GvIB Expert Brief – Juni 2007
ISSN 1872-4876, Jaargang 3 – Nr. 5

Juni 2007

Projectmanagement en informatiebeveiliging: de onmogelijke combinatie?

Frans M. Kanters

Carl Adamse

Ben Elsinga

Shahin Farrokhi

Marten Gorter

Frank Haak

Renato Kuiper

Robert Leyting

Adri Platje

Kelvin Rorive

Roger Wannee

Paul Wielaard

Gerard Zwiers

Het uitrollen van een project is gebaat bij het juist omgaan met tijd, kosten en middelen. Kortom de bekende duivelsdriehoek die in balans moet zijn. Projectmanagement biedt hiervoor handvatten. Informatiebeveiliging kampt – net als elk andere project – ook met dilemma's rond het beheer van deze duivelsdriehoek.

http://www.gvib.nl/
✉ expertbrief@gvib.nl

http://www.ibpedia.nl/

2

INLEIDING EN SITUATIE SCHETS

Informatiebeveiliging is een aspect dat in vrijwel elk project tegenwoordig een rol speelt. Of moet spelen, want in de praktijk wordt het veiligheidsaspect nog wel eens vergeten. Of in een laat stadium aan het einde van het project er bij geplakt. Alsof het vlak voor sluiting van de vergadering nog even behandeld moet worden. Het resultaat hiervan laat zich raden. Onvoldoende aandacht voor informatiebeveiliging, waardoor het project uit de kosten, tijd en middelen loopt. Een ander scenario dat veelvuldig voorkomt is dat het gehele project overnieuw wordt uitgevoerd. Nu dan wel met aandacht voor informatiebeveiliging. Over kostenplaatjes gesproken. Projectmanagement kan hierin een belangrijke rol spelen.

Nu is de markt als het gaat voor methodieken en producten rond projectmanagement niet overvloedig. Prince2 is een bekende, maar er is meer. Denk aan Business Process Redesign, Total Quality Management, Deming circle, de Waterval methode, het denken in ontwikkelingsprocessen en ga zo maar door. Het projectmanagement instituut geeft zelf s jaarlijks het zogenaamde handboek *Body of Knowledge* uit, dat ingaat op de laatste stand van zaken rond projectmanagement.

Een specifiek op informatiebeveiliging gerichte methodiek is er echter niet. Het vreemde is dat juist een onderwerp als informatiebeveiliging een kwaliteitsaspect van de bovenste plank is. De focus moet hierbij niet alleen liggen op het project zelf waar informatiebeveiliging een rol speelt, maar vooral op het aanhaken van de organisatie en de context van de bestaande opzet voor informatiebeveiliging. Vreemd dus dat dit nergens is terug te vinden in enige vorm van projectmanagement.

Het aanhaken bij het Prince2 lijkt voor de hand te liggen, omdat kwaliteit van een project geborgd moet worden in zowel de organisatie als in de projectorganisatie zelf. Maar staar je echter niet blind op Prince2! De methodiek kan leiden tot een soort “lege huls” project, omdat de methode bijvoorbeeld niets zegt over de technieken die noodzakelijk zijn in het project of de manier waarop projectinformatie in rapportages tot stand komt.

De rol van de opdrachtgever is bij het tot stand komen van het project belangrijk. Een ander aspect is het borgen van informatiebeveiliging binnen de bestaande IT afdeling. Als dit niet juist heeft plaatsgevonden dan zal het borgen van informatiebeveiliging in een willekeurig project nooit lukken. Als men bedenkt dat de project levenscyclus wordt omsloten door de product levenscyclus betekent dit dat de kop en de staart van een project waar informatiebeveiliging een rol moet spelen als vanzelf diffuus wordt. Dit komt omdat het mappen van deze twee levenscycli niet gebeurt.

Van belang te beseffen is dat een project waar informatiebeveiliging een rol speelt pas succesvol is als wordt voldaan aan een aantal kritische noten. Allereerst moet er betrokkenheid zijn van zowel de opdrachtgever als de directie (niet te vergeten). Er moet een klinkklare definitie zijn van het beoogde eindresultaat, een overzicht van alle acceptatiecriteria en kwaliteitscriteria en de manier waarop dit gecontroleerd gaat worden. Tot slot is betrokkenheid van de uiteindelijke gebruikers noodzakelijk.

De noodzaak informatiebeveiliging projectmatig aan te lopen start met een organisatie die behoefte heeft aan informatiebeveiliging. Heeft de organisatie wel een visie over informatiebeveiliging? Is er voldoende draagvlak vanuit de directie? Hoe is de *mindset*, of nog beter gezegd de cultuur van de organisatie ten opzichte van informatiebeveiliging?

Er moet een specifiek aan de organisatie missie en visie gekoppeld beleid voor informatiebeveiliging zijn. Dit heeft een duidelijke relatie met veranderingsmanagement met een hoofdrol voor management support en interventiefactoren.

DE ONDERZOEKSVRAGEN

De expertgroep heeft zich gebogen over de volgende vraagstelling:

- Wat is de relatie tussen projectmanagement en informatiebeveiliging?
- Is er een standaard aanpak voor projectmanagement om te zorgen dat informatiebeveiliging juist wordt ingebed in (IT) projecten?
- Uit welke onderdelen bestaat een dergelijk projectmanagement aanpak?
- Wat is de relatie vanuit projectmanagement met de bestaande organisatie rond informatiebeveiliging?

De expertgroep heeft zich vooraf gerealiseerd dat het onwaarschijnlijk is dat al deze vragen in één expertsessie beantwoord konden worden. Uiteindelijk wil zij door vervolgactiviteiten wel graag een antwoord op al deze vragen. Bovenal wil de expertgroep met de in deze expertbrief voorgestelde aanpak een doorstart maken naar een serieuze aanpak die kan doorgroeien naar een methodiek.

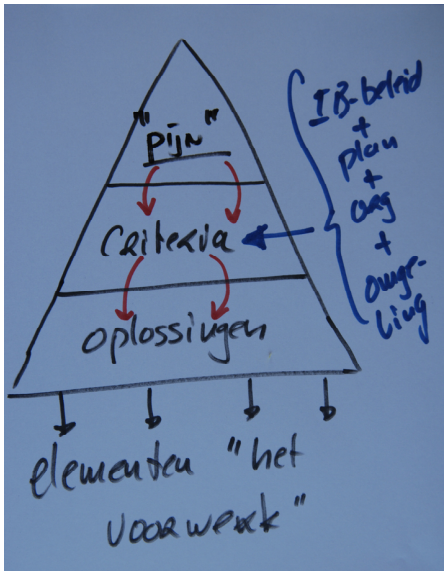
HET VOORWERK

Nog voordat een project start is het van belang om de vertrekpunten ervan te definiëren, speciaal voor wat betreft informatiebeveiliging. Dit staat te boek als het voorwerk, waarin onder andere de zogenaamde kernbegrippen worden geformuleerd. Deze bestaan uit:

- De business case, geredeneerd vanuit informatiebeveiliging
- Betrokkenheid van de opdrachtgever en directie
- Definitie van het eindresultaat
- Acceptatiecriteria
- Kwaliteitscriteria
- Betrokkenheid van de gebruikers

Organisatiepijn

Het voorwerk is tevens het aangewezen moment om de pijn die er rond informatiebeveiliging in een organisatie leeft om te zetten in oplossingen. Deze pijn wordt veelal gevoed door frustraties onder medewerkers en managers rond de huidige operationele beveiligingsmaatregelen en onbekendheid met informatiebeveiliging als onderwerp. Tevens is de match tussen nieuw project, bestaande beveiligingscultuur en uitbreiding in beveiligingsmaatregelen in veel gevallen een lastig te slechten barrière. Uiteindelijk zal deze pijn het beste vertrekpunt blijken om de beveiligingseisen voor het project op de juiste wijze te definiëren. Interviews met relevante stakeholders in de organisatie is hiervoor een uitgelezen hulpmiddel. Het vergt tijd en de inzet van



Figuur 1: *de relatie organisatiepijn versus criteria IB en oplossingen.*

(het liefst) een externe procesbegeleider. Extern omdat dit teveel band met de organisatie voorkomt, wat een te gekleurd beeld zal geven en dus geen heldere formulering van als criteria vertaalde pijn. De illustratie hierboven schetst dit schematisch. Het implementatieproces blijft een ondeelbare lijnverantwoordelijkheid waarbij externen kunnen assisteren, maar niet meer dan dat.

De organisatiepijn rondom informatiebeveiliging vormt de “waarom vraag”. De oplossingen zijn hierop het antwoord, de “hoe vraag”. Deze twee aspecten zijn essentieel om bij stil te staan. Tijdens het opstarten van projecten wordt dit vaak vergeten of te gehaast uitgevoerd. Het gevolg is tijdsverlies in het project omdat ter elfder uur nog een aantal eisen voor informatiebeveiliging opgesteld moet worden. Per definitie levert dit een slecht werkende beveiligingscomponent en een nog slechtere koppeling met de al bestaande operationele beveiligingsomgeving, het geldende beleid voor informatiebeveiliging en de architectuur voor informatiebeveiliging van de organisatie.

In de praktijk nemen organisaties veel te weinig tijd voor het voorwerk. Ook hier als resultaat een slechte koppeling van de beveiligingsoplossingen uit het project (als deze er al komen) en de operationele omgeving die informatiebeveiliging regelt.

Stappen voorwerk

Het voorwerk kent een aantal stappen die allen moeten worden doorlopen. Elke stap kent direct een of meerdere valkuilen. Het voorwerk voorkomt dat een project vroegtijdig in elkaar stort doordat er bijvoorbeeld geen ondersteuning vanuit het topmanagement is, de (eind)gebruikers het project niet ondersteunen of er onvoldoende bij zijn betrokken en er duidelijke bedrijfsdrijfveren zijn opgesteld (uit een onderzoek van de Standish Group, getiteld The Chaos ten). Dit onderzoek wees (het dateert al uit 2000) tevens uit dat het belang van een formele methode zeer gering is.

Voorwerk vaak te kort

Het voorwerk is het moment om de eisen rond informatiebeveiliging te definiëren. Elk ander moment is slechter en levert per definitie een minder resultaat op. Hoe verder het project in zijn levensfase is, des te slechter het moment is om nog aan het opstellen van deze eisen te beginnen. Gedurende het project kunnen eisen wel worden bijgesteld, vooral als deze een relatie hebben met deelprojecten of mijlpalen. Het project is namelijk opgehangen aan een zogenaamde projectlevensfase waarmee de totale duur van een project wordt beschreven. Binnen deze projectlevensfase speelt een aantal productlevensfasen. Om te voorkomen dat informatiebeveiliging binnen deze product levensfasen wordt vergeten moet dit vooraf duidelijk worden gedefinieerd.

Projectmanager met mensenkennis

Hierbij is het blindstaren op Prince2 een valkuil. Het zegt namelijk niets of een projectmanager Prince2 gecertificeerd is. De uiteindelijke kwaliteiten van deze persoon op gebied van beheersing van tijd, kosten en kwaliteit, op vlak van interactie met mensen en de manier waarop deze persoon de verschillende belanghebbenden op een lijn kan krijgen en houden zijn veel belangrijker.

Onvoldoende analyse van de stakeholders

De stakeholders zijn de feitelijke doelgroep van een project. Uiteindelijk zal het project een resultaat opleveren waar medewerkers binnen afdelingen iets mee moeten. Maar de

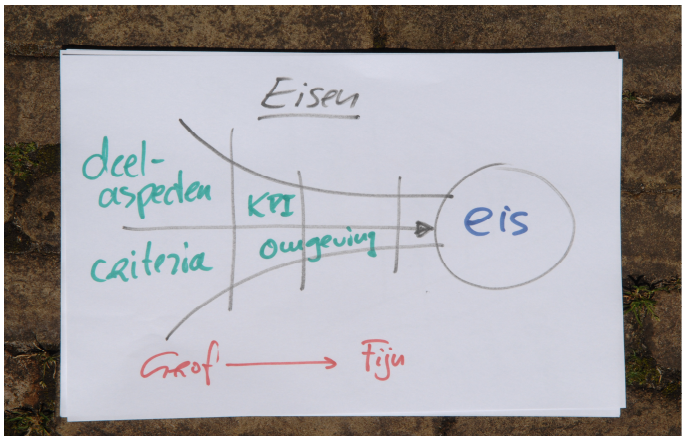
stakeholders binnen het bedrijf, die immers eindverantwoordelijk zijn voor deze groepen medewerkers, zijn de doelgroep. Zij zijn eindverantwoordelijk voor de resultaten van deze groepen medewerkers, en weten dus als geen ander wat men nodig heeft om dit resultaat te bereiken. Er moet dan ook voldoende tijd worden besteed aan de analyse van de stakeholders, zowel op transactioneel als op contextueel vlak. Ook is een omgevingsanalyse noodzakelijk, en moet de rol van personen die een flinke duit in het zakje doen wat beïnvloeden van het project betreft.

Wet en regelgeving

Er zijn nogal wat wetten en vooral regels die invloed kunnen hebben op projecten. Denk aan de Wet Bescherming Persoonsgegevens, SOX en Basel II. Afhankelijk van de omvang van een project, de mate waarin informatiebeveiliging een rol speelt en de reikwijdte van de projecteindresultaten in de organisatie moet de projectleiding hier terdege rekening mee houden. Specifiek op informatiebeveiliging gerichte regelgeving kan voor extra werk in een project zorgen, en moet vroegtijdig worden onderkend. Argumentatie hiervoor kan zijn dat de projectresultaten in de organisatie worden ingebed waar al gebruik wordt gemaakt van een norm, standaard of stuk regelgeving. Voorbeelden hiervan zijn ISO 27001:2005 dat een baseline voor informatiebeveiliging regelt of BS 25999-1 en 2 (voorheen bekend als PAS 56) waarmee de focus meer op business continuïteitsmanagement ligt. De praktijk laat helaas zien dat aansluiting bij de operationele regels te wensen overlaat. Dit zorgt voor stress binnen de verschillende projectteams en uiteindelijk voor een minder eindresultaat dat ook nog eens teveel tijd soupeert.

Werkwijze specificeren eisen

Het vaststellen en ontwikkelen van het normenkader met eisen verdient een speciale aanpak. Om te voorkomen dat elementen worden vergeten is deze aanpak gestoeld op het werken van grof naar fijn. Dit specificeren moet op het juiste niveau in de organisatie en met de juiste mensen worden gerealiseerd. Projectmatig werken op basis van technische systeemanalyse is hierbij het meest doelmatig. Het is van belang bij het specificeren van de eisen rekening te houden met de duivelsdriehoek tijd, kosten en kwaliteit. Informatiebeveiliging is onderdeel van kwaliteit binnen deze duivelsdriehoek, en verdient specifieke aandacht. Tevens moet rekening worden gehouden dat deze eisen via de werkwijze Product Breakdown Structure (PBS) uiteindelijk zullen landen in de maatregelen. Als de eisen eenmaal zijn opgesteld moet hier het geldige classificatieschema worden ingezet om de betrouwbaarheidseisen beschikbaarheid, integriteit en vertrouwelijkheid te toetsen en vast te stellen. Bij het testen moet de testmanager worden betrokken, vooral bij de acceptatiefase. De norm ISO 9126 biedt hiervoor handvatten.



Figuur 2: *Specificeren van eisen: werk van grof naar fijn.*

Professionaliteit projectmanager

Het project valt of staat voor een fors gedeelte met de kwaliteit van de projectmanager - of leider. Belangrijke kenmerken zijn pragmatisch werken, risicomanagement beheersen,

ontwikkelingsmethodiek goed kunnen toepassen en tot slot erg goed begrijpen. Deze persoon moet de werkwijze zoals hier beschreven volledig onderschrijven. Dit element binnen het voorwerk is het belangrijkste aspect. Is een projectmanager niet instaat om de match te maken tussen informatiebeveiliging en het project, de afzonderlijke deelprojecten hierop af te stemmen en de deelnemende partijen ervan te doordringen dat informatiebeveiliging een cruciaal en wellicht het meest cruciale element van het succesvol zijn van een project, stop er dan maar mee. Een dergelijke projectmanager zal zorgen dat dit project per definitie tot mislukken is gedoemd. Overigens zijn titels binnen de bandbreedte CISSP tot gecertificeerd ethisch hacker (en alles wat daartussen zit), geen garantie dat betitelde projectmanager daadwerkelijk in staat is tot het opleveren van een succesvol project met werkelijk aandacht voor informatiebeveiliging. Kennis van projectmanagement is het belangrijkste kenmerk. Daarnaast is affiniteit, kennis en ervaring met informatiebeveiliging gewenst: “walk the walk, talk the talk”. Zonder dit faalt elk project.

Het voorgaande betoog wordt tevens helder als verderop in deze expertbrief het volwassenheidsniveau van een organisatie wordt besproken. Hierin is namelijk het cultuuraspect een van de drijfveren.

Businesscase
Voordat een project überhaupt wordt gestart moet er een businesscase zijn vastgesteld, waarin kristalhelder is uitgewerkt wat de resultaten van het project toevoegen aan de organisatie, zowel vanuit bedrijfsoptiek maar ook voor wat betreft informatiebeveiliging. Het laatste kan ineens duidelijk maken dat informatiebeveiliging een echte “killer applicatie” kan blijken te zijn.

In de businesscase wordt de toegevoegde waarde van het projectresultaat versus de projectkosten in beschreven. Informatiebeveiliging moet hier een expliciete rol in krijgen. In sommige gevallen zal de meerwaarde van informatiebeveiliging het projectresultaat vergroten.

Ook kan de businesscase alleen worden vastgesteld na ampel beraad met stakeholders, de vertegenwoordigers vanuit de verschillende doelgroepen en opdrachtgever. Missie en doelstellingen van de organisatie spelen ook een rol. De rol van de opdrachtgever bij het vaststellen van de business case kan soms diffuus zijn, waardoor een te optimistisch beeld over de business case kan ontstaan. In de loop van het project blijkt het beeld een geheel andere te zijn. Investering in tijd, mensen en middelen is dan al gebeurt.

Management support
Hier is slechts een enkel aspect valide, namelijk zonder management support maakt een project geen enkele kans van slagen. Management support houdt in dat dit gedurende de totale duur van het project het geval moet zijn. Is een lastige bijkomstigheid zo blijkt uit de al eerder aangehaalde Chaos top ten van de Standish Group.

Elementen

Tijdens het voorwerk is het van belang dat er een gedeelde bedrijfsvisie voor een succesvolle implementatiebeveiliging wordt ontwikkeld. Deze visie geldt op een bepaalt moment in de toekomst. Dit wordt de organisatievisie genoemd, die uitgangspunt is voor de kaders, de randvoorwaarden en de condities die noodzakelijk zijn om een projectvisie te kunnen opstellen.

Hier moet onderscheid worden gemaakt tussen twee insteken:

1. Het project: implementatie van informatiebeveiliging in de organisatie
2. Het project: implementatie beveiliging in een project

Voordat het project start is het van belang dat de organisatie zich afvraagt waar informatiebeveiliging begint. Is er überhaupt een visie waar het aspect informatiebeveiliging in ligt opgesloten? In feite moet hier duidelijk worden dat de organisatie behoefte heeft aan informatiebeveiliging. Vanuit deze behoefte wordt een beschrijving gemaakt van de informatiebeveiliging aandachtspunten gerelateerd aan het project. In deze fase is draagvlak van de directie erg belangrijk. De omvang van dit draagvlak en de manier waarop dit zich manifesteert komt al snel boven water drijven als de eerste twee vragen uit deze alinea worden beantwoord. Het formuleren van de projectaandachtspunten voor informatiebeveiliging hebben tevens een directe relatie met de *mindset* van de organisatie voor wat betreft informatiebeveiliging. Het cultuuraspect binnen de organisatie is hierin een belangrijk onderdeel. Kortom, de specifieke visie voor informatiebeveiliging moet gekoppelde zijn aan de organisatie missie en doelstellingen.

Deze visie moet worden uitgerold waarbij alle organisatieonderdelen hun zegje moeten kunnen doen in relatie tot informatiebeveiliging. Hierin is veranderingsmanagement een essentieel onderdeel. Immers, niet alle onderdelen zullen de visie voor informatiebeveiliging op hun eigen merites kunnen beoordelen of eigen wensen hebben of er een eigen draai aan geven. De Standish Group heeft hier onderzoek naar gedaan waaruit blijkt dat managementsupport gekoppeld aan een aantal interventiefactoren een belangrijke succesfactor is. Een andere is de manier waarop het project wordt doorlopen, namelijk de systeemaanpak versus de ontwikkelingsaanpak. Volgens publicaties van Prof. Jaap Boonstra [2] blijkt tevens dat de zogenaamde *strategic deployment* zodanig moet worden beschreven dat het doel en het resultaat niet vermengd worden. De praktijk is veelal anders, want die laat zien dat dit juist wel gebeurt.

Figuur 3: Ontwikkelingsaanpak versus systeemaanpak bij projecten.

Binnen het kader van het voorwerk moet tevens de keuze worden gemaakt tussen de ontwerpaanpak en de ontwikkelingsaanpak. Uit onderzoek blijkt dat in 80% van de projecten organisaties vrijwel automatisch kiezen voor de ontwerpaanpak. Hetzelfde onderzoek wijst uit dat driekwart van deze 80% (vroegtijdig) mislukt. Kijk je naar de ontwikkelingsaanpak, dan blijkt het overgrote deel van op deze aanpak ingestoken projecten het merendeel binnen budget en tijdsraming wordt afgerond.

Q&A is kritisch

De hierboven genoemde stappen van het voorwerk moeten allen worden doorlopen, waardoor de eisen boven tafel komen. Zonder eisen voor informatiebeveiliging kan een project niet gestart worden, sterker nog, mag een project niet gestart worden. Deze eisen moeten voor de start van het project volstrekt helder zijn, en door alle deelnemende partijen worden onderschreven. Tevens is een beheerst acceptatieproces noodzakelijk om ervoor te zorgen dat deze eisen tevens landen in alle deelprojecten en op de detailniveaus bij het uitwerken en vormgeven van alle (deel)projectactiviteiten. De ontwikkelingsaanpak is hiervoor de meest voor de hand liggende aanpak, omdat hiermee het geleidelijk karakter van een ontwikkelingstraject van eisen goed kan worden geregeld. Naarmate je dieper in de projectstructuur terecht komt, en dus op een gedetailleerder niveau aan de projectresultaten gaat werken, zal tevens de mate van detaillering van beveiligingseisen belangrijker worden De ontwikkelingsaanpak maakt dit mogelijk. Bij het uitblijven van een acceptatie proces en een controlemechanisme krijgt functionaliteit de overhand, met alle gevolgen voor kosten, effectiviteit en efficiency. Dit zal pas duidelijk worden als de projectresultaten worden overgedragen naar de operationele beheersorganisatie(s). Dit kan betekenen dat kosten die hier gemaakt worden ineens flink stijgen. Zodra functionaliteit de overhand krijgt wordt er niet meer gestuurd op de resultaten en de doelen. Een Q&A rol moet hierin optreden en sturen. De Q&A rol dient door de projectboard te worden geregeld. Dit betekent dat er kritische proces indicatoren (kpi's) moeten worden gedefinieerd met de projectdoelen als focus. Hierna kan het meten starten. Tevens moeten er kpi's worden gedefinieerd met als focus resultaten. Ook hier weer meten en controleren.

Een ander element dat hier al een rol speelt is de product breakdown structure, kortweg PBS. Dit is in lijn met de manier waarop tijdens het voorwerk aan de beveiligingseisen wordt gewerkt, namelijk van grof naar fijn. Binnen dit bestek is Prince2 juist wel een aanrader, omdat de methodiek sterk is in het verantwoordelijkheid neerleggen bij de opdrachtgever, het plannen op PBS en de focus leggen bij de business case. Alle elementen waar menig beveiligingsexpert niet snel bij nadenkt als zijn mening wordt gevraagd of er een appel wordt gedaan op zijn kennis ten faveure van een project.

Hier speelt wel een kanttekening. Het is namelijk een risico om in een enkele exercitie alle deelproducten die het project moet gaan opleveren direct uit te werken met PBS. Het gevaar loert dat er teveel los zand ontstaat doordat de deelproducten geen geheel vormen. Kies er daarom eerst voor om een architectuur te ontwikkelen (is overigens ook een expertbrief voor beschikbaar) of aansluiting te zoeken bij de architectuur als die er als is. De architectuur zal snel uitsluitsel geven op de vraag "make or buy" en de samenhang van de IT componenten. Het is wel van belang om niet blind te staren op informatiebeveiliging, er moet een goede balans zijn.

Eisen voor informatiebeveiliging

Omdat informatiebeveiliging onderdeel is van grootschalige programma's van een scala aan projecten, moet dit als apart aspect worden beheerd. Daar is deze voorwerkfase dan ook vooral voor bedoeld. In de praktijk blijkt dat informatiebeveiliging als een apart onderwerp wordt aangemerkt en wordt benoemd. Hier gaat het mis, omdat de aansluiting met de projecten volledig zoek raakt. Het gevaar hierbij is dat de eigenaar van een project (geredeneerd vanuit informatiebeveiliging) zich vaak blindstaart op functionaliteit in plaats van informatiebeveiliging. Er moeten dus goede afspraken gemaakt worden met alle betrokkenen rond informatiebeveiliging, en leg dit vast in de projectdocumentatie. Stem deze

vertrekpunten duidelijk af met de stakeholders in de organisatie die en belang hebben bij het project. De focus hierbij moet zijn volledigheid.

Een showstopper voor deze fase is dan ook het moment waarop blijkt dat de eisen voor informatiebeveiliging onvoldoende of in het geheel niet zijn benoemd en opgesteld.

Essentiële vertrekpunten
Andere vertrekpunten die tijdens het voorwerk moeten worden uitgewerkt zijn:

- Nadenken over de betrouwbaarheidseisen in relatie tot de resultaten die het project moet gaan opleveren
- Het uitvoeren van een omgevingsanalyse (Business Impact Analyse)
- Het benoemen van rollen en verantwoordelijkheden van projectleden in relatie tot informatiebeveiliging
- Het beschrijven van je doelgroep. De vraag die moet worden beantwoord luidt hierbij: “Voor wie doe je wat”
- Het beschrijven van de deelresultaten. Ook hier een vraag die voortborduurt op het vorige aandachtspunt, namelijk de doelgroep. De vraag die hier speelt is: “Wat wil de doelgroep uiteindelijk, en welke eisen stelt de doelgroep hieraan?”.
- Opstellen eisen informatiebeveiliging die er vanuit de organisatie worden opgelegd

Gun jezelf de tijd om het voorwerk goed te formuleren. Dit is namelijk de essentie voor elk project.

De volgende stappen zijn nodig in de fase voorwerk:

- Ontwikkelen van een gedeelde visie (het toekomstbeeld, ook wel ‘shared vision’ genoemd)
- Het uit deze visie halen van de bedrijfs – en/of de projectmanagementprocessen
- Opstellen van een functie breakdown structure
- Verfijnen naar een systems breakdown structure
- Verfijnen naar een architectuur of topologie
- Verfijnen naar een Product Breakdown Structure
- Vertalen in Product Flow Diagrammen
- Vertalen naar een Projectplan met mijlpalen en/of gateways.

VOLWASSENHEIDSNIVEAU ORGANISATIE

De mate van volwassenheid van een organisatie bepaald in grote lijnen de wijze waarop met informatiebeveiliging wordt omgegaan in het algemeen, en binnen projecten in het bijzonder. Er zijn meerdere aspecten die bepalen hoe een project aangepakt moet worden. Deze aspecten geven tezamen een duidelijk beeld van het volwassenheidsniveau van een organisatie, en worden aangeduid als volwassenheidskenmerken. Hoe hoger dit niveau is, des te groter de kans dat informatiebeveiliging op de juiste wijze wordt ingebed in de operationele bedrijfssituatie. Dit niveau geeft namelijk aan hoe een organisatie bijvoorbeeld omgaat met standaarden en het beveiligingsproces als geheel. Als een organisatie een hoog volwassenheidsniveau heeft betekent dit dat het voorwerk dat moet worden verricht rondom informatiebeveiliging geringer is in vergelijking met een organisatie waar dit niveau lager is. Het is mogelijk dat er binnen organisaties sprake is van verschillende volwassenheidsniveaus.

Dit kan vooral het geval zijn bij grote multifunctionele organisaties waar verschillende onderdelen zelfstandig functioneren.

De volgende volwassenheidskenmerken spelen een rol:

Cultuur
De bedrijfscultuur bepaalt in grote mate het volwassenheidsniveau van een organisatie. Hier zijn boeken over vol geschreven, en dit valt duidelijk buiten te bestek van deze expertbrief. Wat hier niet buiten valt is awareness, normen en standaarden voor bewustzijn en bewustwording, compliance methodieken en tot slot de mate waar een organisatie überhaupt over informatiebeveiliging discussieert. De uitspraak “soft skills are the organisation’s hardest diamonds” geeft aan dat cultuur als belangrijk volwassenheidskenmerk te boek staat.

Standvastigheid en mate van onzekerheid
Rond een project is het eindresultaat wat telt. Een organisatie kan hier een zekere onzekerheid over hebben, los van het niveau binnen de organisatie of de betrokken functie. Motivatie van de organisatie als geheel of een deel daarvan dat binnen het project een rol speelt geeft een duidelijke draai aan de mate van standvastigheid. Niet gemotiveerd zijn van mensen rond informatiebeveiliging zorgt dat de koppeling naar het project niet gaat lukken. Dit beïnvloedt het eindresultaat. De mate van onzekerheid rond het eindresultaat kan worden weggenomen door een risk assessment uit te (laten) voeren met sturing op fasering, de methodiek waarmee het project wordt aangepakt en bestuurd, de project organisatie en als laatste de verhouding tussen de voorbereiding en de uitvoering.

Projectonzekerheid kan op vier manieren geïdentificeerd [3] worden:
- Variatie
- Voorziene onzekerheid
- Onvoorziene onzekerheid
- Chaos

Variatie is opgehangen rondom de meer traditionele aanpakken, terwijl chaos zich uit in aanpakken die ruimte bieden aan verandering [3].

Besturing
De mate waarin een organisatie controle heeft over haar informatiebeveiliging bepaalt in grote mate het volwassenheidsniveau. Hoe minder volwassen, hoe meer activiteiten noodzakelijk zijn om te zorgen dat de al eerder genoemde koppeling tussen informatiebeveiliging en het project slaagt. Bij controle past ook het kiezen van een juiste strategie voor het in balans krijgen en houden van projectvoorbereiding versus projectuitvoering.

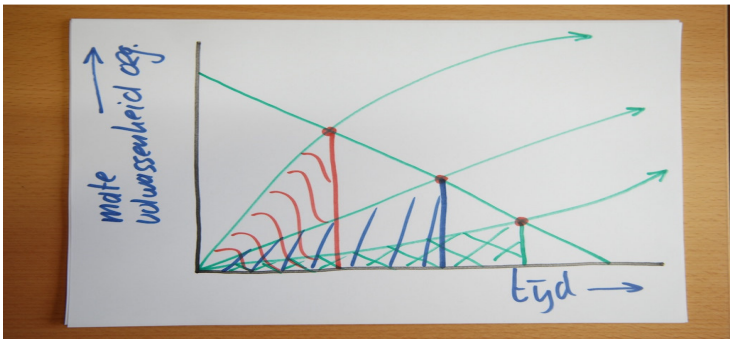
Omvang
Een grote organisatie zal per definitie meer tijd hebben geïnvesteerd in het formaliseren van processen, het opstellen van regels en het doorvoeren van een procesgestuurde werkwijze voor informatiebeveiliging. De rol van de verantwoordelijk manager voor informatiebeveiliging, de security officer (CISO) en eventuele andere functionarissen is hierin van belang. Dit heeft een directe relatie met de projectorganisatie. Zal de CISO participeren hierin? Of juist niet? Twee petten dan? Hier moet goed over nagedacht worden.

Beleid
De aanwezigheid van beleid voor informatiebeveiliging is een belangrijk vertrekpunt voor een project waarin informatiebeveiliging een rol speelt. Het volwassenheidsniveau van een organisatie heeft een directe relatie met dit beleid. Hoe is het tot stand gekomen, en hoe wordt het bijgehouden? Is iedereen binnen de organisatie er van doordrongen dat er überhaupt beleid is? Het geeft aan in hoeverre er is nagedacht over informatiebeveiliging in termen van strategie, organisatie en tactische richtingen. Naarmate beleid en gerelateerde aspecten beter zijn uitgekristalliseerd zal een organisatie sneller en efficiënter informatiebeveiliging kunnen inbedden in een project. De manier waarop de organisatie omgaat met dit beleid is tevens bepalend voor het volwassenheidsniveau. Ofwel, er kan beleid voor informatiebeveiliging zijn, maar als daar niet op de juiste wijze mee wordt omgegaan (denk aan up-to-date houden), dan is dot eerder een negatief aspect dan positief. De wisselwerking tussen de projectorganisatie en de bestaande beveiligingsorganisatie speelt hierbij tevens een belangrijke rol.

Technologie
De mate waarop technologie is ingevoerd en beschikbaar is binnen een organisatie geeft aan hoe het bedrijf met informatiebeveiliging omgaat. Techniek is een logisch gevolg van een uitgezette koers voor informatiebeveiliging. Tenminste als het goed is. Dit aspect speelt en een rol bij het volwassenheidsniveau, maar nog meer binnen het inbedden van informatiebeveiliging in het project zelf. In de praktijk kan namelijk duidelijk worden dat de operationele techniek achterhaald is, niet werkbaar is of juist een extra verbeterslag moet doorlopen om binnen het project en later in de operationele processen juist te kunnen werken. De match tussen eisen (requirements) voor techniek en het volwassenheidsniveau van een organisatie zijn cruciaal in het vaststellen van de wijze waarop deze technologie moet worden ingezet, zowel binnen het project als in een later operationeel stadium.

Complexiteit
Complexiteit heeft twee invalshoeken. De complexiteit van de organisatie zelf speelt een rol. Is het bijvoorbeeld mogelijk binnen een complexe procesgestuurde organisatie projecten los daarvan te laten functioneren? Vooral de wijze waarop het project zelf wordt aangevlogen door fasering, methodiek, projectorganisatie en de verhouding tussen voorbereiding en daadwerkelijk uitvoering is in grote mate afhankelijk van het volwassenheidsniveaus van de organisatie. Een volwassen organisatie zal projecten gestroomlijnd aanlopen. De complexiteit heeft tevens een relatie met security alignment. Als hiervoor duidelijk afspraken zijn gemaakt binnen het bedrijf dan zullen de projectkenmerken als fasering, organisatie en methodiek eenvoudiger in te vullen zijn.

Gezamenlijk bepalen de hierboven beschreven aspecten het volwassenheidsniveau van een organisatie en dus de mate waarop, snelheid en effectiviteit waarmee informatiebeveiliging in het project een rol krijgt toebedeeld en wordt ingebed. Dit verschilt dus per organisatie en wordt in de



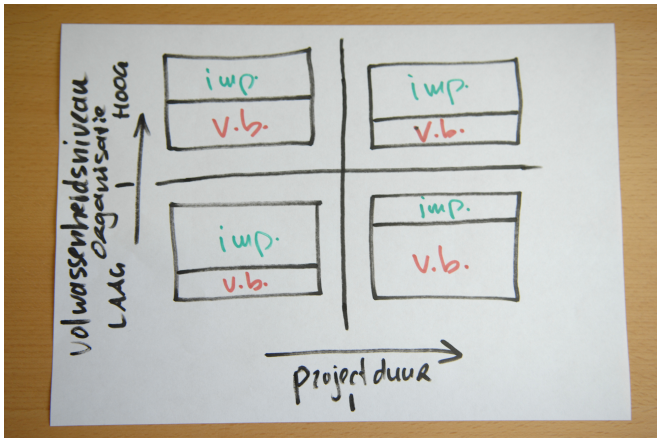
Figuur 4: *Volwassenheidsniveau organisatie versus projectduur.*

figuur hierboven schematisch weergegeven. Hierbij zijn drie scenario's uitgebeeld. Het rode scenario schets een organisatie die een hoog volwassenheidsniveau kent. De aspecten die dit niveau bepalen zijn in grote mate uitgewerkt en ingevuld. De tijd dat een project nodig heeft en dus de tijd dit noodzakelijk is om informatiebeveiliging in te bedden in het project blijven beperkt. Het blauwe en groene scenario schetst een organisatie die dit in mindere mate heeft geregeld. De tijd benodigd voor het project wordt hierdoor automatisch langer. Dit schema geeft aan dat de manier waarop de volwassenheidskenmerken zijn ingevuld in bepalend zijn voor de projectduur en de wijze waarop informatiebeveiliging ingebed wordt in een project. Het schema kent een verfijning als deze kenmerken (complexiteit, cultuur, omvang etc) tevens worden opgenomen. Eventueel kan CMM hierbij een rol spelen.

Management support
De mate waarin het management (top management, hoger en middenmanagement van alle relevante organisatieonderdelen) het project ondersteund is essentieel in het slagen van het project. Zonder managementondersteuning kan een project maar beter gestopt worden. Het management is namelijk de aangewezen plaats om aanwezig potentieel in de organisatie te mobiliseren en in te zetten in een project [4]. Ondersteunt het management het project niet, dan komt er van de inzet van dit potentieel en het gebruik van beschikbare interne kennis niets terecht.

Magisch kwadrant volwassenheidsniveau

Door het volwassenheidsniveau van de organisatie af te zetten tegen de projectduur, en hierbij rekening te houden met de voorbereidingstijd en de implementatietijd (en de balans daartussen!) ontstaat een magisch kwadrant genaamd "balans voorbereiding versus implementatie".



Figuur 5: *Magisch kwadrant "balans volwassenheidsniveau".*

Bij een hoger volwassenheidsniveau zal een organisatie een korte voorbereidingstijd (vb) plus een korte duur voor implementatie nodig hebben. Is het niveau laag dan zal dit een organisatie zijn die veel voorbereiding nodig heeft en snel implementeert. Dit vergt meer projecttijd, en zal in de operationele situatie wellicht leiden tot bijsturing dat ook weer tijd vergt.

Als blijkt dat de organisatie linksonder in het kwadrant zit dan moet eerst worden gewerkt aan de rijpheid van de organisatie. Dit kan bijvoorbeeld door inzet van het INK model of EFQM. Hoe hoger het volwassenheidsniveau van een organisatie des te sneller zal het project worden doorlopen met een efficiënter eindresultaat.

Een andere manier om naar volwassenheid te kijken zijn de zogenaamde "5 stukken van Plato". Dit zijn achtereenvolgens visie, strategie, analyse, manier van communiceren en tot slot de actiebereidwilligheid. Deze vijf elementen moeten in balans zijn, omdat er anders niets te veranderen is in een organisatie.

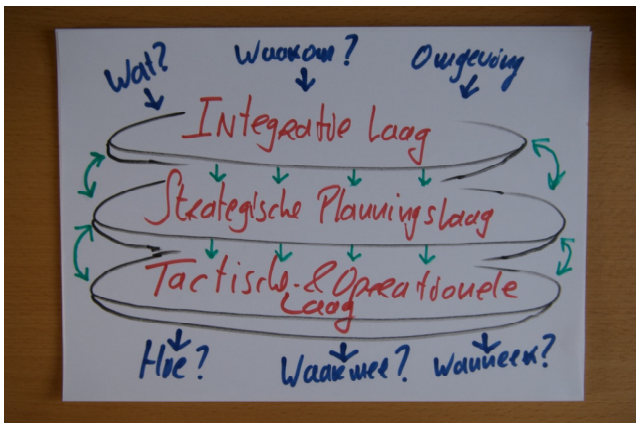
Afrondend

Na afronding van het voorwerk en het vaststellen van het volwassenheidsniveau van de organisatie maakt het feitelijk niet veel uit welke projectmanagement aanpak wordt gebruikt. Het is hierbij van belang om een aanpak te kiezen die past bij de organisatie.

Naast het voorwerk en het volwassenheidsniveau speelt een aantal aanvullende aspecten een rol. Deze worden hieronder beschreven.

GELAAGDE BEHEERSTRUCTUUR

Het beheren en beheersbaar houden van een project is cruciaal in het succesvol zijn ervan. Een gelaagde structuur hiervoor is onontbeerlijk. Deze structuur kent minimaal drie lagen, namelijk de integratie laag waarin je vaststelt wat je als organisatie wilt en welke richting je op wilt gaan, een strategische planningslaag en een laag waarin zowel tactisch als operationeel het project wordt bestuurd (zie figuur 6). Beheer speelt een rol in het continue opstellen en bijstellen van de eisen voor informatiebeveiliging. Het systematisch opstellen van deze eisen en vertalen ervan naar een architectuur en uitdrukken in producten voorkomt dat er een spanningsveld ontstaat tussen het project en het bewust maken van de organisatie voor informatiebeveiliging. Beheer betekent tevens borging, borging dat het beste op niveau van projectboard kan plaatsvinden.



Figuur 6: Gelaagde beheerstructuur project.

Dit orgaan moet mandaat hebben om de Q&A rol uit te kunnen voeren. In feite is dit een integrale verantwoordelijkheid van het senior projectmanagement, die voor borging een directe terugkoppeling moet kunnen geven aan de CEO. Het voorkomt dat er een te grote impact ontstaat op de bestaande beheersorganisatie omdat innovatie een behoorlijk druk kan leggen en veel invloed heeft op de operationele beveiligingsmaatregelen. Dit moet vooraf worden ingeschat, en hoort thuis binnen het voorwerk. De beheerstructuur zorgt vervolgens voor de noodzakelijk wisselwerking tussen project en security organisatie. De trukendoos hiervoor is simpel en eenvoudig, namelijk faseren, stevig risicomanagement en tijdige risicoanalyses.

Een gelaagde beheerstructuur zal zorgdragen voor het denken in processen in plaats van in hiërarchieën. Tevens ontstaat een besturing vanuit het project op de zogenaamde passages of review momenten (in goed Engels gateways), dat veel effectiever blijkt te zijn dan dat er gestuurd wordt op het bereiken van mijlpalen (die een vast onderdeel zijn binnen de ontwerpaanpak). Mijlpalen vormen een groot gevaar doordat dit de projectorganisatie blind kan maken met maar een gedachte, het realiseren ervan. Als hier teveel op wordt gestuurd ontstaan de mijlpalen. Het resultaat zal altijd minder zijn, doordat er niet voldoende tijd wordt

gebruikt door te snel werken, er teveel aan politieke belangen vanuit de organisatie zelf wordt vastgehouden die flink invloed hebben op de projectorganisatie.

Normaliter zal er in een organisatie sprake zijn van meerdere projecten die tegelijkertijd worden uitgevoerd. De gelaagde beheerstructuur is het instrument waarmee deze projecten gelijktijdig bestuurt kunnen worden. Het gaat hierbij om de vertaalslag van het gewenste portfolio van projecten en activiteiten naar een operationeel portfolio. Binnen het gewenste portfolio is sprake van twee aspecten die gezamenlijk door programmamanagement bestuurt worden, namelijk doelen en effecten. Door de effecten te meten – bijvoorbeeld door kwaliteit succes factoren (KSF) en prestatie indicatoren (PI) - kan gestuurd worden op deze doelen, en wordt de “wat” en waarom “vraag” beantwoord. Binnen het operationele portfolio wordt vanuit het doel zicht gekregen op de benodigde inspanning (die is vereist om dat doel te behalen). Door afdwingbare resultaten (KSF’s en PI’s) middels (multi)projectmanagement te besturen ontstaan resultaten. Deze resultaten hebben weer effecten tot gevolg. Hiermee is de cirkel rond. Dit geheel wordt een Strategy Deployment genoemd. In figuur 7 wordt dit schematisch weergegeven.

Figuur 7: Strategy Deployment.

De lijnorganisatie blijft verantwoordelijk voor het beheersen en besturen van deze cyclus. Hierbij moet worden voorkomen dat het resultaat gelijk wordt gesteld met het effect en/of dat het doel gelijk wordt getrokken met het resultaat. Deze twee valkuilen zijn in de praktijk aanleiding voor het volledig mislukken van deze benadering.

De rol van de opdrachtgever

De opdrachtgever heeft een zogenaamde brengplicht waarmee de aandacht voor informatiebeveiliging binnen het project vroegtijdig wordt onderkend. De criteria voor informatiebeveiliging moeten door de opdrachtgever worden opgesteld. De opdrachtgever moet dus eisen geven en stellen waaraan informatiebeveiliging moet voldoen. Laat dit niet doen door de beveiligingsafdeling omdat dit een te enge of zelfs foutieve, niet business georiënteerde focus zal op leveren, met als gevolg dat eisen en wensen vanuit de organisatie gaan botsen. Een andere aspect in de rol van de opdrachtgever is dat hij of zij er scherp op toeziet dat de verantwoordelijke lijnmanagers aansluiting en voeling houden met de cyclus zoals weergegeven in figuur 7.

BOUWSTENEN

Het project moet uit een aantal bouwstenen bestaan. De denkwijze die noodzakelijk is om het project juist te kunnen vormgeven en opstarten is een getrapte vorm. Het bestaat uit een aantal bouwstenen, namelijk functioneel ontwerp, systeemontwerp, architectuur en de (deel)producten. Vooral deelproducten vereist deze denkwijze, aangeduid als bouwstenen.

Hierbij geldt dat er top down moet worden gedefinieerd en gespecificeerd, en bottom up moet worden gebouwd. Dit heet de waterval methode, en moet als zodanig worden beheerd. De eisen en wensen voor informatiebeveiliging moeten op deze wijze worden vastgesteld.

Functioneel ontwerp
Vanuit het voorwerk en de mate waarop de organisatie omgaat met informatiebeveiliging (het volwassenheidsniveau) moet er voor informatiebeveiliging een functioneel ontwerp worden ontwikkeld. De volwassenheidskenmerken van de organisatie spelen hierbij een belangrijke rol.

Systeemontwerp
Vanuit het functionele ontwerp wordt een systeemontwerp ontwikkeld met eisen rond informatiebeveiliging. Zolang deze eisen niet helder zijn, zal de ontwikkeling van deze bouwsteen niet afgerond kunnen worden.

Architectuur
De systeemontwerpen moeten integreren in de bestaande architectuur voor informatiebeveiliging. Er kan aanleiding zijn om een architectuur aan te passen, bijvoorbeeld wanneer sprake is van innovatie. Onderzoek dus ook de al aanwezige architectuur voor informatiebeveiliging, en werk vandaar uit naar het functionele- en technische ontwerp.

Producten
Vanuit de architectuur ontstaan de (deel)producten informatiebeveiliging, bijvoorbeeld een beveiligde manier van op afstand werken waardoor de beveiliging van laptops eenduidig wordt (i.e. er staat geen informatie meer lokaal op de laptop omdat alles via emulatie gebeurt en de medewerkers feitelijk op de centrale systemen werken).

Product Breakdown Structure

De Product Breakdown Structure (PBS) aanpak maakt het mogelijk om de (deel)producten (bijvoorbeeld beveiligingsmaatregelen) die het resultaat van een project moeten zijn in detail te definiëren. Samen met een Work Breakdown Structure (WBS) vormen deze twee aspecten het essentiële onderdeel van elk project.

ONTWIKKELINGSAANPAK ALS STRATEGIE

De ontwikkelingsaanpak blijkt door organisaties niet vaak te worden gekozen als vertrekpunt voor een project. Dit is vreemd omdat uit verschillende onderzoeken [2] blijkt dat de meeste projecten die op basis van de ontwikkelingsaanpak worden bestuurd succesvol zijn. Projecten die daarentegen worden bestuurd volgens de systeemaanpak mislukken, waarbij cijfers aangeven dat het hier gaat om grofweg driekwart van alle projecten die op deze wijze worden aangevlogen.

De tegenhanger van de ontwikkelingaanpak, de ontwerpaanpak, vertrekt vanuit de gedachte dat het topmanagement stuurt, controleert en de verandering initieert. De ontwerpaanpak is oplossingsgericht, werkt in grote mate met deskundigen, en de besluitvorming is geformaliseerd en strak geregisseerd. De versterking va het lerende vermogen van organisaties wordt hierdoor onderbelicht of zelfs geheel vergeten.

Aanpak in 6 stappen

De ontwikkelingsaanpak omvat een zestal stappen. In de eerste stap wordt een zogenaamde "shared vision" ontwikkeld. Ook hier komt de al eerdere aangehaald en belangrijk aspect van managementondersteuning weer terug. Is deze ondersteuning er niet dan komt deze visie er ook niet. Vanuit deze visie worden namelijk in de volgende stap de primaire en secondaire processen gedestilleerd.

De ontwikkelingsaanpak daarentegen denkt en werkt vanuit de organisatie, die gezien wordt als bron van ervaringen. Er is feitelijk maar een doel, en dat is een verbetering redenerende vanuit de bestaande organisatie. De aanpak is probleemgericht, beoogd een vergroting van het veranderingsvermogen van een organisatie en werkt op basis van een concrete werkwijze in plaats van met abstracte modellen. Het (her)gebruik van materie kennis staat centraal, evenals het gebruik van kennis en inzichten van de eigen medewerkers en de inzet van human relations. Dit maakt dat de ontwikkelingsaanpak het aspect "zelfleren van een organisatie" ziet als uitgangspunt van groei, er meetbare effecten zijn op gedrag en voor het organisatieklimaat en analyseert op basis van het besturen van werkprocessen. Deze resultaten vormen het vertrekpunt voor de derde stap waarin de organisatorische structuur wordt vastgesteld. In stap vier wordt vervolgens een aantal parameters bepaalt waarmee deze processen bestuurd kunnen worden. Stap vijf zorgt dat de hiervoor noodzakelijke functies worden ontwikkeld. Beheersen, besturen en controleren vereist de inzet van competenties op het juiste moment en op de juiste plaats in de organisatie. In de laatste stap wordt een keuze gemaakt voor het gereedschap waarmee deze sturing kan worden ondersteund.

De ontwikkelingsstrategie is dan ook de aangewezen aanpak om binnen het voorwerk en de vervolgstappen te worden ingezet om informatiebeveiliging binnen een project in te kunnen bedden.

CONCLUSIES EN VERVOLG

De expertgroep is er in geslaagd om antwoorden te vinden op een groot deel van de gestelde vragen. Er is een aanpak die in grote lijnen bestaat uit de volgende stappen:

- Doorlopen van de stap "Het voorwerk"
- Bepalen volwassenheidsniveau van de organisatie
- Invullen van de gelaagde beheerstructuur (meten van KSF's en PI's)
- Het bouwen van het project met de bouwstenen met o.a. PBS

Binnen deze vier stappen is er een hoofdrol weggelegd voor de ontwikkelingsaanpak.

De uitkomst van de expertbrief sessie is dat er geen standaard projectmanagement methodiek is waarmee informatiebeveiliging juist kan worden ingebed in een project. Van belang is om het voorwerk en het volwassenheidsniveau van de organisatie eenduidig vast te stellen.

De vragen hoe een organisatie projectmanagement het beste kan inzetten om te zorgen dat informatiebeveiliging in een project juist wordt ingebed en aansluit bij de ontwikkelingen binnen dat bedrijf zijn nog onvoldoende beantwoord. De expertgroep zal deze vragen in een vervolg sessie proberen te beantwoorden. De expertgroep is erg benieuwd naar de toegevoegde waarde van deze expertbrief voor u en ontvangt graag commentaar. U kunt uw

reacties sturen naar expertbrief@gvib.nl. Ook indien u deze expertbrief heeft kunnen waarderen stellen wij een e-mail op prijs.

Vervolgvragen

De expertgroep heeft de volgende vervolgvragen openstaan:

- Is er een duidelijk profiel van een projectmanager te definiëren? Het aspect kwaliteit en mensenkennis zijn hierin belangrijke criteria.
- Is het mogelijk om vanuit deze expertbrief een gedetailleerd werkmodel te ontwikkelen waarmee organisaties direct aan de slag kunnen gaan?
- Hoe borg je de betrokkenheid van het management?
- Welke sociale en sociologische aspecten zijn van belang te onderkennen?
- Zijn er modellen en standaarden die deze aanpak kunnen ondersteunen?

LITERATUURLIJST

Voor het tot stand brengen van deze expertbrief heeft de werkgroep de volgende literatuur geraadpleegd:

[1] Projectmanagement, een introductie op basis van Prince 2, B. Hedeman e.a. (2004)
[2] Lopen over water, Prof. J. Boonstra (2000)
[3] Het managen van projectonzekerheid, De Meyer en Pich, Management Select (2002)
[4] Projectmanagement: middel en geen doel, A. Platje, Management Executive (2006)

APPENDIX GEBRUIKTE LICENTIEVORM

De expertbrief wordt gepubliceerd onder de volgende licentie:
http://creativecommons.org/licenses/by-sa/2.5/

Deze pagina ziet er op het moment van schrijven als volgt uit:

creative commons

COMMONS DEED

Naamsvermelding-GelijkDelen 2.5

De gebruiker mag:

- het werk kopiëren, verspreiden, tonen en op- en uitvoeren
- afgeleide werken maken
- gebruik maken van het werk voor commerciële doeleinden

Onder de volgende voorwaarden:

BY: **Naamsvermelding**. De gebruiker dient de naam of andere aanduiding van de maker te vermelden.

Gelijk delen. Indien de gebruiker het werk bewerkt kan het daaruit ontstane werk uitsluitend krachtens dezelfde licentie als de onderhavige licentie worden verspreid.

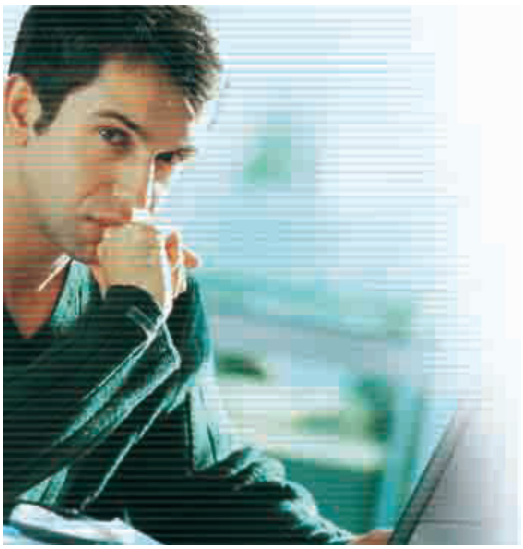
- Bij hergebruik of verspreiding dient de gebruiker de licentievoorwaarden van dit werk kenbaar te maken aan derden.
- De gebruiker mag uitsluitend afstand doen van een of meerdere van deze voorwaarden met voorafgaande toestemming van de rechthebbende.

Het voorgaande laat de wettelijke beperkingen op de intellectuele eigendomsrechten onverlet.

Dit is de vereenvoudigde (human-readable) versie van de volledige licentie.

Vrijwaring

WORDT LID VAN HET GVIB, SPEEL OP ZEKER EN BEVEILIG SAMEN...



Informatiebeveiliging is reeds jaren lang een noodzakelijk, spannend en dynamisch vakgebied. Vrijwel alle beroepen hebben meer dan ooit te maken met vertrouwelijkheid, beschikbaarheid en integriteit van informatie. of u nu als directeur, manager, adviseur of programmeur werkzaam bent. Het Genootschap van Informatie Beveiligers (GvIB) kan u behulpzaam zijn bij al uw vraagstukken op het gebied van informatiebeveiliging.

Wat is het Genootschap van Informatie Beveiligers?
Het GvIB is een open, breed samengesteld genootschap waarin professionals elkaar vinden om professioneel inhoud te geven aan informatiebeveiliging, door het uitwisselen van ideeën, informatie, kennis, inzichten en vooral veel praktijkervaring.

Wat willen wij bereiken?
Wij willen de fysieke, (systeem)technische & organisatorische beveiliging van gegevens en van de gegevensverwerkende middelen tegen inbreuken van binnenuit of buitenaf bevorderen. Ook willen wij de uitwisseling van kennis en ervaring en het netwerken van de in het vakgebied werkzame personen bevorderen. Bijvoorbeeld door middel van deze expertbrief.

De doelgroep
De doelgroep van het GvIB omvat iedereen, die door studie of beroepshalve te maken heeft met informatiebeveiliging, of hiervoor een bijzondere belangstelling heeft. Het snel groeiende ledenbestand kent vele disciplines zoals studenten, informatiearchitecten, technici, managers, organisatieadviseurs, juristen, beveiligingsfunctionarissen en ICT auditors. Onze leden komen voort uit alle mogelijke opleidingen, bedrijven, overheden, organisaties en leveranciers.

Voor de diverse soorten van lidmaatschap verwijzen wij u gaarne naar:

http://www.gvib.nl/afy_info_ID_1022.htm