Handleiding Risicoafweging

Wat houdt een risicoafweging in?

Het doel van een risicoafweging[1] is om na te gaan welke set van maatregelen op het gebied van informatiebeveiliging het best past op jouw praktijk. Op basis van de informatiesystemen, gegevensverwerkingen en -opslag die je in jouw praktijk gebruikt, kom je tot een set aan basismaatregelen. Vervolgens breng je de specifieke bedreigingen in jouw praktijk in kaart en vul je op basis daarvan de set aan maatregelen aan.

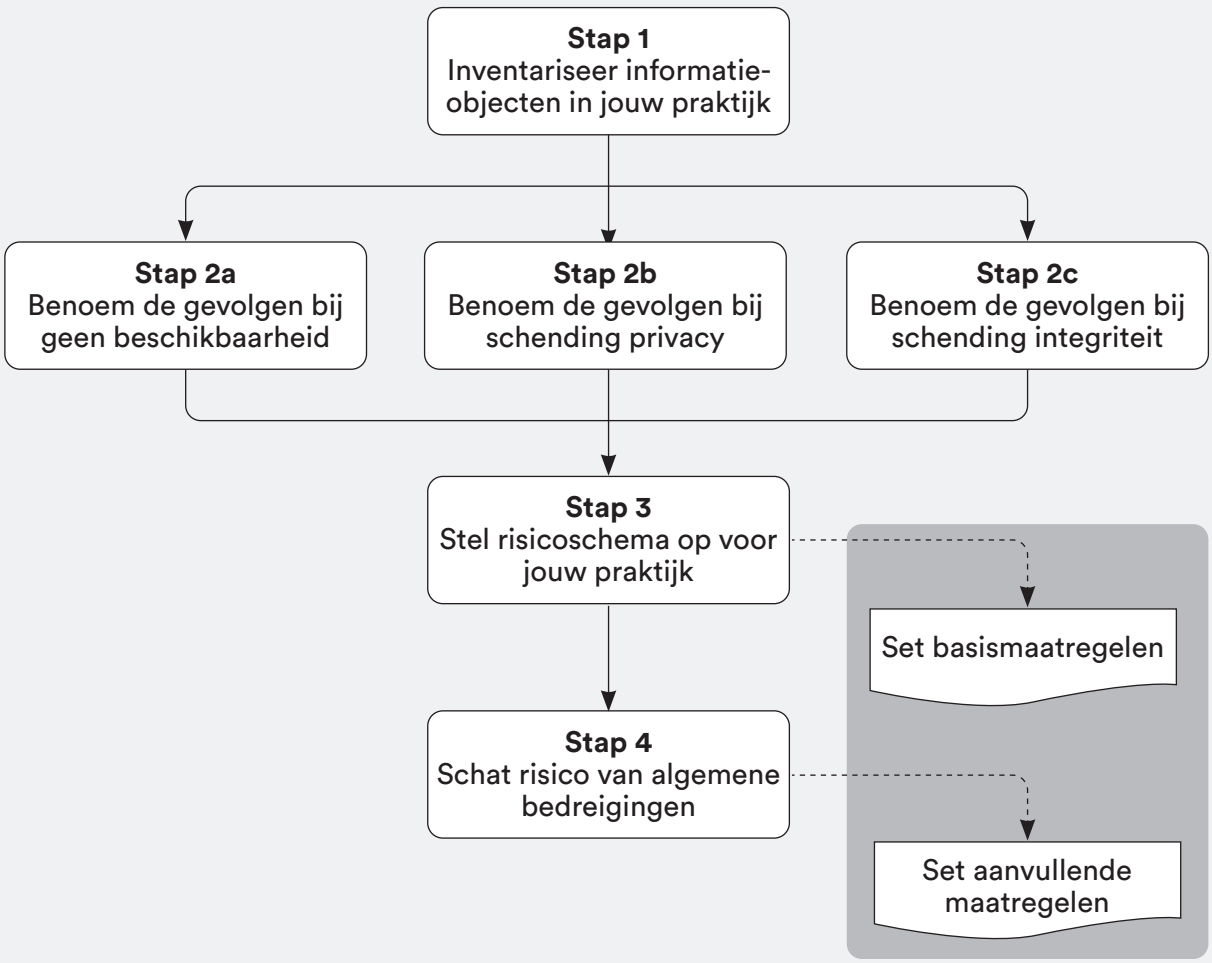
Houd er rekening mee dat je voor een risicoafweging wel tijd moet uittrekken. Bij voorkeur wijs je iemand in de praktijk aan die expertise opdoet op dit gebied, of werk je hierin samen met collega's in andere praktijken. Ook kun je je laten ondersteunen, bijvoorbeeld door je regionale huisartsenorganisatie als die hier expertise op heeft of door externe hulp in te huren.

[1] Er worden verschillende begrippen gehanteerd voor het proces van (informatiebeveiligings)risico's (risicoscenario's) inventariseren, analyseren, beoordelen, beheersmaatregelen selecteren en implementeren. Risicobeoordeling, risk-assessment, DPIA en risk management zijn allemaal verwante termen die één of meer van deze activiteiten kunnen inhouden.

1. Stappenplan risicoafweging

Hoe gaat een risicoafweging in zijn werk? Een risicoafweging bestaat uit vier stappen. Die lichten we hieronder toe.

Figuur 1: Stappenplan risicoafweging



Stap 1 | Inventarisatie informatieobjecten

Informatieobjecten zijn álle dragers van gegevens/informatie die in werkprocessen worden ingezet of tot stand komen of die ad hoc beschikbaar kunnen zijn. Het gaat dus om allerlei soorten objecten: het HIS, de email-box, USB-sticks, uitgeprinte informatie, medicijn-verpakkingen met NAW-gegevens, bestanden op het netwerk (zoals patiëntlijsten), data verzameld door medische apparatuur, digitale of geprinte salarisoverzichten, verslagen van functioneringsgesprekken, whiteboard/prikbord met praktijkmededelingen etc. Maar het gaat ook om personen die kennis hebben van gegevens; denk aan collega's die een recent sterfgeval bespreken in een openbare ruimte.

Hoe heb je al deze informatie opgeslagen? Welke processen spelen een rol in jouw praktijk? Welke informatiesystemen gebruik je om dit werk te ondersteunen en om afgesproken diensten aan de patiënt en andere partijen na te komen? Dit zijn de belangrijkste vragen in stap 1.

Ga als volgt te werk:

a) Benoem de processen in jouw praktijk die gebruikmaken van informatiesystemen. Het handigste is om bij je informatiesysteem-modules te beginnen. En loop rond in de praktijk: wat gebeurt er nog meer met de informatie? Denk ook aan wekelijkse, maandelijkse en jaarlijkse of incidentele processen.

b) Geef per proces aan welke systemen, modules, opslagmedia erbij zijn betrokken (denk ook aan de papieren dossiers).

Proces	Informatieobjecten
1. Afspraken	Je His - centrale functies - agenda
2. Consult	Je His - centrale functies - consultondersteuning - elektronische dossiers - protocollair werken
3. Berichtuitwisseling ziekenhuis	Je His - centrale functies - communicatie
4. Facturering	Je His - facturering
5. Oproepen voor preventie	Je His - preventiemodule
6. Papieren dossier	Handmatig - dossiers achter balie
7. Berichtuitwisseling huisartsenpost	Je BerichtService
8. Toegang tot tweede lijn	Verwijsapplicatie
9. Patiëntenportaal **- e-consult** **- herhaalrecepten** **- afspraken** **- meetwaarden**	Je PatiëntPortaal
10. Praktijkinformatie	Je PraktijkSite
11. Gegevens opvragen in het ziekenhuis	Het ZiekenhuisPortaal
12. Inloggen vanuit huis	Je Toegang
13. Landelijk uitwisselingssysteem	Het Landelijk Schakelpunt

Tabel 1: Voorbeeld van een inventarisatie van processen en bijbehorende informatieobjecten

Stap 2 | Benoem de gevolgen bij geen beschikbaarheid en bij schending privacy of integriteit

In deze stap geef je per proces uit stap 1 aan hoe belangrijk beschikbaarheid is, hoe belangrijk vertrouwelijkheid is en hoe belangrijk de integriteit van gegevens is: de drie pijlers van informatiebeveiliging.

Beschikbaarheid (B): hierbij bepaal je per praktijkproces: kan de informatie ook later (bijvoorbeeld de volgende werkdag) beschikbaar komen, is de informatie nodig om procestaken normaal, als gepland (dezelfde dag) te kunnen uitvoeren, is de informatie onmisbaar voor het uitvoeren van noodzakelijke dagelijkse procestaken (binnen 4 uur) of is de informatie onmisbaar voor veilige zorg (24/7)?

Integriteit (I): hierbij maak je de inschatting:

- kan een foutief gegeven zonder grote consequenties worden hersteld,
- of leiden fouten tot ernstige verstoring van interne werkprocessen,
- of leiden fouten tot verstoring in ketenprocessen (extern) met juridische, financiële of reputatie risico's
- of kunnen fouten zelfs leiden tot (ernstige) gezondheidsschade. Denk aan persoonsverwisseling of fouten (contra-indicaties, allergieën; doseringen; doorverwijzingen) bij invoer, gebruik van onjuiste coderingen of referentietabellen, geautomatiseerde fouten, te laat ingevulde consultverslagen of onderzoekuitslagen.

Vertrouwelijkheid (V): voor het bepalen van de vertrouwelijkheid kijk je naar de bron en doelgroep van de gegevens. Varianten zijn hier:

- informatie uit publiek-toegankelijke bronnen (bv. richtlijnen) of die bedoeld zijn voor algemeen publiek (bv. voorlichting);
- informatie die intern is gemaakt en voor intern gebruik is bedoeld (interne werkwijzen, afspraken, notulen) waarbij openbaarmaking geen schade kan aanbrengen aan de organisatie, relaties of individuen;
- informatie die vertrouwelijk is waarbij openbaarmaking (financiële, reputatie-, juridisch, vertrouwens)schade kan veroorzaken (bijvoorbeeld informatie uit functioneringsgesprekken met medewerkers)
- gegevens die vallen binnen het beroepsgeheim, bijvoorbeeld persoonlijke gezondheidsinformatie, waarbij openbaarmaking een inbreuk kan betekenen op de persoonlijke levenssfeer, overtreding is van wetgeving en waarbij misbruik van deze gegevens kan leiden tot (gezondheids)risico's voor de betrokkenen.

De gevolgen van inbreuken op deze 3 aspecten beschikbaarheid, integriteit en vertrouwelijkheid of de eisen die hieraan kunnen worden gesteld, kunnen worden geclassificeerd. Met deze classificatie bepaal je de mate van inspanning die preventie en/of herstel van inbreuken vergt.

Classificatie ('klasse') informatiebeveiliging	veilige zorg – eis aan beschikbaarheid	schade bij inbreuk op data integriteit	eis aan vertrouwelijkheid
0	de volgende werkdag	herstelbaar, weinig/geen consequenties	Publiek
1	dezelfde dag	verstoring interne processen, herstelbaar	Intern
2	binnen 4 uur	verstoring ketenprocessen, kans op juridische, financiële of reputatie schade	Vertrouwelijk
3	24/7	bovenstaande en mogelijk (ernstige) gezondheidsschade	Geheim

Stap 3 | Stel het risicoschema op voor jouw praktijk en ga met de set basismaatregelen aan de slag

In de derde stap combineer je de gegevens uit de eerste en tweede stap zodanig dat duidelijk wordt op welke vlakken de basismaatregelen zich moeten richten.

Dus: welke (informatie)processen, met welke systemen verwerken we welke gegevenscategorieën? En welke beveiligingsklasse hoort daarbij?

In tabel 2 laten we zien hoe zo'n overzicht eruit kan zien.

Praktijkproces / systeem	Gegevens categorieën	Klasse IB		
		Beschik-baarheid	Integriteit	Vertrou-welijkheid
Primair - 1e lijns zorg/ Je His Je Patiëntportaal Je KIS Je Telefooncentrale	• bijzondere persoons-gegevens (medisch)	3	3	3
Secundair - ondersteunend/ Je PraktijkNetwerk Je Praktijkwebsite	• persoonsgegevens (NAW, geb. datum) • praktijkgegevens - financieel - juridisch (contracten) - beveiliging - algemeen	2 1/2 1/2 0/1	2 1/2 1/2 0/1	2 1/2 1/2 0/1
Tertiair - bestuurlijk/ Je HRM-systeem Je financiële administratie applicatie	• persoonsgegevens (NAW, geb. datum, BSN) • praktijkgegevens - financieel - juridisch (contracten) - beveiliging - algemeen	3 1/2 1/2 0/1	3 1/2 1/2 0/1	3 1/2 1/2 0/1

Tabel 2: voorbeeld van de klassen voor informatiebeveiliging voor verschillende gegevenscategorieën

Bij de hoge beveiligingsklassen 2 en 3 horen de volgende basismaatregelen.

Beschikbaarheid – basisbeveiligingsmaatregelen

- **A.08.13[2] Back-up van informatie**

  Belangrijk is dat de back-up wordt opgeslagen op een medium onafhankelijk van het gebruikte systeem. Zo heb je een herstelpunt dat niet geraakt wordt als het gebruikte informatiesysteem faalt of door hackers wordt gegijzeld. Bij cloud oplossingen is het gebruikelijk dat de aanbieder een back-up functionaliteit faciliteert. Verifieer dan dat dit in het contract ook is afgesproken.

- **A08.14 Redundantie van informatieverwerkende faciliteiten**

  Redundantie betekent dat er een alternatief in werking treedt als het primaire systeem niet functioneert. Denk bijvoorbeeld aan noodstroomvoorziening, of een systeem dat lokaal te gebruiken is als internet uitvalt.

Integriteit – basisbeveiligingsmaatregelen (BBM-I)

- **A.05.37 Gedocumenteerde bedieningsprocedures**

  Zorg dat vastgelegd is hoe met de systemen omgegaan dient te worden door medewerkers, en zie toe op de naleving van deze procedures

Vertrouwelijkheid – basisbeveiligingsmaatregelen

- **A08.24 Gebruik van cryptografie**

  Zorg ervoor dat informatie alleen versleuteld wordt opgeslagen. In de regel mag je dit verwachten van de leverancier van het systeem maar check dat dit ook echt gebeurt.

- **A08.03 Beperking toegang tot informatie**

  Het gaat hier om authenticatie (ben je wie je zegt dat je bent) en om autorisatie (mag je op basis van je rol/functie bij de informatie). 2-Factor authenticatie (combinatie van gebruikersnaam en wachtwoord met aanvullend een token of biometrisch gegeven) is het minimale niveau voor authenticatie. De meeste online diensten (Vecozo, LSP, etc) stellen hogere eisen, zoals gebruik van UZI-pas. Autorisatie regel je in het betreffende informatiesysteem. Meestal is dit gebaseerd op rechten die toegekend worden aan specifieke rollen. Dit wordt in de meeste systemen de autorisatiematrix genoemd.

[2] De nummers A.0#.## verwijzen naar de gelijk genummerde Beheersmaatregelen voor informatiebeveiliging uit de internationale norm ISO/IEC 27002:2022 (nl) voor Informatiebeveiliging, cybersecurity en bescherming van de privacy. Raadpleeg voor toepassing deze volledige beheersmaatregelen, die worden opgenomen in bijlage A van de nieuwe versie van NEN7510-1 die in 2024 wordt verwacht.

Stap 4 | Schat het risico van algemene bedreigingen in en spreek extra maatregelen af

Risico impact en benadering informatiebeveiligingsrisico's

Een informatiebeveiligingsrisico wordt ingeschat door de kans dat (of de frequentie waarin) een inbreuk plaatsvindt te vermenigvuldigen met het effect (ernst, schade) van die inbreuk op beschikbaarheid, vertrouwelijkheid en integriteit. In onderstaande tabel is vastgelegd hoe deze elementen kunnen worden gescoord en tot welke risico-impact dat leidt.

Bijvoorbeeld (kies de waarden die passen bij jouw praktijkorganisatie)

Kans	**Frequentie**			**Score**
klein, <30%	jaarlijks of minder			1
middel, 30-60%	maandelijks-elk kwartaal			2
groot, > 60%	dagelijks-wekelijks			3
Effect	**Ernst**	**Privacy inbreuk**	**Schade**	
gering	geen letsel; ergernis	één, enkele patiënt	< € 500	1
matig	niet blijvend, geen ernstig letsel	selectie van patiënten	€500 - €10000	2
ernstig	ernstig en/of blijvend letsel	mogelijk alle patiënten	> €10000	3

Risico-impact = Kans x Effect

		Kans		
		1	2	3
Effect	1	1	2	3
	2	2	4	6
	3	3	6	9
		Risico-impact		

Informatiebeveiligingsrisico's kunnen als volgt worden aangepakt:

accepteren als onvermijdelijk (beschikbaarheid prevaleert in noodsituaties boven vertrouwelijkheid) of redelijk (kosten/baten).

verminderen van optreden van het risico of de gevolgen door maatregelen

vermijden door het proces of systeem anders in te richten zodat het risico zich niet meer kan voordoen.

verleggen van verantwoordelijkheid voor schade (juridisch; contracten, verzekeren)

Procedure risicobeoordelingen algemene bedreigingen/kwetsbaarheden

a) Startpunt van de risicobeoordelingen zijn algemene potentiële bedreigingen zoals die eerder werden vastgesteld in NHG Praktijkwijzer Informatiebeveiliging 2018 en de InEen top 12 risicogebieden. Je vindt deze nog steeds actuele bedreigingen in de tabel hieronder.

b) Deze kunnen worden aangevuld met specifieke, niet eerder onderkende risico's die uit workshops, meldingen of uit incidenten naar voren komen.

c) Een risico(her)beoordeling vindt minimaal 1x/3jaar plaats in een (groeps)workshop met praktijkmanager(s) uit de HAGRO en een adviseur/deskundige van de regionale huisartsenorganisatie.

d) Het overzicht van risicobeoordelingen en maatregelen wordt vastgelegd in het kwaliteitssysteem.

In tabel 3 vind je een voorbeeld van een risicobeoordeling met bijbehorende maatregelen

Nr	Bedreiging/Risico	Bron	BIV-risico/ Naleving	Kans	Effect	Impact	Aanvullende maatregelen
1	(Natuur)schade van buiten of binnen: brand, overstroming, kabelbreuk/brand, lekkage, overstroming	Webdossier Informatie-beveiliging	Beschik-baarheid	1	3	3	**A07.01** Fysieke beveiligingszones **A08.13** Back-up van informatie **A08.14** Redundantie van informatiever-werkende faciliteiten
2	Inbraak/inbraak, of binnenlopen	Webdossier Informatie-beveiliging	Vertrouwe-lijkheid	2	2	4	**A07.01** Fysieke beveiligingszones **A08.13** Back-up van informatie **A07.07** 'Clear desk' en 'clear screen'

Nr	Bedreiging/Risico	Bron	BIV-risico/ Naleving	Kans	Effect	Impact	Aanvullende maatregelen
3	Insluiping, diefstal door bezoeker/in-braak, of binnenlopen	Webdossier Informatie-beveiliging	Beschik-baarheid, Vertrouwe-lijkheid	2	2	4	**A07.01** Fysieke beveiligingszones **A08.13** Back-up van informatie **A07.07** 'Clear desk' en 'clear screen' **A07.08** Plaatsen en beschermen van apparatuur **A07.06** Werken in beveiligde zones - huisregels
4	Inbraak op intern LAN/werkstations	Webdossier Informatie-beveiliging	Beschik-baarheid, Integriteit, Vertrouwe-lijkheid	1	3	3	**A07.07** 'Clear desk' en 'clear screen' **A08.07** Bescherming tegen malware **A08.19** Installeren van software op operationele systemen **A08.20** Beveiliging netwerkcom-ponenten
5	Foutieve/vertraagde invoer gegevens	Webdossier Informatie-beveiliging	Beschik-baarheid, Integriteit	3	2	6	A05.37 Gedocumenteerde bedienings-procedures
6	Onterechte inzage/ openbaarmaking gegevens door eigen medewerkers	Webdossier Informatie-beveiliging	Vertrouwe-lijkheid	1	3	3	**A06.01** Screening **A05.18** Toegangsrechten **A07.14** Veilig verwijderen of hergebrui-ken van apparatuur **A08.15** Logging
7	Verlies apparatuur/ gegevensdragers	Webdossier Informatie-beveiliging	Beschik-baarheid, Vertrouwe-lijkheid	2	2	4	**A06.02** Arbeidsovereenkomst - ge-dragscode **A05.09** inventarislijst **A08.24** Gebruik van cryptografie (BBM-V)
8	Uitval medewerkers	Webdossier Informatie-beveiliging	Beschik-baarheid	2	2	4	**A05.02** Rollen en verantwoordelijk-heden bij informatiebeveiliging
9	Inzage gegevens door externe medewerkers/ wet- en regelgeving onbekend, waardoor onterecht informatie wordt gedeeld of leveranciers niet goed worden aangestuurd	Webdossier Informatie-beveiliging	Vertrouwe-lijkheid	2	2	4	**A05.15** Toegangsbeveiliging **A05.20** Adresseren van informatiebeveiliging in leveranciers-overeenkomsten
10	Medewerker volgt phishing-link	Webdossier Informatie-beveiliging	Beschik-baarheid, Integriteit, Vertrouwe-lijkheid	2	3	6	**A06.02** Arbeidsovereenkomst - gedrags-code **A06.03** Bewustwording van, opleiding en training in informatiebeveiliging **A08.07** Bescherming tegen malware
11	Te verwijderen apparatuur of papier bevat data	Webdossier Informatie-beveiliging	Vertrouwe-lijkheid	1	3	3	**A07.14** Veilig verwijderen of hergebrui-ken van apparatuur

Nr	Bedreiging/Risico	Bron	BIV-risico/ Naleving	Kans	Effect	Impact	Aanvullende maatregelen
12	Gestolen apparatuur	Webdossier Informatie-beveiliging	Vertrouwe-lijkheid	1	3	3	Zie nr. 2,3
13	Systeem/ apparaat/ toepassing voldoet niet functioneel/ applicaties/koppeling tussen applicaties onvoldoende kwaliteit	Webdossier Informatie-beveiliging	Beschik-baarheid, Integriteit, Vertrouwe-lijkheid	2	2	4	**A05.08** Informatiebeveiliging in projectmanagement
14	Complexiteit organi-satie / management IB	Webdossier Informatie-beveiliging	Beschik-baarheid, Integriteit, Vertrouwe-lijkheid	2	2	4	**A06.03** Bewustwording van, opleiding en training in informatiebeveiliging
15	Tekortschieten naleving (ISMS, wetgeving)/Taken en verantwoorde-lijkheden rondom Informatiebeveiliging niet expliciet gemaakt. Slecht beveiligingsbeleid, slecht management ICT - middelen, geen structurele controles	Webdossier Informatie-beveiliging	Beschik-baarheid, Integriteit, Vertrouwe-lijkheid	2	2	4	Zie nr. 14 **A05.36** Naleving van beleid, regels en normen voor informatiebeveiliging 0930 Directiebeoordeling
16	Ontbrekende/achter-blijvende informatie uit zorgketen	Webdossier Informatie-beveiliging	Beschik-baarheid, Integriteit	2	2	4	**A05.14** Overdragen van informatie **A05.20** Adresseren van informatiebeveiliging in leveranciers-overeenkomsten
17	Verouderde software mbt updates/security patches	Workshop	Beschik-baarheid, Vertrouwe-lijkheid	1	3	3	**A05.20** Adresseren van informatiebeveiliging in leveranciers-overeenkomsten
18	Onbeheerste wijzigin-gen (andere ISP)	Workshop	Beschik-baarheid, Integriteit, Vertrouwe-lijkheid	2	3	6	**A08.32** Wijzigingsbeheer
19	Onvoldoende bekend met wet-, regelgeving, ISMS & toepassing/mede-werkers en externen houden zich niet aan de richtlijnen, zijn zich niet bewust van de gevaren	Workshop	Naleving	2	3	6	**A06.02** Arbeidsovereenkomst - ge-dragscode **A06.03** Bewustwording van, opleiding en training in informatiebeveiliging A08.15 Logging (NEN7513) **A05.34** Privacy en bescherming van persoonsgegevens - AVG

Nr	Bedreiging/Risico	Bron	BIV-risico/ Naleving	Kans	Effect	Impact	Aanvullende maatregelen
20	Logische toegang (toegang tot applicaties en netwerken etc) is niet goed geregeld	Webdossier Informatiebeveiliging	Beschikbaarheid, Vertrouwelijkheid	2	2	4	**A05.15** Toegangsbeveiliging **A05.18** Toegangsrechten
21	Gebruik 'mobile devices' en toepassen telewerken onvoldoende beschermd	Webdossier Informatiebeveiliging	Beschikbaarheid, Vertrouwelijkheid	2	2	4	**A06.07** Werken op afstand
22	Incidenten, kwetsbaarheden worden niet gemeld door medewerkers en worden door de organisatie niet opgepakt	Webdossier Informatiebeveiliging	Beschikbaarheid, Integriteit, Vertrouwelijkheid	2	2	4	**A06.03** Bewustwording van, opleiding en training in informatiebeveiliging **A06.08** Melden van informatiebeveiligingsgebeurtenissen
22	Registratie (medewerkers) niet volledig niet correct	Webdossier Informatiebeveiliging	Integriteit, Vertrouwelijkheid	2	2	4	**A05.02** Rollen en verantwoordelijkheden bij informatiebeveiliging en verantwoordelijkheden informatiebeveiliging **A06.01** Screening **A05.18** Toegangsrechten
23	Beveiliging bij belangrijke leveranciers niet op orde. Beveiliging toegang tot netwerk en/of applicaties / bestanden onvoldoende	Webdossier Informatiebeveiliging	Vertrouwelijkheid	2	3	6	**A05.20** Adresseren van informatiebeveiliging in leveranciersovereenkomsten **A08.24** Gebruik van cryptografie (BBM-V) **A05.18** Toegangsrechten **A05.34** Privacy en bescherming van persoonsgegevens - AVG
24	Er is onvoldoende kennis en adequate procedures voor het beheer van ICT middelen.	Webdossier Informatiebeveiliging	Beschikbaarheid, Integriteit, Vertrouwelijkheid	2	2	4	**A05.02** Rollen en verantwoordelijkheden bij informatiebeveiliging en verantwoordelijkheden informatiebeveiliging **A06.03** Bewustwording van, opleiding en training in informatiebeveiliging **A08.03** Beperking toegang tot informatie **A05.20** Adresseren van informatiebeveiliging in leveranciersovereenkomsten
25	Downloads vanuit het HIS (Je HIS) komen lokaal op C://uwpraktijknetwerk	Incident202227	Vertrouwelijkheid	2	2	4	**A08.03** Beperking toegang tot informatie
26	Je risico niet eerder genoemd	Je werkoverleg					

Tabel 3: Risicobeoordeling

Aan de slag na de risicoafweging

Na afronding van de risicoafweging, ga je aan de slag met het beleidsplan. De beschrijving daarvan vind je in het webdossier Informatiebeveiliging van NHG, LHV en InEen, te vinden op www.lhv.nl.