17.05.2024	Internal
Status of documentation	Approved
Version	V.1.0
Saved by user	MMC | Muench
Save date	21.05.2024

Assurance statement NIS 2

– – AD - Associated documentation

Münch Management Consultancy

GEM

Version	Date	Author	Type of change	Status of documentation
0.1	Version	Date	Author	Type of change
Status of documen-tation	0.1	Version	Date	Author
Type of change	Status of docu-mentation	0.1	Version	Date
	SIA			02.05.2024
	Select an ele-ment.			Select an element.
	Select an ele-ment.			Select an element.
	Select an ele-ment.			Select an element.
	Select an ele-ment.			Select an element.
	Select an ele-ment.			Select an element.
	Select an ele-ment.			Select an element.

Teamdrive MMC_Management Systems

Select an element.	Place of storage
MMC	Teamdrive MMC_Management Systems

Xylem

Place of storage	MMC	Teamdrive MMC_Management Systems
Information security	IS	
Information security management system	ISMS	
MMC	Teamdrive MMC_Manage-ment Systems	
IS	Xylem	

NIS 2 Compliance assessment, carried out May 02 to May 15th 2024 by MMC

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

[8]		
[9]		
[10]		

Prerequisite:

- Access to the following folders and files:N/A

Table of contents

1 Introduction

This Assurance Statement is issued on behalf of and for the top management of Xylem Water Solutions Nederland B.V., hereinafter referred to as Xylem.

2 General

The NIS 2 Directive (Network and Information System Security) is an EU-wide regulation that aims to ensure a high common level of security of network and information systems in the EU. It extends the requirements and scope of the original NIS Directive to address the increasing cybersecurity threat landscape. The Directive will be relevant for a wider range of sectors and businesses, including key service providers and digital services. It must be transposed into national law by October 2024. Key elements include risk management measures, reporting obligations in the event of security incidents and increasing national cybersecurity capacities.

In addition to a preamble, the final text of the NIS 2 Directive dated December 14, 2022, consists of nine chapters, whereby "Chapter IV, Cybersecurity Risk-Management Measures and Reporting Obligations", was used as the relevant chapter in the context of this assurance statement for securing the supply chain of Xylem's customers.

3 Approach

3.1 Relevant international certifications

The compliance of the risk mitigation measures currently implemented by Xylem as part of its

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

certifications with the requirements of the

- NIS 2 Directive, Chapter IV,

was reviewed.

3.2 Relevant chapter and articles of the NIS 2 Directive

Chapter IV of the NIS 2 Directive contains the following six articles:

- 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.

The certifications ISO 27001, ISO 20000, ISO 27017, and ISO 27701 of Xylem collectively cover a broad spectrum of security and privacy management practices that significantly correspond with the NIS2 requirements.

4 CYBERSECURITY RISK-MANAGEMENT MEASURES AND REPORTING OBLIGATIONS

The management system, named "Business Management System", that covers all aspects of the above mentioned international as well as national standards is comprehensively documented, using different tools as well as single files, mainly MS Word and MS Excel based.

4.1.1 Objective evidence

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

4.2 Governance

The requirements addressing governance are covered by seven policies, addressing general as well as specific information security aspects, including cyber security, cloud security and data protection issues.

4.2.1 Objective evidence

- 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

A legal and permit register documents all relevant legal requirements, while contractual and reporting requirements are covered by an additional document.

4.2.2 Objective evidence

- RC_A.18.1_2024_Legal and permit register

Once a year, several internal as well as external audits are performed and well documented.

4.2.3 Objective evidence

- RC_9.2_20240115_Audit plan_XDE_XNL_LUD
- RC_9.2_20240115_Audit report_XDE_XNL_LUD_signed
- RC_9.2_20240115_Action list_XDE_XNL_LUD

There is a training program, accompanied by regular training, that translates and interprets information security requirements into Xylem-specific requirements. The effectiveness of training sessions is evaluated.

4.2.4 Objective evidence

- DP_7.2_Training and awareness
- AD_7.2_Training program
- RC_7.2_20240219_List of participants BMS Awareness training_LAB
- RC_7.2_20240105_List of participants BMS Awareness training_XLC_Recording
- PT_7.3_20240105_BMS_Awareness_Training_2024_Recording
- PT_7.3_20240108_BMS Awareness Training_SMS 2024
- PT_7.3_20240108_BMS_Awareness_Training_2024
- PT_7.3_Transition ISO 27001-2022
- PT_7.3_20240227_The importance of a living BMS

All management relevant tasks are documented within an action management system.

4.2.5 Objective evidence

- AD_8.1_2024_Action management_Xylem

4.3 Cybersecurity risk-management measures

The holistic risk management approach covers a broad range of different risk types, including cyber security risks.

4.3.1 Objective evidence

- DP_6.1_Risk management
- RC_6.1_202404_Risk management
- RC_6.1_2024_Risk management_2022

In case of cyber security risks get real, there are specific actions within the current BC planning.

4.3.2 Objective evidence

- AD_A.17.1_2024_BC_manual_Xylem

The risk management process is documented in a clear and comprehensible manner, including the risk assessment and risk treatment activities.

4.3.3 Objective evidence

- PD_6.1_Risk management_EN_V.2.12

Information security incident management is part of a holistic and well documented security incident management process as an integral component of Xylem's integrated management system. It includes information security events and incidents, corresponding communication lists as well as invocations into the business continuity planning, including the ICT readiness of services within the scope of the ISMS.

4.3.4 Objective evidence

- AD_8.1_2024_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

The backup of critical systems and data is outsourced to a tier 4 data center provider, controlled by frequent supplier audits. An intrusion detection and prevention system are in place, an external examination according to German KRITIS-requirements is scheduled end of June 2024. This examination takes into consideration monitoring as well as forensic issues as well.

4.3.5 Objective evidence

- AD_8.1_2024_Action management_Xylem

A policy regulates the interaction with service providers and suppliers, the criticality of service providers and vendors is determined and tracked as part of the risk management process.

4.3.6 Objective evidence

- 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

Network security is maintained by a specific organizational unit within Xylem, controlled by the management system officer (MSO), respectively local management system officer (LMSO) at different sites within the scope of the ISMS.
1st party, 2nd party as well as 3rd party audit are performed regularly, the results will be controlled by the top management within the management review at least once a year.

4.3.7 Objective evidence

- RC_9.3_202402007_Minutes of management review_Xylem

Operational policies and documented procedures provide rules to operate ICT issues within the scope, covering amongst others basic identity and access management, protection against malware, configuration management, backup and cryptography.

4.3.8 Objective evidence

- 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

Human resource issues are site specific partly outsourced to Xylem internal HR partners, controlled by a personnel and personal management policy and subsequent documentation derived from it.

4.3.9 Objective evidence

- PL_A.5.1_Personnel and personnel management

4.4 Reporting obligations

Communication lists regulate topic-specific contact for both interested parties and interest groups. This also includes relevant contacts with authorities for the reporting of notifiable security incidents.

4.4.1 Objective evidence

- DP_A.5.1_Service Reporting
- AD_9.4_2024_Contract management and service reporting
- AD_4.1_2024_Context of the oganization_Xylem
- RC_7.4_2024_Communication lists_BOI
- RC_7.4_2024_Communication lists_LAB
- RC_7.4_2024_Communication lists_LUD
- RC_7.4_2024_Communication lists_XDE
- RC_7.4_2024_Communication lists_XNL

The implementation of an outsourced Security Operations Center (SOC) is in preparation. Currently respective tasks are taken over by the MSO or rather LMSO.

4.4.2 Objective evidence

- RC_A.6.1_2024_Project list

4.5 Use of European cybersecurity certification schemes

The supply chain according to ISMS relevant services and goods is addressed through a supplier management policy that provides internal guidance on how and what issues have to be addressed within supplier contractual agreements, including This includes non-disclosure agreements (NDAs) as well as other contractual agreements, related to supplier relationship.

4.5.1 Objective evidence

- 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

To ensure the consistent quality of contractual agreements, Xylem uses a standard set of ready-made contractual agreements in the form of approved templates specifically for the scope of the ISMS.

4.5.2 Objective evidence

- 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 Standardisation

As of May 2024, this requirement of the NIS 2 directives is not covered by Xylem's BMS yet beside the under clause 3.1 mentioned valid certifications.

4.6.1 Objective evidence

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

4.7 Inherent limitations

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls. Because of inherent limitations in its internal control, those controls may provide reasonable, but not absolute, assurance that its commitments and system requirements related to security, availability, integrity and confidentiality are achieved.

Examples of inherent limitations of internal controls related to security include:

a. Vulnerabilities in information technology components as a result of design by their manufacturer or developer
b. Breakdown of internal control at a service provider, supplier or business partner and
c. Persistent attackers with the resources to use advanced technical means and sophisticated social engineering techniques specifically targeting the entity.

Furthermore, projections of any evaluation of effectiveness to future periods are subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

5 Conclusion

In our opinion, these ISO certifications collectively provide a substantial foundation that supports compliance with the comprehensive and dynamic cybersecurity requirements of the NIS2 Directive. By leveraging the structured frameworks provided by ISO 27001, ISO 20000, ISO 27017, and ISO 27701, Xylem can effectively address the complex and evolving cybersecurity requirements of NIS2, thereby enhancing their overall security posture and regulatory compliance.

Dordrecht, May 17, 2024 ..... A. Damme .....
Place, date — CEO Xylem Water Solutions Nederland B.V.

Bruckberg, May 17, 2024 ..... Gunnar Muench Digital unterschrieben von Gunnar Muench Datum: 2024.06.05 12:20:59 +02'00' .....
Place, date — CEO Münch Management Consultancy