Informatieveiligheidsbeleid SURF

Strategisch beleid

Auteur(s) : CISO-team
Versie : 1.3
Datum : 3 mei 2023

Inhoudsopgave

Voorwoord

Informatie is een belangrijke asset voor SURF en haar leden. Informatie dient niet alleen op een makkelijke manier verzameld, bewaard en ontsloten te worden: gegevens dienen ook veilig te zijn. Dat is een belang dat niet alleen voor SURF groot is, maar ook voor alle mensen die bij instellingen werken en studeren en samen met SURF medewerkers dagelijks gebruik maken van onze gezamenlijke ICT-infrastructuur. Informatieveiligheid is bovendien een belangrijke motivator en facilitator van vernieuwing.

Veiligheid kan op gespannen voet staan met andere wensen zoals efficiëntie en gebruiksvriendelijkheid. Door het hanteren van best practices en principes creëren we een duidelijk kader waarbinnen informatieveiligheid passend kan worden geborgd aan de hand van vijf principes. Er is geen algemeen geldende oplossing: het gaat erom per situatie de juiste keuzes te maken. Deze principes worden toegepast op onze interne bedrijfsvoering, maar ook op onze SURF diensten.

Wij zijn trots op de kwaliteit van SURF dienstverlening aan instellingen en willen dat aantoonbaar maken. Met het uitspreken van onze ambitie om onze ISO 27001 certificering voor een groot deel van onze diensten te behouden en uit te breiden leggen we de lat hoog. Dat doen we bewust, omdat de aantoonbaarheid van onze kwaliteitsstandaard belangrijk is voor ons en onze leden.

Bij SURF zit security in ons DNA, maar we moeten niet vergeten dat veilig met informatie omgaan een continue inspanning vraagt van al onze medewerkers en gebruikers. Gedrag en bewustzijn zijn ontzettend belangrijk omdat kleine acties zoals het klikken op een link, kunnen leiden tot een grootschalige ransomware aanval. Hoewel het bewustzijn bij SURF hoog is, is ook SURF kwetsbaar voor cyberaanvallen en incidenten. Daarom besteden we veel aandacht aan de menselijke kant in onze veiligheidsprincipes. Samen bouwen we aan een veilige onderwijs en onderzoeksomgeving voor Nederland.

Jet de Ranitz
Voorzitter Raad van Bestuur

1 Inleiding

SURF is de coöperatie voor innovatieve IT-diensten aan het Onderwijs en Onderzoek. Het succes van SURF hangt sterk samen met de kwaliteit van het verwerken van informatie, het meenemen van veiligheid bij het ontwikkelen van nieuwe technologieën en het beveiligen van onze computersystemen. We kunnen niet meer zonder het digitaal verzamelen, vastleggen en delen van informatie met zowel interne als externe partners en collega's. Bovendien ontwikkelt en levert SURF innovatieve IT-diensten aan haar instellingen en fungeren we als kennisinstituut voor het Onderwijs. Onze missie: "SURF maakt betrouwbare en innovatieve ICT-voorzieningen mogelijk, waarmee het Nederlandse onderwijs en onderzoek kan uitblinken." De diensten van SURF moeten aan een hoge kwaliteitsstandaard voor informatieveiligheid voldoen om dit voor instellingen mogelijk te maken.

De digitale werkelijkheid is constant in beweging en dat brengt steeds nieuwe en andere risico's met zich mee voor de Informatieveiligheid. De risico's vormen een bedreiging voor de kwaliteit en continuïteit van processen en voor het behalen van de strategische doelen van SURF als ook de aangesloten instellingen. De bedreigingen kunnen de beschikbaarheid, integriteit en vertrouwelijkheid van informatie beïnvloeden. Voorbeelden van bedreigingen zijn kwetsbaarheden in systemen of ongeautoriseerde toegang tot informatie. Dit kan de kwaliteit van onze diensten aan onze instellingen beïnvloeden en bij incidenten tot reputatieschade leiden.
Ook de privacy van medewerkers, docenten, studenten, onderzoekers en gasten kan schade oplopen. Informatiebeveiliging is daarom van cruciaal belang.

Informatieveiligheid vraagt steeds om bijstelling zodat er een passend beveiligingsniveau blijft. Dat komt onder andere door nieuwe dreigingen en kwetsbaarheden, de aangescherpte eisen om te voldoen aan de wet- en regelgeving rondom gegevensbescherming en privacy (AVG), en de afspraken met onderzoek- en onderwijspartners.

Het verkleinen en beheersen van de risico's vraagt om inspanningen op organisatorisch, procesmatig en technologisch vlak. Daarnaast moeten bestuurders, medewerkers en gasten van SURF zich ook bewust worden van de risico's en hun handelen daarop afstemmen.

Informatieveiligheid is niet te bereiken door alleen een aantal technische en organisatorische maatregelen vast te stellen. Door de continue veranderende omstandigheden is het een dynamisch proces. Een vijftal informatieveiligheidsprincipes zijn leidend voor informatieveiligheid binnen SURF. Maatregelen, procedures en richtlijnen en eventuele interpretaties worden hieraan getoetst.

Er zijn belangrijke relaties tussen informatierisico's en risico's op andere deels overlappende veiligheidsthema's zoals internationale veiligheid en crisismanagement. Dit beleid is onderdeel van integrale veiligheid bij SURF. Bij het opstellen van het beleid is gebruik gemaakt van het SURF SCIPR Model Informatieveiligheidsbeleid.

In het voorliggend beleid zijn de best practices van de voormalig SURF werkmaatschappijen samengebracht en geharmoniseerd. Tevens is het geactualiseerd aan nieuwe dreigingen en ontwikkelingen rond security. Het vervangt daarmee alle voorgaand beleid op dit onderwerp.

2 Kaders en ambitie

2.1 Informatieveiligheid en informatiebeveiliging

De begrippen informatieveiligheid en informatiebeveiliging worden vaak door elkaar gebruikt, maar ze hebben niet dezelfde betekenis. Informatieveiligheid richt zich op het beschikbaar, integer en vertrouwelijk houden van informatie. Hiervoor moeten informatie en informatiesystemen beschermd worden tegen mogelijke bedreigingen. Dit wordt gedaan door het nemen, onderhouden en controleren van beveiligingsmaatregelen, ook informatiebeveiliging genoemd. De eindverantwoordelijkheid voor informatieveiligheid ligt bij de Raad van Bestuur (RvB) van SURF.

Dit informatieveiligheidsbeleid draagt eraan bij dat SURF voldoet aan de van toepassing zijnde wet- en regelgeving, waaronder de AVG, wettelijke bewaartermijnen, de auteurswet, de Wet beveiliging netwerk- en informatiebeveiliging (Wbni) en de Wet Computercriminaliteit III.

De reikwijdte van dit informatieveiligheid beleid is zowel de interne bedrijfsvoering, de diensten die SURF ontwikkelt en de diensten die door SURF aangeboden worden aan de instellingen.

2.2 Ambitie en doelstellingen

Ambities

- SURF wil een voorbeeld zijn op het gebied van security voor haar instellingen voor zowel kennis- en informatiesysteemveiligheid;
- Interne gebruikers van diensten en voorzieningen zijn zich bewust van informatieveiligheidsrisico's en stemmen hun handelen en gebruik van (digitale) hulpmiddelen hierop af;
- SURF wil de kwaliteit van de dienstverlening aan gebruikers verbeteren waarbij een goede balans is gevonden tussen informatieveiligheid en andere aspecten zoals functionaliteit, gebruiksvriendelijkheid, kosten en privacy;

Doelstellingen

- SURF wil als organisatie en voor diensten aantoonbaar volwassenheidsniveau 3 halen zoals in het Normenkader Informatiebeveiliging HO beschreven staat;
- SURF laat het deel van de dienstverlening waarbij SURF een leveranciersrol vervult waarbij ISO-certificering marktconform is, de implementatie van informatieveiligheid toetsen door certificering tegen ISO27001;
- SURF wil het aantal security-incidenten met een "Aanzienlijke" of "Catastrofale" impact, zoals gedefinieerd in het "Business Impact Criteria en Risico Acceptatie Criteria" document van SURF, tot nul beperken;
- SURF wil de downtime in de SURF services die optreedt als gevolg van een security incident, waarbij de downtime redelijkerwijs door SURF voorkomen had kunnen worden, tot nul beperken.

2.3 Kennis- en informatiesystemenveiligheid

Het informatieveiligheidsbeleid gaat enerzijds over kennisveiligheid en anderzijds over gepaste beveiliging van de IT-hulpmiddelen (informatiesysteemveiligheid).

Kennisveiligheid betreft de gepaste en bewuste veilige omgang met informatie en het verantwoord gebruik van betrokken (IT-)middelen. Hierbij wordt informatie breed geïnterpreteerd en omvat alle vormen van informatie (dus niet alleen digitale informatie) die SURF of haar relaties genereren en beheren.

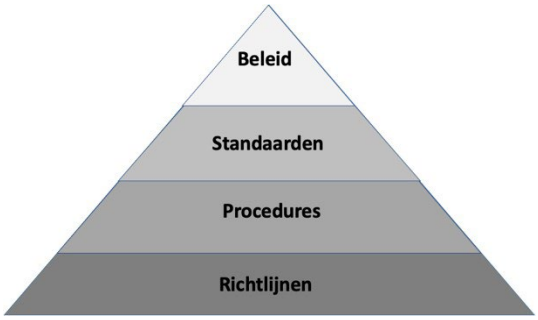
Informatiesysteemveiligheid draait om het aanbieden van passende diensten en IT-hulpmiddelen om kennisveiligheid te ondersteunen. Dit is locatie-onafhankelijk en omvat alle IT-diensten (zowel door SURF zelf als extern beheerd) en (digitale) hulpmiddelen, zowel zakelijk als privé-eigendom, waarop informatie van SURF verwerkt of opgeslagen wordt.

Zodoende richt het informatieveiligheidsbeleid zich op de volgende twee doelgroepen:

1. In het kader van kennisveiligheid: alle gebruikers van informatie van SURF (medewerkers, gasten en externe relaties).
2. In het kader van informatiesystemenveiligheid: alle aanbieders van IT-systemen en diensten

2.4 Security documentatie

De documentatie voor informatieveiligheid bestaat uit vier lagen. De bovenste drie lagen zijn documenten die verplicht zijn.



Op strategisch niveau bevinden zich beleidsstukken. Beleid beantwoordt de vraag waarom wij informatieveiligheid belangrijk vinden en waar wij op richten. Een voorbeeld van beleid is het Informatieveiligheidsbeleid.

Op tactisch niveau worden standaarden beschreven waar SURF aan voldoet. Deze documenten beantwoorden de vraag wat we gaan doen en geven aan hoe wij zaken inrichten. Voorbeelden van standaarden zijn de Baseline Informatiebeveiliging SURF en het ISMS-handboek.

Op operationeel niveau worden procedures beschreven. In deze documenten wordt beschreven hoe wij omgaan met informatieveiligheid, en hoe wij onze taken verrichten. Een voorbeeld van een procedure is de incident procedure.

De vierde laag bevat richtlijnen. Richtlijnen helpen ons om standaarden te vertalen naar pragmatische oplossingen. Vaak zijn er meerdere manieren om een standaard te vertalen naar een concrete maatregel. Voorbeelden zijn richtlijnen voor cryptografie of het instellen van

security headers. Richtlijnen zijn bedoeld om de organisatie houvast te geven en zijn niet verplicht.

2.5 Security control framework

Naast dit beleidsstuk zijn er zowel voor kennisveiligheid als voor veiligheid van informatiesystemen risico-gebaseerde control frameworks inclusief baselines die de vereiste controlemaatregelen nader specificeren en operationele richtlijnen bevatten. Deze sluiten aan bij het specifiek voor onderwijs- en onderzoeksinstellingen ontwikkelde SURF Normenkader Informatie Beveiliging Hoger Onderwijs (IBHO). Het IBHO is gebaseerd op best practices zoals die zijn vastgelegd in de ISO-27000-serie. Het IBHO omschrijft een norm voor de volwassenheid van de informatiebeveiliging volgens volwassenheidsniveaus uit het NBA-model.

Hieronder volgt een opsomming van de verschillende aandachtsgebieden van het security control framework. Het security control framework wordt door de Chief Information Security Officer (CISO) vastgesteld, periodiek geactualiseerd en geijkt om gepaste beschermingen tegen dreigingen te nemen.

Kennisveiligheid	Veiligheid van informatiesystemen
• Gebruik van geschikte IT-middelen • Informatieveiligheid Bewustwording • Clear Desk, Clear Screen • Screening Personen • Dreigingsmanagement en Anti-spionage • Autorisaties • In dienst – Doorstroom - Uit dienst • Procedures Thuiswerken • Sancties • Geheimhoudingsverklaringen en Verplichtingen • Draagbare Media en Procedures bij Dataoverdracht • Leveranciersmanagement • Data Archivering en Dataretentie • Crisis en Incidentbeheer • Project en Verandermanagement	• Beheer IT Bedrijfsmiddelen en Diensten • Gevoelige Toegangsbeheersing • Kwetsbaarhedenmanagement • Netwerkbeveiliging • Logging & Monitoring • Uptime en Beschikbaarheidsmonitoring • Beveiligingsmonitoring • Werkplekbeveiliging • Identiteit en Toegangsbeheer • Fysieke Beveiliging • Back-up en Terugzetten • Veilige Softwareontwikkeling • Preventie van Datalekken • Applicatiebeveiliging • Systeemverharding en Patchmanagement • Dataretentie en Verwijdering • Systeemcommunicatie • Incidentprocessen • Gebruiksvoorwaarden en Handleidingen • Certificaat en Sleutelbeheer

2.6 Vaststelling en wijzigingen

De RvB stelt dit informatieveiligheidsbeleid vast. Minimaal één keer per 3 jaar, of na een substantiële verandering van het instellingsbeleid of belangrijke ontwikkelingen op cyberveiligheidsgebied, wordt het beleid geëvalueerd en indien nodig bijgesteld en opnieuw vastgesteld.

3 Beleidsprincipes

3.1 Informatieveiligheidsprincipes

SURF heeft vijf beleidsprincipes voor informatieveiligheid vastgesteld. Deze helpen om te bepalen welke beveiligingsmaatregelen er nodig zijn. Een beleidsprincipe heeft een naam en bestaat uit een kern, korte uitleg met achtergrond en de belangrijkste implicaties.

Maatregelen uit de baselines zijn niet altijd toepasbaar in alle situaties. In die gevallen moeten er vervangende maatregelen genomen worden waarmee het achterliggende principe tot zijn recht komt en de risico's voldoende afgedekt worden, volgens het uitgangspunt "*Comply or explain*". De specifieke maatregelen gaan over "*comply*" en de principes dienen als referentie voor "*explain*". Om vast te stellen of vervangende maat- regelen leiden tot een acceptabel restrisico worden deze getoetst worden aan de beleidsprincipes.

De vijf hierna vermelde beleidsprincipes helpen bij de communicatie over en de implementatie van het informatieveiligheidsbeleid. Op basis van deze vijf beleidsprincipes zijn controlemaatregelen geformuleerd die relevant zijn voor de bescherming van informatie en processen van SURF.

3.2 Principe: Risicogebaseerd

	Risicogebaseerd Informatiebeveiliging is risicogebaseerd 
Kern	We baseren de maatregelen op de mogelijke veiligheidsrisico's van onze informatie, processen en IT-faciliteiten.
Achtergrond	Het delen van kennis (openheid) is een belangrijke kernwaarde van SURF. Voor een goede risicoafweging bij het beschermen van informatie en het treffen van de juiste maatregelen, is het van belang om de waarde van informatie via informatieclassificatie vast te stellen. Als de waarde van informatie bekend is kan een bij de risico's passende mate van beveiliging worden bepaald. Proportionaliteit daarin is gewenst mede om de beschikbare financiële middelen efficiënt te gebruiken.

Implicaties	• Voor alle informatieverwerkingen bepaalt de gegevensverantwoordelijke de informatieclassificatie. Een beperkte business impact assessment is onderdeel van de classificatie. • Een gegevensbeschermingseffectbeoordeling (DPIA – Data Protection Impact Assessment) in het kader van de AVG (Algemene Verordening Gegevensbescherming) maakt, indien persoonsgegevens betrokken zijn, onderdeel uit van de risicoanalyse. • Maatregelen worden getroffen om het vastgestelde risico ten aanzien van beschikbaarheid, integriteit en vertrouwelijkheid naar het geaccepteerde niveau te brengen. • Informatiesets hebben één gegevensverantwoordelijke en een gedefinieerde bron. • Gegevens-, systeem- en procesverantwoordelijke zijn belast met de implementatie en operationele handhaving van controlemaatregelen op basis van het uitgangspunt van "*comply or explain*". • Afwijkingen kunnen worden geaccepteerd binnen de risicobereidheid van SURF. • Voor afwijkingen moet het risico-acceptatieproces worden gevolgd. Afhankelijk van mogelijke impact vindt acceptatie op een passend managementniveau plaats. • Maatregelen zijn zo ingericht dat hun effect meetbaar en dus controleer en aantoonbaar is. • De relatief hoogste risico's (rekening houdend met vereiste inspanningen) worden als eerste gemitigeerd. • Maatregelen zijn qua kosten in balans met de vermindering van risico's (proportionaliteitsprincipe). • SURF blijft verantwoordelijk voor adequate bescherming van informatie bij gebruik van externe diensten en leveranciers voor informatieverwerking. Waar van toepassing bevatten contracten veiligheidseisen en/of eisen ten aanzien van externe toetsing/certificering die compliance aantonen.

3.3 Principe: Iedereen

	Iedereen Informatiebeveiliging is een verantwoordelijkheid van iedereen 
Kern	Iedereen is en voelt zich verantwoordelijk voor een juist en veilig gebruik van middelen en bevoegdheden.

Achtergrond	Iedereen is zich bewust van de waarde van informatie en handelt daarnaar. Deze waarde wordt bepaald door de mogelijke schade als gevolg van verlies van beschikbaarheid, integriteit of vertrouwelijkheid. Van zowel medewerkers als derden wordt verwacht dat ze bewust omgaan met informatie in welke vorm dan ook en dat ze actief bijdragen aan de veiligheid van de geautomatiseerde systemen en de daarin opgeslagen informatie. Het succes van beveiliging staat of valt met goede communicatie. Deze communicatie wordt daarom actief bevorderd, op en tussen alle niveaus binnen SURF.
Implicaties	• Alle gebruikers worden actief geïnformeerd over hun verantwoordelijkheden ten aanzien van het gebruik van digitale middelen en informatie. Dit is vastgelegd in de zogenaamde Acceptabel Use Policy (AUP) dat ook de kaders voor monitoring en toezicht/controle van gebruikers bevat. • Schending van wetgeving, voorschriften en regels op gebied van informatiebeveiliging kan leiden tot sanctionerende maatregelen. • Het veilig omgaan met informatie en informatiedragers is een onderdeel van de arbeidsovereenkomst van alle medewerkers. • Informatieveiligheid krijgt aandacht bij indiensttreding van medewerkers en bij jaargesprekken en periodieke overleggen. • Informatieveiligheid krijgt aandacht in reguliere overleggen in afdelingen en projecten. • Medewerkers spreken elkaar aan op onveilige omgang met informatie en systemen. • Medewerkers melden security-incidenten en (vermoedens van) kwetsbaarheden bij het SIRT.

3.4 Principe: Altijd

	Altijd Informatiebeveiliging is een continu proces 
Kern	Informatiebeveiliging zit in het DNA van al onze werkzaamheden.
Achtergrond	De omgeving verandert continu; cyberdreigingen nemen toe en af; processen veranderen, medewerkers inhuurkrachten en gasten veranderen et cetera. Eenmalig de maatregelen bepalen en implementeren is onvoldoende om een veilig klimaat te behouden. Informatiebeveiliging heeft alleen zin als dit een continu proces is van het nemen van maatregelen, bewustzijn en controles.

Implicaties	• Er wordt een Information Security Management Systeem (ISMS) ingericht waarmee door middel van een verbetercyclus (plan, do, check en act) implementatie van het informatieveiligheidsbeleid en controlemaatregelen risicogebaseerd opgevolgd en verbeterd worden. • Periodiek worden audits en assessments uitgevoerd om het beleid en de genomen maatregelen te controleren op effectiviteit (controleerbaarheid). • Bij instroom van nieuwe medewerkers is er aandacht voor de bewustwording van de risico's en de beveiligingsprocedures van SURF rond toegang en gebruik van informatie en (privé) IT-middelen. • Periodiek worden accounts met hoge privileges gevalideerd. • SURF organiseert regelmatig cybersecurity-awareness activiteiten voor de diverse doelgroepen binnen en verbonden aan SURF. • Bij aanpassingen in rollen, taken, en verantwoordelijkheden van een persoon worden ook de autorisaties daarmee in overeenstemming gebracht en aangepast. • Er is een proces ingericht om het dreigingsbeeld voor SURF te bepalen en periodiek bij te stellen. Nieuwe dreigingen leiden waar nodig tot aanpassing van maatregelen. • Tevens is er een operationeel SOC (Security Operations Center) ingericht om dreigingen proactief in kaart te brengen en hierop reactief snel te kunnen reageren bij incidenten.

3.5 Principe: Security by Design

	Security by Design Integrale aanpak informatiebeveiliging 
Kern	Informatiebeveiliging is vanaf de start een integraal onderdeel van ieder project of iedere verandering met betrekking tot informatie, processen en IT-faciliteiten.
Achtergrond	*Security by Design* betekent dat al tijdens de start van een project, het ontwerp van een nieuwe applicatie of IT-omgeving en bij technische of functionele veranderingen rekening wordt gehouden met de beveiliging van gegevens en de continuïteit van de processen. Dit voorkomt (vaak dure) herstelwerkzaamheden achteraf.

Implicaties	• Voor elk nieuw project/software-inkoop/innovatie worden de security-eisen (control framework) vanaf de start meegenomen. • Security is integraal onderdeel van architectuur en kaders vanuit het control framework worden meegenomen in relevante architectuur producten. • Voor een dienst of product live gaat wordt de toepassing van de security eisen getoetst en/of getest. • Bij elk IT-systeem of inrichting wordt ter bevordering van informatiebeveiliging het principe van *least privilege* en *need to know* gehanteerd. Dat betekent dat er niet meer rechten verleend worden dan nodig zijn voor adequate functie- en bedrijfsuitoefening. • Scheiding van verantwoordelijkheden wordt toegepast in processen en procedures (denk hierbij aan onderscheid tussen gebruikers en functioneel of technisch beheerders). • Toegang is persoonsgebonden en tot natuurlijke personen te herleiden. • Er wordt een richtlijn security in projecten vastgesteld, gebaseerd op de maatregelen die voortkomen uit de informatieclassificatie en maatregelen die mogelijk voortvloeien uit de gegevensbeschermingseffectbeoordeling in het kader van de AVG.

3.6 Principe: Security by Default

	Security by Default Standaard veilig en beperkt toegang 
Kern	Gebruikers hebben alleen toegang tot informatie en IT-faciliteiten die zij nodig hebben voor hun werkzaamheden. Het openstellen van informatie is een bewuste keuze.
Achtergrond	*Security by Default* betekent dat in elke configuratie de aanwezige security opties standaard geïmplementeerd worden en zodoende wordt informatieveiligheid zo veel mogelijk geborgd. Dit voorkomt ongewenste en ongecontroleerde toegang tot (persoons)gegevens. Openstellen van informatie is daarmee altijd een bewuste keuze na een zorgvuldige afweging.

Implicaties	• In de beveiligingsbaseline zijn de standaarden voor de configuratie van informatiesystemen is vastgelegd. • Het principe bij initiële inrichting van een informatiesysteem of een infrastructuur is "*dicht, tenzij*". • Afwijking van de initiële inrichting volgt het principe "*Comply or explain*." • Security is geborgd in het change- en architectuurmanagementproces. • Toegang tot informatie is rol-gebaseerd, waardoor gebruikers alleen toegang hebben tot informatie die zij nodig hebben voor hun werkzaamheden (vastgelegd in een autorisatieschema) dan wel bepaalt de informatie-eigenaar zelf wie toegang krijgt. • Logging- en auditprocessen zijn zodanig ingeregeld dat toegang tot informatie en IT-systemen herleidbaar is naar individuen.

4 Governance

4.1 ISMS-handboek

Hieronder worden kort een aantal governance-onderdelen benoemd. Deze onderdelen zijn verder uitgewerkt in het ISMS-handboek. Het ISMS-handboek beschrijft hoe de governance van informatieveiligheid ingericht is en wat de taken en verantwoordelijkheden zijn van de verschillende managementniveaus. Omdat informatieveiligheid risico gebaseerd is, bevat het ISMS-handboek ook een beschrijving van Risk Management en de bijbehorende verbetercyclus. Security Incident beheer is hier verder uitgewerkt, en bewustwording en training. Het ISMS-handboek wordt door de Chief Information Security Officer (CISO) vastgesteld en periodiek geactualiseerd en geijkt.

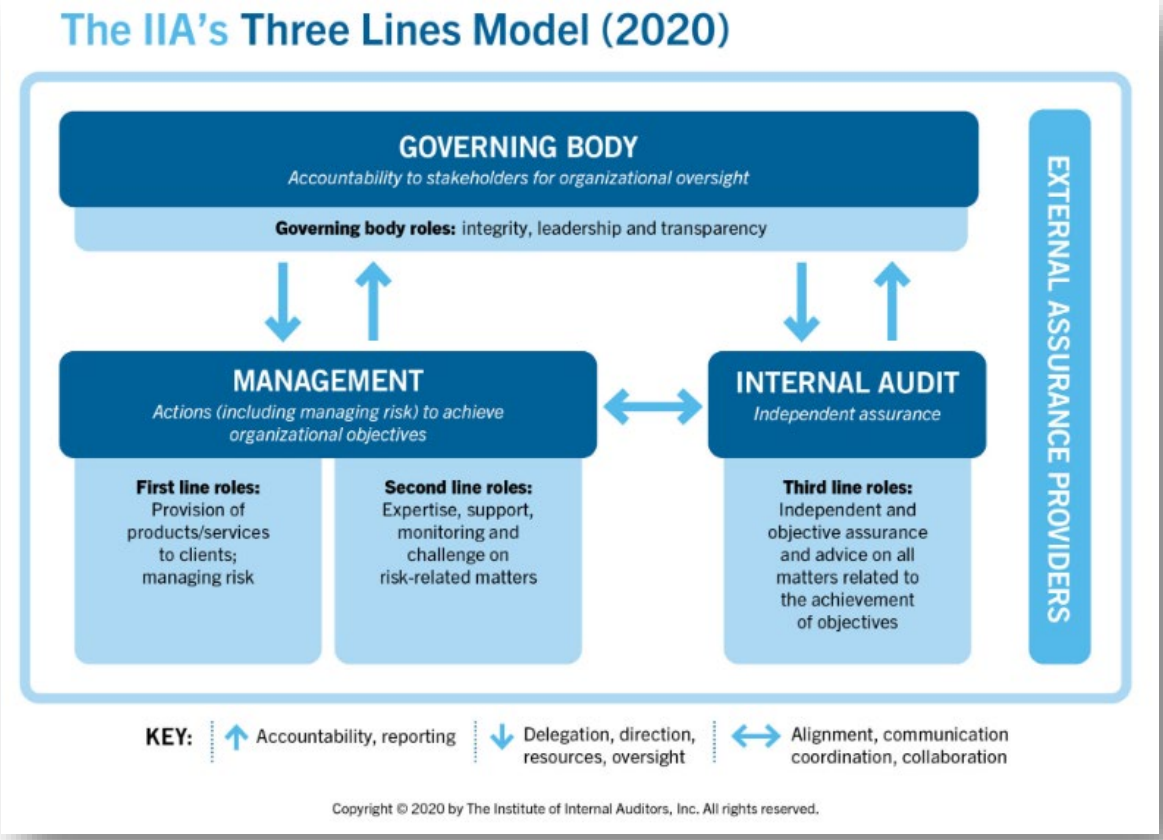
4.2 Managementniveaus

De verantwoordelijkheden in het kader van de governance van informatieveiligheid zijn verdeeld over de organisatorische managementniveaus strategisch, tactisch en operationeel met bijbehorende rollen, verantwoordelijkheden, overlegvormen en rapportagelijnen. Deze rollen en verantwoordelijkheden worden uitvoeriger beschreven in het ISMS-handboek.

Strategisch	RvB, afdelingsmanagers, CISO
Tactisch	(Information) Security Officers
Operationeel	SOC, SIRT

4.3 Three Lines Model

De IB-Governance bij SURF is ingericht volgens het Three Lines Model. Dit model wordt algemeen toegepast als model om Governance, Risk en Compliance (GRC) te borgen in een operationele organisatie. Dit model wordt verder toegelicht in het ISMS-handboek.



Figuur: Three Lines Model (bron: The Institute of Internal Auditors)

4.4 Risk management en verbetercyclus

Het ISMS (Information Security Management System) is ondersteunend aan de doelstelling om informatieveiligheid over een langere periode op een steeds hoger niveau uit te voeren. Het hebben van een ISMS is geen eenmalige activiteit of een project. Het is een voortdurend risk-management proces dat binnen de organisatie uitgevoerd wordt. Voor het uitvoeren van informatiebeveiliging wordt binnen het ISMS gewerkt via een verbetercyclus, zoals de PDCA-cyclus. PDCA staat hierbij voor plan (beleid), do (uitvoering), check (meten) en act (planning).

Op basis van het ISMS maakt de CISO jaarlijks een verslag voor de RvB over het afgelopen jaar en een jaarplan op hoofdlijnen voor het komende jaar. Het jaarverslag is mede gebaseerd op de resultaten van de periodieke controles/audits en er wordt onder andere ingegaan op incidenten, resultaten van risicoanalyses (inclusief genomen maatregelen) en andere initiatieven die het afgelopen jaar hebben plaatsgevonden.

Om risico gebaseerde informatiebeveiliging toe te kunnen passen op het gewenste volwassenheidsniveau is het belangrijk om in controle te zijn van risico's door middel van een risicomanagement aanpak. Risicoanalyses zijn daarom integraal onderdeel van het ISMS. In het ISMS-handboek staat verder beschreven hoe maatregelen ingezet worden om risico's tot acceptabele niveaus terug te brengen.

De CISO stelt een operationele uitwerking van risicomanagement vast en de RvB bepaalt de risicobereidheid. Afhankelijk van het restrisico voor de organisatie kunnen risico's alleen bewust genomen worden op het volgende niveau:

Inschatting	Bevoegd tot accepteren
Kritiek of "Hoog en domeinoverstijgend"	RvB
Hoog	Manager
Medium	Proceseigenaar
Laag	Geen formele acceptatie vereist

Tabel: Risico-acceptatie matrix

4.5 Bewustwording en training

Beleid en maatregelen zijn niet voldoende om risico's op het terrein van informatieveiligheid uit te sluiten. De mens zelf creëert de grootste risico's. Bij SURF werken we daarom voortdurend aan het vergroten van het beveiligingsbewustzijn van medewerkers om kennis van risico's te verhogen en veilig en verantwoord gedrag aan te moedigen. Onderdeel van het beleid zijn regelmatig terugkerende bewustwordings- campagnes voor alle medewerkers, studenten, derden en met name operationele beheerders. Verhoging van het beveiligingsbewustzijn is een verantwoordelijkheid van zowel de leidinggevenden, de CISO en de ISO's. Bewustwording is een onderdeel van het introductieprogramma voor nieuwe medewerkers. Het vormgeven van bewustwording en training wordt verder uitgewerkt in het awareness/communicatie-jaarplan voor informatieveiligheid.

4.6 Security Incidentbeheer

Security incidentbeheer gaat over het detecteren, vastleggen en afhandelen van gebeurtenissen die een inbreuk doen op de informatiebeveiliging en de bedrijfsvoering negatief kunnen beïnvloeden. Belangrijk hierbij is dat alle betrokkenen herkennen wanneer er sprake is van een security incident en dit ook melden. Van incidenten kan worden geleerd. Incidentregistratie en periodieke rapportage over opgetreden incidenten horen dan ook thuis in een volwassen informatiebeveiligingsomgeving.

SURF heeft als dienst voor de instellingen het SURFcert en het SURFsoc. SURFcert is het landelijke CERT voor de sector van Onderwijs en onderzoek. Incidenten die de sector raken of impact hebben op onze instellingen worden gemeld bij het SURFcert. SURF is net als de instellingen een afnemer van SURFcert voor incidenten die mogelijk sectorbrede gevolgen hebben. Incidenten die vooral intern impact hebben worden gemeld bij het SIRT (Security Information Response Team).

Het doel van het SIRT is het oplossen van security incidenten om zo doende de continuïteit van SURF te ondersteunen en haar reputatie te beschermen. Het SIRT is gerechtigd om elke, achteraf te verantwoorden, actie op de SURF IT-omgeving te ondernemen om een lopend risico/incident

te mitigeren. Indien mogelijk worden hierbij betrokken medewerkers vooraf geïnformeerd en geconsulteerd.

SURFsoc is de dienst waar instellingen op aan kunnen sluiten. Binnen het SOC wordt er actief gemonitord op beveiligingsincidenten, kwetsbaarheden en dreigingen. SURF is ook afnemer van SURFsoc en richt op basis van SURFsoc een intern SOC in. Het doel van het interne SOC is om security incidenten vroegtijdig op te merken en indien mogelijk te voorkomen of de impact te minimaliseren.

De incidenten worden afgehandeld volgens de security incidentprocedure waar de afhandeling van datalekken een onderdeel van is. Als er persoonsgegevens in het geding zijn, wordt afgestemd met de FG. De inrichting en taken van het SIRT en SOC worden verder uitgewerkt in het ISMS Handboek en het SIRT Charter.

SURF heeft een procedure voor Responsible Disclosure waardoor melders van kwetsbaarheden in de informatiesystemen de garantie hebben dat SURF, onder voorwaarden, geen juridische stappen tegen hen onderneemt en met hen samenwerkt om de kwetsbaarheden op te lossen of mitigeren.