Vulnerability Governance Framework

Rethinking Vulnerability Management as Governance

Whitepaper
Juli 2026 – Version 1.0

Jona van der Wel
Chief Information Security Officer

Published by Welvantage

Inhoudsopgave

Managementsamenvatting

Vulnerability Management is in veel organisaties niet bestuurbaar. Toch lijkt het proces vaak onder controle doordat rapportages groen kleuren, terwijl onder de oppervlakte kwetsbaarheden en bijbehorende risico's zich opstapelen. Dit is het comfortbeeld waar veel CISO's tegenaan lopen: het beeld van beheersing waarbij de daadwerkelijke risicopositie onzichtbaar is.

Dit ontstaat als uitvoering en risicosturing geen samenhangend systeem vormen en geen basis bieden voor besluitvorming. Operationele activiteiten functioneren los van risicoduiding en bestuurlijke afwegingen. Er worden patches geïnstalleerd, maar er ontbreekt inzicht om grip te houden op de risicopositie. Hierdoor blijven risico's bestaan zonder bewuste bestuurlijke keuzes.

Het Vulnerability Governance Framework doorbreekt dit probleem. Het brengt Vulnerability Management terug tot een samenhangend geheel. De Pijlers, het Maturity Model, en het Operating Model geven aan wat er nodig is, wat er moet verbeteren en hoe dit in de organisatie landt. Hiermee wordt Vulnerability Management daadwerkelijk bestuurbaar.

Inleiding

Technische kwetsbaarheden in software vormen een blijvend en groeiend risico voor organisaties. In een groot deel van succesvolle cyberaanvallen wordt misbruik gemaakt van bekende kwetsbaarheden, vaak kwetsbaarheden waarvoor al mitigerende maatregelen beschikbaar zijn. In moderne IT-omgevingen ontstaan maandelijks grote aantallen nieuwe kwetsbaarheden; honderden tot duizenden tegelijk zijn geen uitzondering. Het identificeren, prioriteren en mitigeren van deze kwetsbaarheden, Vulnerability Management, is daarmee een vast onderdeel in het beveiligingslandschap. Helaas wordt het nog vaak als operationeel proces gezien.

Schijn van beheersing
In de praktijk werkt die benadering niet: is er vaak weinig grip op Vulnerability Management. Vrijwel altijd zijn er meer kwetsbaarheden dan organisaties aankunnen. Tegelijkertijd maken legacy-systemen, toenemende complexiteit en operationele beperkingen het niet altijd mogelijk om kwetsbaarheden volledig en op tijd op te lossen. Het proces draait wel, maar beheersing ontbreekt.

Voor CISO's blijft het overzicht vaak beperkt. Het oplossen van kwetsbaarheden wordt vaak vooral gezien als een primair IT-proces. Zolang patches en kwetsbaarheden volgens vaste cycli afgehandeld worden, wordt Vulnerability Management gezien als ‘in control’. Maar vaak ontbreekt inzicht in wat er buiten die processen valt. Naar beperkingen in scope, ooit gemaakte uitzonderingen en issues die simpelweg nooit opgelost zijn, kijkt niemand. Hierdoor is het echte onderliggende risico niet zichtbaar.

Dit is het precies het comfortbeeld dat CISO's vaak voorgeschoteld krijgen. Vanuit de IT-afdeling of (cloud)-leverancier worden rapportages gemaakt die geoptimaliseerd zijn voor performance en uptime. “100% van de patches geïnstalleerd binnen SLA” klinkt goed, maar zegt weinig over de werkelijke risicopositie. De groene rapportages geven een perceptie van controle, wat echte sturing op risico onmogelijk maakt.

Dit kan leiden tot onbewuste acceptatie van risico's. Als geen goed zicht is op openstaande kwetsbaarheden en de bijbehorende risico's, is risicosturing niet mogelijk. Risico's blijven daardoor bestaan, zonder dat daar een bewuste keuze aan ten grondslag ligt. Op bestuurlijk niveau is dan onvoldoende zichtbaar welke risico’s feitelijk worden gedragen.

Het gemis is een kader voor Vulnerability Management waarin dit probleem wordt behandeld als governance-vraagstuk. Zonder samenhangend kader ontbreekt de structuur om kwetsbaarheden en risico’s in relatie tot elkaar te beoordelen. Bestaande standaarden zoals ISO en NIST bieden richting, maar geven onvoldoende houvast om kwetsbaarheden concreet te vertalen naar sturing en besluitvorming. Daardoor blijft Vulnerability Management lastig bestuurbaar op bestuursniveau.

Het Framework
Om het probleem van lastige bestuurbaarheid van Vulnerability Management op te lossen, en dit als governance-vraagstuk te benaderen, is dit Framework ontworpen. Het biedt een samenhangend governance- en besturingskader dat inzichtelijk maakt hoe Vulnerability Management wordt ingericht

en aangestuurd. Daarbij maakt het duidelijk hoe operationele keuzes zich vertalen naar bestuurlijke afwegingen en besluitvorming.

Een belangrijk onderdeel ervan is het Maturity Model, dat inzicht geeft in het huidige niveau en helpt bij het bepalen van een passend streefniveau. Hiermee wordt zichtbaar waar de organisatie nu staat en welke stappen nodig zijn om tot een hoger niveau van beheersing te komen. Dit voorkomt dat verbeteringen ad hoc worden ingezet en maakt ontwikkeling richtinggevend en meetbaar.

De scope richt zich op het bestuurbaar maken van technische kwetsbaarheden waarvoor mitigatie mogelijk is. Dit omvat patches, maar ook andere kwetsbaarheden zoals configuratiefouten. Het Framework is daarmee breder dan alleen patchmanagement. Preventieve ontwikkelpraktijken en secure software development vallen buiten scope.

Het Framework is primair ontwikkeld voor CISO's. Daarnaast is het ook relevant voor andere stakeholders, zoals risicomanagers en IT-managers. Ten slotte biedt het auditors een kader om governance, besluitvorming en volwassenheid van Vulnerability Management te beoordelen.

Dit Framework is een aanvulling op bestaande frameworks, zoals ISO en NIST. Daar waar deze frameworks zeggen dat Vulnerability Management nodig is en een model bieden voor operationele afhandeling, biedt dit Framework een vertaalslag van operationele handelingen naar bestuurlijke keuzes. Het uitgangspunt is dat Vulnerability Management een continu proces is dat vraagt om structureel inzicht, expliciete keuzes en doorlopende aandacht.

Het Framework bestaat uit vier onderdelen die in samenhang moeten worden toegepast. De Pijlers vormen het fundament, het Maturity Model maakt het niveau inzichtelijk, het Operating Model beschrijft de inrichting en Continue Verbetering zorgt voor ontwikkeling over tijd. Deze onderdelen versterken elkaar en worden in samenhang uitgewerkt, ondersteund met een praktijkvoorbeeld en aangevuld met reflectie op beperkingen en toekomstige ontwikkeling.

1. De Pijlers van Vulnerability Management

Om grip te krijgen op Vulnerability Management is het noodzakelijk om zeven kernonderdelen te onderscheiden. Deze zeven kernonderdelen zijn de Pijlers van Vulnerability Management en vormen een samenhangend en onderling afhankelijk geheel. Het ontbreken of niet goed functioneren van een of meerdere Pijlers ondermijnt de werking van het geheel.

De Pijlers vervullen ieder een eigen functie in het organiseren en besturen van het proces. Twee Pijlers zijn structurerend en bepalen de inrichting en verankering. Drie Pijlers zijn uitvoerend en beschrijven hoe Vulnerability Management in de praktijk functioneert, zowel regulier als onder tijdsdruk. De overige Pijlers zijn sturend en maken inzicht, prioritering en sturing mogelijk. Hieronder volgt een korte omschrijving van alle Pijlers.

1. Beleid & Governance
Vulnerability Management moet verankerd zijn in beleid en bestuurlijke kaders. Hierin wordt bepaald welke normen leidend zijn voor het kwetsbaarhedenproces en geven richting aan frequentie, risicobenadering en omgang met uitzonderingen. De pijler zorgt ervoor dat deze normen worden vastgelegd en ook worden doorvertaald naar besluitvorming en uitvoering. Zonder duidelijke governance is de invulling van Vulnerability Management op basis van individueel *best effort*, waardoor consistentie en herleidbaarheid niet zeker zijn.

2. Rollen & Verantwoordelijkheden
Een effectief Vulnerability Managementproces heeft een heldere rolverdeling en eigenaarschap nodig. Het moet duidelijk zijn wie verantwoordelijk is voor elke activiteit in het proces. Deze Pijler borgt dat verantwoordelijkheden zijn toegewezen en verankerd in de organisatie. Besluitvorming is gekoppeld aan vastgestelde rollen en sluit aan op belegd risico-eigenaarschap. Zonder deze Pijler ontstaat onduidelijkheid over mandaat en verantwoordelijkheid, waardoor besluitvorming niet herleidbaar is en aanspreekbaarheid ontbreekt.

Binnen dit Framework worden onder andere de volgende rollen onderscheiden: Beheerders, IT-Manager, en IT-Director, de Vulnerability Analist, Risicomanager, CISO en een verbindende rol in de vorm van de Vulnerability Manager.

3. Proces & Werkwijze
Deze Pijler beschrijft hoe Vulnerability Management structureel is ingericht en uitgevoerd. Het gaat hier om de operationele processen, maar ook om de processen op tactisch en strategisch niveau. Een vastgestelde werkwijze draagt bij aan heldere verwachtingen van alle betrokkenen en geeft de mogelijkheid tot cyclisch verbeteren (zoals PDCA). Goede processen en werkwijzen zijn consistent, herhaalbaar en voorkomen dat Vulnerability Management afhankelijk wordt van individuen. Zonder deze Pijler ontbreekt die consistentie, waardoor uitvoering niet betrouwbaar plaatsvindt.

4. Tooling & Scanning
Tooling & Scanning ondersteunt Vulnerability Management door het inzichtelijk maken van assets en kwetsbaarheden en het faciliteren van herstel. Scanning vormt een belangrijk controlemiddel op het

gehele Vulnerability Managementproces, maar alleen als het voldoende dekking heeft en geïntegreerd is in de werkwijze. Deze Pijler richt zich op de inzet, inrichting en samenhang van tooling in relatie tot het proces. Zonder deze Pijler ontbreekt een volledig en betrouwbaar beeld van de kwetsbaarheden in het IT-landschap, waardoor risico's niet zichtbaar zijn en gestuurd wordt op een vertekend beeld van de werkelijkheid.

5. Metrics & Rapportages
Zonder inzicht is geen sturing mogelijk. Metrics en rapportages maken Vulnerability Management bespreekbaar en bestuurbaar op operationeel, tactisch en strategisch niveau. Het gaat niet alleen om het verzamelen van kwetsbaarhedendata en doorlooptijden, maar ook om de duiding daarvan in het licht van risico en impact. Binnen dit Framework dienen metrics als signalen en hulpmiddelen voor besluitvorming. Kwetsbaarhedendata moet gebruikt worden voor analyse, en de analyse moet leiden tot besluitvorming. Geen enkele metric weerspiegelt het volledige risico en professionele interpretatie blijft essentieel.

Goede rapportages zijn afgestemd op de informatiebehoefte van verschillende stakeholders en vertalen technische inzichten naar betekenisvolle stuurinformatie voor prioritering en besluitvorming. Zonder deze Pijler ontbreekt een vertaling naar bestuurlijk niveau, waardoor sturing en besluitvorming versnipperd en impliciet plaatsvinden.

6. Risicosturing
Niet iedere kwetsbaarheid vraagt dezelfde urgentie of aanpak. Risicosturing zorgt ervoor dat prioritering voortkomt uit een afweging van waarschijnlijkheid en impact, in lijn met de risicobereidheid van de organisatie. Deze afweging vindt plaats binnen belegd risico-eigenaarschap, zodat duidelijk is wie verantwoordelijk is voor het maken van keuzes. Daarmee verbindt deze Pijler Vulnerability Management met bredere risicokaders waar het bestuur verantwoordelijkheid over heeft. Zonder deze Pijler ontbreekt risicoafweging en raken keuzes los van het risicoprofiel van de organisatie.

7. Spoedproces
Deze Pijler beschrijft het vermogen van de organisatie om Vulnerability Management tijdelijk in een versnelde modus te laten functioneren in het geval van tijdkritische kwetsbaarheden. In het geval van een tijdkritische kwetsbaarheid moet het proces en besluitvorming versneld worden doorlopen. In het spoedproces is daarom vooraf nagedacht over afwijkende mandaten, prioriteringsmechanismen en communicatielijnen. Versnelling vindt plaats binnen vastgestelde kaders, zodat snelheid niet ten koste gaat van beheersing en verantwoording. Zonder deze Pijler is een organisatie niet in staat om tijdkritische kwetsbaarheden snel op te lossen, of ontstaat versnelling buiten het sturingsmodel waardoor controle verloren gaat.

De Pijlers vormen gezamenlijk het normatieve kader voor het inrichten en beoordelen van Vulnerability Management. In het volgende hoofdstuk wordt dit kader gebruikt om volwassenheid te duiden en inzichtelijk te maken in hoeverre organisaties deze Pijlers daadwerkelijk beheersen.

2. Het Vulnerability Management Maturity Model

Het Vulnerability Management Maturity Model is een gestructureerd model om de volwassenheid van Vulnerability Management te bepalen. Het model helpt om het totaal en elke Pijler afzonderlijk te beoordelen en zwakke plekken te identificeren. Het totale volwassenheidsniveau van Vulnerability Management wordt echter niet bepaald door het gemiddelde, maar door de laagst scorende Pijler, de *floor-score*.

Het principe van de *floor-score* benadrukt dat het Vulnerability Managementproces functioneert op het niveau van de zwakste Pijler. Door de onderlinge afhankelijkheid van de Pijlers kan een sterk ontwikkeld onderdeel de tekortkomingen in een andere Pijler niet compenseren. De effectiviteit van het geheel wordt simpelweg ondermijnd door een zwak of afwezig onderdeel. De individuele scores per Pijler zijn wel relevant om verbeterpotentieel te duiden, maar de *floor-score* bepaalt de feitelijke volwassenheid.

Het Maturity Model kent zes niveaus. Omdat de niveaus geen lineair einddoel vormen, is het hoogste niveau niet voor elke organisatie noodzakelijk. Elke organisatie moet een eigen streefniveau bepalen. Het passende niveau hangt af van risico- en dreigingsprofiel, sector en wettelijke en maatschappelijke context.

Niveau 0 – Niet bestaand
Op dit niveau ontbreekt Vulnerability Management volledig. Er is geen visie, geen beleid en geen sturing. Patch- en mitigatieactiviteiten vinden willekeurig en ongecontroleerd plaats, meestal als onderdeel van regulier beheer of naar aanleiding van incidenten. Kwetsbaarheden zijn niet structureel inzichtelijk en risico's worden niet expliciet herkend of besproken.

Niveau 1 – Hectisch
Vulnerability Management is ad-hoc en reactief. Er bestaan losse initiatieven, maar samenhang ontbreekt. Beleid is verouderd of onvolledig, verantwoordelijkheden zijn onduidelijk en gebruik van tooling is beperkt. Er wordt voornamelijk gereageerd op incidenten of externe signalen. Het proces is onvoorspelbaar en sterk afhankelijk van individuele inzet en urgentie.

Niveau 2 – Reactief
De eerste structurele elementen zijn aanwezig. Beleid en rollen zijn formeel vastgelegd, maar nog onvoldoende uitgewerkt of verankerd. Scanning en patching vinden regelmatig plaats, maar zonder duidelijke tactische sturing of prioritering. Rapportages bevatten analyses, maar sluiten niet aan op de informatiebehoefte van verschillende stakeholders. Het proces blijft kwetsbaar en leunt sterk op specifieke personen.

Niveau 3 – Proactief
Vulnerability Management functioneert als een geïntegreerd en beheersbaar proces. Beleid wordt periodiek geëvalueerd en aangepast, stakeholders zijn in beeld en verantwoordelijkheden zijn duidelijk belegd. Tooling is geïntegreerd met andere IT-systemen, zoals de CMDB, en risicoduiding is onderdeel

van besluitvorming. Dit niveau is een stabiele basis voor volwassen Vulnerability Management en is voor organisaties zonder uitzonderlijke beveiligingseisen een realistisch niveau.

Niveau 4 – Geautomatiseerd
Het proces is grotendeels geautomatiseerd en datagedreven. Scanning, analyse en het toepassen van patches of mitigerende maatregelen verlopen in hoge mate automatisch. Rapportages zijn grotendeels realtime en afgestemd op verschillende bestuurlijke niveaus. Governance-kaders worden ondersteund door risicoanalyses en structurele feedbackloops.

Niveau 5 – Innoverend
Op het hoogste volwassenheidsniveau vervult de organisatie een voortrekkersrol binnen het domein van Vulnerability Management. Er wordt actief geëxperimenteerd met innovatieve technieken zoals AI-ondersteunde analyse, voorspellende modellen en verregaande automatisering. Risicosturing is gebaseerd op business-impact, actuele dreigingsinformatie en strategische context. Samenwerking is transparant en gestoeld op duidelijk eigenaarschap. Dit niveau is vooral relevant voor organisaties met een zeer hoog dreigingsniveau, zoals defensie- en inlichtingenorganisaties en gespecialiseerde cybersecuritybedrijven, en dient als richtinggevend voorbeeld voor de sector.

Vulnerability Management is in dit model pas volwassen als risico-inzichten leiden tot bewuste bestuurlijke keuzes. Zolang Vulnerability Management alleen resulteert in operationele acties, ontbreekt bestuurbaarheid en is het proces niet volwassen. Het volgende hoofdstuk beschrijft hoe het Operating Model deze vertaalslag organiseert en waar uitvoering overgaat in risicosturing en besluitvorming.

3. Het Operating Model voor Vulnerability Management

Het doel van het Operating Model is om Vulnerability Management effectief en bestuurbaar te laten functioneren. Het model beschrijft hoe uitvoering, risicosturing en besluitvorming samenkomen in een samenhangend systeem en het maakt duidelijk waar operationele afhandeling overgaat naar risicokeuzes en bestuurlijke verantwoordelijkheid.

Dit Operating Model staat los van organisatiestructuur en kan in elke organisatie toegepast worden. Het beschrijft de noodzakelijke samenhang om Vulnerability Management als governanceproces te laten werken. Daarmee voorkomt het dat risico's tussen uitvoering, risicosturing en bestuur onzichtbaar worden. Het model is technologie- en tooling-agnostisch.

Opbouw Operating Model

Het Operating Model is opgebouwd uit twee functionele kolommen, risicosturing en uitvoering, die zijn georganiseerd over drie lagen: strategisch, tactisch en operationeel. De risicokolom richt zich op het duiden en beoordelen van kwetsbaarheden en op het nemen van besluiten over prioriteit en urgentie. De uitvoeringskolom richt zich op het daadwerkelijk oplossen van kwetsbaarheden. Op strategisch niveau wordt richting en kaderstelling bepaald, op tactisch niveau gestuurd op prioritering en samenhang, en op operationeel niveau uitgevoerd. De kolommen zijn functioneel gescheiden en hebben ieder eigen verantwoordelijkheden.

Rollen binnen de Risicokolom
Binnen de Risicokolom zitten rollen die zich richten op het signaleren en duiden van kwetsbaarheden in hun context. Op operationeel niveau analyseert de Vulnerability Analist individuele kwetsbaarheden en interpreteert technische bevindingen als potentiële risico's. Op tactisch niveau kijkt de Risicomanager naar het totale kwetsbaarhedenlandschap en vertaalt risico's naar businessimpact.

Op strategisch niveau is de CISO de schakel tussen risicosturing en bestuurlijke besluitvorming. De CISO bewaakt de bestuurbaarheid van Vulnerability Management als systeem en initieert besluitvorming of escalatie naar het bestuur of risico-eigenaar als risico's buiten de vastgestelde risico-appetite vallen. De verantwoordelijkheid van de risicokolom ligt bij het duiden en agenderen van risico's. Besluitvorming over die risico's is de verantwoordelijkheid van de risico-eigenaar of het bestuur.

Rollen binnen de Uitvoeringskolom
Binnen de uitvoeringskolom bestaan rollen die verantwoordelijk zijn voor het afhandelen van kwetsbaarheden. Op operationeel niveau installeren Beheerders patches en voeren andere technische mitigerende maatregelen uit. Op tactisch niveau zorgt de IT-manager voor planning, prioritering en capaciteitsinzet, waarbij kwetsbaarheden worden geprioriteerd in het bredere IT-werk.

Op strategisch niveau is de IT Director verantwoordelijk voor het organiseren van de uitvoeringscapaciteit. De verantwoordelijkheid van de uitvoeringskolom ligt bij het oplossen en mitigeren van kwetsbaarheden.

Uitbesteding en het Operating Model
In de praktijk is IT-uitvoering vaak (deels) uitbesteed, bijvoorbeeld via SaaS/Cloud of managed services. Dit leidt regelmatig tot de misvatting dat verantwoordelijkheid voor kwetsbaarheden bij de leverancier ligt. Governance, prioritering en risico-eigenaarschap blijven altijd intern. De CISO blijft verantwoordelijk voor risicosturing rondom kwetsbaarheden en de IT Director blijft verantwoordelijk voor de uitvoering. Het Operating Model blijft toepasbaar, ook bij outsourcing.

De Vulnerability Manager
Tussen de twee Kolommen en over alle lagen heen bevindt zich de rol van Vulnerability Manager. Deze rol heeft regie over het functioneren van Vulnerability Management als geheel en is centraal coördinatiepunt. De rol bewaakt flow, voortgang en duidelijkheid, lost knelpunten op en zorgt dat afspraken worden vastgelegd en nagekomen. Hij/zij verzorgt rapportages en zorgt dat informatie tijdig beschikbaar is voor alle betrokkenen. Indien nodig is de Vulnerability Manager ook het eerste escalatiepunt in het proces.

Informatie- en rapportagelijnen
Rapportages zijn bedoeld om inzicht, sturing en besluitvorming te ondersteunen. Kwetsbaarheden worden in de risicokolom geduid en geagendeerd en vormen input voor prioritering en opvolging binnen de uitvoeringskolom, voortgang en knelpunten worden vervolgens teruggekoppeld. Het is daarbij essentieel dat de ruwe en de geduide informatie transparant beschikbaar is voor alle

betrokkenen. De Vulnerability Manager verzorgt de rapportages afgestemd op de informatiebehoeften van de verschillende stakeholders.

Het Model neemt zelf geen besluiten, het faciliteert alleen besluitvorming. Besluiten over individuele risico's worden genomen door de risico-eigenaren en het bestuur draagt eindverantwoordelijkheid voor het totale risicoprofiel. De CISO bewaakt het proces en initieert escalatie wanneer risico's buiten de risico-appetite vallen. Daarnaast kan de werking van het Operating Model periodiek worden getoetst, bijvoorbeeld via interne controle of audit, als onderdeel van governance- en assurance-processen.

Schaalbaarheid en context

Dit Operating Model is een richtinggevend kader voor het organiseren van Vulnerability Management, onafhankelijk van organisatiestructuur of schaal. Het is essentieel dat alle verantwoordelijkheden zijn belegd en functioneren, maar de wijze waarop rollen worden ingevuld kan variëren. In grote organisaties kunnen meerdere personen betrokken zijn, zelfs voor dezelfde rollen, terwijl in kleinere organisaties rollen kunnen worden gecombineerd. Daarmee is dit model toepasbaar in verschillende organisaties en structuren.

In het Operating Model krijgen de zeven Pijlers concreet vorm. Beleid & governance bepalen de kaders, Rollen & verantwoordelijkheden structureren eigenaarschap, en Proces & werkwijze, Tooling & scanning en het Spoedproces geven invulling aan de dagelijkse en versnelde werking. Metrics & rapportages maken sturing mogelijk en Risicosturing geeft richting aan prioritering en bijsturing. Het Operating Model maakt hiermee zichtbaar hoe Vulnerability Management bestuurbaar gemaakt wordt.

4. Continue Verbetering van Vulnerability Management

Continue Verbetering is nodig om het Vulnerability Managementproces naar een hoger volwassenheidsniveau te laten groeien en te zorgen dat het op dat niveau blijft. Door veranderende dreigingen en technologische ontwikkelingen is continue verbetering nodig om op hetzelfde niveau te blijven. Het Framework gebruikt hiervoor de PDCA-cyclus als mechanisme voor Continue Verbetering.

De PDCA-cyclus (Plan, Do, Check, Act) is een methode om Vulnerability Management blijvend te ontwikkelen. Deze cyclus bestaat uit vier fasen (voorbereiden, uitvoeren, controleren, en bijsturen) en is een veelgebruikte methode voor gestructureerde procesverbetering. De cyclus kan worden toegepast op individuele onderdelen van Vulnerability Management en op het geheel. Activiteiten op elk niveau kunnen worden gepland en uitgevoerd, waarna gecontroleerd wordt of de juiste resultaten zijn bereikt. Afwijkingen en nieuwe inzichten vormen basis voor bijsturing.

In dit Framework ligt het zwaartepunt in de Plan-fase, omdat een sterke voorbereiding bepalend is voor de rest van het proces. Juist in de voorbereiding worden scope, prioriteiten, afhankelijkheden en risico's bepaald. Effectieve uitvoering (Do), controle (Check) en bijsturing (Act) zijn in sterke mate afhankelijk van de kwaliteit van de voorbereiding.

Continue Verbetering is alleen mogelijk als periodiek inzicht verkregen wordt in de volwassenheid van Vulnerability Management. Zonder inzicht in het niveau per Pijler is niet duidelijk waar bijsturing nodig is. Alleen als sterke en zwakke onderdelen zichtbaar zijn, kan het volwassenheidsniveau van worden verhoogd. Het Framework schrijft echter geen vaste meetmethode voor. Continue Verbetering is hiermee een integraal onderdeel van governance en sturing en sluit aan bij gangbare governance- en compliance-kaders, zoals ISO-normen, het NIST Cyber Security Framework en NIS2.

5. Illustratief praktijkvoorbeeld

Dit praktijkvoorbeeld illustreert hoe Vulnerability Management structureel kan falen als essentiële onderdelen van het Framework ontbreken. Dit voorbeeld gaat over een enterprise-organisatie met meer dan 3000 medewerkers, verspreid over meerdere vestigingen. Ondanks aantoonbare investeringen in security, professionals, beleid en tooling, kwam Vulnerability Management niet goed van de grond. De organisatie bleef kampen met grote aantallen achterstallige kwetsbaarheden en had onvoldoende inzicht in het totale risicoprofiel.

Risicosturing in isolatie
Vanuit de Risicokolom leek Vulnerability Management in eerste instantie goed ingericht. De verantwoordelijkheid was formeel belegd bij de CISO en er was actueel beleid, gebaseerd op best practices. Er werd ook gestuurd op risico: het interne SOC voerde dagelijks kwetsbaarheidsscans uit en analyseerde kwetsbaarheden op basis van meerdere factoren, waaronder CVSS-scores en kritikaliteit van systemen en assets. Bij kwetsbaarheden met een hoog ingeschat risico werden meldingen uitgestuurd.

In de praktijk bleef deze risicosturing echter grotendeels binnen de Risicokolom. Analyses vonden plaats binnen het team van de CISO en het SOC, maar werden niet vertaald naar businessimpact of naar een totaalbeeld van het kwetsbaarhedenlandschap. Inzichten en trends werden dus niet structureel gebruikt voor besluitvorming of sturing buiten de Risicokolom. Risico's waren bekend, maar niet overdraagbaar.

Inhoudelijke risico-inzichten bestonden dus, maar kregen geen bestuurlijk gewicht. Door het ontbreken van formele rapportages en door een structureel groene audit-rapportage ontstond een comfortbeeld van beheersing. Hierdoor waren oplopende kwetsbaarheden geen aanleiding voor ingrijpen.

Management zonder stuurinformatie
IT-management maakte bij deze organisatie geen onderdeel uit van het Vulnerability Managementproces. De IT Director en de IT-Managers hadden geen formele rol en werden niet verantwoordelijk gehouden voor het beheer van kwetsbaarheden. Op basis van het principe van *need-to-know* ontvingen zij geen concrete stuurinformatie over kwetsbaarheden.

Het gevolg was dat het IT-management kwetsbaarhedenherstel niet meenam in planning en prioritering. Zonder inzicht, mandaat en formele verantwoordelijkheid was het kwetsbaarhedenprobleem niet goed bekend bij het IT-management en werden er andere prioriteiten gesteld. De IT-afdeling kreeg het simpelweg te druk voor Vulnerability Management.

Uitvoering zonder regie
Daarbij ontbrak een duidelijke verbindende structuur tussen Risicosturing en Uitvoering: er was geen Vulnerability Manager aangesteld die het hele proces overzag. Discussies ontstonden over juistheid en eigenaarschap van kwetsbaarheden, afspraken werden niet eenduidig vastgelegd of opgevolgd en

prioriteiten werden inconsistent gesteld. Er was geen duidelijke coördinerende rol en geen structureel escalatiemechanisme. Problemen in het proces bleven daardoor bestaan.

In de uitvoering kwam de verantwoordelijkheid vrijwel volledig terecht bij de Beheerders. Zij behoorden tot de weinigen met toegang tot het kwetsbaarhedenportaal van de scantooling en hadden zicht op de technische bevindingen. Deze informatie was echter niet vertaald naar context, prioriteit of concrete sturing. Beheerders moesten zelf analyses uitvoeren en keuzes maken, terwijl dit diepgaande securitykennis vereist die zij niet altijd hadden. Bovendien was er bij problemen ook geen mogelijkheid tot escalatie.

Kwetsbaarhedenherstel werd daarmee afhankelijk van individuele inzet en beschikbare tijd, in plaats van structurele borging. Vanuit de Risicokolom werd van de Beheerders verwacht dat zij zelf kwetsbaarhedenanalyse deden en de juiste acties uitvoerden. Tegelijkertijd werden zij hierop niet aangestuurd door hun managers. De Beheerders hadden geen structurele ruimte voor kwetsbaarhedenherstel en inspanningen die wel werden geleverd werden niet erkend. De Beheerders stonden in een onmogelijke spagaat.

Awareness als compensatie
Om de achterstallige kwetsbaarheden terug te dringen werd vanuit het securityteam ingezet op extra awareness voor Beheerders. De aanname was dat zij patching niet belangrijk genoeg vonden en dat betere awareness zou leiden tot ander gedrag. In de praktijk had dit nauwelijks effect. Beheerders kregen geen extra tijd of prioriteit, structurele knelpunten bleven bestaan en er was nog steeds geen managementsturing voor kwetsbaarhedenherstel.

Awareness fungeerde hiermee als vervanging voor structurele sturing. Gedrag werd aangesproken terwijl ontwerp en inrichting tekortschoten. Ondanks inzet en betrokkenheid in zowel de Risicokolom als de Uitvoeringskolom bleef het resultaat uit en nam frustratie toe.

Duidende analyse
Deze organisatie zat feitelijk op *floor-score* maturity niveau 1. Ondanks de aanwezigheid van afzonderlijke onderdelen functioneerde Vulnerability Management niet als samenhangend geheel. Risicosturing en Uitvoering opereerden grotendeels los van elkaar.

De Pijler Beleid & Governance was formeel ingericht en functioneerde op papier, maar werd niet doorvertaald naar sturing en verantwoordelijkheid. De Pijler Rollen & Verantwoordelijkheden faalde fundamenteel. IT-management had geen formele rol, verantwoordelijkheden waren niet vastgelegd en de verbindende rol tussen de kolommen, de Vulnerability Manager, ontbrak. Ook Proces & Werkwijze was niet goed ingericht. Er bestond geen eenduidig herhaalbaar proces en het Vulnerability Managementproces was sterk afhankelijk van individuen.

Tooling & Scanning was aanwezig en actief in gebruik, maar zonder duidelijke borging van betrouwbaarheid. Metrics & Rapportages ontbraken voor Vulnerability Management vrijwel volledig, waardoor risico-inzichten geen vaste plek kregen in besluitvorming. Binnen Risicosturing werden wel pogingen gedaan om kwetsbaarheden te duiden, maar bleven adviserend en leidden niet tot bestuurlijke keuzes. Het Spoedproces was afwezig en werd ad hoc ingevuld.

Dit leidde ertoe dat het Operating Model in deze organisatie niet functioneerde: de Risicokolom beschikte over inzicht, de Uitvoeringskolom over capaciteit, maar zonder verbinding, escalatie of bestuurlijke verankering. Het resultaat was onvermijdelijk: Vulnerability Management bleef steken op een zeer laag volwassenheidsniveau.

6. Beperkingen en ontwikkelperspectief

Zelfs bij consistent gebruik heeft dit Framework enkele duidelijke grenzen. In dit hoofdstuk worden de grenzen benoemd en wordt geanticipeerd op logische ontwikkelrichtingen die ontstaan zodra organisaties het Framework structureel toepassen.

Het Framework biedt geen oplossing voor structureel onoplosbare kwetsbaarheden, het maakt ze alleen zichtbaar en bestuurbaar. Afhankelijkheden in legacy-systemen, verouderde technologie of een disproportionele verhouding tussen inspanning en risico maken dat er altijd een blijvend risico aanwezig blijft. Het is onrealistisch te veronderstellen dat complexe IT-omgevingen langdurig zonder kwetsbaarheden kunnen bestaan.

Het is aan organisaties zelf om met deze onoplosbaarheid om te gaan. Structureel onoplosbare kwetsbaarheden zullen moeten worden gewogen en eventueel met mitigerende maatregelen, bewust worden geaccepteerd binnen de vastgestelde risico-appetite. Organisaties zouden hier aparte kwetsbaarhedenregisters voor moeten opstellen. Het Framework faciliteert de risicosturing, maar neemt zelf geen besluiten. De verantwoordelijkheid hiervoor blijft liggen bij de risico-eigenaren en, waar nodig, bij de CISO of het bestuur.

Naast deze beperkingen maakt het Framework ook duidelijke ontwikkelrichtingen zichtbaar. Door kwetsbaarheden en het onderliggende landschap inzichtelijk te maken, kan het Framework dienen als input voor bredere bestuurlijke risicobesluitvorming, bijvoorbeeld binnen Enterprise Risk Management. Deze interactie verloopt via de Risicokolom via de rol van de CISO, zonder dat het Framework zelf onderdeel wordt van bestuurlijke besluitvorming.

Deze ontwikkelrichtingen liggen buiten het Framework zelf. Het Framework fungeert als fundament dat blootlegt waar verdere organisatorische en bestuurlijke keuzes noodzakelijk zijn, zonder deze keuzes te dicteren.

Bij consistent gebruik draagt het Framework bij aan het verder uitkristalliseren van Vulnerability Management als een zelfstandig domein binnen cybersecurity, met eigen rollen, besluitvorming en volwassenheidsniveau's. AI vergroot de druk op organisaties, maar verandert niet het probleem. Het maakt vooral zichtbaar of organisaties in staat zijn om risico-inzichten daadwerkelijk om te zetten in bestuurlijke keuzes.

Conclusie

Vulnerability Management is in veel organisaties niet bestuurbaar. De oorzaak van structurele problemen ligt vooral bij het ontbreken van samenhang tussen risicosturing en uitvoering.

Dit Framework maakt van Vulnerability Management een organisatiebreed governanceproces. Met de Pijlers, het Maturity Model, het Operating Model en Continue Verbetering wordt zichtbaar hoe Vulnerability Management ingericht en bestuurd kan worden en hoe het proces volwassen kan worden. Vulnerability Management is pas volwassen als risicosturing, uitvoering en besluitvorming met elkaar zijn verbonden en leiden tot bewuste bestuurlijke keuzes.

Het Framework is een aanvulling op bestaande normen en standaarden zoals ISO en NIST. Het biedt CISO's en bestuur een kader om voorbij het comfortbeeld van controle te kijken en structurele zwaktes in hun organisatie bloot te leggen. In een context van AI en toenemende complexiteit wordt die bestuurbaarheid essentieel. De kernvraag is dan ook niet of organisaties kwetsbaarheden hebben, maar of zij in staat zijn ze als samenhangend systeem te overzien en te sturen.

Literatuurlijst

Crowdstrike, 2026 Global Threat Report, 2026. https://www.crowdstrike.com/explore/2026-global-threat-report

Enisa, Enisa Threat Landscape, 2025. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2025

Mandiant, M-Trends 2025 Raport, 2025. https://services.google.com/fh/files/misc/m-trends-2025-en.pdf

NCTV, Cybersecuritybeeld Nederland, 2025. https://www.nctv.nl/documenten/2025/11/26/cybersecuritybeeld-nederland-2025

NIST, NIST Cybersecurity Framework 2.0, 2024. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf

Verizon, Data Breach Investigations Report, 2026. https://www.verizon.com/business/resources/reports/dbir/

Colofon

Published by Welvantage

Auteur

Jona van der Wel
Chief Information Security Officer

Certificeringen

CISSP, CISM

Context

Dit document is gebaseerd op praktijkervaringen in cybersecurity-governance en Vulnerability Management. De inhoud weerspiegelt de persoonlijke visie van de auteur en vormt geen formeel standpunt van een specifieke organisatie.

Doel en scope

Deze whitepaper introduceert een governance-framework voor Vulnerability Management. Het document is bedoeld als besturend en duidend kader voor CISO's en andere governance-stakeholders. Het is geen implementatiehandleiding of technisch voorschrift.

Relatie tot bestaande kaders

Het Framework vormt een aanvulling op bestaande normen en standaarden, zoals ISO/IEC 27001 en NIST, en richt zich op bestuurbaarheid, samenhang en volwassenheid van Vulnerability Management.

Versie

Versie 1.0
Juli 2026