17.05.2024	Internal
Status van de documentatie	Approved
Versie	V.1.0
Opgeslagen door gebruiker	MMC | Muench
Noteer datum	21.05.2024

Assurance statement NIS 2

– – AD - Bijbehorende documentatie

Münch Management Consultancy

Kwaliteit

Version	Date	Author	Type of change	Status of documentation
0.1	Versie	Datum	Auteur	Soort wijziging
Status van de documentatie	0.1	Versie	Datum	Auteur
Soort wijziging	Status van de documentatie	0.1	Versie	Datum
	SIA			02.05.2024
	Selecteer een element.			Select an element.
	Selecteer een element.			Select an element.
	Selecteer een element.			Select an element.
	Selecteer een element.			Select an element.
	Selecteer een element.			Select an element.
	Selecteer een element.			Select an element.

Teamdrive MMC_Management Systems

Selecteer een element.	Place of storage
MMC	Teamdrive MMC_Management Systems

Xylem

Plaats van opslag	MMC	Teamdrive MMC_Management Systemen
Information security	IS	
Information security management system	ISMS	
MMC	Teamdrive MMC_Management Systemen	
IS	Xylem	

NIS 2 Nalevingsbeoordeling, uitgevoerd van 02 mei tot 15 mei 2024 door MMC

No.	Name of documentation	Description
[1]	AD_2024_NIS 2 Compliance Assessment_XNL	NIS 2 Compliance assessment, carried out May 02 to May 15th 2024 by MMC
[2]		
[3]		
[4]		
[5]		
[6]		
[7]		

[8]		
[9]		
[10]		

Voorwaarde:

- Toegang tot de volgende mappen en bestanden:N.v.t.

Inhoudsopgave

1 Introductie

Deze Assuranceverklaring wordt afgegeven namens en voor het topmanagement van Xylem Water Solutions Nederland B.V., hierna te noemen Xylem.

2 Algemeen

De NIS 2-richtlijn (Network and Information System Security) is een EU-brede verordening die tot doel heeft een hoog gemeenschappelijk niveau van beveiliging van netwerk- en informatiesystemen in de EU te waarborgen. Het breidt de vereisten en het toepassingsgebied van de oorspronkelijke NIS-richtlijn uit om het toenemende landschap van cyberbeveiligingsdreigingen aan te pakken. De richtlijn zal relevant zijn voor een breder scala van sectoren en bedrijven, waaronder belangrijke dienstverleners en digitale diensten. Het moet uiterlijk in oktober 2024 in nationaal recht zijn omgezet. Belangrijke elementen zijn onder meer risicobeheersmaatregelen, rapportageverplichtingen in geval van beveiligingsincidenten en het vergroten van de nationale cyberbeveiligingscapaciteiten.

Naast een preambule bestaat de definitieve tekst van de NIS 2-richtlijn van 14 december 2022 uit negen hoofdstukken, waarbij "Hoofdstuk IV, Cybersecurity Risk-Management Measures and Reporting Obligations", werd gebruikt als het relevante hoofdstuk in het kader van deze assurance-verklaring voor het beveiligen van de toeleveringsketen van de klanten van Xylem.

3 Naderen

3.1 Relevante internationale certificeringen

De naleving van de risicobeperkende maatregelen die momenteel door Xylem worden genomen als onderdeel van haar

- ISO/IEC 20000-1:2018,
- ISO/IEC 27001:2013,
- ISO/IEC 27017:2015 en
- ISO/IEC 27701:2019

certificeringen met de eisen van de

- NIS 2-richtlijn, hoofdstuk IV,

werden beoordeeld.

3.2 Relevante hoofdstukken en artikelen van de NIS 2-richtlijn

Hoofdstuk IV van de NIS 2-richtlijn bevat de volgende zes artikelen:

- Artikel 20, Governance, NIS 2-richtlijn.
- Artikel 21, Maatregelen voor het beheer van cyberbeveiligingsrisico's, NIS 2-richtlijn.
- Artikel 22, gecoördineerde beoordelingen van veiligheidsrisico's op het niveau van de Unie van kritieke toeleveringsketens, NIS 2-richtlijn.
- Artikel 23, Rapportageverplichtingen, NIS 2-richtlijn.
- Artikel 24, Gebruik van Europese regelingen voor cyberbeveiligingscertificering, NIS 2-richtlijn.
- Artikel 25, Normalisatie, NIS 2-richtlijn.

De certificeringen ISO 27001, ISO 20000, ISO 27017 en ISO 27701 van Xylem bestrijken gezamenlijk een breed spectrum aan beveiligings- en privacybeheerpraktijken die aanzienlijk overeenkomen met de NIS2-vereisten.

4 MAATREGELEN VOOR HET BEHEER VAN CYBERBEVEILIGINGSRISICO'S EN RAPPORTAGEVERPLICHTINGEN

Het managementsysteem, genaamd "Business Management System", dat alle aspecten van de bovengenoemde internationale en nationale normen omvat, is uitgebreid gedocumenteerd, met behulp van verschillende tools en afzonderlijke bestanden, voornamelijk gebaseerd op MS Word en MS Excel.

4.1.1 Objectief bewijs

- AD_5.1_BMS-framework_Xylem
- AD_6.3_BMS manual_XYLEM

4.2 Governance

De vereisten met betrekking tot governance worden gedekt door zeven beleidslijnen, die zowel algemene als specifieke informatiebeveiligingsaspecten behandelen, waaronder cyberbeveiliging, cloudbeveiliging en gegevensbeschermingskwesties.

4.2.1 Objectief bewijs

- PL_A.5.1_Beheerder
- PL_A.5.1_Bedrijfsbeheersysteem
- PL_A.5.1_Wijzigings- en releasebeheer
- PL_A.5.1_Beleid voor ontwikkelaars
- PL_A.5.1_Eindgebruiker
- PL_A.5.1_Personeel en personeelsbeheer
- PL_A.5.1_Beheer van leveranciers

Een juridisch en vergunningenregister documenteert alle relevante wettelijke vereisten, terwijl contractuele en rapportagevereisten worden gedekt door een aanvullend document.

4.2.2 Objectief bewijs

- RC_A.18.1_2024_Juridisch en vergunningenregister

Eenmaal per jaar worden er meerdere interne en externe audits uitgevoerd en goed gedocumenteerd.

4.2.3 Objectief bewijs

- RC_9.2_20240115_Audit plan_XDE_XNL_LUD
- RC_9.2_20240115_Audit report_XDE_XNL_LUD_signed
- RC_9.2_20240115_Actie list_XDE_XNL_LUD

Er is een trainingsprogramma, vergezeld van regelmatige trainingen, dat informatiebeveiligingseisen vertaalt en interpreteert naar Xylem-specifieke vereisten. De effectiviteit van trainingen wordt geëvalueerd.

4.2.4 Objectief bewijs

- DP_7.2_Opleiding en bewustmaking
- AD_7.2_Trainingsprogramma
- RC_7.2_20240219_Deelnemerslijst BMS Awareness training_LAB
- RC_7.2_20240105_Deelnemerslijst BMS Awareness training_XLC_Recording
- PT_7.3_20240105_BMS_Bewustwording_Training_2024_Opname
- PT_7.3_20240108_BMS Bewustzijn Training_SMS 2024
- PT_7.3_20240108_BMS_Bewustwording_Training_2024
- PT_7.3_Transitie ISO 27001-2022
- PT_7.3_20240227_Het belang van een levend BMS

Alle beheerrelevante taken worden gedocumenteerd in een actiebeheersysteem.

4.2.5 Objectief bewijs

- AD_8.1_2024_Actie management_Xylem

4.3 Maatregelen voor het beheer van cyberbeveiligingsrisico's

De holistische benadering van risicobeheer omvat een breed scala aan verschillende soorten risico's, waaronder cyberbeveiligingsrisico's.

4.3.1 Objectief bewijs

- DP_6.1_Risicobeheer
- RC_6.1_202404_Risicobeheer
- RC_6.1_2024_Risico management_2022

In het geval dat cyberbeveiligingsrisico's reëel worden, zijn er specifieke acties binnen de huidige BC-planning.

4.3.2 Objectief bewijs

- AD_A.17.1_2024_BC_handleiding_Xyleem

Het risicomanagementproces wordt op een duidelijke en begrijpelijke manier gedocumenteerd, inclusief de risicobeoordeling en risicobehandelingsactiviteiten.

4.3.3 Objectief bewijs

- PD_6.1_Risico management_EN_V.2.12

Het beheer van informatiebeveiligingsincidenten maakt deel uit van een holistisch en goed gedocumenteerd proces voor het beheer van beveiligingsincidenten als een integraal onderdeel van het geïntegreerde beheersysteem van Xylem. Het omvat gebeurtenissen en incidenten op het gebied van informatiebeveiliging, bijbehorende communicatielijsten en aanroepen in de bedrijfscontinuïteitsplanning, met inbegrip van de ICT-gereedheid van diensten binnen het toepassingsgebied van het ISMS.

4.3.4 Objectief bewijs

- AD_8.1_2024_Actie management_Xylem
- DP_A.16.1_Beheer van beveiligingsincidenten
- DP_A.5.1_Beheer van incidenten en serviceaanvragen
- DP_A.5.1_Probleembeheer
- DP_A.17.1_Continuïteits- en beschikbaarheidsbeheer

De back-up van kritieke systemen en gegevens wordt uitbesteed aan een tier 4-datacenterprovider, die wordt gecontroleerd door frequente leveranciersaudits. Er is een inbraakdetectie- en preventiesysteem aanwezig, een extern onderzoek volgens de Duitse KRITIS-vereisten is gepland voor eind juni 2024. Bij dit onderzoek wordt zowel rekening gehouden met monitoring als met forensische kwesties.

4.3.5 Objectief bewijs

- AD_8.1_2024_Actie management_Xylem

Een beleid regelt de interactie met dienstverleners en leveranciers, de kriticiteit van dienstverleners en verkopers wordt bepaald en bijgehouden als onderdeel van het risicobeheerproces.

4.3.6 Objectief bewijs

- PL_A.5.1_Beheer van leveranciers
- AD_A.15.2_Leverancier evaluation_BOI
- AD_A.15.2_Leverancier evaluation_LAB
- AD_A.15.2_Leverancier evaluation_LUD
- AD_A.15.2_Leverancier evaluation_XDE
- AD_A.15.2_Leverancier evaluation_XNL

De netwerkbeveiliging wordt onderhouden door een specifieke organisatorische eenheid binnen Xylem, gecontroleerd door de management system officer (MSO), respectievelijk local management system officer (LMSO) op verschillende locaties binnen het toepassingsgebied van het ISMS.
1st party, 2nd party en 3rd party audit worden regelmatig uitgevoerd, de resultaten zullen minimaal één keer per jaar worden gecontroleerd door het topmanagement binnen de management review.

4.3.7 Objectief bewijs

- RC_9.3_202402007_Notulen van de review_Xylem van de directie

Operationeel beleid en gedocumenteerde procedures bevatten regels om ICT-kwesties binnen het toepassingsgebied uit te voeren, waaronder basisidentiteits- en toegangsbeheer, bescherming tegen malware, configuratiebeheer, back-up en cryptografie.

4.3.8 Objectief bewijs

- PL_A.5.1_Beheerder
- PL_A.5.1_Eindgebruiker
- DP_7.2_Opleiding en bewustmaking
- DP_7.5_Controle van gedocumenteerde informatie
- DP_5.1_Zakelijke relatie en serviceniveau managment_XYLEM

- DP_A.5.1_Servicerapportage
- DP_A.5.1_Beheer van de vraag en de capaciteit
- DP_A.5.1_Beheer van incidenten en serviceaanvragen
- DP_A.5.1_Probleembeheer
- DP_A.16.1_Beheer van beveiligingsincidenten
- DP_A.17.1_Continuïteits- en beschikbaarheidsbeheer
- DP_A.5.1_Beheer van servicemiddelen en -configuratie

Personeelszaken zijn locatiespecifiek en deels uitbesteed aan interne HR-partners van Xylem, gecontroleerd door een personeels- en persoonlijk managementbeleid en de daaruit voortvloeiende documentatie.

4.3.9 Objectief bewijs

- PL_A.5.1_Personeel en personeelsbeheer

4.4 Rapportageverplichtingen

Communicatielijsten regelen themaspecifieke contacten voor zowel geïnteresseerden als belangengroepen. Dit omvat ook relevante contacten met autoriteiten voor het melden van meldingsplichtige beveiligingsincidenten.

4.4.1 Objectief bewijs

- DP_A.5.1_Servicerapportage
- AD_9.4_2024_Contractbeheer en servicerapportage
- AD_4.1_2024_Context van de oganization_Xylem
- RC_7.4_2024_Communicatie lists_BOI
- RC_7.4_2024_Communicatie lists_LAB
- RC_7.4_2024_Communicatie lists_LUD
- RC_7.4_2024_Communicatie lists_XDE
- RC_7.4_2024_Communicatie lists_XNL

De implementatie van een uitbesteed Security Operations Center (SOC) is in voorbereiding. Momenteel worden de respectievelijke taken overgenomen door de MSO of beter gezegd LMSO.

4.4.2 Objectief bewijs

- RC_A.6.1_2024_Lijst van projecten

4.5 Gebruik van Europese regelingen voor cyberbeveiligingscertificering

De toeleveringsketen volgens ISMS-relevante diensten en goederen wordt aangepakt door middel van een leveranciersbeheerbeleid dat interne richtlijnen biedt over hoe en welke problemen moeten worden aangepakt binnen contractuele overeenkomsten met leveranciers, waaronder Dit omvat geheimhoudingsovereenkomsten (NDA's) en andere contractuele overeenkomsten met betrekking tot de relatie met leveranciers.

4.5.1 Objectief bewijs

- PL_A.5.1_Beheer van leveranciers
- AD_A.15.2_Leverancier evaluation_BOI
- AD_A.15.2_Leverancier evaluation_LAB
- AD_A.15.2_Leverancier evaluation_LUD
- AD_A.15.2_Leverancier evaluation_XDE
- AD_A.15.2_Leverancier evaluation_XNL

Om de consistente kwaliteit van contractuele afspraken te waarborgen, maakt Xylem gebruik van een standaardset van kant-en-klare contractuele afspraken in de vorm van goedgekeurde templates specifiek voor de scope van het ISMS.

4.5.2 Objectief bewijs

- TP_CR_A.13.2_Geheimhouding agreement_EN_V.2.0
- TP_CR_A.13.2_Xyleem Third_Party_Connection_Agreement_EN_V.2.0_

4.6 Normalisatie

Vanaf mei 2024 wordt deze eis van de NIS 2-richtlijnen nog niet gedekt door het BMS van Xylem, naast de onder clausule 3.1 genoemde geldige certificeringen.

4.6.1 Objectief bewijs

- https://www.bsigroup.com/en-US/validate-bsi-issued-certificates/client-directory-profile/SENSUS-0047717332-000

4.7 Inherente beperkingen

Er zijn inherente beperkingen in de doeltreffendheid van elk systeem van interne controle, met inbegrip van de mogelijkheid van menselijke fouten en het omzeilen van controles. Vanwege inherente beperkingen in haar interne beheersing kunnen deze controles redelijke, maar niet absolute, zekerheid bieden dat haar verbintenissen en systeemvereisten met betrekking tot beveiliging, beschikbaarheid, integriteit en vertrouwelijkheid worden nagekomen.

Voorbeelden van inherente beperkingen van interne controles met betrekking tot beveiliging zijn:

a. Kwetsbaarheden in IT-componenten als gevolg van het ontwerp ervan door de fabrikant of ontwikkelaar
b. Uitsplitsing van de interne controle bij een dienstverlener, leverancier of zakenpartner en
c. Hardnekkige aanvallers met de middelen om geavanceerde technische middelen en geavanceerde social engineering-technieken te gebruiken die specifiek gericht zijn op de entiteit.

Bovendien is bij prognoses van een evaluatie van de doeltreffendheid voor toekomstige perioden het risico verbonden dat de controles ontoereikend worden als gevolg van veranderingen in de omstandigheden of dat de mate van naleving van het beleid of de procedures verslechtert.

5 Conclusie

Naar onze mening bieden deze ISO-certificeringen samen een substantiële basis die de naleving van de uitgebreide en dynamische cyberbeveiligingsvereisten van de NIS2-richtlijn ondersteunt. Door gebruik te maken van de gestructureerde kaders van ISO 27001, ISO 20000, ISO 27017 en ISO 27701, kan Xylem effectief inspelen op de complexe en evoluerende cyberbeveiligingsvereisten van NIS2, waardoor hun algehele beveiligingshouding en naleving van de regelgeving worden verbeterd.

Dordrecht, 17 mei 2024 ..... A.Damme .....
Plaats, datum — CEO Xylem Water Solutions Nederland B.V.

Bruckberg, 17 mei 2024 ..... Gunnar Muench Digital unterschrieben von Gunnar Muench Datum: 2024.06.05 12:22:41 +02'00' .....
Plaats, datum — CEO Münch Management Consultancy