Informatiebeveiliging voor functioneel beheerders

SYSQA B.V. Almere

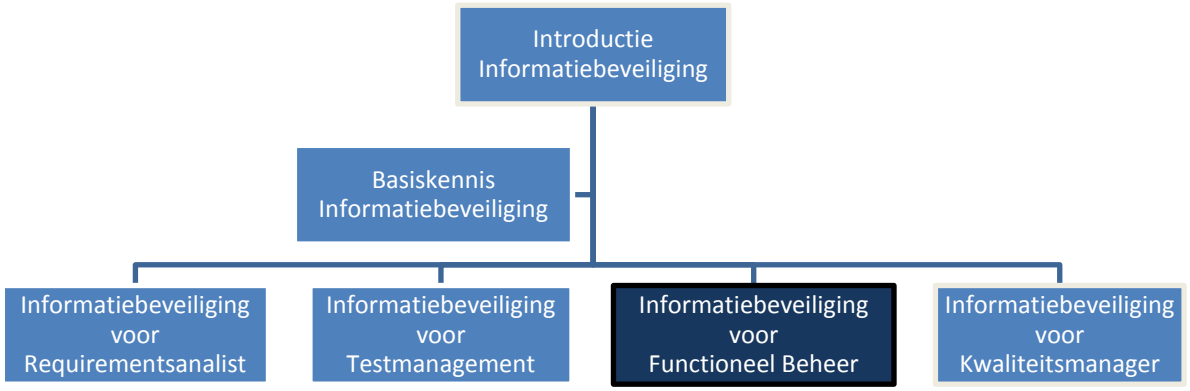
Datum : 16-04-2013
Versie : 1.0
Status : Definitief
Opgesteld door :

Inhoudsopgave

1 Inleiding

1.1.1 Relatie met andere documenten van expertisegroep Security

De expertisegroep Security van SYSQA B.V. heeft een set van documenten over informatiebeveiliging opgeleverd.



In donkerblauw is het voorliggende document weergegeven.

1.2 Doel en veronderstelde voorkennis

Dit document is bedoeld om functioneel beheerders meer handvatten te geven bij het uitvoeren van de beheertaken. Er wordt verondersteld dat de functioneel beheerder basiskennis heeft van informatiebeveiliging. Op de kennisbank van SYSQA staat een introductie tot informatiebeveiliging. Dit document verstrekt die basiskennis.
Verder kunnen de documenten voor requirementsanalist, testmanager en kwaliteitsmanager als aanvulling worden gezien. In die documenten worden per rol specifieke zaken beschreven waar een functioneel beheerder op z'n minst de hoofdlijnen behoort te weten.

Deze introductie gaat uit van een beheerorganisatie die is opgezet volgens het BiSL model. De vereiste basiskennis van het model is vastgelegd in het document "Introductie BiSL" dat op de kennisbank staat.

In deze introductie "Informatiebeveiliging voor functioneel beheerders" staan geen uitputtende beschrijvingen. Er worden vooral aandachtspunten benoemd om rekening mee te houden als het gaat om informatiebeveiliging. Dit document stelt de functioneel beheerder in staat om meer kritische vragen op het gebied van informatiebeveiliging te stellen in zijn of haar opdracht en daarmee informatiebeveiliging naar een hoger niveau te tillen.

1.3 Indeling van het document

In deze introductie wordt eerst een algemeen beeld geschetst van de verantwoordelijkheden die de functioneel beheerder heeft ten aanzien van de informatiebeveiliging. Vervolgens worden het uitvoerend niveau en het sturend niveau van BiSL belicht vanuit het oogpunt van informatiebeveiliging. In deze introductie is geen hoofdstuk opgenomen voor het richtinggevende niveau van BiSL. De kwaliteitsmanager vervult een rol in deze laag en hoe die rol kan worden ingevuld is beschreven in het document informatiebeveiliging voor kwaliteitsmanagers. De functioneel beheerders krijgen tips hoe tijdens het dagelijks werk invulling kan worden gegeven aan informatiebeveiliging.
Als laatste zijn referenties opgenomen naar interessante en relevante artikelen in relatie tot informatiebeveiliging.

2 Informatiebeveiliging voor functioneel beheerder

Binnen het werkgebied van functioneel beheer worden de behoeften aan informatievoorziening in het bedrijfsproces vertaald naar ondersteuning door geautomatiseerde en niet-geautomatiseerde informatievoorziening. Functioneel beheerders geven invulling aan de uitvoering van het beleid van de organisatie op deze onderwerpen en ondersteunen de gebruikers en het management ten aanzien van informatievoorziening.

Het beleid ten aanzien van informatiebeveiliging dat door de organisatie is opgesteld wordt door de functioneel beheerders ingevuld in het administratieve arbeidsproces en de geautomatiseerde informatievoorziening. Voor de functioneel beheer organisatie wordt de informatievoorziening in drie niveaus verdeeld:

- De coöperatieve informatievoorziening, de complete verzameling van alle systemen;
- Het bedrijfsproces, de verzameling systemen voor een afdeling of proces;
- Het systeem, een informatie voorziening voor een enkele taak.

Het beleid ten aanzien van informatiebeveiliging moet per niveau worden ingeregeld. Binnen elk niveau moet per proces of systeem worden bepaald welke maatregelen moeten worden genomen ten aanzien van informatiebeveiliging. Een algemene aanpak volstaat niet aangezien de risico's per proces of systeem binnen een bedrijfsproces uniek zijn.. Voorbeeld: De systemen waarin persoonsgegevens zijn opgeslagen vertegenwoordigen een zwaarder risico dan een kennisbank.

2.1 Beeldvorming van het niveau van informatiebeveiliging

Bij de aanvang van een opdracht zijn er een aantal manieren om een beeld te krijgen bij het niveau van informatiebeveiliging bij de opdrachtgever. De collega beheerders kunnen aangeven welke richtlijnen er gelden ten aanzien van informatiebeveiliging. Is er bijvoorbeeld voor elk systeem een eigenaar van de gegevens bepaald? Wordt deze eigenaar geraadpleegd als de functioneel beheerders een verzoek krijgen om gegevens buiten het systeem beschikbaar te maken?
Een security awareness training en een geheimhoudingsverklaring kunnen een onderdeel zijn van de startkwalificatie. De diepgang van de security awareness training is een indicatie van de inrichting van informatiebeveiliging. Mocht de organisatie geen security awareness training faciliteren, gebruik dit dan als aanleiding om door te vragen rondom het informatiebeveiligingsbeleid.
Requirementsdocumenten en/of specificaties van een systeem of wijziging bevatten optioneel een paragraaf over informatiebeveiliging. Deze documenten geven een indicatie van de aandacht voor informatiebeveiliging bij de realisatie of wijziging van een systeem.

3 Beheer op uitvoerend niveau

Het is belangrijk dat nieuwe bedrijfsprocessen en (niet-)geautomatiseerde systemen voldoen aan de informatiebeveiligingsrichtlijnen. Bij het opstellen of wijzigen van deze processen en systemen moet hierop worden getoetst. Een beheerder die een nieuw of gewijzigd proces of systeem in gebruik neemt, moet zich ervan bewust zijn wat dat voor consequenties heeft voor de informatiebeveiliging.
In hoeverre zijn de functioneel, applicatie en technisch beheerders betrokken bij bedrijfskritische processen? De beheerders hebben veel met de uitvoering van informatiebeveiligingsprocessen te maken. Zij voeren de informatiebeveiligingsmaatregelen uit. Daarnaast onderkennen de functioneel beheerders in veel gevallen als eerste een informatiebeveiligingsincident.
Zijn de functioneel beheerders, applicatie beheerders en technisch beheerders bekend met het informatiebeveiligingsbeleid en kennen ze het informatiebeveiliging incidentenproces?
Hoe is het patchbeleid? Loopt men ver achter of voert beheer een gebalanceerd beleid. Installeert men niet meteen alle patches i.v.m. risico's en wacht men totdat uit het veld/de markt genoeg zekerheid is?
Naast de beheerders zijn ook gegevens-, systeem- en proceseigenaren in het beheerproces betrokken. Zijn zij zich bewust van de nieuwe risico's die het gewijzigde of nieuwe systeem met zich meebrengt?

3.1 Informatiebeveiliging in het cluster gebruikersbeheer

De processen binnen gebruiksbeheer zorgen voor een continue en optimale ondersteuning bij het dagelijks gebruik van de informatievoorziening door de eindgebruikers. Door gebruikersbeheer uit te voeren wordt invulling gegeven aan het IB subdomein "Beschikbaarheid".

3.1.1 Aandachtspunten bij gebruikersondersteuning

Gebruikers die problemen ondervinden bij het gebruik van het informatiesysteem wenden zich tot de functioneel beheerder. Wanneer de problemen zijn ontstaan door onjuist gebruik van het systeem, assisteert de functioneel beheerder de gebruiker zodat het werkproces kan worden voortgezet. De problemen kunnen ook zijn ontstaan door fouten in de informatievoorziening of inefficiënt gekozen oplossingen. Van die situaties maakt de functioneel beheerder een issue dat de aanzet is voor een wijzigingsverzoek. Tijdens het administratieve proces waarbij gegevensinvoer en -uitvoer plaatsvindt, zijn de gegevens niet beschermd door IB maatregelen die in het informatiesysteem zijn gebouwd. Gebruikers kunnen bijvoorbeeld opdrachten aan functioneel beheerders verstrekken om gegevens van het informatiesysteem onbeveiligd beschikbaar te maken buiten de applicatie. De functioneel beheerders herkennen de situaties waarin potentieel sprake is van (opzettelijk) misbruik van de mogelijkheden om gegevens in en uit te voeren. De functioneel beheerder weet hoe moet worden gehandeld bij potentieel misbruik van in en uitvoer van gegevens en kent de routes om aanvragen voor informatie te toetsen aan het beveiligingsbeleid.

3.1.2 Beheer bedrijfsinformatie veilig uitvoeren

De inhoud van de informatievoorziening moet correct en actueel zijn om het systeem de gewenste uitkomsten te laten genereren. De bedrijfsinformatie speelt in dat proces een belangrijke rol. Bedrijfsinformatie is de verzameling van de parameters en bedrijfsregels die in de informatievoorziening zijn opgenomen. Het is belangrijk dat de bedrijfsinformatie gestructureerd beheerd wordt zodat de integriteit van de informatievoorziening gewaarborgd blijft. Wijzigingen in bedrijfsinformatie kunnen voortkomen uit de gebruikersondersteuning, wijzigingenbeheer, operationele ICT aansturing, technologische ontwikkelingen, de keten en behoeftemanagement.

3.1.3 Operationele ICT ondersteuning voor voldoende beschikbaarheid

De functioneel beheerder bewaakt de beschikbaarheid, capaciteit en bruikbaarheid van (de delen van) het informatiesysteem dat bij een ICT leverancier is ondergebracht. Niet alleen het systeem zelf wordt beheerd, maar ook de afspraken rondom verwerkingen en opdrachten en de afgesproken diensten vallen hier onder. Er kunnen bijvoorbeeld afspraken worden gemaakt over de momenten waarop het informatiesysteem beschikbaar moet zijn, of hoeveel belasting van het informatiesysteem moet kunnen worden afgehandeld. Al deze activiteiten worden uitgevoerd om te waarborgen dat informatievoorziening beschikbaar is wanneer de business of externe klant die nodig heeft om het primaire proces uit te voeren.

3.2 Informatiebeveiliging in het cluster Functionaliteitenbeheer

3.2.1 Specificeren van integere vernieuwing

De functioneel beheerder heeft een verantwoordelijkheid bij het verwerken van de IB eisen in de requirements en waar van toepassing in de (functioneel) ontwerpen. Bij collegiale review of inspectie van ontwerpdocumentatie reviewt de functioneel beheerder op IB aspecten. Bij de review worden bijvoorbeeld ISO 27001 en ISO 27002 (Information Security Management) als referentiekader gebruikt samen met de ISO 25000 (Software product Quality Requirements and Evaluation). Interne documenten met standaarden voor informatiebeveiliging worden eveneens als referentiekader gebruikt. De IB aspecten worden ondergebracht in de niet functionele kwaliteitseisen en de functionele kwaliteitseisen die de functioneel beheerder opstelt. De functioneel beheerder zorgt dat de beide vormen van kwaliteitseisen en de inrichting van het administratieve proces op elkaar aansluiten. De IB eisen die in het geautomatiseerde deel van het informatiesysteem zijn geïmplementeerd liggen in lijn met de IB maatregelen die in de administratieve organisatie zijn geïmplementeerd zodat de automatisering en het werkproces op elkaar aansluiten zonder dubbele maatregelen of witte vlekken.

De niet geautomatiseerde IV omvat de onderdelen van het proces die buiten de applicatie worden uitgevoerd. Ook buiten de applicatie is er sprake van informatiebeveiliging. Denk hierbij aan de uitvoer van gegevens naar een printer die beveiligd is met een pincode, een e-mail die versleuteld wordt verstuurd of documenten die in een afgesloten kast moeten worden bewaard. Gegevens zijn beschermd door een applicatie zolang de gegevens binnen de beveiligde applicatie blijven. Als gegevens worden afgedrukt op een printer en de gebruiker laat de print onbeheerd achter, dan liggen gegevens die in een applicatie worden beschermd tegen ongeautoriseerd raadplegen toch 'op straat'. Autorisatiebeheer om te voorkomen dat gegevens kunnen worden uitgevoerd kan een oplossing zijn.

Bij testen van het gerealiseerde softwarepakket moet de beheerder er aan denken om naast de functionele specificaties ook testgevallen uit te voeren op de niet functionele specificaties. Bij de teststrategie moet expliciet overwogen worden of beveiliging van belang is en of er dus beveiligingstesten moeten worden uitgevoerd.

Onder het voorbereiden van de transitie wordt een plan gemaakt om de nieuw gerealiseerde informatievoorziening te implementeren binnen de gebruikersorganisatie. Het invoeren van de onderdelen van het proces die zijn ontworpen in het kader van IB wordt hierin ook gepland. Een goed voorbereide transitie zorgt er voor dat wijzigingen soepel worden ingevoerd in de organisatie. De beschikbaarheid van de dienstverlening wordt hiermee gewaarborgd.

3.2.2 Veilig uitvoeren van het administratieve proces

Bij de verwerking van gegevens buiten een geautomatiseerd systeem om is ook sprake van informatiebeveiliging. Formulieren met gegevens over functioneringsgesprekken moeten bijvoorbeeld in een afgesloten kast worden bewaard tot ze zijn ingevoerd in het informatiesysteem. De processen die buiten het geautomatiseerde systeem worden uitgevoerd moeten ook voldoen aan de eisen van informatiebeveiliging. Bij het opstellen van deze processen zorgt de functioneel beheerder weer voor een juiste implementatie van de informatiebeveiliging.

3.3 Verbindende processen op het uitvoerende niveau

De verbindende processen wijzigingenbeheer en transitie hebben geen activiteiten voor informatiebeveiliging. In deze processen wordt nog niet, of niet meer gewerkt aan de inhoud van informatievoorziening. Binnen wijzigingenbeheer wordt besloten of een wijziging wel of niet wordt doorgevoerd. De wijziging wordt inhoudelijk niet behandeld, maar wel beoordeeld. Vanuit het perspectief van prioriteren en de controle of (een set van) wijzigingen impact hebben op de informatiebeveiliging is het van belang dat functioneel beheerders betrokken zijn bij de samenstelling van releases/patches/updates. Bij transitie wordt de gewijzigde informatievoorziening geïmplementeerd in de gebruikersorganisatie. In deze fase wordt de inhoud van de informatievoorziening niet meer ontworpen of gerealiseerd.

4 Beheer op sturend niveau

4.1 Planning en Control

Planning en control is verantwoordelijk voor de aansturing ten aanzien van tijd en inzet van mensen. Vanuit de richtinggevende laag van het BiSL model worden richtlijnen en standaarden opgelegd voor het informatiebeveiligingsdomein. Binnen planning en control moet zorg worden gedragen dat deze richtlijnen en standaarden in releases worden ingepland zodat deze tijdig kunnen worden gerealiseerd. De visie op informatiebeveiliging die op het richtinggevende niveau wordt ontwikkeld moet in de sturende laag worden vertaald naar praktisch uitvoerbare plannen. Planning en Control zorgt dat er op het juiste moment mensen en middelen beschikbaar zijn om IB maatregelen te implementeren.

4.2 Financieel management

Financieel management is verantwoordelijk voor het maken, onderhouden en bewaken van een kosten efficiënte informatievoorziening. Bij een investeringsbeslissing worden de baten van de investering bepaald. Informatiebeveiliging heeft geen directe financiële opbrengst, de baten moeten dus op een ander vlak worden gezocht. Informatiebeveiliging beperkt risico's op verminderde beschikbaarheid van het informatiesysteem, onvoldoende integriteit van de gegevens die worden verwerkt en ongeoorloofd gebruik van gegevens. Wanneer een bedrijf op deze gebieden tekort schiet heeft dit invloed op de afnemers van de producten of diensten. Afnemers kiezen na incidenten op een van de gebieden beschikbaarheid, integriteit of vertrouwelijkheid voor een andere aanbieder van de dienst of het product. Het verlies van afnemers en dus inkomsten moet door het financieel management worden betrokken bij het besluit om een wijziging door te voeren. Het financieel management moet voor de verschillende systeemonderdelen in kaart brengen waar financiële risico’s liggen en hoe groot die zijn. De financiële risicoanalyse is nodig om te bepalen op welke systeemonderdelen en functies IB maatregelen nodig zijn.

4.3 Behoeftemanagement

Een van de aandachtsgebieden van behoeftemanagement is informatiekwaliteit. De andere zijn ergonomie, geschiktheid, randvoorwaarden en eisen. Behoeftemanagement wordt gevoed vanuit de uitvoerende en richtinggevende bedrijfsprocessen. Bij het uitvoeren van het bedrijfsproces worden suggesties gedaan om de informatievoorziening aan te passen zodat die geschikter wordt voor dagelijks gebruik. Sommige van de behoeften van het bedrijfsproces vallen binnen het domein van informatiebeveiliging. De behoeften van het bedrijfsproces ten aanzien van informatiebeveiliging worden als zodanig herkend. Binnen behoeftemanagement wordt de afstemming gemaakt met planning en control om de behoefte al dan niet aan te merken om te realiseren. Een behoefte kan ook het startpunt zijn voor de richtinggevende laag om de visie op informatiebeveiliging te herzien.

4.4 Contract management

De afspraken die met de leverancier zijn gemaakt over ondersteuning van de informatievoorziening staan centraal bij contractmanagement. De beschikbaarheid van de informatievoorziening is beslist een domein waarover afspraken moeten worden gemaakt. Er moet bijvoorbeeld een optimum worden gevonden voor de beschikbaarheid van een informatiesysteem. Een hoge beschikbaarheid brengt hoge kosten met zich mee. Een (te) lage beschikbaarheid kost de organisatie goodwill en omzet. Contract management zal om deze reden in nauwe samenhang worden uitgevoerd met financieel management

Gegevens en hele systemen kunnen bij een leverancier worden ondergebracht omdat dat voordelen met zich meebrengt. Een aanbieder van cloud oplossingen neemt de zorg voor een deel van het beheer over zodat de business zich kan richten op haar kernactiviteiten. Met een cloud oplossing legt de organisatie een applicatie of de gegevens die de applicatie bevat of beide onder bij een externe partij. De partij die gebruik maakt van de cloud oplossing moet nadenken over de afspraken die met de leverancier worden gemaakt over de toegang tot de applicatie, de toegang tot de gegevens binnen de applicatie en de back-ups die van de gegevens worden gemaakt. De beveiligingseisen die aan de eigen beheersorganisatie zouden worden gesteld, moeten ook worden toegepast op de externe leverancier er moet worden nagedacht of er aanvullende eisen nodig zijn aangezien gegevens zijn opgeslagen zijn op een fysieke locatie die buiten het bedrijf ligt. Gevoelige gegevens kunnen versleuteld opgeslagen worden in de database zodat alleen de eigenaar van de gegevens deze kan benaderen.

5 Bijlage1

5.1 Bronvermelding en overige informatie

Links naar richtlijnen en standaarden:

ISO 25010	http://nl.wikipedia.org/wiki/ISO_25010
ISO 27001	https://nl.wikipedia.org/wiki/ISO/IEC_27001
ISO 31000	https://en.wikipedia.org/wiki/ISO_31000

Vraag bij product management na of er exemplaren van de ISO normen beschikbaar zijn binnen SYSQA.

Bronvermelding
Remko van der Pols, Ralph Donatz, Frank van Outvorst (2012)
BiSL - Een framework voor business informatiemanagement; Haren Publishing
ISBN 10: 9087536879; ISBN 13: 9789087536879