



CIS Controls

Dit document beschrijft de informatiebeveiligingsmaatregelen die "klant" wil toepassen in de organisatie. De beheersmaatregelen zijn opgesteld en worden uitgevoerd volgens de bepalingen in het informatiebeveiligingsbeleid van "klant". De beheersmaatregelen zijn onder andere ebaseerd op de 18 best practices vanuit het CIS control framework.

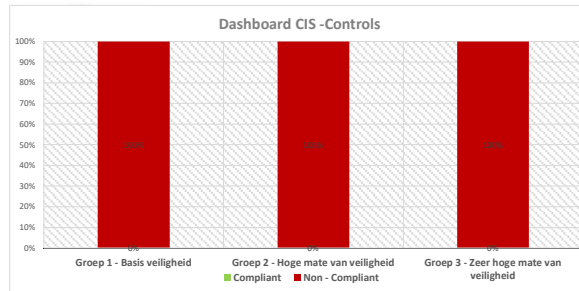
De 18 CIS Controls zijn ieder voorzien van meerdere subcontrols. In totaal zijn dit er meer dan 150. Binnen versie 8 van de CIS Controls is er een definiering op basis van 3 groepen (Implementation groups) uitgewerkt. Deze 3 groepen zijn bedoeld om een verschil toe te kennen aan verschillende soorten organisaties (o.a. grote van de organisatie) en de daar bij behorende security volwassenheid.

Group 1 past bij een kleine organisatie met (56) basis security maatregelen;

Group 2 past bij een wat grotere organisatie met (130) basis en uitgebreide security maatregelen;

Group 3 past bij een zeer security volwassen organisatie met (153) basis en zeer uitgebreide security maatregelen.

"Klant" concentreert zich op de maatregelen die beschreven zijn in "Group 1 & 2" en zal proberen daar waar het reëel en werkbaar is voor "klant" aan te voldoen.



Compliant
Non - Compliant

CIS Control	Groep 1 - Basis veiligheid	Groep 2 - Hoge mate van veiligheid	Groep 3 - Zeer hoge mate van veiligheid
CIS 01 - Inventory and Control of Enterprise Assets	0%	0%	0%
CIS 02 - Inventory and Control of Software Assets	0%	0%	0%
CIS 03 - Data Protection	0%	0%	0%
CIS 04 - Secure Configuration of Enterprise Assets and Software	0%	0%	0%
CIS 05 - Account Management	0%	0%	NA
CIS 06 - Access and Control management	0%	0%	0%
CIS 07 - Continuous Vulnerability Management	0%	0%	NA
CIS 08 - Audit Log Management	0%	0%	0%
CIS 09 - Email and Web Browser Protections	0%	0%	0%
CIS 10 - Malware Defenses	0%	0%	NA
CIS 11 - Data Recovery	0%	0%	NA
CIS 12 - Network Infrastructure Management	0%	0%	0%
CIS 13 - Network Monitoring and Defense	NA	0%	0%
CIS 14 - Security Awareness and Skills Training	0%	0%	NA
CIS 15 - Service Provider Management	0%	0%	0%
CIS 16 - Application Software Security	NA	0%	0%
CIS 17 - Incident Response Management	0%	0%	0%
CIS 18 - Penetration Testing	NA	0%	0%

CONTROL 01 Inventory and Control of Enterprise Assets 5 Safeguards IG1 2/5 IG2 4/5 IG3 5/5	CONTROL 02 Inventory and Control of Software Assets 7 Safeguards IG1 3/7 IG2 6/7 IG3 7/7	CONTROL 03 Data Protection 14 Safeguards IG1 6/14 IG2 12/14 IG3 14/14
CONTROL 04 Secure Configuration of Enterprise Assets and Software 12 Safeguards IG1 7/12 IG2 11/12 IG3 12/12	CONTROL 05 Account Management 6 Safeguards IG1 4/6 IG2 6/6 IG3 6/6	CONTROL 06 Access Control Management 8 Safeguards IG1 5/8 IG2 7/8 IG3 8/8
CONTROL 07 Continuous Vulnerability Management 7 Safeguards IG1 4/7 IG2 7/7 IG3 7/7	CONTROL 08 Audit Log Management 12 Safeguards IG1 3/12 IG2 11/12 IG3 12/12	CONTROL 09 Email and Web Browser Protections 7 Safeguards IG1 2/7 IG2 6/7 IG3 7/7
CONTROL 10 Malware Defenses 7 Safeguards IG1 3/7 IG2 7/7 IG3 7/7	CONTROL 11 Data Recovery 5 Safeguards IG1 4/5 IG2 5/5 IG3 5/5	CONTROL 12 Network Infrastructure Management 8 Safeguards IG1 1/8 IG2 7/8 IG3 8/8
CONTROL 13 Network Monitoring and Defense 11 Safeguards IG1 0/11 IG2 6/11 IG3 11/11	CONTROL 14 Security Awareness and Skills Training 9 Safeguards IG1 8/9 IG2 9/9 IG3 9/9	CONTROL 15 Service Provider Management 7 Safeguards IG1 1/7 IG2 4/7 IG3 7/7
CONTROL 16 Applications Software Security 14 Safeguards IG1 0/14 IG2 11/14 IG3 14/14	CONTROL 17 Incident Response Management 9 Safeguards IG1 3/9 IG2 8/9 IG3 9/9	CONTROL 18 Penetration Testing 5 Safeguards IG1 0/5 IG2 3/5 IG3 5/5