Classificatie	Intern
Status van documentatie	Goedgekeurd
Versie	V.1.1
Opgeslagen door gebruiker	MMC | Muench
Save date	12.06.2025

Assurance Statement NIS 2

– AD - Bijbehorende documentatie –

Münch Management Consultancy

Geschiedenis van verandering

Versie	Datum	Auteur	Type verandering	Status van documentatie
0.1	05.06.2025	GEM	Creatie	Gepland
0.2	06.06.2025	SIA	Kwaliteitsborging	Ter goedkeuring
1.0	09.06.2025	GEM	Goedkeuring	Goedgekeurd
1.1	12.06.2025	GEM	Redactionele wijzigingen	Goedgekeurd
	DD.MM.YYYY			Select an element.
	DD.MM.YYYY			Select an element.
	DD.MM.YYYY			Select an element.
	DD.MM.YYYY			Select an element.
	DD.MM.YYYY			Select an element.
	DD.MM.YYYY			Select an element.

Distributielijst

Organisatorische eenheid	Plaats van opslag
MMC	Teamdrive MMC_Management Systems

Termen en definities

Term	Afkorting	Beschrijving
Informatiebeveiliging	IS	
Informatiebeveiligingsbeheersysteem	ISMS	
Münch Management Consultancy	MMC	
Xylem Water Solutions Nederland B.V.	Xylem	

Bijbehorende documentatie

Nee.	Naam van documentatie	Beschrijving
[1]		
[2]		
[3]		
[4]		
[5]		
[6]		
[7]		
[8]		
[9]		
[10]		

Vereiste:

- Toegang tot de volgende mappen en bestanden:
  N/A

Inhoudsopgave

1 INLEIDING 4

2 ALGEMEEN 4

3 BENADERING 4

3.1 Relevante internationale certificeringen 4

3.2 Relevante hoofdstukken en artikelen van de NIS 2-richtlijn 4

4 RISICOBEHEERSMAATREGELEN VOOR CYBERBEVEILIGING EN RAPPORTAGEVERPLICHTINGEN 4
4.1.1 Objectief bewijs 4

4.2 Bestuur 5
4.2.1 Objectief bewijs 5
4.2.2 Objectief bewijs 5
4.2.3 Objectief bewijs 5
4.2.4 Objectief bewijs 5
4.2.5 Objectief bewijs 5

4.3 Maatregelen voor het beheer van cyberbeveiligingsrisico's 5
4.3.1 Objectief bewijs 5
4.3.2 Objectief bewijs 5
4.3.3 Objectief bewijs 6
4.3.4 Objectief bewijs 6
4.3.5 Objectief bewijs 6
4.3.6 Objectief bewijs 6
4.3.7 Objectief bewijs 6
4.3.8 Objectief bewijs 6
4.3.9 Objectief bewijs 6
4.3.10 Objectief bewijs 7

4.4 Rapportageverplichtingen 7
4.4.1 Objectief bewijs 7
4.4.2 Objectief bewijs 7

4.5 Gebruik van Europese cyberbeveiliging certificeringsregelingen 7
4.5.1 Objectief bewijs 7
4.5.2 Objectief bewijs 7

4.6 Standaardisatie 8
4.6.1 Objectief bewijs 8

4.7 Inherente beperkingen 8

5 CONCLUSIE 8

1 Inleiding

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

2 Algemeen

De NIS 2-richtlijn (netwerk- en informatiesysteembeveiliging) is een EU-brede verordening die moet zorgen voor een hoog gemeenschappelijk niveau van beveiliging van netwerk- en informatiesystemen in de EU. De richtlijn breidt de eisen en het toepassingsgebied van de oorspronkelijke NIS-richtlijn uit om het hoofd te bieden aan de toenemende dreiging van cyberbeveiliging. De richtlijn zal relevant zijn voor een groter aantal sectoren en bedrijven, waaronder belangrijke dienstverleners en digitale diensten. De richtlijn moet uiterlijk in oktober 2024 zijn omgezet in nationale wetgeving. Tot de belangrijkste elementen behoren risicobeheersmaatregelen, rapportageverplichtingen bij beveiligingsincidenten en het vergroten van de nationale cyberbeveiligingscapaciteit.

Naast een inleiding 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" is gebruikt als het relevante hoofdstuk in de context van deze betrouwbaarheidsverklaring voor het beveiligen van de toeleveringsketen van Xylem's klanten.

3 Benadering

3.1 Relevante internationale certificeringen

De naleving van de risicobeperkende maatregelen die Xylem momenteel implementeert als onderdeel van zijn

- ISO/IEC 20000-1:2018,
- ISO/IEC 27001:2022,
- ISO/IEC 27017:2015 en
- ISO/IEC 27701:2019

certificeringen met de vereisten van de

- NIS 2 Directive, Chapter IV,

werd herzien.

3.2 Relevante hoofdstukken en artikelen van de NIS 2-richtlijn

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

- Article 20, Governance, NIS 2 Directive.
- Article 21, Cybersecurity risk-management measures, NIS 2 Directive.
- Article 22, Union level coordinated security risk assessments of critical supply chains, NIS 2 Directive.
- Article 23, Reporting obligations, NIS 2 Directive.
- Article 24, Use of European cybersecurity certification schemes, NIS 2 Directive.
- Article 25, Standardisation, NIS 2 Directive.

De certificeringen ISO 27001, ISO 20000, ISO 27017 en ISO 27701 van Xylem dekken gezamenlijk een breed spectrum van beveiligings- en privacy beheerpraktijken die in belangrijke mate overeenkomen met de vereisten van NIS2.

4 RISICOBEHEERSMAATREGELEN VOOR CYBERBEVEILIGING 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 op basis van MS Word en MS Excel.

4.1.1 Objectief bewijs

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

4.2 Bestuur

De vereisten met betrekking tot governance worden afgedekt door zeven beleidsregels, waarin zowel algemene als specifieke informatiebeveiligingsaspecten aan bod komen, waaronder cyberbeveiliging, cloudbeveiliging en gegevensbescherming.

4.2.1 Objectief bewijs

- PL_A.5.1_Administrator
- PL_A.5.1_Business management system
- PL_A.5.1_Change and release management
- PL_A.5.1_Developer_Policy
- PL_A.5.1_Enduser
- PL_A.5.1_Personnel and personnel management
- PL_A.5.1_Supplier management

Een wettelijk en vergunningenregister documenteert alle relevante wettelijke vereisten, terwijl contractuele en rapportagevereisten in een aanvullend document worden behandeld.

4.2.2 Objectief bewijs

- RC_A.18.1_2025_Legal and permit register

Eens per jaar worden er verschillende interne en externe audits uitgevoerd en goed gedocumenteerd.

4.2.3 Objectief bewijs

- RC_9.2_20250218_Audit plan_XDE_XNL_LUD
- RC_9.2_20250218_Audit report_XDE_XNL_LUD_signed
- RC_9.2_20250218_Action list_XDE_XNL_LUD

Er is een trainingsprogramma, vergezeld van regelmatige training, dat informatiebeveiligingsvereisten vertaalt en interpreteert in Xylem-specifieke vereisten. De effectiviteit van trainingssessies wordt geëvalueerd.

4.2.4 Objectief bewijs

- DP_7.2_Training and awareness
- AD_7.2_Training program
- RC_7.2_20250217_List of participants PL Admin and PL User_LAB
- RC_7.2_20250221_List of participants BMS Awareness training_LAB
- RC_7.2_20250217_List of participants BMS Awareness training__ PL Admin and PL User_LAA
- RC_7.2_20250218_List of participants BMS Awareness training_LUD

Alle managementrelevante taken worden gedocumenteerd in een actiebeheersysteem.

4.2.5 Objectief bewijs

- AD_8.1_2025_Action 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_Risk management_V.1.16
- RC_6.1_202502_Risk management

Als cyberbeveiligingsrisico's reëel worden, zijn er specifieke acties binnen de huidige BC-planning.

4.3.2 Objectief bewijs

- AD_A.17.1_2025_BC_manual_Xylem
- RC_20220919_Minutes of Update BCDR Plans

Het risicomanagementproces is op een duidelijke en begrijpelijke manier gedocumenteerd, inclusief de risicobeoordeling

en de risicobehandelingsactiviteiten.

4.3.3 Objectief bewijs

- PD_6.1_Risk management_EN_V.2.16

Er zijn objectieve bewijzen volgens tests en oefeningen van BC-plannen

4.3.4 Objectief bewijs

- RC_20220919_Minutes of Update BCDR Plans

Het beheer van informatiebeveiligingsincidenten maakt deel uit van een holistisch en goed gedocumenteerd beheersproces voor beveiligingsincidenten als integraal onderdeel van het geïntegreerde beheersysteem van Xylem. Het omvat informatiebeveiligingsgebeurtenissen en -incidenten, bijbehorende communicatielijsten en invocaties in de bedrijfscontinuïteitsplanning, inclusief de ICT-gereedheid van diensten binnen het bereik van het ISMS.

4.3.5 Objectief bewijs

- AD_8.1_2025_Action management_Xylem
- DP_A.16.1_Security incident management
- DP_A.5.1_Incident and Service Request Management
- DP_A.5.1_Problem Management
- DP_A.17.1_Continuity and availability management

De back-up van kritieke systemen en gegevens wordt uitbesteed aan een tier 4-datacenterleverancier, gecontroleerd door regelmatige leverancierscontroles. Er is een systeem voor inbraakdetectie en -preventie, een extern onderzoek volgens de Duitse KRITIS-eisen is gepland voor eind juni 2024. In dit onderzoek wordt ook rekening gehouden met monitoring en forensische kwesties.

4.3.6 Objectief bewijs

- AD_8.1_2025_Action management_Xylem

Een beleid regelt de interactie met serviceproviders en leveranciers, de kriticiteit van serviceproviders en leveranciers wordt bepaald en bijgehouden als onderdeel van het risicomanagementproces.

4.3.7 Objectief bewijs

- PL_A.5.1_Supplier management
- AD_A.15.2_Supplier evaluation_BOI
- AD_A.15.2_Supplier evaluation_LAB
- AD_A.15.2_Supplier evaluation_LUD
- AD_A.15.2_Supplier evaluation_XDE
- AD_A.15.2_Supplier evaluation_XNL

Netwerkbeveiliging wordt onderhouden door een specifieke organisatorische eenheid binnen Xylem, gecontroleerd door de managementsysteemfunctionaris (MSO), respectievelijk de lokale managementsysteemfunctionaris (LMSO) op verschillende locaties binnen het toepassingsgebied van het ISMS.
Een audit door een 1st partij, een 2nd partij en een 3rd partij wordt regelmatig uitgevoerd en de resultaten worden gecontroleerd door het topmanagement in het kader van de directiebeoordeling die minstens een keer per jaar plaatsvindt.

4.3.8 Objectief bewijs

- RC_9.3_20250219_Minutes of Management review

Operationeel beleid en gedocumenteerde procedures bieden regels voor het beheer van ICT-kwesties binnen het toepassingsgebied, waaronder basis-identiteits- en toegangsbeheer, bescherming tegen malware, configuratiebeheer, back-up en cryptografie.

4.3.9 Objectief bewijs

- PL_A.5.1_Administrator
- PL_A.5.1_Enduser
- DP_7.2_Training and awareness
- DP_7.5_Control of documented information

- DP_5.1_Business relationship and service level managment_XYLEM
- DP_A.5.1_Service Reporting
- DP_A.5.1_Demand and capacity Management
- DP_A.5.1_Incident and Service Request Management
- DP_A.5.1_Problem Management
- DP_A.16.1_Security incident management
- DP_A.17.1_Continuity and availability management
- DP_A.5.1_Service Asset and Configuration Management

Personeelszaken zijn locatie specifiek en worden deels uitbesteed aan interne HR-partners van Xylem, gecontroleerd door een personeels- en personeelsmanagementbeleid en de daaruit afgeleide documentatie.

4.3.10 Objectief bewijs

- PL_A.5.1_Personnel and personnel management

4.4 Rapportageverplichtingen

Communicatielijsten regelen onderwerp specifieke contacten voor zowel belanghebbende partijen als belangengroepen. Hieronder vallen ook relevante contacten met autoriteiten voor het melden van beveiligingsincidenten die gemeld moeten worden.

4.4.1 Objectief bewijs

- DP_A.5.1_Service Reporting
- AD_9.4_2025_Contract management and service reporting
- AD_4.1_2025_Context of the oganization_Xylem
- RC_7.4_2025_Communication lists_BOI
- RC_7.4_2025_Communication lists_LAB
- RC_7.4_2025_Communication lists_LUD
- RC_7.4_2025_Communication lists_XDE
- RC_7.4_2025_Communication lists_XNL

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

4.4.2 Objectief bewijs

- RC_A.6.1_2025_Project list

4.5 Gebruik van Europese cyberbeveiliging certificeringsregelingen

De toeleveringsketen volgens ISMS relevante diensten en goederen wordt aangepakt via een beleid voor leveranciersbeheer dat interne richtlijnen geeft over hoe en welke kwesties moeten worden aangepakt in contractuele overeenkomsten met leveranciers, inclusief geheimhoudingsovereenkomsten (NDA's) en andere contractuele overeenkomsten met betrekking tot de leveranciersrelatie.

4.5.1 Objectief bewijs

- PL_A.5.1_Supplier management
- AD_A.15.2_Supplier evaluation_BOI
- AD_A.15.2_Supplier evaluation_LAB
- AD_A.15.2_Supplier evaluation_LUD
- AD_A.15.2_Supplier evaluation_XDE
- AD_A.15.2_Supplier evaluation_XNL

Om de consistente kwaliteit van contractuele overeenkomsten te waarborgen, gebruikt Xylem een standaardset kant-en-klare contractuele overeenkomsten in de vorm van goedgekeurde sjablonen, specifiek voor de reikwijdte van het ISMS.

4.5.2 Objectief bewijs

- TP_CR_A.13.2_Non disclosure agreement_EN_V.2.0
- TP_CR_A.13.2_Xylem Third_Party_Connection_Agreement_EN_V.2.0_

4.6 Standaardisatie

Vanaf mei 2025 wordt deze vereiste van de NIS 2-richtlijnen nog niet gedekt door het GBS 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 aan de effectiviteit van elk systeem van interne controle, waaronder de mogelijkheid van menselijke fouten en het omzeilen van controles. Vanwege de inherente beperkingen van de interne controle kunnen deze controles een redelijke, maar geen absolute, zekerheid bieden dat aan de verplichtingen en systeemvereisten met betrekking tot beveiliging, beschikbaarheid, integriteit en vertrouwelijkheid wordt voldaan.

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

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

Bovendien zijn projecties van een evaluatie van de effectiviteit naar toekomstige perioden onderhevig aan het risico dat controles ontoereikend worden door 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 naleving van de uitgebreide en dynamische cyberbeveiligingsvereisten van de NIS2-richtlijn ondersteunt. Door gebruik te maken van de gestructureerde kaders die ISO 27001, ISO 20000, ISO 27017 en ISO 27701 bieden, kan Xylem effectief omgaan met de complexe en veranderende vereisten voor cyberbeveiliging van NIS2, waardoor hun algehele beveiligingshouding en naleving van de regelgeving wordt verbeterd.

Gunnar Muench

Digital unterschrieben von Gunnar Muench
Datum: 2025.06.12 03:50:40 +02'00'

.....

Plaats, datum

.....

CEO Xylem Water Solutions Nederland B.V.

Bruckberg, 09.06.2025

.....

Plaats, datum

Dordrecht, 22-06-2025

.....

CEO Münch Management Consultancy