze onderdelen uitgewerkt te zijn. Voor een uitgebreide beschrijving van deze onderdelen wordt verwezen naar 'De Code voor Informatie-beveiliging' (NEN-ISO/IEC 27002, te verkrijgen bij het Nederlands Normalisatie-instituut) en naar 'Informatiebeveiliging, het IABB-procesmodel voor een gestructureerde aanpak' (van Stichting SURF). In deze starterkit wordt in paragraaf 2.2 kort ingegaan op de genoemde onderdelen.

Bij beperkte beschikbaarheid van capaciteit en middelen, maar ook als er nog geen commitment van het bestuur is, kunnen toch een aantal stappen gezet worden waarmee de status van informatiebeveiliging binnen de instelling kan worden vastgesteld. Daarop ligt de focus in deze starterkit informatiebeveiliging.

1.3 Werkwijze

Deze starterkit informatiebeveiliging is daarom opgebouwd volgens een gefaseerde aanpak (beschreven in hoofdstuk 2), zodat meteen begonnen kan worden, ook door degenen die er alleen voor staan: er is nog geen bestuurlijk commitment en er zijn slechts beperkte middelen voor informatiebeveiliging

Door in deze uitgangssituatie in de fases 1 en 2 een aantal relatief eenvoudige zaken op te pakken (hoofdstukken 3 en 4) kan vervolgens in fase 3 worden gewerkt aan het kweken van bestuurlijk commitment (hoofdstuk 5) voor een meer structurele aanpak van informatiebeveiliging.
Die meer structurele aanpak wordt beschreven in fase 4 (hoofdstuk 6), de projectmatige uitvoering van het Plan van Aanpak. De starterkit sluit af met een beschrijving van de beheerfase (fase 5, hoofdstuk 7).

1.4 Relatie met andere documenten

Er wordt door SURF-ibo en het CIO-beraad gewerkt aan een aantal andere documenten met betrekking tot informatiebeveiliging. De belangrijkste is de **Leidraad Informatiebeveiliging**, waarin een **model informatiebeveiligingsbeleid** is opgenomen, dat door instellingen in het hoger onderwijs vrijwel ongewijzigd kan worden overgenomen. Het model is gebaseerd op de good practices uit de sector zelf.

Het hebben van een vastgesteld beleidsdocument is echter niet voldoende. Om op een gestructureerde manier aandacht te kunnen besteden aan informatiebeveiliging is er meer nodig. Deze **Starterkit Informatiebeveiliging** beschrijft hoe van een situatie waarin vrijwel niets geregeld is gekomen kan worden tot zo'n gestructureerde aanpak van informatiebeveiliging.

Daarnaast worden door SURF-ibo en het CIO-beraad regelmatig andere documenten (leidraden, dan wel starterkits) opgesteld, waarmee de sector op deelonderwerpen aan de slag kan. Op dit moment gaat het om een 'Leidraad Classificatie' en de 'Starterkit Business Continuity Management'.

2 Gefaseerde aanpak

Een goede, structurele en bestuurlijk gedragen inbedding van informatiebeveiliging in de organisatie kan je het best gefaseerd invoeren. Bedoeling is dat je in fase 1 een ruwe inventarisatie maakt van hoe de organisatie in elkaar zit en wat er al gedaan is op het gebied van informatiebeveiliging. Die inventarisatie mag best enkele maanden in beslag nemen. Op basis van het beeld dat uit de inventarisatie naar voren komt, kun je in fase 2 korte termijn acties en maatregelen afleiden: het zogenaamde 'laaghangende fruit' kan direct worden geoogst. Verder ga je in deze fase maatregelen voor de langere termijn bedenken en die als aparte projecten uitwerken in het Plan van Aanpak.

In fase 3 ga je met de korte termijn oogst en het lange termijn Plan van Aanpak de dialoog aan met het dagelijks bestuur (College van Bestuur, Raad van Bestuur, Directie) van je instelling. Doel van dat overleg is het verkrijgen van commitment en middelen om meer structureel aandacht te kunnen besteden aan informatiebeveiliging.

In fase 4 ga je de projecten uit het Plan van Aanpak uitvoeren, samen met de belanghebbenden in de organisatie. Niet alles tegelijk, maar per project. Je hebt hiervoor een periode van een jaar of drie.

In fase 5 gaat het om het beheer van informatiebeveiliging in de gehele organisatie, waarvoor de Plan-Do-Check-Act -cyclus (PDCA) wordt toegepast. De fasering ziet er op hoofdlijnen als dus volgt uit:

1. Inventarisatie huidige situatie
2. Korte termijn verbeteringen en opstellen Plan van Aanpak
3. Dialoog met het College van Bestuur
4. Projectmatige uitvoering Plan van Aanpak
5. Beheerfase

Informatiebeveiliging is iets dat de gehele organisatie aangaat. Maar het is niet de bedoeling dat iedereen op elkaar zit te wachten of naar elkaar wijst. Te vaak horen we nog de uitspraak "De ICT-afdeling behoort er voor te zorgen dat we veilig kunnen werken". Dat gaat maar zeer ten dele op.

Ben je diegene die informatiebeveiliging in z'n pakket heeft of wil je informatiebeveiliging in je instelling gaan oppakken, dan kun je dus starten met de fasen 1 en 2. Dat kan ook zonder bestuurlijk commitment en zonder al te veel budget. Fase 3 is cruciaal. De uitkomst daarvan is bepalend voor de verdere uitvoering van de fasen 4 en 5. Voor fase 4 zullen personen uit de hele organisatie een bijdrage moeten gaan leveren en zullen ook budgetten beschikbaar gesteld moeten worden.

Het maakt eigenlijk niet uit of je start vanuit een functie in de afdeling Informatiemanagement of dat je in de ICT-afdeling werkt. Betrokkenheid bij het onderwerp is in eerste instantie het belangrijkste.

In de volgende hoofstukken geven we per fase aan hoe je dit aan kunt pakken.

3 Fase 1: inventarisatie huidige situatie

3.1 Inleiding

Zoals gezegd kun je starten met een inventarisatie van de huidige situatie met betrekking tot informatiebeveiliging in je onderwijsinstelling.

Waar gaat het dan om?
1. de technische infrastructuur: welke systemen hebben we en welke diensten / toepassingen worden daarmee aangeboden;
2. wat is de kwetsbaarheid van de primaire processen (onderwijs en onderzoek) bij verstoringen in die infrastructuur;
3. wat er geregeld is aan beleid en procedures;
4. worden incidenten geregistreerd en wat/hoe leren we daarvan;
5. wordt er iets aan bewustwording gedaan.

Met deze vragen ga je een kennismakingsrondje langs belangrijke functionarissen maken. Denk bijvoorbeeld aan:
- ICT-beheerder(s)
- HRM
- Financiën
- Onderwijs
- Onderzoek
- Facilitaire zaken (gebouwbeheer, bedrijfsbeveiliging)
- Auditafdeling
- Informatiemanagement / CIO of vergelijkbaar

Hieronder wordt voor elk van de vijf genoemde vragen of aandachtspunten aangegeven hoe je daarmee om kan gaan.

3.2 Technische infrastructuur

Omdat er op technisch gebied ongetwijfeld al de nodige maatregelen zijn genomen begin je de inventarisatie daar, met een kennismaking met de ICT-beheerder of –beheerders en een gesprek over welke 'spullenboel' aanwezig is en hoe deze beheerd wordt. Denk hierbij aan servers, netwerken, firewalls, virusscanners, spamfilters, malware detectors, et cetera; en vergeet de werkplekautomatisering niet. Vaak bestaat er wel een inventarislijst of kan deze eenvoudig worden opgesteld. Wanneer het technisch beheer en onderhoud is uitbesteed zal er met dat bedrijf gesproken moeten worden.

Naast hardware is het ook verstandig dat je inventariseert van welke platforms gebruik gemaakt wordt en wat daarmee gedaan wordt. Bijvoorbeeld: waarmee of waarop draait het personeelssysteem, de financiële administratie / boekhouding, het CRM-systeem, e-mail en agenda's, identity management systemen, enzovoort. Maar ook, waarmee verzorgt jullie instelling de studentenadministratie, de behaalde studieresultaten, de uitkomsten van onderzoeksprojecten en de opdrachten die voor derden zijn uitgevoerd. Als het goed is heb je na deze interviews een ruw beeld van de technische infrastructuur, de beveiligingsmaatregelen daarin en hoe het beheer en onderhoud geregeld is. Neem voor deze interviews met ICT-beheerders de tijd. Maak van je bevindingen steeds een gespreksverslag en laat dat door de beheerders corrigeren en/of uitbreiden, zodat je iets hebt om op terug te vallen. Vraag de ICT-beheerders of ze wijzigingen in de technische infrastructuur aan je willen doorgeven, zodat je het beeld actueel kunt houden. Zorg voor een goede relatie met de beheerders, je zult ze later nog nodig hebben.

3.3 Inventarisatie kwetsbaarheid bedrijfsprocessen

Bij informatiebeveiliging zijn er twee belangrijke vragen: wat beveiligen we en waarom?
Kan er nog gedoceerd worden als het netwerk niet beschikbaar is, hoe lang kunnen studenten zonder hun elektronische leeromgeving, in welke mate wordt onderzoek gehinderd als internet niet beschikbaar is, of als de onderzoeksresultaten door onbevoegden zijn gewijzigd? Deze vragen dien je te stellen aan de personen die hier eindverantwoordelijkheid voor dragen. Per instelling kunnen dat personen met verschillende functies of rollen zijn. Bij een procesgeoriënteerde instelling zijn dat de proceseigenaren. In veel gevallen zijn er systeemeigenaren benoemd, maar het kan ook zijn dat de systemen "eigendom" zijn van de ICT-afdeling, waarbij er dan wel sprake is van functionele beheerders die dan feitelijk de rol van verantwoordelijke voor informatie vervullen.

Door vast te stellen welke primaire en secundaire processen binnen jouw onderwijsinstelling belangrijk zijn en te inventariseren hoe deze verlopen, kan je vaak al inzicht krijgen in waar de risico's liggen.
Het is goed om daarbij onderscheid te maken in de diverse processen voor onderwijs, onderzoek (indien van toepassing) en bedrijfsvoering. Elk van deze processen hebben hun eigen, soms ogenschijnlijk tegenstrijdige, eisen ten aanzien van informatiebeveiliging. Hoewel onderwijs en onderzoek gebaat zijn bij een zo groot mogelijke openheid, is het van groot belang om persoonsgegevens goed te beschermen en onderzoeksdata te beschermen tegen verlies en tegen ongeoorloofd kopiëren of wijzigen. Ook de informatie en middelen die ten behoeve van de bedrijfsvoering worden gebruikt dienen optimaal beschermd te worden.

Een manier om op een eenvoudige wijze de kwetsbaarheid van bedrijfsprocessen te inventariseren is dat je -samen met de "eigenaren van de informatie"- onderstaande tabel invult. Hierin geven jullie per proces (per applicatie) aan hoe het staat met de getroffen maatregelen ten aanzien van beschikbaarheid, integriteit en vertrouwelijkheid.

Per veld vullen je een getal in van 1 tot 3:
1 wil zeggen dat er niets is gedaan op het gebied van informatiebeveiliging,
2 betekent dat er wel al iets is gedaan, maar naar mening van de invuller nog niet voldoende en
3 betekent dat er voldoende is gedaan.

Enkele voorbeelden:
Vragen die bij beschikbaarheid gesteld kunnen worden:
- Worden er back-ups gemaakt?
- Is het systeem redundant uitgevoerd?
- Is uitwijk geregeld?

Vragen ten aanzien van integriteit en vertrouwelijkheid kunnen zijn:
- Zijn er technische maatregelen genomen om de informatie af te schermen tegen ongeoorloofd gebruik?
- Hoe is de toegang tot de gegevens geregeld; vindt er (sterke) authenticatie plaats?
- Is identity management geregeld; worden bijv. accounts opgeruimd als iemand vertrokken is?
- Is er zoiets al role based access control of kan iemand, zodra hij/zij geauthentiseerd is, alle gegevens wijzigen of verwijderen?

Proces / Applicatie	Onderwijs			Onderzoek			Bedrijfsvoering		
	B	I	V	B	I	V	B	I	V
Elektronische Leeromgeving (bijv. Blackboard)									
Mail									
Agenda									
Studenten portfolio									
Enterprise Resource Planning									
Studenten Informatie Systeem									
Onderzoeksdata (bv. Metis)									
Customer Relationship Management									
WEB / Content Management System (internet en/of Intranet)									
Ruimtebeheer applicatie									
Toegangscontrole									
Cameratoezicht									
……									

B= Beschikbaarheid
I= Integriteit
V= Vertrouwelijkheid

Uit de ingevulde tabel zal blijken waar de grootste urgentie zit om maatregelen te treffen. Als bijv. blijkt dat de integriteit van het Student Informatie Systeem (SIS) niet goed geregeld is, loopt de instelling waarschijnlijk een groot risico. De persoonsgegevens die in het SIS zijn opgeslagen kunnen mogelijk op straat komen te liggen of gemanipuleerd worden. Behalve dat de Wet Bescherming Persoonsgegevens mogelijk wordt overtreden, is de kans groot dat in geval van een beveiligingsincident de instelling grote imagoschade oploopt.

3.4 Beleid en procedures

Naast deze kwetsbaarheid inventarisatie kun je inventariseren hoe het staat met het beleid en de procedures. Door onderstaande lijst in te vullen kan je vrij snel in beeld brengen wat er al bestaat op het gebied van beleid en procedures.

Onderwerp	Status (kleurindicatie *)	referentiedocument
Informatiebeveiligingsbeleid		
Beveiligingsorganisatie		
Overzicht bedrijfsmiddelen		
Classificatiesysteem		
Acceptable Use Policy (gebruiksreglement)		
Is er iets opgenomen in het studentenstatuut		
Is er iets opgenomen in de CAO		
Zijn er aansluitvoorwaarden voor het netwerk		
Is er een wachtwoordbeleid		
Is er een Identity managementbeleid waarin bijv. is vastgelegd hoe de provisioning van accounts is geregeld		
Is er een integriteitscode en/of gedragscode voor medewerkers		
Is er een incidentregistratie		
Zijn er richtlijnen voor systeembeheer en change management		
Wordt er iets aan logging en monitoring gedaan		
Is er aandacht voor bedrijfscontinuïteit		
Is er enig ander beleidsdocument, zoals een archiefbeleid, privacy-statement, beleid rondom toegang tot gebouwen, etc.		
Wordt er op één of andere wijze iets gedaan aan bewustwording		

*) Kleurindicatie

	Onvoldoende / niet aanwezig
	Gedeeltelijk
	Voldoende

Met de inventarisatie van beleid en procedures en de beknopte risicoanalyse van de informatiesystemen heb je een eerste beeld van de status van de informatiebeveiliging boven tafel gekregen.

3.5 Incidenten

En als je toch aan tafel zit bij een beheerder vraag dan ook of er een systeem is ingericht voor incidentregistratie, zoals een helpdesksysteem. Worden in dit systeem naast beschikbaarheidsincidenten ook andere beveiligingsincidenten geregistreerd of wordt daarover op een andere wijze een overzicht bijgehouden of gerapporteerd. Denk hierbij bijvoorbeeld ook aan de registratie van gestolen laptops, de afhandeling van incidentmeldingen van SURFnet e.d.
In de meeste gevallen zul je over beveiligingsincidenten horen: "We lossen het gewoon op", terwijl incidentregistratie een belangrijk instrument is om te bepalen in welke mate de genomen beveiligingsmaatregelen ertoe bijdragen dat het aantal incidenten juist afneemt. In een latere fase kom je hier op terug.

3.6 Bewustwording

Ga na of er al iets gedaan wordt aan bewustwording. Dit kan op een aantal manieren. Doel ervan is om gebruikers te informeren over de risico's bij het gebruik van IT-middelen en hen vooral ook te

wijzen op de verantwoordelijkheden die zij zelf op dit gebied hebben. Bij een hoger onderwijs instelling zijn hier drie doelgroepen te onderkennen: studenten, medewerkers en management. Deze vereisen elk een eigen aanpak, waarbij onderzoekers (en wellicht ook de ICT- en functioneel beheerders) daarin mogelijk weer onderscheiden dienen te worden van andere medewerkers.

Bij de inventarisatie van de status van bewustwording kun je kijken of er op de website van de instelling informatie over informatiebeveiliging is te vinden, of er via posters of mailings iets aan bewustwording wordt gedaan. Gesprekken met de afdeling communicatie, personeelszaken en studentenzaken kunnen hierbij helpen. Een vorm van bewustwording (bewustmaking) kan bijvoorbeeld ook het uitdelen van het ICT-reglement bij indiensttreding of bij aanvang van de studie zijn. Dit onderwerp ga je zeker ook in het Plan van Aanpak opnemen.

3.7 Tot slot van fase 1

In een situatie dat je je werk probeert uit te voeren zonder dat er expliciet sprake is van bestuurlijk commitment heb je een bepaalde attitude nodig om het maximale uit de situatie te halen, zonder je toekomstige positie te schaden. Je houding naar je gesprekspartners moet gekenmerkt worden door een dienstverlenende klantgerichte stijl: "Vertel me hoe jouw processen in elkaar zitten en tegen welke problemen je aanloopt, dan kan ik wellicht in een vervolgfase helpen die problemen op te lossen". Het heeft weinig zin om daarover al te veel verwachtingen te wekken, want als het bestuur niet bereid is om informatiebeveiliging serieus op te pakken, dan kun je die beloftes vermoedelijk later niet waarmaken.

4 Fase 2: kortetermijnverbeteringen en opstellen Plan van Aanpak

4.1 Laaghangend fruit

Je beschikt nu over twee inventarisaties waaruit kortetermijnmaatregelen kunnen worden afgeleid:
1. de inventarisatie van de kwetsbaarheid van de bedrijfsprocessen onderwijs, onderzoek en bedrijfsvoering, en
2. het overzicht over de aanwezigheid van beleid en procedures voor de diverse onderdelen van informatiebeveiliging.

De onderwerpen 'incidenten' en 'bewustwording' neem je later mee in het Plan van Aanpak.

Ad. 1) Kwetsbaarheid van primaire processen

De tabel van pagina 9 is hieronder als fictief voorbeeld ingevuld.

Proces / Applicatie	Onderwijs			Onderzoek			Bedrijfsvoering		
	B	I	V	B	I	V	B	I	V
Elektronische leeromgeving (bijv. Blackboard)	2	1	1						
Mail	2	1	1	2	1	1	2	1	1
Agenda	2	1	1	2	1	1	2	1	1
Student portfolio	1	1	1						
ERP							2	2	2
SIS	3	2	1				3	2	1
Metis (onderzoeksdata)				2	1	1			
CRM	1	2	1				1	2	1
WEB / CMS	1	2	1				1	2	1

1 wil zeggen dat er niets is gedaan op het gebied van informatiebeveiliging,
2 betekent dat er wel al iets is gedaan, maar naar mening van de invuller nog niet voldoende en
3 betekent dat er voldoende is gedaan.

De quick wins die je uit dit overzicht kunt afleiden zijn meestal de 1-tjes. Bij beschikbaarheid zijn dat in dit voorbeeld dus de Studenten portfolio, het CRM-systeem en de website met het bijbehorende content management systeem. Bespreek met de systeemeigenaren en –beheerders welke maatregelen de beschikbaarheid kunnen verbeteren en wat dat moet kosten. Zet die kosten af tegen het ongemak van het telkens uitvallen van zulke systemen. Wellicht dat je er relatief eenvoudig iets aan kunt doen. Minimale maatregelen zijn beveiligingspatches van leveranciers en anti-virusmaatregelen.

De 1-tjes voor integriteit en vertrouwelijkheid kunnen je meestal gecombineerd aanpakken. Na bespreking van verbeteringsmogelijkheden en kosten met de systeemeigenaren en –beheerders kies je voor de meest eenvoudige. De overige, vaak duurdere, verbeteringen neem je mee in het Plan van Aanpak, als aparte projecten.

Ad 2) Beleid en procedures

De tabel van pagina 14 is hier als fictief voorbeeld ingevuld.

Onderwerp	Status	Referentiedocument
Informatiebeveiligingsbeleid		
Beveiligingsorganisatie		
Overzicht bedrijfsmiddelen		
Classificatiesysteem		
Acceptable Use Policy (gebruiksreglement)		
Is er iets opgenomen in het studentenstatuut		
Is er iets opgenomen in de CAO		
Zijn er aansluitvoorwaarden voor het netwerk		Wordt in de praktijk echter niet gecontroleerd; iedereen kan een laptop aan het netwerk hangen...
Is er een wachtwoordbeleid		
Is er een Identity managementbeleid waarin bijv. is vastgelegd hoe de provisioning van accounts is geregeld		
Is er een integriteitscode voor medewerkers		Wordt niet gehandhaafd; er is ook geen meldpunt integriteitsschendingen
Is er een incidentregistratie		
Zijn er richtlijnen voor systeembeheer en change management		
Wordt er iets aan logging en monitoring gedaan		
Is er aandacht voor bedrijfscontinuïteit		
Is er enig ander beleidsdocument, zoals een archiefbeleid, privacy-statement, beleid rondom toegang tot gebouwen, etc.		Toegangsbeleid
Wordt er op één of andere wijze iets gedaan aan bewustwording		Er is een website met informatie over de beveiliging van de PC

Op basis van een dergelijk overzicht kan je beoordelen waaraan op de langere termijn gewerkt zal moeten worden (fase 3), maar ook waar de quick wins kunnen liggen. Deze laatste ga je in fase 2 aanpakken.

Het is wel verstandig dat je de geselecteerde quick wins vooraf bespreekt met de portefeuillehouder ICT in het bestuur. Die is waarschijnlijk wel gevoelig voor verbetering van de situatie en zal zijn goedkeuring hieraan wel willen verlenen. Op deze manier doorbreek je de patstelling dat het bestuur nog geen formeel commitment heeft afgegeven voor een structurele aanpak van informatiebeveiliging in de gehele instelling en dek je je netjes in.

Een voorbeeld van een quick win is de Acceptable Use Policy, waarvoor al een SURF-ibo-template bestaat. Deze policy kun je eenvoudigweg overnemen. Het is wel belangrijk dat deze door het bestuur wordt vastgesteld. Het kan dus noodzakelijk zijn dat je deze, vooruitlopend op verdere besluitvorming over informatiebeveiliging, apart moet voorleggen aan het bestuur. Het is verstandig om ook dit onderwerp voor te bespreken met de portefeuillehouder ICT. Zorg er vervolgens voor dat er namens de portefeuillehouder ICT door de afdeling communicatie over de bedoeling van de gedragscode duidelijk gecommuniceerd wordt en dat de studenten en medewerkers er elk jaar aan 'herinnerd' worden (bewustwording). In fase 3 ga je er voor zorgen dat er mensen zijn die daadwerkelijk optreden wanneer overtredingen geconstateerd worden (geloofwaardigheid/handhaving). Dit wordt overigens niet in één dag bereikt; het opzetten en uitvoeren van handhaving zal ook onderdeel uitmaken van je Plan van Aanpak en in het bijzonder van het inrichten van een informatiebeveiligingsorganisatie, waarin verantwoordelijkheden en bevoegdheden zijn belegd.

Als er nog geen wachtwoordbeleid is (of alleen op papier), dan kan je daar bijvoorbeeld ook werk van maken. Het is voor studenten en medewerkers veel prettiger wanneer er met behulp van één wachtwoord toegang verkregen kan worden tot meerdere diensten en applicaties (single-sign-on). De introductie van een sterk wachtwoordbeleid (minimaal 8 tekens, hoofdletters en cijfers) wordt dan ook gemakkelijker geaccepteerd omdat één wachtwoord nog wel te onthouden is. Een dergelijk wachtwoordbeleid kan je ook laten meenemen in het identity management systeem, waardoor ook met dat wachtwoord toegang verkregen kan worden tot diensten van derde partijen.

Welke de korte termijnacties ook zijn die uit een dergelijke aanpak naar voren komen, zorg er voor dat de meerwaarde aantoonbaar is. Dit vormt straks een belangrijk onderdeel van het verkrijgen van bestuurlijk commitment.

4.2 Opstellen Plan van Aanpak

Door middel van het Plan van Aanpak ga je een begin maken met het vormgeven van meer structurele aandacht voor informatiebeveiliging. Het Plan van Aanpak beslaat een periode van zo'n drie jaar. Gedurende die periode zul je de daarin opgenomen projecten uitvoeren en de voorgestelde maatregelen implementeren.

Het doel van je Plan van Aanpak is om daarmee in een paar jaar toe te werken naar een situatie waarin informatiebeveiliging een normaal onderdeel is van het bestuur en beheer van de instelling. Zoals aandacht voor de kwaliteit van het onderwijs dat ook is.

Omdat het ondoenlijk is om in een keer de ideale situatie, zoals beschreven in de Code voor Informatiebeveiliging, te bereiken, ga je ook in het Plan van Aanpak faseren. Maar, in tegenstelling tot de bouw van een huis dat begint met een fundering die betrouwbaar is, moet je in jouw geval aan verschillende onderdelen tegelijk werken. Je zitten teveel in een kip-ei-situatie gevangen en je kunt 'het fundament' niet afronden zonder ook andere aspecten te behandelen.

Waar gaat het over? Je hebt te maken met beleid, met mensen, met techniek en met procedures. Het heeft weinig zin dat je nu achtereenvolgens een voldragen beleidsdocument maakt, daarvoor formeel goedkeuring vraagt en krijgt, vervolgens de informatiebeveiligingsorganisatie inricht, dan de bedrijfsmiddelen inventariseert en een classificatiesysteem daarvoor opzet, vervolgens een risicoanalyse uitvoert, daarna maatregelen selecteert en implementeert, dan een bewustwordings-programma opzet, het personeel opleidt, en ga zo maar door. Beter is het dat je van alles een beetje doet en vervolgens toe werkt naar een stapsgewijze verbetering van de situatie; een soort cyclische spiraal omhoog.

4.2.1 De basis

Probeer voort te bouwen op de resultaten die je in de inventarisatiefase al verkregen hebt.

- **Technische infrastructuur**

Je hebt in fase 1 een inventarisatie gemaakt van wat we voor het gemak de 'spullenboel' hebben genoemd: welke systemen hebben we en welke diensten worden daarmee aangeboden aan wie. In deze fase ga je er voor zorgen dat elk systeem een eigenaar heeft en dat die eigenaar dat ook weet. De HRM-afdeling is verantwoordelijk voor het medewerkersbestand dat onderdeel uitmaakt van bijv. het ERP-systeem. De directeur van de HRM-afdeling is hiervoor verantwoordelijk. Wellicht is hij ook verantwoordelijk voor het studenteninformatiesysteem (SIS). Hoe dan ook, je maakt een lijst van systemen en hun eigenaren.

Vervolgens is het van belang dat je over het beheer van die systemen afspraken maakt: wie mag gegevens invoeren of wijzigen, wie zorgt voor onderhoud, wie mag updates installeren en onder welke condities (change management). Vaak is impliciet wel duidelijk wie waarvoor verantwoordelijk is, maar is dit slecht gedocumenteerd. Stel een beheerdocument op in overleg met alle betrokkenen (systeemeigenaren en ICT-beheerders), waarin het beheerproces is beschreven in termen van wie is verantwoordelijk voor en hoe wordt dit uitgevoerd. In een

volgende fase ga je dit (laten) vertalen naar de functieomschrijving van betrokkenen. Spreek ook af wie verantwoordelijk is voor het onderhoud van het beheerdocument, bijvoorbeeld als een beheerder van functie verandert moet dat worden verwerkt.

➢ **Eerst de grootste risico's**
Je hebt in fase 1 ook een eerste risico-inventarisatie gemaakt en daaruit wat laaghangend fruit geoogst. Nu er management commitment is kun je ook de overige risico's (de resterende 1-tjes) gaan aanpakken. Werk in overleg met de systeem eigenaren en IT-beheer uit welke maatregelen getroffen kunnen worden om bijvoorbeeld de integriteit en vertrouwelijkheid van informatie en informatiesystemen te verhogen en maak voor elk ervan een korte projectomschrijving.

➢ **De factor mens…**
Bij informatiebeveiliging is de factor mens belangrijk; er wordt wel eens gezegd 'de zwakste schakel', maar beter is er van uit te gaan dat het de grootste uitdaging is. Het is verstandig dat je een aantal gedragsregels introduceert waarmee het gewenste gedrag kan worden afgedwongen:
- Een ICT-gebruiksreglement (Acceptable Use Policy) voor zowel medewerkers als studenten
- Een informatiebeveiligingsparagraaf in het Studentenstatuut
- Informatiebeveiliging (omgang met de regels) als vast agendapunt bij functioneringsgesprekken
- Aansluitvoorwaarden voor het netwerk
- Een intranetsite over informatiebeveiliging, met informatie over meldpunten, met tips over computerbeveiliging, adviezen over sociale netwerksites, etc.

De introductie van dit soort maatregelen laat je uiteraard via het bestuur lopen. Je zorgt voor goede communicatie rondom de introductie van elk van deze zaken. Denk ook na over hoe je de handhaving ervan organiseert.

4.2.2 Verdieping van de basis

Nadat je de basis hebt gelegd ga je deze verder uitbouwen en verdiepen. Daarvoor is het prettig hulp te krijgen van iemand die dit al eens vaker verzorgd heeft. Je kunt dus het beste wat kennis en expertise inhuren om hier de juiste dingen op de juiste manier te verrichten.

➢ **Baseline informatiebeveiliging**
De eerder genoemde Code voor Informatiebeveiliging omschrijft voor alle relevante informatie-beveiligingsonderwerpen best practices, waaruit -al naar gelang de concrete situatie bij de individuele onderwijsinstelling- een aantal overgenomen kunnen worden. Het probleem zit in de tussenzin "al naar gelang de concrete situatie bij de individuele onderwijsinstelling". De analyse wat wel en wat niet noodzakelijk is aan informatiebeveiligingsmaatregelen blijkt in de praktijk lastig.

Geadviseerd wordt dat je een beknopte 'baseline informatiebeveiliging' toepast, die bestaat uit een set basismaatregelen, waarvan de meerwaarde inmiddels wel is aangetoond. Zo'n baseline zou het volgende kunnen omvatten.

Hoofdstuk Code voor Informatiebeveiliging	Baseline
5. Beveiligingsbeleid	Beschrijving en formele vaststelling IB-beleid op hoofdzaken
6. Organisatie van de informatiebeveiliging	Beschreven en ingerichte organisatie voor informatiebeveiliging, waarin rollen en verantwoordelijkheden benoemd zijn en de betreffende personen ook weten wat er van hen verwacht wordt
7. Beheer van bedrijfsmiddelen	Eigenaren, procedures voor beheer en onderhoud van bedrijfsmiddelen zijn beschreven. Onderdeel hiervan zijn regels voor aanvaardbaar gebruik, alsmede classificatie van informatie en systemen
8. Beveiliging van personeel	Denk aan: passende functiebeschrijvingen, duidelijke arbeidsvoorwaarden, tekenen geheimhoudingsverklaring voor bepaalde functies, identiteitscontrole, toegangsrechten tot geclassificeerde informatie, bewustwording m.b.t. informatiebeveiliging, hun verantwoordelijkheid en aansprakelijkheid, periodieke personeelsbeoordelingen, retournering van bedrijfsmiddelen bij vertrek
9. Fysieke beveiliging en beveiligingsomgeving	Maak een overzicht van de kritieke ruimten, zoals de serverruimte en zorg voor adequate beveiliging daarvan, alsmede voor regels en richtlijnen voor de toegang tot deze ruimtes. Introduceer een clear-desk policy. Zorg voor noodstroom (minimaal voor veilige afsluiting van systemen bij stroomuitval)
10. Beheer van communicatie en bedieningsprocessen	Er moeten richtlijnen zijn voor systeembeheer en voor het inschakelen van derden. Daarnaast kan functiescheiding nodig zijn, evenals een scheiding tussen ontwikkeling en productie. Beheeractiviteiten dienen gelogd te worden. Beveilig de kantoorautomatisering, viruscontrole, back-up en restore
11. Toegangsbeveiliging	Regel het beheer van gebruikstoegang, -bevoegdheden en speciale permissies. Beveilig netwerken, applicaties en systeemtools. Logging en monitoring moet functioneren
12. Verwerving, ontwikkeling & onderhoud van informatiesystemen	Change management, beveiliging testgegevens, onderhoud systeemprogrammatuur
13. Beheer van informatiebeveiligings-incidenten	Zorg voor een meldpunt incidenten en procedures voor de afhandeling ervan. Periodieke rapportages aan de ICT-portefeuillehouder zijn zinvol: probeer te leren van gemaakte fouten
14. Bedrijfscontinuïteitsbeheer	Neem informatiebeveiliging op in het proces van bedrijfscontinuïteitsbeheer
15. Naleving	Naleving van wettelijke voorschriften, zoals intellectuele eigendomsrechten (licenties op software!), bescherming persoonsgegevens (privacy), e.d. Het voorkomen van misbruik van IT-voorzieningen behoort hier ook toe

In het Plan van Aanpak kun je voor elk van deze onderdelen een project opnemen, waarbij je inzicht in de benodigde planning en kosten geeft. Bijlage 1 bevat een voorbeeld inhoudsopgave van een standaard Plan van Aanpak. Bijlage 2 geeft een sjabloon van een projectaanpak. Het is verstandig dat je goed let op de beheersbaarheid van de uitvoering van deze projecten. Het formuleren van beleid voor informatiebeveiliging doe je voor de gehele instelling, dus zowel voor Onderwijs, Onderzoek als Bedrijfsvoering. Maar het invoeren van maatregelen voor verbetering van de beveiliging kun je het beste faseren. Bijvoorbeeld eerst de systemen met een hoog risico (zeg maar de resterende 1-jes uit de risico-tabel) en vervolgens de concern informatiesystemen. Die fasering maakt ook de financiering van de maatregelen beter haalbaar. Jouw Plan van Aanpak is onderwerp van het gesprek met het management.

4.3 Tot slot van fase 2

In deze fase stel je je nog steeds dienstverlenend en klantgericht op. Je probeert maatjes te zijn met de belanghebbenden waar je mee om tafel zit. Geef aan dat jouw missie is hen te helpen hun werk beter en veiliger uit te voeren en dat het je bedoeling is het bestuur te overtuigen van het nut en de meerwaarde voor de gehele organisatie van informatiebeveiliging. Dat geldt evenzeer voor je contacten met de ICT-portefeuillehouder; hij is als het ware de entree naar het gehele bestuur toe. Laat hem merken wat je ambities zijn en dat je streeft naar bestuurlijk commitment.

5 Fase 3: de dialoog met bestuurders

Nu je een aantal korte termijnacties hebt geïmplementeerd en daarmee de meerwaarde van informatiebeveiliging aangetoond hebt én je Plan van Aanpak gereed is, is de tijd rijp om eens met je bestuurders te gaan praten over een meer structurele aanpak van informatiebeveiliging. Dat kun je het beste via de ICT-portefeuillehouder insteken. Veelal is dit degene die ook verantwoordelijk is voor bedrijfsvoering. Bij sommige instellingen is de voorzitter van het bestuur verantwoordelijk voor informatiebeveiliging. Hoe dan ook, zoek de meest voor de handliggende bestuurder als ingang naar het voltallige College uit.

5.1 De agenda

De agenda van je overleg met het College van Bestuur zou als volgt kunnen zijn:

- verstrek een overzicht van de genomen korte termijn maatregelen en hun meerwaarde voor de organisatie (zowel financieel als qua risico-inperking);
- benadruk dat informatiebeveiliging dus loont en de algemene missie en doelstelling van de organisatie ondersteunt. Doe dat in termen van de bijdrage van maatregelen op het gebied van informatiebeveiliging aan de governance (goed bestuur) en compliance (voldoen aan wet- en regelgeving en andere afspraken) van de organisatie;
- geef vervolgens aan welke risico's voor de primaire processen nog bestaan en wat de gevolgen kunnen zijn als er iets mis gaat;
- benadruk dat structurele aandacht voor informatiebeveiliging kan helpen de primaire processen in tact te houden, en
- licht het Plan van Aanpak toe en de daarvoor gemaakte planning en budgettering;
- vraag expliciet steun voor de uitvoering van het Plan, zowel moreel als qua middelen (menskracht en budget).

5.2 Wat wil je bereiken

De uitkomst van het overleg met het College van Bestuur moet bij voorkeur het volgende zijn:

- algemeen begrip van het belang van informatiebeveiliging voor de governance en compliance van de organisatie;
- in het verlengde daarvan specifiek inzicht dat het beheersen van informatiebeveiliging een bijdrage levert aan het bereiken van de missie en doelstellingen van de gehele organisatie
- inzicht in het feit dat informatiebeveiliging géén ICT-feestje is, maar de gehele organisatie aangaat;
- begrip dat het verstandig is wanneer op strategisch niveau gekeken wordt naar de risico's op het gebied van ARBO- en milieuveiligheid, fysieke beveiliging en informatiebeveiliging en ook hun onderlinge verbanden.
  Op strategisch niveau zal getracht moeten worden verstandig om te gaan met eventuele spanningen die verschillende wet- en regelgeving op deze (deel)gebieden met zich mee kunnen brengen. Voorbeeld: een sprinkler installatie in de computerruimte is uit oogpunt van brandpreventie verdedigbaar; uit oogpunt van de beveiliging van informatie(systemen) zeker niet!
- dat informatiebeveiliging wordt ingebed in de planning- en budgetcyclus van de instelling, net als andere issues, zoals nieuwbouw, investeringen in onderwijsmiddelen, onderzoeksfinanciering, et cetera;
- dat er ruimte gegeven wordt voor de professionalisering van informatiebeveiliging binnen de instelling en dat die ruimte vertaald wordt naar het inrichten van een informatiebeveiligingsorganisatie, met bijbehorende taken, verantwoordelijkheden, overlegstructuren en middelen (waaronder scholing).

Dit lijkt heel wat en dat is het ook; het lijkt wellicht het een utopisch eindplaatje, maar met minder kun je in eerste instantie ook tevreden zijn. Het minimaal haalbare is, dat het College van Bestuur gefascineerd is geraakt door de dingen die je hebt laten zien en daarbij verteld hebt. Als blijft

hangen dat informatiebeveiliging méér is dan ICT en een bijdrage kan leveren aan het bereiken van de overall doelstellingen van de instelling, dan is de basis gelegd (governance en compliance). In vervolgbesprekingen kan verder gebouwd worden op die basis: het proces van interactie met het bestuur kan beginnen.

5.3 Het proces

Je kunt van bestuurders niet verwachten dat ze direct na de eerste bespreking laaiend enthousiast zijn over het onderwerp informatiebeveiliging. Bereid je je er maar op voor dat een aantal bestuurders niet bij die vergadering aanwezig kan zijn, een deel de stukken niet gelezen heeft en anderen vol kritische vragen zitten. Je zult in Jip-en-Janneke-taal moeten uitleggen dat structureel aandacht besteden aan (onder andere) informatiebeveiliging bijdraagt aan de bestuurbaarheid en 'het in control zijn' van de organisatie. Dat moet je met voorbeelden aantonen (laaghangend fruit). Je kunt ter voorbereiding ook eens informeren hoe collega Security Officers bij bevriende onderwijsinstellingen hun bestuurders overtuigen; je hoeft het wiel niet opnieuw uit te vinden. En ook bestuurders vragen zich af "Hoe doen anderen dat?" Bespreek met elkaar welke best practices er op dit gebied zijn.

Als het allemaal een beetje stroef verloopt, vraag dan of je niet eens wat meer tijd mag besteden aan een presentatie over nut & noodzaak van informatiebeveiliging. En/of stel een aantal vragen in de trant van "hoe lang duurt het voordat de directeur financiën er achter komt dat de cijfers op de balans niet kloppen?", "welke claims kunnen we verwachten van opdrachtgevers voor wetenschappelijk onderzoek, als de onderzoeksresultaten uitgelekt zijn en bij de concurrent liggen?". Vraag bestuurders eens waar ze wakker van liggen en 'toon aan' (betoog overtuigend) dat informatiebeveiliging helpt hun nachtrust te garanderen.

Waar het om gaat is bestuurders regelmatig even te herinneren aan het nuttige werk dat je verricht. Spreek met ze af dat je periodieke rapportages zult verzorgen, die begrijpelijk en nuttig voor ze zijn in het licht van governance en compliance. Spreek af dat informatiebeveiliging meegenomen wordt in de jaarlijkse planning- en budgetcyclus en organiseer dat met de betreffende mensen in de organisatie.

Spreek ook af dat de uitvoering van het Plan van Aanpak in die rapportages meegenomen wordt: wat hebben we gedaan, met welk resultaat en wat gaan we het komende kwartaal aanpakken. Kleine stapjes, maar wel vastberaden. Zodra de informatiebeveiligingsorganisatie er is en de taken en verantwoordelijkheden benoemd zijn ben je in staat om die kleine stapjes daadwerkelijk te nemen. De basis is gelegd en je kunt aan de slag.

5.4 Tot slot van fase 3

In het proces van dialoog met het College van Bestuur stel je je niet alleen dienstverlenend op, je zult ook de nodige overtuigingskracht hanteren, door argumenten naar voren te brengen die iets betekenen voor bestuurders. Dus: géén ICT-jargon! Maar argumenten die hun aanspreken. Je kunt zoiets voorbereiden en oefenen, door bijvoorbeeld eerst eens apart te gaan zitten met de portefeuillehouder ICT in het bestuur.

Uiteindelijk mag je verwachten dat je missie tot het gewenste resultaat leidt. Je hebt dan het commitment en de middelen om bij eigenaren, beheerders en gebruikers ook meer dwingend samenwerking te verlangen en ook handhaving van gemaakte afspraken vorm te geven. Het bouwen kan beginnen.

6 Fase 4: projectmatige uitvoering Plan van Aanpak

6.1 De Basis

Je begint met de uitvoering van de projecten die je bij de paragrafen 4.2.1.1. t/m 4.2.1.3 hebt geselecteerd en in het Plan van Aanpak opgenomen.

6.2 Verdieping van de basis

Vervolgens ga je beginnen met de verdieping van de basis (paragraaf 4.2.2). Je werkt daarmee toe naar structurering volgens de Code voor Informatiebeveiliging. Hieronder worden de belangrijkste onderwerpen c.q. projecten kort benoemd.

6.2.1 Beleid

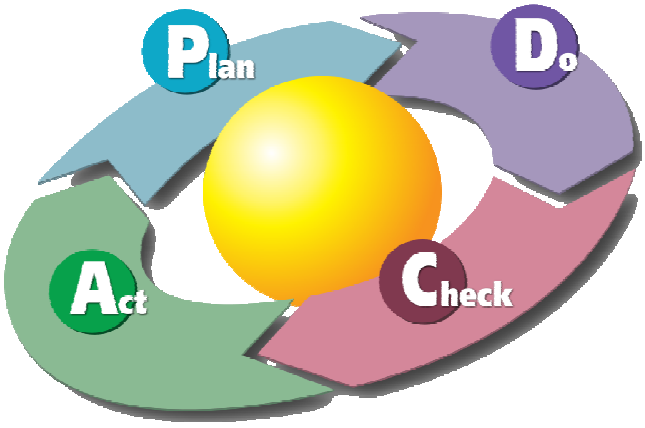
Gebruik de Leidraad Informatiebeveiliging van SURF-ibo en het CIO-beraad als beleidsdocument. Je hoeft alleen de naam van je instelling op de daarvoor bestemde plaatsen in te vullen en de namen van rollen of functionarissen en directies en afdelingen te customizen naar je eigen instelling en je bent klaar.

6.2.2 Inrichten informatiebeveiligingsorganisatie

Het is belangrijk dat je vastlegt waar de verantwoordelijkheden ten aanzien van informatiebeveiliging liggen. Iemand van het management is eindverantwoordelijk. Aan die persoon moet ook worden gerapporteerd. Een Security Officer of gelijkwaardige functionaris (jij wellicht) is verantwoordelijk voor de beleidsvoorbereiding en voor de uitvoering van het beleid. De Security Officer moet wel ondersteund worden door een bijvoorbeeld een programmaraad, adviesgroep of klankbordgroep. Door hier ook vertegenwoordigers van de gebruikersgroep in op te nemen wordt het draagvlak vergroot.

6.2.3 Inrichten van de PDCA-cyclus

Informatiebeveiliging is geen statisch geheel. Je hebt beleid gemaakt. Vervolgens wordt het beleid geïmplementeerd. Na implementatie wordt er gecontroleerd op naleving en wordt op basis van nieuwe inzichten of nieuwe risico's het beleid aangepast. Op die manier ontstaat een cyclus, ook wel de PDCA-cyclus van Deming genoemd waarbij PDCA staat voor Plan, Do, Check en Act. Schematisch ziet dit er als volgt uit:



Hoe je in de praktijk voor informatiebeveiliging zo'n cyclus inricht lijkt lastig, maar vermoedelijk bestaat iets dergelijks al voor de jaarlijkse budgetplanning. Nu je ook voor informatiebeveiliging kunt beschikken over een budget ligt het voor de hand daarbij aan te sluiten. Dat doe je ook met je voortgangsrapportages. Informatiebeveiliging wordt zo integraal onderdeel van de budgetcyclus en dat heeft als voordeel dat het onderwerp zichtbaar is en blijft.

6.2.4 Inrichten risicomethodiek

Een risicoanalyse levert informatie op, waarmee het management in staat wordt gesteld te beslissen welke risico's (of combinaties van risico's) een te grote potentiële schade vormen en met welke maatregelen deze risico's verkleind kunnen worden.

De eenvoudigste aanpak is uitgaan van basismaatregelen voor informatiebeveiliging die zijn vastgelegd in een checklist. Diverse organisaties (bijvoorbeeld NGI en NIVRA) hebben zulke checklists gepubliceerd; de Code voor Informatiebeveiliging is in wezen ook een checklist, maar wel een uitgebreide.

Checklists kunnen variëren in breedte en diepgang. Zo bestaan er korte vragenlijsten met 'de 10 geboden' voor informatiebeveiliging, maar ook uitgebreidere baselines. Er wordt in de sector Onderwijs en Onderzoek veelal gewerkt met een uitgebreide set van basismaatregelen (baseline) die overal en altijd geïmplementeerd moeten zijn. Daarbovenop kunnen, afhankelijk van de risico's in bijzondere situaties extra maatregelen worden ingevoerd. Het CIO-beraad heeft in overweging om ook een advies over risicoanalyses op te stellen.

Mocht het nodig zijn om een heuse risicoanalyse op te stellen, dan wordt er onderscheid gemaakt tussen een kwalitatieve risicoanalyse, waarbij de risico's geschat worden en een kwantitatieve risicoanalyse, waarbij de risico's in meetbare waarden worden uitgedrukt, zoals in geld. Hiervoor zijn verschillende methodieken in de markt verkrijgbaar (CRAMM, Information Security Forum, e.d.). Deze zijn vooral geschikt voor administratieve systemen, maar minder voor e-mailsystemen en voor onderzoek. Deze laatste horen in de baseline thuis.

6.2.5 Inrichten van het incidentmanagementproces

Een goed georganiseerd incidentbeheer, inclusief escalatieniveaus, helpt om erger te voorkomen. Een minimale invulling is het bijhouden van een incidentadministratie en te leren van wat er gebeurt. Richt dus een meldpunt in en communiceer dit met medewerkers en studenten.

De incidenten worden geregistreerd volgens de standaard indeling eSCIRT.net Incident Classification, waardoor een objectieve vergelijking met incidenten bij andere instellingen mogelijk wordt. De incidenten worden afgehandeld en dienen als input voor de incident-rapportages, waarover in het operationeel overleg wordt gesproken. Bij constatering van bepaalde trends kan hierop meteen worden ingespeeld, bijvoorbeeld door het nemen van extra maatregelen of een bewustwordingscampagne.

Voor de incidentafhandeling kan een incident responseteam worden ingericht. Vergeet hierbij niet goed vast te leggen wie in voorkomende gevallen de communicatie op zich neemt. Bij calamiteiten waarbij bijvoorbeeld het imago van de instelling in het geding kan komen, is het verstandig om iemand van de communicatieafdeling verantwoordelijk te maken voor de communicatie met de pers.

Verder is een goed contact met de juridische afdeling aan te bevelen. Indien aanwezig is het ook verstandig een goed contact op te bouwen met de vertrouwenspersoon en met privacyfunctionaris van de instelling.

Zorg daarnaast dat er periodiek in de rapportages gemeld wat voor soort incidenten zijn voorgekomen en hoe daarmee is omgesprongen.

6.2.6 Inrichten van de communicatie- en rapportagestructuur

Het is belangrijk dat over nut en noodzaak van informatiebeveiligingsmaatregelen wordt gecommuniceerd. Kies de vorm die het beste bij de instelling past. Een beveiligingswebsite, een wiki en bijvoorbeeld posters tezamen kunnen helpen om de bewustwording op peil houden.

De keuze van een rapportagestructuur zal moeten aansluiten bij de inrichting van de governance bij de instelling. Door de planningscycli van informatiebeveiliging, fysieke beveiliging, ARBO-veiligheid en bedrijfscontinuïteit parallel te laten lopen, kan op strategisch niveau aandacht geschonken worden aan de samenhang van (de risico's van) deze onderwerpen. Dit kan leiden tot richtlijnen hoe daarmee op tactisch en operationeel niveau moet worden omgegaan.

6.2.7 Uitvoeren van de overige deelprojecten informatiebeveiliging

Alle in het Plan van Aanpak voorgestelde projecten moeten worden uitgevoerd. Doorgaans worden projectteams samengesteld uit de informatiebeveiligingsorganisatie en aangevuld met belangrijke proceseigenaren en gebruikers. Het voert te ver om hier een uitgebreid verhaal te houden over projectmanagement. Indien noodzakelijk kan externe expertise worden ingehuurd.

Het Plan van Aanpak beslaat een periode van drie jaar. Dat biedt de mogelijkheid om elk project goed uit te voeren: de korte termijn verbeteracties eerst en het inrichten van de structurele aanpak via bovengenoemde projecten daarna. Waar het om gaat is dat er voortgang gerapporteerd kan worden aan het College van bestuur. Het is niet erg wanneer er eens vertraging optreedt. Analyseer de oorzaken en neem passende maatregelen. Zolang er een stijgende lijn in de gerealiseerde situatie zit mag je tevreden zijn.

6.3 Tot slot van fase 4

In fase 4 heb je nog steeds een dienstverlenende en klantgerichte houding. Maar daar komen nu een aantal aspecten bij. Je hebt mandaat om informatiebeveiliging organisatiebreed te professionaliseren. Je ben nu ook deskundig en hebt (gelegitimeerde) meerwaarde in overlegsituaties. Natuurlijke bondgenoten bij je missie zijn in elk geval de interne auditors, die straks veel eenvoudiger kunnen aantonen of de regels worden nageleefd en of er nagedacht is over de diverse risico's die de instelling per definitie loopt. IT-beheerders kunnen het moeilijk krijgen wanneer je ze een bepaalde veiliger werkwijze wilt laten volgen, maar de meerwaarde daarvan is met behulp van de ICT-portefeuillehouder toch snel inzichtelijk te maken. Zelfs het lijnmanagement zal uiteindelijk blij zijn met de veranderingen die je introduceert.

7 Fase 5: beheerfase

7.1 Inleiding

Nadat je de projecten uit je Plan van Aanpak hebt uitgevoerd is daarmee informatiebeveiliging als proces ingericht en gaat de beheerfase volgens de PDCA-cyclus van start. Je hebt veel en nuttig werk verricht: het beleid is vastgesteld, taken en verantwoordelijkheden zijn belegd, de processen zijn ingericht en procedures zijn opgesteld.

7.2 Governance

Onderdeel van governance is dat aan alle soorten risico's en hun onderlinge verwevenheid aandacht geschonken wordt. Je doet er dus verstandig aan om met de verantwoordelijken voor ARBO-veiligheid, fysieke beveiliging en bedrijfscontinuïteit kennis te maken en samen te werken. Ook zij doen mee in de jaarlijkse budgetcyclus en het is de kunst om onderlinge interferentie tussen deze risico's tijdig te signaleren en eventuele tegengestelde belangen op te lossen.

7.3 Privacy

Over relevante wet- en regelgeving zijn voldoende aanknopingspunten te vinden in de eerder genoemde Leidraad Informatiebeveiliging, in het bijzonder in het model informatiebeveiligingsbeleid. Wat privacy betreft is het verstandig de privacy officer, of welke benaming er ook gebruikt wordt, te betrekken in de afweging of de baseline toereikend is, of dat aanvullende beveiligingsmaatregelen genomen moeten worden. Dat laatste is vaak aan de orde als het om bescherming van persoonsgegevens gaat.

7.4 Budgetcyclus

Voor zover je daar al niet mee begonnen was tijdens de uitvoering van het Plan van Aanpak hanteer je vanaf nu een jaarcyclus, waarin nieuwe projecten in het jaarplan worden opgenomen en aangesloten wordt bij de reguliere rapportagemomenten.

Werk naar een situatie toe waarin algemene zaken, zoals het opstellen van een informatie-beveiligingsplan voor de gehele instelling of een externe audit, gefinancierd worden uit het centrale ICT-budget. De beveiliging van informatiesystemen komt ten laste van het informatiesysteem zelf. Beveiligingskosten van werkplekken maken integraal onderdeel uit van de werkplekkosten.

7.5 Meten van de status van informatiebeveiliging

In de beheerfase kun je (laten) controleren of er volgens het vastgestelde beleid wordt gewerkt, of incidenten op het gebied van informatiebeveiliging correct worden afgehandeld en of op regelmatige basis gerapporteerd wordt aan de opdrachtgever(s), zijnde CvB of CIO. Op basis van opgedane ervaringen kun je zo nodig aanvullende maatregelen definiëren, die vervolgens in de PDCA-cyclus weer worden geaccordeerd en uitgevoerd.

Maar, omdat de technologie voortschrijdt, de organisatie zich ontwikkelt en zelfs bedreigingen komen en gaan is het belangrijk op enig moment te inventariseren hoe de status van informatiebeveiliging zich verhoudt tot die nieuwe technologie, nieuwe bedreigingen, enz.
Je kunt daarvoor de interne auditors vragen de organisatie op deze aspecten door te lichten, maar dat kan ook via een derde partij. Het gaat er daarbij om de risico's van nieuwe ontwikkelingen, zoals virtualisatie en cloud computing, af te zetten tegen de beveiligingssituatie in de instelling, zowel qua aanwezige techniek, als qua kennis, houding en gedrag van medewerkers en studenten. Het is belangrijk dat hieraan periodiek aandacht wordt besteed.

7.6 Bewustwording en training

Beleid en maatregelen zijn niet voldoende om risico's op het terrein van informatiebeveiliging uit te sluiten. In de praktijk blijkt de mens meestal de belangrijkste speler. Daarom moet het bewustzijn voortdurend worden aangescherpt, zodat kennis van risico's wordt verhoogd en het (veilig en verantwoord) gedrag wordt aangemoedigd. Onderdeel van het beleid zijn de regelmatig terugkerende bewustwordingscampagnes voor medewerkers, studenten en gasten. Zulke campagnes kunnen aansluiten bij landelijke campagnes in het hoger onderwijs, zo mogelijk in afstemming met beveiligingscampagnes voor ARBO, milieu en fysiek. Verhoging van het beveiligingsbewustzijn is zowel een verantwoordelijkheid van de (decentrale) Security Managers als de (centrale) Security Officer; uiteindelijk is ook hiervoor het College van Bestuur eindverantwoordelijk.

7.7 Controle naleving en sancties

De Information Security Officer initieert in samenwerking met de interne auditor de controle op de uitvoering van de informatiebeveiligingsjaarplannen.

De externe controle wordt uitgevoerd door onafhankelijke accountants. Dit is gekoppeld aan het jaarlijkse accountantsonderzoek en wordt zoveel mogelijk gecoördineerd met de normale Planning & Control cyclus. Steeds vaker is er ook sprake van branche audits, zoals bijvoorbeeld de SURFAudit.

De bevindingen van de interne en externe audits zijn input voor de nieuwe jaarplannen.

De naleving bestaat uit algemeen toezicht op de dagelijkse praktijk van het security management proces. Van belang hierbij is dat lijnmanagers hun verantwoordelijkheid nemen en hun medewerkers aanspreken in geval van tekortkomingen. Voor de bevordering van de naleving van de Wet Bescherming Persoonsgegevens vervult de functionaris gegevensbescherming een belangrijke rol.

Mocht de naleving ernstig tekort schieten, dan kan de instelling de betrokken verantwoordelijke medewerkers een sanctie op te leggen, binnen de kaders van de CAO en de wettelijke mogelijkheden.

7.8 Tot slot van fase 5

Als je alle stappen uit deze starterkit hebt uitgevoerd en je fase 5 een keer hebt doorlopen, kun je concluderen dat alle facetten van informatiebeveiliging zijn belegd en het cyclische proces om de informatiebeveiliging actueel te houden is ingericht.

Bijlage 1: Plan van Aanpak

Standaard plan van aanpak

Voorwoord

Het standaard plan van aanpak, dat in dit artikel is weergegeven, heeft met name betrekking op de ontwikkeling van informatiesystemen.
Daarnaast is het dermate generiek, dat het ook voor andersoortige trajecten gebruikt kan worden. De specifieke detailpunten kunnen dan enigszins afwijken.

Management samenvatting

Op een beknopt aantal pagina's worden de 'high-lights' uit het Plan van Aanpak weergegeven, aangevuld met de geldigheidscondities van het Plan van aanpak.
Tot slot wordt een overzicht van alle beslispunten voor de opdrachtgever gegeven.

Introductie

De introductie is gericht op het Plan van Aanpak en het tot stand komen ervan. Ingegaan wordt op de volgende aspecten:

1. **Aanleiding**
   Hierbij wordt ingegaan op de oorzaak die geleid heeft tot het formuleren van de projectopdracht, het effectueren ervan en de omstandigheden waaronder dit Plan van Aanpak tot stand is gekomen. Indien van belang zal worden verwezen naar gevoerde gesprekken en referenties.

2. **Accordering en bijstelling**
   Hier wordt opgenomen op welke wijze het Plan van Aanpak wordt goedgekeurd en bijgesteld. De voortgang en bijstellingen op het plan worden vastgesteld middels de voortgangsrapportage. Nadat voorgestelde wijzigingen zijn goedgekeurd is impliciet het Plan van Aanpak bijgesteld. Het actuele Plan van Aanpak wordt op deze wijze gevormd door het oorspronkelijke Plan van Aanpak en de voortgangsrapportages.

3. **Toelichting op de opbouw van het plan**
   Hierin wordt de structuur van het plan toegelicht.

Projectopdracht

In dit hoofdstuk wordt de gewenste verandering in beeld gebracht. De opdracht wordt afgebakend, door middel van het beantwoorden van de 'waarom', de 'waarover' en de 'wat'-vragen. Deze zaken worden in 'opdrachtgevers bewoordingen' aan de orde gebracht. De paragrafen worden als volgt ingevuld:

1. **Projectomgeving**
   Wat is het beschouwingsgebied?
   Hierin wordt een schets gegeven van het beschouwingsgebied in termen van organisatie eenheden en bedrijfsprocessen. Tevens wordt aangegeven wat de problemen en oorzaken zijn die aanleiding geven tot de ontwikkeling van het resultaat.

2. **Doelstelling project**
   Waarom heeft de opdrachtgever het resultaat nodig en wat wil de opdrachtgever met het resultaat bereiken?
   In deze paragraaf wordt een beschrijving gegeven van de doelstellingen van het te ontwikkelen resultaat, zoals aangegeven door de opdrachtgever. Met name wordt hierbij de koppeling gelegd naar bedrijfsprocessen. Hierbij is het van belang om te weten, waarop de opdrachtgever wordt afgerekend. Iedere doelstelling wordt zo mogelijk onderbouwd door kwalitatieve en kwantitatieve gegevens.

3. **Opdrachtformulering**
   Wat is de projectopdracht?
   Waarover gaat het project procesmatig (afbakening)?
   Deze paragraaf beschrijft de opdracht, voortvloeiend uit de doelstelling, zoals aangegeven door de opdrachtgever. Hierbij wordt expliciet aangegeven welke zaken wel en welke zaken niet tot de verantwoordelijkheid van het project worden gerekend. Aangegeven wordt ook of het een resultaat- of een inspanningsverplichting betreft.

4. **Op te leveren producten en diensten**
   Wat is het resultaat van het project?
   Waarover gaat het project inhoudelijk (afbakening)?
   Deze paragraaf bevat de specificatie van de op te resultaten zoals aangegeven door de opdrachtgever. Dit is een nadere uitwerking van de projectopdracht, zoals aangegeven bij de opdrachtformulering.

5. **Eisen en beperkingen**
   In deze paragraaf worden de acceptatiecriteria en beperkingen vermeld, die de opdrachtgever stelt aan het resultaat en de eisen en beperkingen die gesteld worden aan de gebruikte resources en aan de wijze, waarop het resultaat tot stand komt. De eisen moeten zo nauwkeurig mogelijk worden gekwantificeerd. Indien mogelijk worden er ook prioriteiten vastgesteld.

6. **Cruciale succesfactoren**
   Deze paragraaf beschrijft de door de opdrachtgever onderkende en specifiek voor deze opdracht geldende cruciale succesfactoren. Het moet zowel de opdrachtgever als de projectmanager duidelijk zijn welke maatregelen mogelijk zijn c.q. door beiden genomen moeten worden om deze factoren te beïnvloeden.

Van groot belang is de juiste interpretatie van een aantal onderdelen van de Projectopdracht :

- *De Doelstelling geeft aan wat het achterliggende **doel** is van het starten van het project. Dit kan het doorvoeren van een organisatorische verandering zijn op uiteenlopende niveaus, zoals klant-, bedrijfs-, efficiëntie-, of middelenniveau.*
- *De Opdrachtformulering geeft weer door welk **middel** de opdrachtgever de gewenste doelstelling denkt te bereiken.*
- *De Eisen en beperkingen geven aan welke **eisen** de opdrachtgever stelt aan het eindresultaat en het procesmatige verloop van de opdracht.*
- *De Cruciale Succesfactoren geven aan, welke door de opdrachtnemer **beïnvloedbare zaken** er vanuit de opdrachtgever gezien essentieel zijn om het resultaat zo goed mogelijk te laten aansluiten bij de te bereiken doelstelling.*

Aanpak

In het hoofdstuk Aanpak wordt de brug geslagen tussen het afgebakende resultaat en de inrichting van het project, door middel van beantwoording van de 'hoe'-vraag. Doel is om door middel van Aanpak overeenstemming te verkrijgen over de te volgen weg, om te komen tot het gewenste resultaat.

Per eindresultaat wordt aangegeven welke activiteiten zullen worden uitgevoerd en eventueel welke tussenresultaten worden opgeleverd. Tevens wordt hierbij ingegaan op het waarom van de gekozen oplossing. Daarbij wordt verwezen naar de cruciale succesfactoren, de resultaten van de uitgevoerde risico analyse, en de geformuleerde eisen en beperkingen ten aanzien van proces, resultaat en kwaliteit. Als de projectmanager daarin op basis van de uitgangspositie, cruciale succesfactoren, risico analyse of kwaliteitseisen onduidelijkheid of onvolledigheid vaststelt, geeft hij aan hoe hij met deze zaken omgaat.

De projectmanager zal het project structureren en faseren om aan te geven in welke globale stappen hij de projectopdracht denkt uit te voeren.

Bij het structureren groepeert hij de gewenste eindresultaten primair naar algemene aandachtsgebieden. De volgende algemene aandachtsgebieden worden onderkend:
- ontwikkeling resultaat;
- voorbereiding gebruik, dit zijn de activiteiten die samenhangen met het (her)inrichten van de gebruikersorganisatie;
- voorbereiding beheer, dit zijn de activiteiten die samenhangen met het (her)inrichten van de beheerorganisatie;
- acceptatie gebruik, het voorbereiden en uitvoeren van de gebruikers-acceptati;e
- acceptatie beheer, het voorbereiden en uitvoeren van de beheeracceptatie;
- kennis, dit zijn de activiteiten die samenhangen met het opbouwen van materiekennis met betrekking tot het resultaat (ook van het gebruik en het beheer ervan) en de activiteiten die samenhangen met de overdracht van deze kennis naar de staande organisatie.

Afhankelijk voor het type project worden de voor het project te hanteren aandachtsgebieden afgeleid uit de algemene aandachtsgebieden. Ook spelen andere criteria bij het structureren een rol, bijvoorbeeld:
- risicofactoren
- cruciale succesfactoren
- kwaliteitseisen

Naast het structureren zal het project tevens in de tijd worden gefaseerd om formele meet- en beslismomenten te verkrijgen. De fasering wordt gericht op de beslissingen die de opdrachtgever wil nemen en vindt onder meer plaats op basis van invoeringstijdstip of product.

Per aandachtsgebied en verdere onderverdeling, wordt aangegeven door welke activiteiten het eindresultaat wordt bereikt, wat de samenhang van de activiteiten is en welke tussenresultaten worden opgeleverd binnen c.q. buiten de projectopdracht. Indien nodig kan de samenhang gevisualiseerd worden in de vorm van een eenvoudig netwerkplan zonder kwantitatieve gegevens. Conform de structuur en fasering wordt dit hoofdstuk in paragrafen opgedeeld.

Projectinrichting en voorwaarden

Projectinrichting

Het doel van projectinrichting is het zichtbaar maken van de wijze waarop de projectmanager van plan is het project in te richten om de opdracht uit te voeren volgens de voorgestelde aanpak. Hierbij zal de gekozen inrichting afhankelijk zijn van de resultaten van de risico analyse, kwaliteitseisen en de cruciale succesfactoren.

Afhankelijk van de opdracht en de organisatie komen de OPAFIT aspecten aan de orde:
- **Organisatie**
  waarbij aangegeven wordt hoe de projectorganisatie eruit komt te zien inclusief taken en verantwoordelijkheden. Deze worden per persoon en per rol gesteld
- **Personeel**
  waarbij de eisen aan de gewenste inzet en beschikbaarheid van personeel worden

aangegeven zoals condities voor het betrekken van personeel, per groep de vereiste vakkennis, skills gerelateerd aan de plannen

- **Administratieve procedures**
  waarin alle binnen en rond het project van toepassing zijnde procedures worden genoemd
- **Financing**
  alle financiële zaken worden hier behandeld, bij voorkeur met verwijzingen of, bij afwezigheid, expliciet opgenomen zoals tariefwijzigingen, facturering, subcontractors, btw en dergelijke;
- **Informatie**
  waarbij ingegaan wordt op alle informatie rond het project, overleg- en rapportagestructuren;
- **Techniek**
  waarbij wordt ingegaan op de voorgestelde inrichting qua hard- en software, werkplekken, hulpmiddelen en dergelijke.

Voorwaarden aan opdrachtnemer

Opsomming van voorwaarden, die gerealiseerd dienen te worden door de opdrachtnemer om het project volgens plan te kunnen uitvoeren. Deze voorwaarden zijn gerelateerd aan en aanvullend op de inrichtingsaspecten.

Voorwaarden aan opdrachtgever

Idem als voorwaarden aan opdrachtnemer, echter met opdrachtgever i.p.v. opdrachtnemer.

Voorwaarden aan derden

Idem als voorwaarden aan opdrachtnemer, echter met derden i.p.v. opdrachtnemer.

Plannen

In het hoofdstuk plannen wordt de resultante vastgelegd van het evenwicht tussen activiteiten, tijd, geld en middelen teneinde de opdracht te kunnen uitvoeren. De verschillende paragrafen worden als volgt ingevuld:

Normen en aannames
Hierbij worden de gehanteerde normen, aannames en veronderstellingen zowel ten aanzien van de schattingen als ten aanzien van planning vermeld, zoveel mogelijk per eenheid verbijzonderd. Deze kunnen afkomstig zijn uit geraadpleegde literatuur aangevuld met 'ervaringscijfers'.

1. **Activiteitenplan**
   In deze paragraaf worden de uit te voeren activiteiten beschreven. De detaillering hiervan is sterk afhankelijk van de opdrachtformulering en de fase waarin het project zich bevindt. Per activiteit wordt weergegeven de benodigde inspanning, de tijdsduur, de samenhang met andere activiteiten en het benodigde resourceniveau.

2. **Mijlpalen-/Productenplan**
   Het mijlpalenplan geeft de meet- of beslismomenten weer. Hierbij worden de meest belangrijke momenten voor toetsing en sturing benadrukt.
   Het productenplan geeft de momenten weer waarop de (tussen)producten zullen worden opgeleverd en geaccepteerd.

3. **Resourceplan**
   Het resourceplan verschaft duidelijkheid over personele en overige middelen. Het plan geeft weer over welke perioden inzet benodigd is. Bij de personele middelen wordt tevens het niveau van de resource aangegeven.

4. **Financieel plan**
   In deze paragraaf wordt inzicht gegeven in de kosten (mensen, middelen en overig) van het project. Aangegeven worden de resources die in de planning zijn opgenomen, de hiervoor gehanteerde tarieven en de hieruit resulterende verwachte kosten.

Kwaliteitsborging

Dit hoofdstuk geeft inzicht in de relatie tussen de voorgestelde maatregelen en de door de opdrachtgever gestelde eisen ten aanzien van de kwaliteit. Hiernaast worden maatregelen getroffen om onderkende risico's uit te sluiten of de gevolgen te minimaliseren, en de cruciale succesfactoren te beïnvloeden.

Als uitgangspunt worden de door de opdrachtgever gestelde kwaliteitseisen gehanteerd. Deze worden verbijzonderd naar de te stellen kwaliteitseisen per product. De voorgestelde maatregelen in het proces zijn een vertaling van deze vastgestelde productkwaliteitseisen.

Naast maatregelen in het proces om te voldoen aan de kwaliteitseisen per product worden additioneel maatregelen getroffen voor de kwaliteit van de tussenproducten of het proces zelf. Laatstgenoemde wordt ontleend aan ondermeer de vereiste kwaliteit van besturing of het minimaliseren van risico's.

Alle maatregelen zijn in het proces ingebouwd en zijn dus elders in het plan van aanpak opgenomen als activiteit, inrichtingsaspect of voorwaarde. Dit hoofdstuk geeft het totaaloverzicht van de invulling van het kwaliteitsaspect.

De paragrafen worden als volgt ingevuld:

1. **Productkwaliteit**
   Eisen per product per kwaliteitsattribuut voorzien van weging en acceptatiecriteria. Relatie met de gestelde eisen aan, en acceptatiecriteria van, het projectresultaat

2. **Proceskwaliteit**
   Eisen te stellen aan het proces.
   Voorbeelden hiervan zijn:
   - vakbekwaamheid
   - gebruik van (systeem)ontwikkelmethode
   - procedures
   - gebruik van methode voor projectmanagement;
   - uitbesteding en inkoop

   Controle achteraf is mogelijk door verificatie en validatie.

3. **Voorgestelde maatregelen**
   Maatregelen in het proces met per maatregel de relatie naar de eisen.
   Voorbeelden hiervan zijn:
   - opleidingsplan
   - gebruik van methode voor systeemontwikkeling
   - testplan
   - gebruik van Managing Projects als methode voor projectmanagement.

4. **Maatregelen ter verificatie en validatie**
   Voorbeelden hiervan zijn:
   - audits
   - reviews.

Bovenstaande, mogelijk lange en droge opsomming van, relaties kunnen visueel meer inzichtelijk worden gemaakt door deze op te nemen in een matrix.

Overige plannen

In dit hoofdstuk worden alle plannen opgenomen die niet op tijd, geld en middelen zijn gericht. De invulling is afhankelijk van de projectbehoefte.

Voorbeelden:
- communicatieplan
- documentatieplan
- configuratiebeheerplan
- beveiligingsplan.

Bijlagen

In dit hoofdstuk wordt verwezen naar de relevante standaards en projectprocedures. In het voorkomend geval zal verwezen worden naar reeds bestaande c.q. gebruikelijke bedrijfsstandaards. Voorwaarde is wel dat deze gedocumenteerd zijn.

In de bijlagen worden ook Begrippen en definities opgenomen om begripsverwarring te voorkomen. De begrippenlijst hoeft niet uitputtend te zijn, alleen de gehanteerde begrippen in het Plan van Aanpak komen hiervoor in aanmerking.

Bijlage 2: Inhoudsopgave projectplan

Inhoud projectplan[1]

Onderdeel projectplan	Opmerkingen
Inhoudsopgave en managementsamenvatting	Zinvol als het gaat om de grote lijnen van begroting, doorlooptijd en inzet van mensen afgezet tegen de beoogde doelstelling. Index en managementsamenvatting zijn alleen nodig als het projectplan omvangrijk is. Van belang is om na te gaan of er een doelgroep voor is, die geen tijd heeft om het plan in detail te beoordelen, maar er toch kennis van moet nemen.
Uitgangssituatie en context	In dit onderdeel wordt niet alleen de achtergrondsituatie van het project geschetst - de aanleiding en de problematiek - maar wordt ook geprobeerd een beeld te krijgen van alle bij de verandering betrokken partijen. In een onderwijsinstelling zijn dat vaak studenten en medewerkers; maar ook alumni, plaatselijk bedrijfsleven, overheidsorganen, toeleverende en afnemende instellingen zijn voorbeelden van partijen die de context van een project in een onderwijsinstelling kunnen vormen. Daarnaast kunnen de kenmerken van project en organisatie en raakvlakken met andere projecten worden opgenomen.
Projectdoelstelling, randvoorwaarden, verwacht resultaat en opbrengsten	De doelstelling van het project moet voor alle betrokkenen helder zijn. Wordt het goede probleem opgelost? Waarom wordt gekozen voor deze prioriteit? Door het omschrijven van de resultaten en opbrengsten van het project kan duidelijk worden waarom het project belangrijk is voor de organisatie. Welke bijdrage levert dit project aan de organisatie? Zijn de doelen *SMART* omschreven (*specifiek, meetbaar, acceptabel, realistisch, tijdgebonden*)? Ook de randvoorwaarden van het project moeten in beeld worden gebracht. Is er voldoende tijd en geld beschikbaar? Zijn de juiste mensen beschikbaar en is er voldoende draagvlak binnen de organisatie? Wat is het werkterrein van het project en ook: wat valt er buiten het project en de verantwoordelijkheid van de projectgroep?
Aanpak en fasering	Vooral wanneer de doorlooptijd wat langer is (bijvoorbeeld een studiejaar om een nieuwe activiteit in het volgend cursusjaar te kunnen starten) is het zinvol een fasering aan te brengen. Bij de overgang van de ene naar de andere fase hoort dan idealiter ook een keuzemoment om te evalueren, bij te stellen en zo nodig zelfs te stoppen. Een gebruikelijke fasering is die van 'oriëntatie', 'voorbereiding', 'ontwerp en inrichting van de nieuwe situatie', 'uitvoering', 'integratie' en 'evaluatie'. Maar afhankelijk van het project kunnen andere faseringen opportuun zijn. Per fase kunnen andere personen betrokken zijn bij het project, kan de communicatie verschillen; kortom kan de aanpak worden aangepast aan de situatie.
Betrokkenen / projectorganisatie	Welke mensen gaan het project uitvoeren? Is er een geschikte projectleider? Vaak raken mensen betrokken bij een project vanuit hun functie, enthousiasme of vanwege een overschot aan nog te besteden 'niet-lesgebonden' taakuren. Wat de achtergrond ook is: de taken moeten goed verdeeld worden, met de zekerheid dat ze worden uitgevoerd zo goed mogelijk aansluitend bij capaciteiten en ontwikkelingsmogelijkheden van mensen. Het is zinvol van tevoren vast te leggen wie wat doet en wat de verantwoordelijkheden en bevoegdheden van het projectteam zijn.

[1] Gebaseerd op: http://www.schoolvoorbeeld.com/bedrijfskundigeinvalshoek/projectmanagement/projectplan/index.html#01c1c5939f0728001

Onderdeel projectplan	Opmerkingen
Begroting	De beschikbare (geringe) hoeveelheid geld is soms een hindernis bij de uitvoering van een project. Daar staat tegenover dat voor veel projecten subsidie of sponsering een optie kan zijn, en dat lang niet alle projecten en veranderingen kostbaar zijn. Het opstellen van een begroting vraagt ervaring met het inschatten van de kosten. Meestal gaat het om twee belangrijke hoofdkosten: materiële kosten en uren die besteed worden aan het project. Als het project is gestart moet door een nauwkeurige administratie het budget goed worden bewaakt.
Planning	De planning is er om twee aspecten van de tijd te bewaken. De tijd die betrokkenen besteden aan het project en de totale doorlooptijd van het project. Hoewel dat niet altijd zo concreet wordt benoemd is de tijd die wordt besteed ook een geldkwestie: interne uren kunnen in principe maar één keer uitgegeven worden. Daar is ook meteen de samenhang met de doorlooptijd. Een lange doorlooptijd is eigenlijk per definitie een risicofactor voor het slagen van een project.
Risicoanalyse	Een risicoanalyse wordt uitgevoerd om de slagingskans van het project in kaart te brengen en maatregelen te formuleren om een oplossingsrichting aan te geven voor mogelijke problemen. Deze werkwijze wordt gevolgd om een goede afweging te kunnen maken en de besluitvorming te ondersteunen (o.a. op het gebied van taken en formatie). Een risicoanalyse kan worden opgesteld aan de hand van een checklist. Bij voorkeur al voor aanvang van het project, gevolgd door een meer gedetailleerde risicoanalyse in het begin, als het projectteam is samengesteld. Geformuleerde risico's vormen aandachtspunten, geen argumenten om het traject niet te willen volgen of de besluitvorming negatief te beïnvloeden.
Kwaliteitszorg	Kwaliteitszorg binnen een project kan op verschillende manieren plaatsvinden. Als binnen een schoolorganisatie al een een systeem van kwaliteitszorg in gebruik is, kunnen procedures en afspraken worden gebruikt binnen het project. Soms kan het nodig zijn speciaal voor een project afspraken te maken in het kader van kwaliteitszorg. Het is dan goed deze te vermelden in het projectplan of aan te geven welke maatregelen er zijn genomen om de kwaliteit van het project te bewaken.
Communicatie	Communicatie is van essentieel belang; vaak is een goede communicatie een succesfactor voor een project. 'Herhaling is de kracht van reclame': dat geldt niet alleen voor reclame, maar voor alle communicatievormen. Juist in een didactische organisatie moet bekend zijn dat niet elke boodschap bij iedereen voor 100 % aankomt. Denk daarom niet dat iedereen weet waar het over gaat als iets in een personeelsvergadering is gezegd of in het weekbulletin heeft gestaan.
Veranderingsanalyse	In een (veranderings)project verandert soms de structuur van de organisatie of de taken van mensen veranderen. Het is goed zodra daarover duidelijkheid bestaat (of na discussie) deze veranderingen vast te leggen. Veel lastiger is het, maar ook noodzakelijk, om culturele aspecten van verandering te omschrijven. Het kan gaan om een cultuurverandering binnen de organisatie, zoals de omslag naar een meer professionele organisatie die in stappen wordt gemaakt en zichtbaar wordt in een project, maar ook om bijvoorbeeld de vraag hoe om te gaan met weerstand.