NOREA
DE BEROEPSORGANISATIE VAN IT-AUDITORS

Cyber Security Assessment (NOREA-CSA)

Analyse Cyber Security Standaarden en Frameworks

Augustus 2015

Inhoud

1 Inleiding

Dit document geeft een initieel overzicht van de volgende belangrijke standaarden en frameworks op het gebied van Cyber Security:

- *ISF – Standard of Good Practice (SoGP) en Cyber Resilience Framework*
- *SANS – Critical Controls for Effective Cyber Defense*
- *ISACA – Cybercrime Audit/Assurance Program*
- *PAS 555 – Cyber security risk. Governance and management*
- *NIST – Cybersecurity Framework*
- *ISO 27032 – Guidelines for cybersecurity*

Van iedere standaard/*framework* wordt een korte beschrijving gegeven op basis van de zeven categorieën binnen de *Cyber Security Assessment*.

Deze categorieën zijn:

1. Organisatie & *Governance*
2. Gedrag & Cultuur
3. Waardeketen (stakeholders) <-> risico's
4. Inzicht in het technologie landschap (software, middleware en hardware)
5. Wet- & regelgeving
6. Detectie
7. Reactie

Per categorie wordt een '**waardevol score**' gegeven: deze score geeft aan in hoeverre de desbetreffende standaard / het *framework* handvatten (maatregelen of *guidance*) biedt om risico's af te dekken. De volgende classificatie wordt hierbij gebruikt:

– standaard / *framework* biedt geen *guidance*

0 standaard / *framework* biedt beperkte *guidance*

\+ standaard / *framework* biedt goede *guidance*

Deze informatie is als input gebruikt voor de CSA Excel tool.

2 ISF – Information Security Forum

2.1 Inleiding

Het ISF (www.securityforum.org) is een non-profit organisatie waarbij bedrijven, die een belang hebben in informatiebeveiliging of risk management, zich als lid kunnen aansluiten. Het doel van het ISF is het ondersteunen van bedrijven op het gebied van informatiebeveiliging, door het ontwikkelen van *best practices* en het uitwisselen van kennis.

Het ISF heeft een *Standard of Good Practice for Information Security (SoGP)* ontwikkeld waarin de maatregelen zijn beschreven die nodig zijn om de vertrouwelijkheid, integriteit en beschikbaarheid (VIB) van informatie te waarborgen. De *Practice* is onderverdeeld in de dimensies *governance, risk, compliance, people, process* en *technology*. Cybercrime krijgt beperkt aandacht in de SoGP, acht normen (zie CF11.2) gaan specifiek in op beveiligingsmaatregelen tegen cybercrime.

In aanvulling op de Standard heeft het ISF een *Cyber Resilience Framework (CRF)* ontwikkeld. Dit *Framework* is bedoeld om organisatie te ondersteunen in de strijd tegen cybercrime. Het *Framework* beschrijft geen kant en klare verzameling maatregelen waarmee cybercrime buiten de deur is te houden. Deze *silver bullet* bestaat ook niet. Het *Framework* biedt een leidraad om te inventariseren in welke mate een organisatie in staat is te anticiperen en te reageren op beveiligingsincidenten als gevolg van cybercrime. Hierbij komt de keten van het samenwerken met externe partijen, het uitvoeren van een assessment en het reageren op incidenten uitgebreid aan de orde (zie pagina 17 en 18 *"Framework summary"*).

2.2 Organisatie & Governance

De SoGP besteedt **beperkt** aandacht aan de organisatie van de informatiebeveiliging en *governance*. In een aantal maatregelen wordt aandacht besteed aan de rol van de CISO (p.12) en een *governing body* (p.10), een visie of beschrijving van hun rol of samenwerking is niet opgenomen. Het *Framework* besteedt echter **relatief veel** aandacht aan de inrichting van de organisatie en *governance*. Deze elementen worden als uitgangspunt genomen en gepositioneerd als de lijm die de andere onderdelen van het *Framework* ondersteunt en samenbrengt. De *governance* omspant eigenlijk het *Framework*, waarbij een rol is weggelegd voor de IT Security function (p.34) t/m een *Cyber Resilience Leader* (p.35) en *Cyber Champion*. Ook externe partijen (*Technical partners*, p.34 en 35) hebben expliciet een rol in de *governance*, een verbinding die zeker nodig is om de nieuwe dreigingen het hoofd te kunnen bieden.

Waardevol Score:

SoGP: 

Framework: 

2.3 Gedrag & Cultuur

Het *Framework* (p.18 onderdeel B) besteedt **beperkt** aandacht aan het gedrag en de cultuur binnen een organisatie. Het belang van een security awareness programma wordt onderkend in de fase waarin security incidenten gedetecteerd moeten worden. De SoGP besteedt **expliciet aandacht** aan *awareness* (CF2.2) om een cultuur te stimuleren die positief staat tegenover informatiebeveiliging.

Waardevol Score:

SoGP: 

Framework: 

2.4 Waardeketen (stakeholders) <-> risico's

Het *Framework* werkt een concept van een *malspace* (p.8) uit waarin het veld van cybercrime wordt geschetst. In de *space* krijgen alle spelers een plaats, waaronder de organisatie zelf, leveranciers, afnemers en cybercriminelen. Zelfs tools en technieken hebben een plaats in de *malspace*. Spelers en objecten in het model kunnen ook van rol veranderen, bijvoorbeeld als gevolg van inbreuken kunnen systemen onderdeel uit gaan maken van de *malspace* (p.10 alinea 2). Hiermee onderstreept het *Framework* het dynamische en verweven karakter van een organisatie met zijn omgeving vanuit het perspectief van cybercrime.

De assets van een organisatie worden in het Framework gebruikt als uitgangspunt (p.9 alinea 1). De acties van cybercriminelen zijn gericht op deze assets. In de praktijk zal het meestal gaan om de gegevens die op systemen zijn opgeslagen, maar de definitie is zo ruim dat iedere "waarde", waaronder zowel digitale documenten als digitaal geld, als asset gezien kan worden. De *assets* vormen ook het uitgangspunt in de SoGP (CF3, *Asset Management*), hierbij is de *Practice* gericht op het opsommen van technische maatregelen die genomen moeten worden om fysieke *assets* te beschermen. De verschillende uitgangspunten van het *Framework* en SoGP blijken ook uit de beschrijving van de *stakeholders*. Het *Framework* ziet verschillende stakeholders in het meer IT technische gebied van cybercrime (p.8 en 9, de *Malspace*), terwijl de SoGP *stakeholders* definieert als externe partijen aan wie verantwoording afgelegd moet worden, zoals aandeelhouders en auditors (SG2.2 *Stakeholder Value Delivery*).

Waardevol Score:

SoGP: 

Framework: 

2.5 Inzicht in het technologie landschap (software, middleware en hardware)

De software en hardware zijn volgens de SoGP de te beschermen objecten (p.6 rechter kolom *Statement of Good Practice*). Het grootste deel van de maatregelen in de *Practice* is gericht op het beschermen van de beschikbaarheid, integriteit en vertrouwelijkheid van deze objecten. Het *Framework* hanteert het idee van hardware en software **minder sterk**. In de beschrijving van de *malspace* (p.9) spelen hard- en software wel een rol, maar minder centraal en daarbij dynamisch. Zo kunnen *mobile devices* gebruikt worden om informatie te ontsluiten naar de buitenwereld maar vormen daardoor tegelijk een bedreiging voor de assets van de organisatie.

Waardevol Score:

SoGP: 

Framework: 

2.6 Wet- & regelgeving

Op het gebied van wet- en regelgeving geven de SoGP (p. 36 SR2.1.3) en het *Framework* (p.40, *law enforcement partners*) **beide** aan dat samenwerking met politie en justitie **noodzakelijk** is. De SoGP voegt hier nog de verplichting aan toe vanuit het oogpunt van *compliance*.

De nieuwe dreigingen en vooral de gevolgen van het manifest worden van de dreigingen laten zich niet eenduidig afbakenen. Hierbij moet bijvoorbeeld rekening worden gehouden met imagoschade, identiteitsdiefstal en het openbaar worden van vertrouwelijke bedrijfsinformatie.

Waardevol Score:

SoGP: 

Framework: 

2.7 Detectie

Voor het detecteren van relevante gebeurtenissen heeft het *Framework* het onderdeel *"Cyber situational awareness"* (p.18, gele blok) opgezet. In dit onderdeel wordt benadrukt dat het belangrijk is informatie te verzamelen en deze te kunnen verwerken (kwantiteit en kwalitatieve analyse). De SoGP omvat een reeks technische maatregelen voor het detecteren van illegale activiteiten in de IT infrastructuur, waaronder IDS/IPS (CF10.6), illegale datastromen (o.a. CF8.7) en het monitoren van mobiele *devices* (CF14.3.5) en draadloze netwerken (CF9.6).

Waardevol Score:

SoGP: 

Framework: 

2.8 Reactie (crisis management)

Het *Framework* beschrijft een aanpak waarmee bedrijven kunnen bepalen in welke mate zij zich bewust zijn van de nieuwe externe dreigingen (p.22 *Cyber situational awareness*), deze kunnen opvangen (p.24 *Cyber resilience assessment*) en erop kunnen reageren (p.26 *Cyber responses*). Ook de SoGP biedt veel aanknopingspunten om deze maatregelen in te richten.

Waardevol Score:

SoGP: 

Framework: 

3 SANS Institute

3.1 Inleiding

De publicatie *"Critical Security Controls for Effective Cyber Defense"* (zie http://www.sans.org/critical-security-controls/) Het doel van de publicatie is het geven van de maatregelen die nodig zijn om waardevolle bezittingen, infrastructuur en informatie langs geautomatiseerde weg te bewaken. De maatregelen zijn samengesteld door een samenwerking van vooral Amerikaanse overheidsorganisaties.

De maatregelen hebben vooral betrekking op het verbeteren van de beveiliging van technische componenten. In de Controls is expliciet opgenomen dat het document een specifieke verzameling is van technische maatregelen om schade te detecteren, te voorkomen en te mitigeren (p.2 alinea 3).

Het *SANS Institute* verdeelt de maatregelen in een aantal categorieën, van *quick win* tot en met *advanced sub-controls* (zie p.4 *Structure of the Critical Controls Document*). Hierdoor kunnen organisaties prioriteiten stellen bij het bepalen van de maatregelen die voor hen relevant zijn. Voor iedere maatregel is een beschrijving opgenomen van de wijze waarop hackers misbruik kunnen maken van het ontbreken of niet functioneren van de maatregelen. Daarnaast zijn beschrijvingen opgenomen hoe de implementatie van de maatregelen getoetst kan worden. Deze indeling heeft het voordeel dat hiermee een context geschetst wordt waarmee de beveiligingsmaatregelen toegespitst kunnen worden op de eigen organisatie.

3.2 Organisatie & Governance

Red teams (p.80 *Critical Control 20 Penetration Tests and Red Team Exercises*) hebben de taak om de effectiviteit van beveiligingsmaatregelen te testen. In de Controls wordt aandacht besteed aan de activiteiten van red teams en welke aanpak zij kunnen volgen. De *governance* van informatiebeveiliging, de tegenpool van de red teams, komt **beperk**t aan de orde in de *Controls*.

Waardevol Score: 0

3.3 Gedrag & Cultuur

Het gedrag en de cultuur krijgen de nodige aandacht, ondanks de nadruk die ligt op maatregelen in IT infrastructuur. De twee gebieden worden vaak genoemd (p.41 *Appropriate Training* en p.75 *Incident response*) als onderdeel of aspect van IT beveiligingsmaatregelen. Voor medewerkers in een organisatie besteden de controls aandacht aan awareness programma's. Het belang van deze programma's wordt onderstreept in de oefeningen van red teams (p.80), *waar social engineering* als belangrijk aanvalsmiddel wordt neergezet. Voor IT medewerkers adviseren de

Controls om periodiek *skills assessments* (p.41 *Critical Control 9*) te houden. Voor de vastgestelde tekortkomingen of leemten kunnen vervolgens trainingsprogramma's worden opgezet.

Waardevol Score: 

3.4 Waardeketen (stakeholders) <-> risico's

De Controls hebben duidelijk het uitgangspunt gekozen om vanuit risico's naar beveiligingsmaatregelen te kijken (p.3 *Prioritization*). Het advies wordt gegeven om eerst die maatregelen te nemen die het meest mitigerende effect hebben tegen de grootste risico's. De *Controls* gaan er vanuit dat de waarde van de organisatie is opgenomen in fysieke IT assets (p.2 *"The goal of the critical controls is to protect critical assets, infrastructure, …"*). De aandacht gaat vooral uit naar de beveiliging van deze *assets*. *Stakeholders* binnen en rond de organisatie, zoals management, leveranciers en afnemers, worden vrijwel niet belicht. In de *Controls* ontbreekt onder andere het opstellen van een stakeholder analyse voor de organisatie.

Waardevol Score: 

3.5 Inzicht in het technologie landschap (software, middleware en hardware)

De software en hardware van een organisatie nemen een centrale plaats in binnen de kritieke maatregelen. De eerste twee *Controls* (p.6 *(un)authorized devices* en p.*12 (un)authorized software*) hebben betrekking op het inventariseren en in beeld hebben en houden van alle, zowel legale als illegale, hard- en softwarecomponenten binnen de IT infrastructuur. Ook *wireless devices* (p.35) en BYOD krijgen expliciet aandacht omdat deze componenten kwetsbaar zijn voor misbruik.

De kennis over componenten in de IT infrastructuur is een belangrijk uitgangspunt voor veel Controls. Op basis hiervan zijn bijvoorbeeld maatregelen uitgewerkt om illegale hard- en software en afwijkend gedrag van componenten te signaleren. De kennis wordt ook gebruikt om toegang tot netwerkvoorzieningen bij het aansluiten van (mogelijk illegale) hard- en software te blokkeren, voordat misbruik mogelijk wordt.

Waardevol Score: 

3.6 Wet- & regelgeving

In de *Controls* wordt beperkt aandacht besteed aan wet- en regelgeving. Enkele punten waarbij wetgeving aan de orde komt is bij het vaststellen van de bewaartermijn van backups (p.39 *Data recovery*) en het doen van aangifte om te voldoen aan wet- en regelgeving bij het afhandelen van security incidenten (p.74 *Legal requirements in case of incidents*).

Waardevol Score: 

3.7 Detectie

Detectie vormt een rode draad in de *Critical Controls*. De rol van detectie ligt vooral in het signaleren van afwijkingen van gebruikelijk gedrag van IT componenten (*Critical Control 14*, zie ook p.87 voor detectie van aanvallers). Bij meerdere maatregelen wordt aangegeven dat afwijkend gedrag moet worden gelogd en gesignaleerd naar een centrale beheerder of IT security functie.

Waardevol Score: 

3.8 Reactie (crisis management)

De *Controls* beschrijven de inrichting van een *incident response* proces (p.74 *Critical Control 18 Incident Response*) waarmee inbreuken op de beveiliging afgehandeld kunnen worden. De *red teams* kunnen gebruikt worden om de effectiviteit van de afhandeling te toetsen en te verbeteren. De rol van leveranciers en afnemers blijft onderbelicht. De *Controls* besteden aandacht aan *third parties* (p.74 punt 5) bij de afhandeling van incidenten, waarbij hun rol echter beperkt is tot het geven van informatie over de afhandeling. De inrichting van bijvoorbeeld een *Emergency Response Team* of andere organisatie voor de afhandeling van een incident of crisis komt niet aan bod, hiervoor wordt op p.74 alinea 4 verwezen naar de separate publicatie NIST 800-61 over dergelijke teams.

Waardevol Score: 

4 ISACA – Cybercrime Audit/Assurance Program

4.1 Inleiding

ISACA heeft in 2012 een *"Cybercrime Audit/Assurance Program"* ontwikkeld, gebaseerd op COBIT 4.1. In iedere stap van het *Program* is een referentie opgenomen naar relevante normen van het COBIT *framework* (p.7 alinea 2). Het doel van het *Program* is het geven van een onafhankelijk beeld van de maatregelen om cybercrime te voorkomen (p.12 *"Objective"*).

Het Program benadrukt dat *cybersecurity* geen IT issue is, maar een issue dat is geïntegreerd in de gehele bedrijfsvoering (p.11 alinea 3). Het bestrijden van cybercrime bestaat uit een keten van *awareness*, preventie, detectie, incident management, crisis management en samenwerking met politie en justitie (p.11 alinea 4). De onderverdeling wordt weliswaar genoemd in de managementsamenvatting maar de genoemde onderdelen komen niet op zichzelf herkenbaar in het *Program* terug. Het *Program* is vooral een samenvatting en nieuwe ordening van COBIT normen die te maken hebben met informatiebeveiliging en opvolging van security incidenten.

In het *Assurance Program* (p.7 alinea 3) is een referentie opgenomen naar het COSO *framework*. Deze referenties (p.13 en verder) zijn specifiek bedoeld voor auditors die *assurance* geven op basis van het *Program*.

4.2 Organisatie & Governance

De *governance* rond de bestrijding van cybercrime neemt een belangrijke plaats in binnen het Program (p.6 alinea 2). Er is veel aandacht voor het opstellen van richtlijnen en *policies* waarvan de opzet en het bestaan worden getoetst. Ook de processen voor beheersing van bijvoorbeeld beveiliging van systemen en incidenten zijn opgenomen in het *Program*.

Het *Program* stelt voor twee nieuwe organisatieonderdelen op te richten, de *Cybercrime Taskforce* (p.15 footnote 1 en p.18 *assurance program* deel 4.1) en een CSIRT (p.30 footnote 1). De taskforce krijgt de verantwoordelijkheid om alle IT gerelateerde criminaliteit, waaronder fraude, af te handelen. Hierdoor kan de verantwoordelijkheid van een bestaande afdeling, bijvoorbeeld fraude onderzoek, worden opgerekt om ook cybercrime gerelateerde incidenten af te handelen. Dit laatste is duidelijk wel een taak die 24x7 uitgevoerd moet worden. Voor dit laatste stelt het *Program* voor een CSIRT in te richten, die zich vooral richt op de operationele detectie en afhandeling van incidenten.

Het *Program* (p.18 norm 4.1.2.2) benadrukt dat in de *taskforce* voldoende mandaat beschikbaar moet zijn om op alle terreinen binnen een bedrijf, waaronder public relations en vertegenwoordigers van de business, gemandateerde besluiten (p.18 norm 4.2.1) te kunnen nemen en uitvoeren.

Waardevol Score: 

4.3 Gedrag & Cultuur

Het *Program* noemt *awareness* als cruciaal onderdeel (p.11 alinea 5) en startpunt in de aanpak tegen cybercrime. Dit wordt vertaald in het *Program* met het geven van trainingen aan medewerkers op alle niveaus in de organisatie, van senior executives tot aan medewerkers op operationeel niveau. Training vormt ook een belangrijk aandachtspunt voor leden van de *taskforce* en het CSIRT. *Awareness* wordt hierbij verankerd in de *Human Resource policy* (p.19 norm 5.1.1.3).

Waardevol Score: 

4.4 Waardeketen (stakeholders) <-> risico's

Het *Program* besteedt aandacht aan de *stakeholders* binnen de organisatie en IT leveranciers, bijvoorbeeld *cloud* dienstverleners, die mogelijk een rol kunnen spelen bij de afhandeling van cybercrime incidenten (p.20 norm 5.1.3). De klanten van de organisatie komen niet terug als *stakeholder*.

De assets en het uitvoeren van een risicoanalyse spelen een centrale rol in het Program. In het onderdeel *"Risk Analysis and Asset Prioritization"* (p.27) wordt beschreven hoe *assets* in kaart kunnen worden gebracht. Een *"asset"* kan zowel een fysiek object als een logisch proces zijn, zolang het geraakt kan worden door cybercrime.

Waardevol Score: 

4.5 Inzicht in het technologie landschap (software, middleware en hardware)

Het inzicht in het technologie landschap is een belangrijk uitgangspunt in het Program. Hiermee wordt inzichtelijk gemaakt welke IT componenten relevant zijn in het kader van cybercrime. Het Program noemt een reeks specifieke hard- en softwarecomponenten (p.24 IT Management), maar deze lijst kan niet volledig zijn. Voor ieder *cybersecurity assessment* zal opnieuw een inventarisatie gemaakt moeten worden om er zeker van te zijn dat alle relevante IT componenten in scope zijn.

Het *Program* geeft expliciet aan dat gesteund moet worden op *audits* en *assessments* die eerder zijn uitgevoerd (p.12 "Scope"). Zonder deze ondersteuning bestaat het risico dat een cybersecurity assessment een te omvangrijk onderzoek wordt waarbij wel alle aspecten van

informatiebeveiliging worden geraakt maar de doorlooptijd en vereiste diepgang waarschijnlijk in het gedrang komen.

Waardevol Score: 

4.6 Wet- & regelgeving

De wet- en regelgeving komt op meerdere plaatsen aan bod in het Program (p.12 alinea 3). De meest prominente plaats is het contact met politie en justitie in het geval van het doen van aangifte. Het Program benadrukt dat het belangrijk is contacten te onderhouden met *"…appropriate law enforcement agencies"* (p.11 en p.30 norm 8.2.2) om in geval van een incident snel te kunnen handelen. Het CSIRT wordt ook genoemd als partij om tijdens de afhandeling van incidenten relevante wet- en regelgeving, bijvoorbeeld voor transparantie en meldingsplicht, in het oog te houden.

Waardevol Score: 

4.7 Detectie

Het *Program* besteedt op meerdere plaatsen aandacht aan detectie, het wordt aangegeven als één van de belangrijkste gebieden (p.11 *"…with processes covering"*). De signalen van verdachte activiteiten zijn hierbij afkomstig van geautomatiseerde systemen zoals IDS/IPS en firewalls en de fysieke bewaking van objecten. Het CSIRT en het *incident management proces* zijn de kanalen waar alle signalen van mogelijk misbruik en/of cybercrime samenkomen.

Waardevol Score: 

4.8 Reactie (crisis management)

De reactie op een incident of crisis krijgt uitgebreid aandacht in het Program (p.11 alinea 4). Het uitgangspunt vormen *policies* die aan verschillende normen worden getoetst. Voor het afhandelen van incidenten staat het CSIRT opgesteld. Wanneer cybercrime leidt tot een crisis kan het *crisis management committee* (p.45) worden ingericht.

Waardevol Score: 

5 PAS 555 Cyber security risk. Governance and management

5.1 Inleiding

De PAS 555 specificatie is opgesteld door de *Cyber Alliance*, een samenwerking van onder andere Cisco, Symantec en G4S. Het opstellen van de specificatie, die is uitgegeven op 31 mei 2013, is gefaciliteerd door het *British Standards Institution*. Een PAS (*Publicly Available Specification*) kan gezien worden als een best-practice die de basis kan vormen voor een nog op te stellen *British Standards* (BS) norm.

De specificatie is geschreven voor het top management van bedrijven om een context te scheppen voor cyber security. In de specificatie zijn een reeks resultaten (*"outcomes"*) beschreven waaraan voldaan moet worden. De specificatie zelf geeft niet aan op welke wijze de resultaten bereikt moeten worden, het management kan hier zelf invulling aan geven. De specificatie geeft wel voor ieder resultaat verwijzingen naar *British Standard* (BS) normen die aan kunnen geven hoe een resultaat te bereiken.

In de specificatie is een keten van maatregelen uitgewerkt voor de stappen *Risk assessment, Protection and mitigation, Detection and response, en Recovery*. In het assessment wordt bepaald welke waarden van een organisatie beschermd moeten worden, in de overige stappen welke maatregelen genomen moeten worden om deze waarden te beschermen. *Governance* is gepositioneerd voor de besturing van deze keten. Verder is een prominente plek ingeruimd voor het continu verbeteren van de weerbaarheid tegen cybercrime.

De concentratie van PAS 555 op resultaten, terwijl weinig aandacht is voor de wijze waarop de resultaten bereikt moeten worden, blijkt onder andere uit de omvang van de specificatie. De resultaten zijn beschreven op drie pagina's die alle stappen in de keten van maatregelen beschrijven. De organisatie kan eigen processen gebruiken om tot die resultaten te komen of andere standaarden adopteren, zoals bijv. ISO/IEC 27001. PAS 555 bevat een referentietabel met o.a. ISO/IEC 27001, ISO/IEC 20000 en ISO/IEC 31000.

5.2 Organisatie & Governance

PAS 555 besteedt veel aandacht aan de *governance* en organisatie van *cyber security*. Ongeveer één derde van de normen heeft betrekking op leiderschap en besturing.

De specificatie geeft aan dat één eigenaar voor cyber security binnen de organisatie aangewezen moet worden. Deze eigenaar moet op voldoende hoog niveau in de organisatie gepositioneerd zijn, afhankelijk van de dreiging die van cybercrime uitgaat voor de specifieke organisatie. Verder moeten verantwoordelijkheden, bevoegdheden en middelen eenduidig en specifiek worden toegewezen.

Een centrale boodschap is dat cyber security een integraal onderdeel uit moet maken van alle activiteiten van de organisatie. De verantwoordelijkheid ligt zowel bij het top management als medewerkers, leveranciers en partners en de levenscyclus van gebruikte technologie.

Waardevol Score: 

5.3 Gedrag & Cultuur

Het gedrag en de cultuur van de organisatie worden vooral belicht vanuit de voorbeeldfunctie die het hogere management heeft. PAS 555 geeft wel aan dat awareness zich moet uitstrekken over de gehele *extended enterprise* (= de keten van leveranciers, eigen organisatie en afnemers). De aandacht voor *awareness* en gedrag van medewerkers wordt genoemd maar blijft beperkt.

Waardevol Score: 

5.4 Waardeketen (stakeholders) <-> risico's

De eerste stap in de waardeketen (zie Inleiding) is het opstellen van een risicoanalyse. De uitkomsten van deze analyse zijn een lijst van relevante assets en bedreigingen. De risicoanalyse in PAS 555 geeft alleen op hoofdlijnen handvatten voor het uitvoeren van de analyse. Een verdieping naar categorieën en soorten bedreigingen, zoals intern en extern, wordt niet gemaakt.

De stappen *protection and mitigation*, *detection and response* en *recovery* van PAS 555 beschrijven op hoofdlijnen de maatregelen die genomen moeten worden om assets te beveiligen in deze stappen. In deze onderdelen wordt echter beperkt een relatie gelegd met assets, bedreigingen of risicoanalyse uit de eerste stap van de waardeketen. De samenhang tussen de stappen is hierdoor niet altijd duidelijk.

Waardevol Score: 

5.5 Inzicht in het technologie landschap (software, (ook) middleware, hardware)

Het technologie landschap wordt niet als zodanig herkend in PAS 555. Hard- en software hebben een plaats als asset in de risicoanalyse, hierbij worden ook maatregelen geïdentificeerd die genomen moeten worden voor de beveiliging. De specificatie meldt hierbij expliciet dat in alle levensfasen van een *asset* maatregelen genomen moeten worden.

Het inzicht in het IT landschap is niet onderkend als relevant in PAS 555. De risicoanalyse en bedreigingen zijn algemeen geformuleerd en hebben ook betrekking op hard- en software. PAS 555 geeft aan dat afwijkingen van trends die wijzen op cybercrime gedetecteerd moeten worden, maar laat achterwege dat hard- en software hierin een belangrijk rol spelen.

Waardevol Score: 

5.6 Wet- & regelgeving

Wet- en regelgeving komen beperkt aan bod in PAS 555. Beide worden genoemd bij de afhandeling van cyber security incidenten, vooral gericht op het beperken van schade (aansprakelijkheid). Twee resultaten besteden aandacht aan wetgeving te weten *Investigation* en *Legal process*. Voor beide resultaten is niet aangegeven met welke andere resultaten of stappen in de waardeketen deze een relatie hebben.

Waardevol Score: 

5.7 Detectie

De detectie en afhandeling van cyber security incidenten is beschreven in de stap *detection and response*. Een positief punt hierbij is dat expliciet samenwerking gezocht wordt met externe partijen, niet alleen om informatie te verzamelen maar ook om informatie te delen over cybercrime en bedreigingen. Verder wordt expliciet onderscheid gemaakt naar interne en externe bronnen als het gaat om bedreigingen. Hiermee geeft PAS 555, op hoofdlijnen, een duidelijk beeld over het detecteren en afhandelen van incidenten.

Waardevol Score: 

5.8 Reactie (crisis management)

De reactie op een cyber incident wordt op hoofdlijnen beschreven in PAS 555. In de specificatie wordt geen onderscheid gemaakt tussen verschillende categorieën of mate van impact van incidenten. Verder worden geen handreikingen gegeven voor een in te richten organisatie zoals CSIRT of crisisorganisatie. Hierdoor biedt de specificatie weinig houvast voor het bepalen van specifieke maatregelen.

Waardevol Score: 

6 NIST Cybersecurity Framework

6.1 Inleiding

Het *National Institute of Standards and Technology* (NIST) is onderdeel van het Amerikaanse ministerie van Commercie en in 1904 ingesteld om de Amerikaanse achterstand t.a.v. industriële competitie op het gebied van kennis en kunde weg te nemen. Het NIST *Cybersecurity framework* is opgesteld in februari 2014 met als doel invulling te geven aan de opdracht van de Amerikaanse president om de kritische infrastructuur weerbaarder te maken tegen cyber aanvallen. In dat kader is NIST gevraagd met betrokken partijen een *framework* voor beheersing van *cybersecurity* risico's te ontwikkelen op basis van bestaande standaarden, richtlijnen en praktijkvoorbeelden.

Het *framework* is opgesteld voor eigenaren en beheerders van kritische infrastructuren. Tevens biedt het Amerikaanse ministerie van *"Homeland Security"* door middel van een *"Critical Infrastructure Cyber Community C³ Voluntary Program"* hulp aan deze doelgroep om te ondersteunen bij het adopteren van het *Cybersecurity Framework* en het beheersen van hun cyber risico's. Daarnaast heeft NIST een *roadmap* ontwikkeld om het *Framework* door te ontwikkelen.

Het *framework* is gebaseerd op verschillende normen ten aanzien van informatiebeveiliging, IT risico beheersing en kritische infrastructuur, zoals IS027001:2013, COBIT 5, CCS CSC, ISA 62443-2-1:2009, ISA 62443-3-3:2013 en NIST SP 800-53 Rev.4. Het *Framework* is geschreven vanuit een actie gerichte aanpak die aansluit op de plan-do-check-act cyclus waarbij dit vertaald is naar de stappen *Identify, Protect, Detect, Respond* en *Recover*. Daarbij wordt een vorm van *"capability maturity model"* middels *Framework* implementatie lagen (*"Implementation Tiers"*) ingezet om het perspectief van een organisatie op de gewenste en huidige stand van zaken weer te geven. Deze lagen zijn:

- Laag 1: Deels
- Laag 2: Risico bewust
- Laag 3: Herhaalbaar
- Laag 4: Adaptief

Deze lagen worden bezien vanuit de perspectieven op de aanwezigheid en volwassenheid van een risico management proces, geïntegreerd risico management programma en externe participatie. Daarnaast kan dit in deze gelaagde aanpak worden gebruikt om het huidige en gewenste profiel tegen elkaar af te zetten en zo prioritering aan te brengen in verbeteracties.

6.2 Organisatie & Governance

Het *NIST Cybersecurity Framework* geeft in de opbouw en aanpak aandacht aan de *governance* en organisatie van cyber security. Daarbij wordt de rol van het management, de organisatie en operatie ook in algemene termen genoemd. *Governance* vormt een apart onderdeel van de normen en een groot deel van de normen heeft ook betrekking op processen, rollen en verantwoordelijkheden.

Het *framework* richt zich met name vanuit risk management perspectief op de organisatie en *governance* aspecten. Tevens worden high level adviezen gegeven over de interactie tussen niveaus binnen de organisatie. Concrete invulling van de wijze waarop dit dient te worden belegd, ontbreekt. Wel wordt aangegeven dat verantwoordelijkheden, bevoegdheden en resources eenduidig en specifiek moeten worden toegewezen.

Een centrale boodschap is dat *cyber security* vanuit risico management perspectief een integraal onderdeel uit moet maken van alle activiteiten van de organisatie. De verantwoordelijkheid ligt zowel bij het top management als medewerkers, leveranciers en partners en de *life cycle* van gebruikte technologie.

Waardevol Score: 

6.3 Gedrag & Cultuur

In het algemeen wordt het belang van gedrag en cultuur in het NIST *Cybersecurity Framework* erkend. Ook is het aspect acceptatie van verandering zeer expliciet gemaakt door aandacht te geven aan beperkingen die mogelijk komen vanuit de organisatie ten aanzien van mogelijke privacy gerelateerde implicaties.

De vertaling naar *awareness* en gedragsverandering is beperkt in de onderliggende normen, ondanks het feit dat *awareness* en training een eigen onderdeel binnen de normen vormt.

Het gedrag en de cultuur van de organisatie worden vooral belicht vanuit de voorbeeldfunctie die het hogere management heeft.

Waardevol Score: 

6.4 Waardeketen (stakeholders) <-> risico's

Binnen het *NIST Cybersecurity Framework* is specifieke aandacht voor de *"business environment"*. Daarin wordt high level inzicht gevraagd in de rol van de organisatie en in de relatie van de waardeketen met stakeholders. Daarnaast komt dit aspect ook terug in de risicoanalyse. De uitkomst van deze analyse is een lijst van relevante assets en bedreigingen. De risicoanalyse in het NIST Cybersecurity Framework geeft alleen op hoofdlijnen handvatten voor het uitvoeren van de analyse. Een verdieping naar soorten bedreigingen, zoals intern en extern, wordt niet gemaakt.

De stappen *Protect, Detect, Response* en *Recover* van het NIST Cybersecurity Framework beschrijven op hoofdlijnen de maatregelen die genomen moeten worden om assets te beveiligen. In deze onderdelen wordt echter beperkt een relatie gelegd met assets, bedreigingen of risicoanalyse uit de *Identify* stap. De samenhang tussen de stappen is hierdoor niet altijd duidelijk.

Waardevol Score: 

6.5 Inzicht in het technologie landschap (software, middleware en hardware)

Het technologie landschap wordt niet als zodanig herkend in het *NIST Cybersecurity Framework*. Hard- en software hebben een plaats als asset in de risicoanalyse, hierbij worden ook maatregelen geïdentificeerd die genomen moeten worden voor de beveiliging. Het *framework* meldt hierbij expliciet dat in alle levensfasen van een asset maatregelen genomen moeten worden.

Het inzicht in het IT landschap is impliciet onderkend als relevant in *NIST Cybersecurity Framework*. De risicoanalyse en bedreigingen zijn algemeen geformuleerd en hebben ook betrekking op hard- en software. Wel bevatten de maatregelen in de fasen *Protect, Detect, Respond* en *Recover* diverse maatregelen op netwerk, software en hardware niveau.

Waardevol Score: 

6.6 Wet- & regelgeving

Wet- en regelgeving komen beperkt aan bod in het *NIST Cybersecurity Framework*. Wel wordt inzicht in *legal requirements* als onderdeel van *governance* genoemd. Echter, er wordt niet concreet gemaakt hoe dit inzicht moet worden verkregen. Wel is er specifieke aandacht voor privacy aspecten met betrekking tot de implementatie.

Waardevol Score: 

6.7 Detectie

De detectie en afhandeling van cyber security incidenten is beschreven in de stappen *Protect, Detect* en *Respond*. Ook wordt expliciet samenwerking gezocht met externe partijen, niet alleen om informatie te verzamelen maar ook om informatie te delen over cybercrime en bedreigingen. De verbinding naar reguliere bestaande processen binnen organisaties is hierbij een sterke pre.

Waardevol Score: 

6.8 Reactie (crisis management)

Reactie is als onderdeel van het *Respond* onderdeel expliciet geborgd in het *NIST Cybersecurity Framework*. In het *framework* wordt geen onderscheid gemaakt tussen verschillende categorieën of mate van impact van incidenten. Verder worden geen handreikingen gegeven voor een in te richten organisatie zoals CSIRT of crisisorganisatie. Hierdoor biedt het *framework* weinig houvast voor het bepalen van specifieke maatregelen. Anderzijds biedt het *NIST Cybersecurity Framework* via de stap *Recover* wel weer concrete handvatten voor afhandeling van een incident na de crisis en hoe weer in control te komen en naar de toekomst te leren over hetgeen de organisatie is overkomen.

Waardevol Score: 

7 ISO/IEC 27032 Guidelines for cybersecurity

7.1 Inleiding

De *Joint Technical Committee* ISO/IEC, *information technology Subcommittee* heeft in juli 2012 de ISO 27032 opgesteld. De basis van deze standaard is de analyse dat er een gat zit tussen aandachtsgebieden van de information *security, internet security, netwerk security* en *ICT security* organisaties als zij het hebben over Cyberspace. Dit ook nog eens gekoppeld aan onvoldoende samenwerking vanwege de verschillende *stakeholders* die hierachter zitten heeft geleid tot deze internationale standaard.

Nieuwe risico's voor gebruikers van cyberspace en het verlies van privacy hebben grote aantrekkingskracht op misbruikers daarvan. Cybercrime is snel gegroeid van simpele geïsoleerde gebruikersproblematiek tot complexe aanvallen van criminele syndicaten, en de bestrijding daarvan is niet voldoende meegegroeid. Deze standaard richt zich specifiek op *issues* met *malware* aanvallen, *social engineering* en delen en coördineren van informatie. Sommige onderwerpen worden alleen genoemd, men verwijst daarbij dikwijls naar andere ISO standaarden. Deze standaard moet vooral gezien worden als een set van security concepten en terminologieën die vooral bedoeld zijn voor security specialisten.

7.2 Organisaties & Governance

De ISO/IEC 27032 besteedt beperkt aandacht aan de organisatie van informatiebeveiliging en bijbehorende *Governance*. In hoofdstuk 13 wordt enige aandacht besteed aan mensen en organisaties. Wel wordt er ingegaan op de verschillende rollen die in aanraking komen met Cybersecurity maar dan meer vanuit ieder zijn taak, risico en mogelijke *best practices*. Vaak ook een verwijzing naar andere ISO/IEC standaarden.

Waardevol Score: 0

7.3 Gedrag & Cultuur

De standaard gaat beperkt in op gedrag bijvoorbeeld in hoofdstuk 9 aan de hand van het cyberrisico welke door een gedragscomponent wordt veroorzaakt en geeft dan een *best practice* om deze te beperken. Als laatste wordt in hoofdstuk 13 aangegeven dat awareness en training van mensen binnen de organisatie een belangrijk onderdeel is om blijvend weerbaarheid te ontwikkelen. Opvallend is de opmerking dat er ook getraind zou moeten worden met verschillende scenario's om de realiteit zo veel mogelijk te benaderen. In hoofdstuk 12.5.3.2 wordt nader ingegaan op de ontwikkeling van de *awareness* en training van de staf.

Waardevol Score: 0

7.4 Waardeketen (stakeholders) <-> risico's

Het perspectief van de waarde- of dreigingsketen voor stakeholders komt zeer nadrukkelijk naar voren. Genoemd worden consumenten & providers in hoofdstuk 7. Aan de hand hiervan worden assets beschreven in hoofdstuk 8 welke persoonlijk of organisatie specifiek worden uitgewerkt. Langs deze lijn worden vervolgens de dreigingen, zwaktes en aanval mechanismes nader beschreven. Hierbij wordt de link gelegd op de in de inleiding besproken drie issues waarop deze standaard zich met name richt.

Waardevol Score: +

7.5 Inzicht in het technologie landschap (software, middleware en hardware)

Dit komt uitgebreid aan bod in de analyse, op zowel applicatie-, server- en netwerk niveau in de gehele opzet.

Waardevol Score: +

7.6 Wet- & regelgeving

Op het gebied van wet en regelgeving wordt verwezen naar de autoriteiten als belangrijke partner.

Waardevol Score: -

7.7 Detectie

Met name in bijlage A worden tactieken besproken die helpen inzicht te verschaffen in de pre analyse fase en *readyness* van de organisatie. Ook het onderdeel netwerkmonitoring in hoofdstuk 11.4.2.3 besteedt nadrukkelijk aandacht aan detectie en opvolging. Verder wordt er een link gelegd met het instellen van *controls* op diverse niveaus in hoofdstuk 12.

Waardevol Score: +

7.8 Reactie (crisis management)

Opvolging door middel van een CERT. Daarnaast is ook kort beschreven de aanpak van support en escalatie in hoofdstuk 11.4.2.4

Waardevol Score: 0