



Informatiebeveiliging in de zorg

Worsteling tussen compliance, zorg en secure werken

Roel Lijnema
ISO – Bergman Clinics maart 2024
-06-39533675

Inhoud

- Compliance / wetgeving / richtlijnen
- Control framework
De juiste dingen doen (CIS-controls)
- Toepassing framework
 - Leveranciers
 - MSP
 - Z-Cert – leveranciersrisicomanagement
 - Awareness

Klantcase: voldoen aan wet- en regelgeving en securitybeleid invullen

Roel Lijnema, Information Security Officer bij Bergman Clinics, vertelt tijdens deze sessie over de wet- en regelgeving waar de organisatie mee te maken krijgt. Hoe gaan ze bijvoorbeeld om met NEN7510 (richtlijn voor de zorg) en op welke manier zijn ze nu al bezig met NIS2? Hoe geven zij hun securitybeleid vorm?

– Roel Lijnema, Bergman Clinics



[+ Verwijzers](#)

[Mijn Bergman Clinics](#)

[Over ons](#)



[Behandelingen](#)

[Vestigingen](#)

[Medisch specialisten](#)

[Afspraak maken](#)

[Contact](#)

[Home](#) > [Over ons](#)



Wij zijn het grootste netwerk van
focusklinieken voor planbare medische zorg
in Nederland



[Informatie aanvragen](#)

[Contact opnemen](#)

Bergman Clinics heeft in Nederland verschillende locaties. Op veel locaties worden meerdere zorgprogramma's aangeboden. Zowel verzekerd als onverzekerd.

Alkmaar | Almere | Amersfoort | Amsterdam | Arnhem |
Bilthoven | Breda | Capelle aan den IJssel | Den Bosch |
Den Haag | Doetinchem | Driebergen | Ede | Emmeloord |
Enschede | Haarlem | Heerenveen | Hilversum | Hoozeveen |
Lelystad | Loenen aan de Vecht | Naarden | Rijswijk |
Rotterdam | Utrecht | Veenendaal | Zaanland | Zwolle

- 1 Bewegen
- 2 Ogen
- 3 Huid & Vaten
- 4 KNO
- 5 Vrouw
- 6 Maag & Darm

Hey, Boy Clinics

Memira



Voor de overzichtelijkheid zijn niet alle vestigingen getoond. Kijk op de website voor alle actuele klinieken incl. openingstijden.



Aantal cliënten
300.000



56

Team Bergman Clinics
1.395 Fte
233 Medisch
Specialisten



35 jaar



Verwijzingen door huisartsen naar medische specialistische zorg

Top 10

Korte toegangstijden
tot gepland eerste consult

22 dagen

[illegible]

Document	Section 4 Grouping: 2007
Form	9-0
Version	20.07.00

Compliance

Definitie

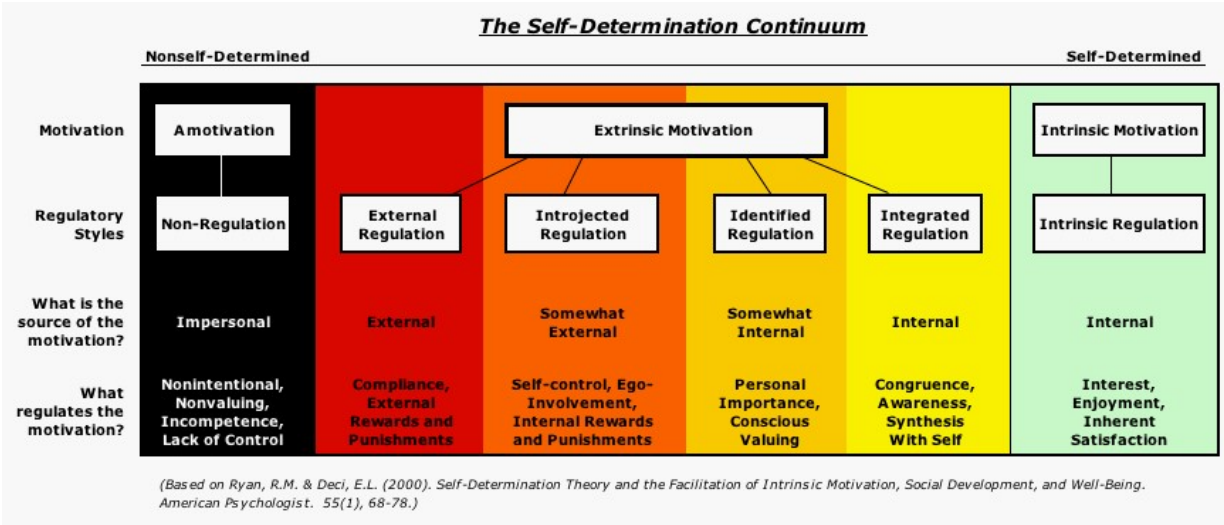
- *'Het bevorderen van en het doen toezien op de naleving van externe en interne regels die relevant zijn voor de integriteit van de organisatie. Regels en normen die de organisatie zelf stelt, horen daar uitdrukkelijk bij.'*

De laatste jaren verschuift compliance steeds meer van 'toezien op naleving van regels' naar 'bevorderen van integriteit'. Voor sommige organisaties is de volgende definitie van compliance daarom meer passend:

- *'Compliance is het versterken van de integriteit van de organisatie, haar bestuur, haar medewerkers, de markt en haar data'.*

(compliance-instituut)

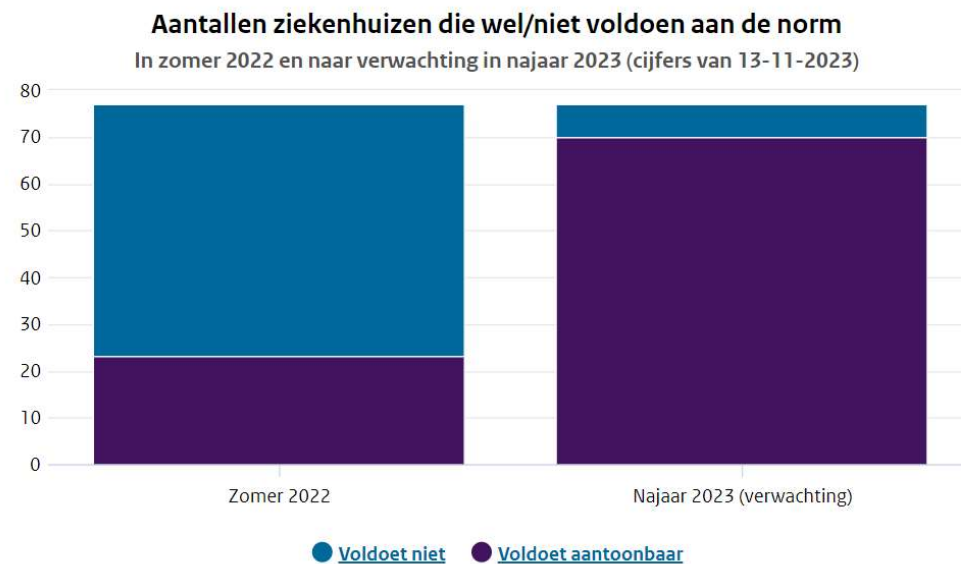
Wet & Regelgeving



Privacy/informatiebeveiliging		
Algemene verordening gegevensbescherming (AVG)	Wet	25-5-2018
KNMG Handreiking Inzage-recht door nabestaande	Richtlijn	26-11-2020
KNMG richtlijn Omsaan met medische gegevens	Richtlijn	22-9-2022
NEN 7513_2018 Medische informatica*	Norm	18-5-2018
NEN 7510_2017 Informatiebeveiliging in de zorg*	Norm	1-2-2020
NEN 7512_2015 Informatiebeveiliging in de zorg, vertrouwensbasis voor gegevensuitwisseling*	Norm	1-1-2015
NTA 7516 Medische informatica (veiligie communicatie)*	Norm	1-5-2019
NHIS Richtlijn Informatie-uitwisseling tussen huisarts en medisch specialist	Richtlijn	1-12-2017
Uitvoeringswet Algemene verordening gegevensbescherming (UAVG)	Wet	1-7-2021
Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg	Wet	1-7-2020
Wet gebruik burgerservicenummer in de zorg	Wet	18-12-2021
Wet Digitale overheid	Wet	1-7-2023
Wetsvoorstel Elektronische gegevensuitwisseling in de Zorg	Voorstel	1-7-2023
ePrivacy verordening	Voorstel	nvt
Zorg Toekomst		



IGJ – stand van zaken NEN7510



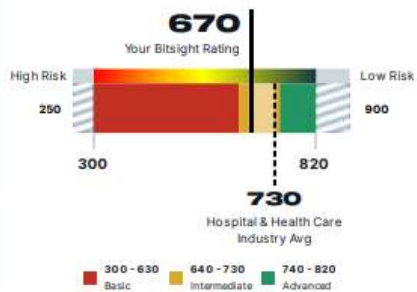


Bergman Clinics B.V.

COMPARATIVE INDUSTRY
Hospital & Health Care

WEBSITE
bergmanclinics.nl

Bitsight Security Rating



Likelihood of Ransomware Incidents

2.4x as Likely vs a 750+ company

High Risk Low Risk

Source:

<https://www.bitsight.com/resources/datasheet-bitsight-security-ratings-correlate-ransomware>

Likelihood of Data Breach Incidents

2x as Likely vs a 700+ company

High Risk Low Risk

Source:

<https://www.bitsight.com/resources/datasheet-bitsight-security-ratings-correlate-breaches>

en nu? ...In Control



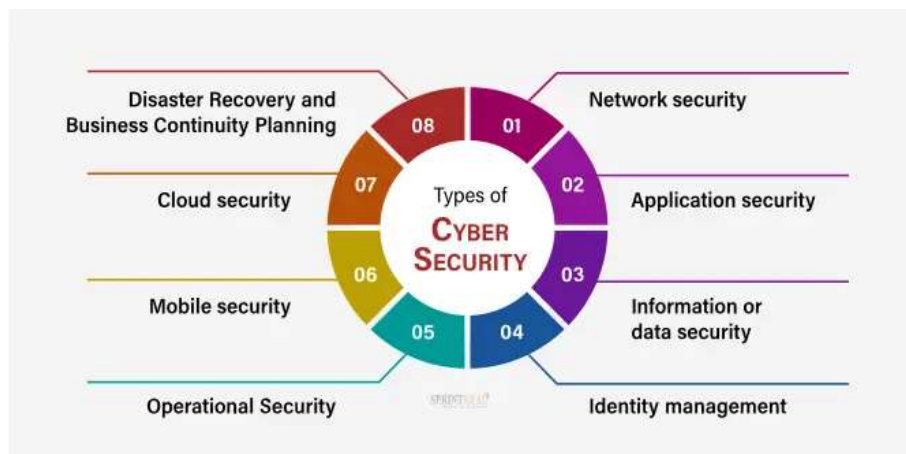
**TECHNICAL
CONTROLS**



**ADMINISTRATIVE
CONTROLS**



**PHYSICAL
CONTROLS**



EXECUTIVE SUMMARY

1.

Threat landscape

Cyber Attacks are Significantly Up

- Phishing attacks are up significantly
- New vulnerabilities with exploits in the wild are being disclosed at a faster rate
- Use of Z-Cert and ENISA threat landscape



2.

Cyber risk

25% likelihood of a significant breach via a supply chain attack

- Double down on visibility;
No security measure works 100%
- Revisit and update supply chain security standards and contracts

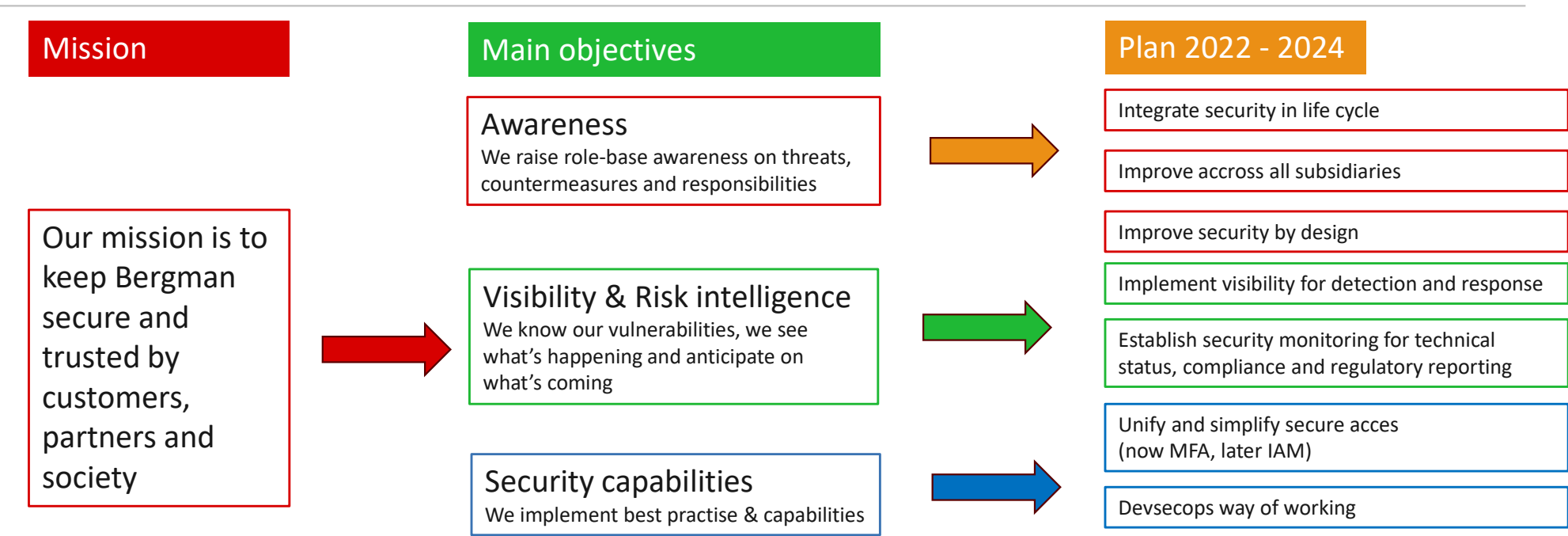
3.

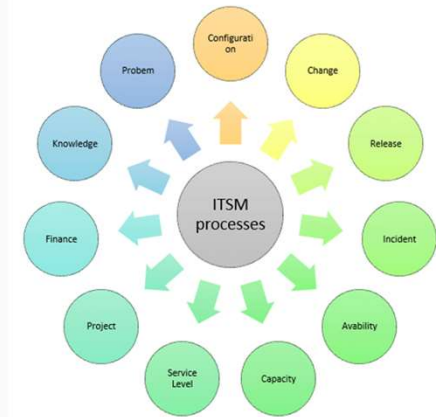
Readiness and resilience

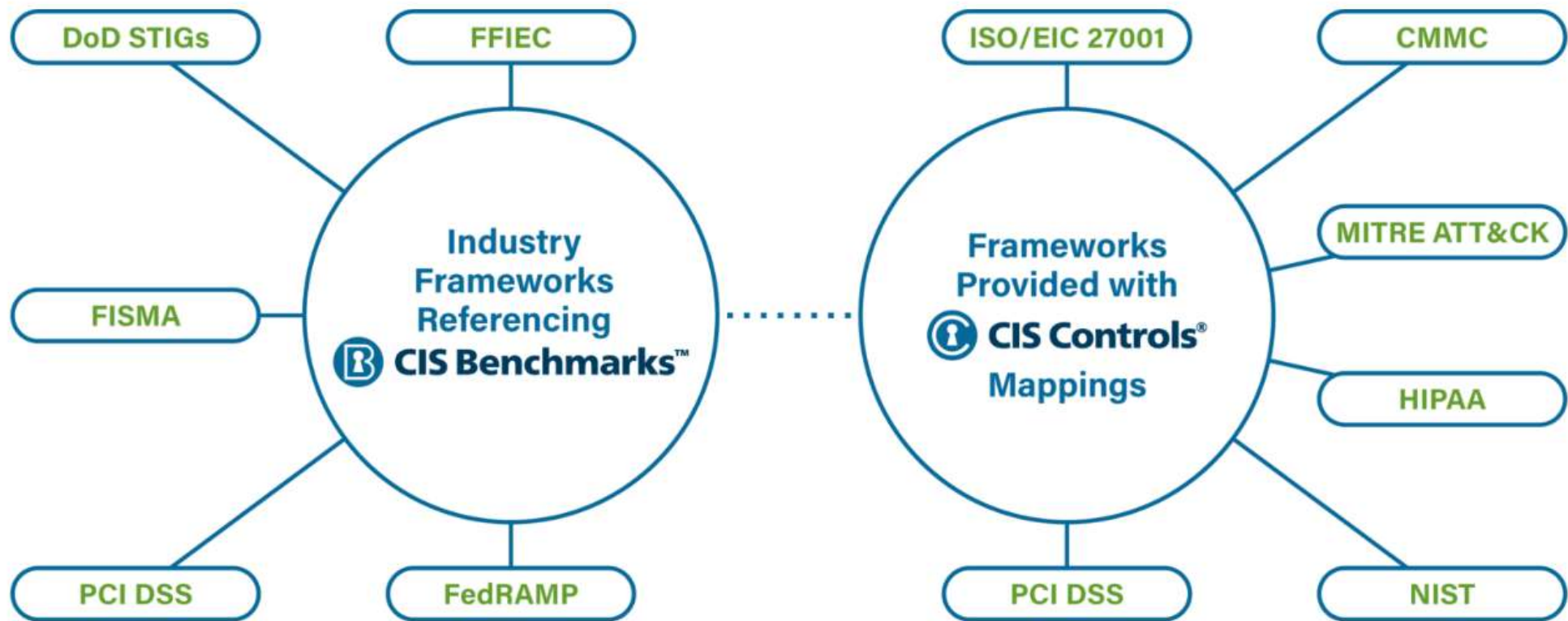
% likelihood of ransomware incident with expected loss \$10M

- EDR live and visibility growing
- Awareness training next level (KnowBe4)
- Preparing IAM tooling/implementation
- Tabletop

Overview – Security strategy & action plan – annual roadmap









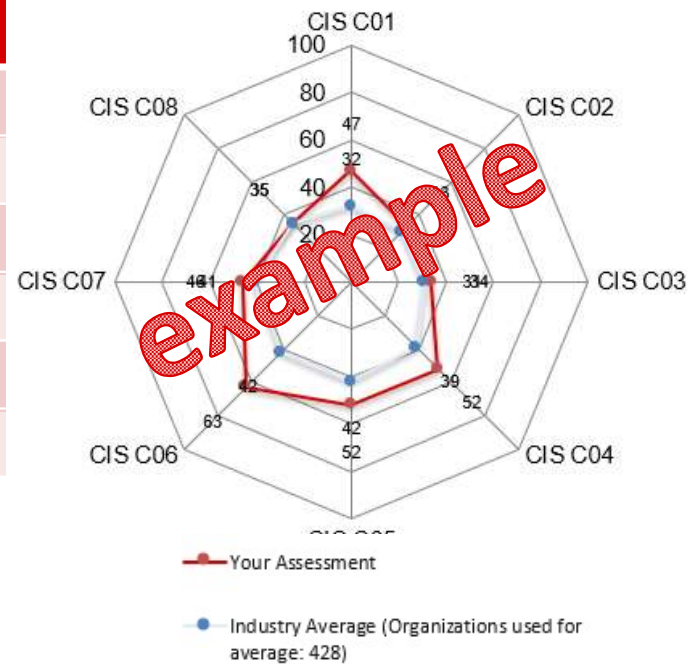
PROGRESS IN CYBERSECURITY



	Initiatives	On Track	to accelerate	Roadmap
Identify	Implement continuous cybersecurity posture visibility. Build risk owner's matrix and update quarterly.	A large, light grey rectangular area that spans the width of the 'On Track', 'to accelerate', and 'Roadmap' columns. It contains a large, red, diagonal watermark that reads "confidential".		
Protect	Implement strong identity with adaptive authentication. Improve security hygiene and patching posture. Update email security.			
Detect	Incorporate threat feeds in SOC workflows.			
Respond	Improve incidence response with automated playbooks			
Recover	Review & update business continuity plan every quarter			

Policy defined	Maturity
No policy	
Informal policy	
Partial written policy	
Written policy	
Approved written policy	
Not Applicable	

Policy implemented	Maturity
Not implemented	
Parts of policy implemented	
Implemented on some systems	
Implemented on most systems	
Implemented on all systems	
Not Applicable	

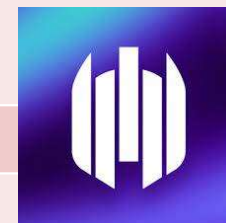


Control Reported	Maturity
Not reported	
Parts of poilicy reported	
Reported on some systems	
Reported on most systems	
Reported on all systems	
Not applicable	




Control Automated	Maturity
Not automated	
Parts of policy automated	
Automated on some systems	
Automated on most systems	
Automated on all systems	
Not applicable	

Rapportage Security



CIS	Control	Risk	Status		Project
1	Inventory and control of assets			previder	
2	Inventory and control of software				
3	Data protection				
4	Secure configuration of enterprise assets/ software				
5	Accountmanagement				
6	Acces control management				



COMPUTER EMERGENCY
RESPONSE TEAM
VOOR DE ZORG

Kleur	Risk
	High
	Medium
	Low

Rapportage Security

CIS	Control	Risk	Status	Project
7	Continuous vulnerability management			
8	Audit Log management			
9	Email and web browser protections			
10	Mallware defense			
11	Data recovery			



COMPUTER EMERGENCY
RESPONSE TEAM
VOOR DE ZORG

Rapportage Security

Samenwerking met leveranciers

BERGMAN
CLINICS

CIS	Control	RestP	Pro
12	Network infrastructure management		
13	Network monitoring and defense		
14	Security awareness and skills training		
15	Service Provider management		
16	Application software security		
17	Incident response management		
18	Penetration testing		

Bergman Clinics werkt samen met verschillende leveranciers voor bijvoorbeeld ondersteunende diensten zoals schoonmaken, wassen en steriliseren. Ook voor medische apparatuur, borst- of heupimplantaten, persoonlijke beschermingsmiddelen en voor medicatie zijn er verschillende leveranciers. Daarnaast heeft bijvoorbeeld ook de IT-afdeling eigen leveranciers.

Wij beschouwen onze leveranciers als belangrijke partners bij het versterken van onze positieve impact op milieu, maatschappij en bestuur, en het verminderen van onze voetafdruk. Eind 2022 hebben wij een contract getokend met EcoVadis, een platform dat zowel ons als onze leveranciers toetst op duurzaamheidswaarden, zoals goede werkomstandigheden voor medewerkers, gedragsregels binnen het bedrijf en een milieubeleid.

previder

KnowBe4
Human error. Conquered.

BERGman
CLINICS