Third-Party Risk Management (TPRM) and Cybersecurity maturity requirements

Purpose

This policy outlines the scope and guidelines for managing the risks associated with the use of third parties providing digital services or products within Port of Antwerp-Bruges. The goal is to ensure that all interactions with third parties, including suppliers, service providers, consultants, and other external entities, comply with our standards for cybersecurity, compliance, and operational integrity.

Security classification

This document has a security classification of '**Public**', which means that there are no restrictions on distribution.

Version history

Nr.	Beschrijving	Bewerker	Datum
1.0	Final version	Yannick Herrebaut	30 august 2024
1.1	Final version, update	Jan Meuris	27 november 2024
1.2	Final version, update	Jan Meuris	27 januari 2025
1.3	Final version, update	Jan Meuris	10 februari 2025

Scope

Port of Antwerp-Bruges is designated as an 'essential' entity under Belgian NIS2 legislation. The aim of this law is to strengthen measures in the areas of cybersecurity, incident management, and the supervision of entities that provide services essential to maintaining critical societal or economic activities. The law is also intended to improve the coordination of government policies in the field of cybersecurity.

As a NIS2 entity Port of Antwerp-Bruges, hereinafter referred to as POAB, is legally obligated to ensure the security of its supply chain, including security-related aspects of its direct suppliers or service providers.

The Third-Party Risk Management (TPRM) policy maintained by POAB, is designed to identify, manage, and mitigate risks associated with the use of third parties, in compliance with the requirements of the NIS2 Directive. It applies to all third parties providing digital services or products.

Therefore we advise all organizations within the supply chain of POAB to comply, at a minimum, with the measures outlined in the CyberFundamentals (CyFun®) Framework at the **Basic level**. Furthermore, POAB's TPRM program consists of several steps.

TPRM Program

1. **Classification and Triage**

Each supplier of digital services or products carries a different level of risk and importance for POAB. Therefore POAB classifies and triages all suppliers to ensure the appropriate focus and priorities are established. To prioritize the inherent risks of suppliers for POAB, a risk weighting matrix is used, in addition to the general context of POAB. All suppliers are classified into 4 Tiers:

Tier 1	Very high risk
Tier 2	High risk
Tier 3	Medium risk
Tier 4	Low risk

Based on the classification different elements, either individually or combined, are used for risk analysis:

- ISO/IEC 27001 certification with the relevant scope of application or CyberFundamentals (CyFun®) certification (level essential) or verification (level important or basic)
- Cybersecurity Questionnaire
- Security rating

In addition, depending on the services or products, a connection is made to other applicable guidelines and policies, including:

- Non-functional requirements
- External access statement
- Cybersecurity policy for external parties
- Data processing agreement

General overview of requirements and measures:

Tier	Requirements

Tier 1	- **NIS2 compliance** (ISO/IEC 27001 certified or CyFun Important Verified)
	  o Extensive questionnaire (If no ISO/IEC 27001 or CyberFundamentals Important Verified certification)
	  o Standard questionnaire (If ISO/IEC 27001 or CyberFundamentals Important Verified certification)
	- **Security rating**[1]
	- **Non-Functional Requirements**
	- **Cybersecurity policy for third parties** (if applicable)
	- **External access statement** (if applicable)

Tier 2	- **NIS2 compliance** (ISO/IEC 27001 certified or CyFun Basic Verified)
	  o Extensive questionnaire (If no ISO/IEC 27001 or CyberFundamentals Basic Verified certification)
	  o Standard questionnaire (If ISO/IEC 27001 or CyberFundamentals Basic Verified certification)
	- **Security rating**
	- **Non-Functional Requirements**
	- **Cybersecurity policy for third parties** (if applicable)
	- **External access statement** (if applicable)

Tier 3	- **Security rating** - **Non-Functional Requirements** - **Cybersecurity policy for third parties** (if applicable) - **External access statement** (if applicable)
Tier 4	- **Non-Functional Requirements** - **Cybersecurity policy for third parties** (if applicable) - **External access statement** (if applicable)

[1] **Attack surface scanning** combined with **digital footprint** mapping.

Suppliers are periodically assessed. During each reassessment, their performance, compliance with contractual obligations, and cybersecurity measures are evaluated.

The frequency of these reassessments is based on the risk category of the service provider:

- **Tier 1:** Annual reassessment
- **Tier 2:** Reassessment every 3 years
- **Tier 3:** Reassessment every 5 years
- **Tier 4:** Ad hoc reassessment

In addition to periodic reassessments, POAB also conducts reassessments based on specific triggers indicating an increased risk:

- **Incidents or security breaches:**
  If a service provider is involved in a data breach, operational disruption, or any other incident impacting POAB.
- **Structural changes at the service provider:**
  In cases of mergers, acquisitions, or significant changes in ownership or business strategy.
- **Contractual or operational changes:**
  If there are modifications to the services provided or contract terms.
- **Negative reports or warnings:**
  If external sources (such as audits, news reports, or regulators) indicate increased risks associated with a service provider.

2. **Engagement**

Based on the classification assigned in step 1, POAB presents the corresponding measures to the potential supplier, who must commit to adhering to these measures.

For Tier 1, Tier 2, and Tier 3, a 'security rating score' is used to assess the cybersecurity maturity of the (potential) supplier.

For Tier 1 and Tier 2 suppliers, an (online) questionnaire, which will be provided by POAB, must also be completed. POAB will review the completed questionnaire and ask additional questions if necessary. Only when POAB positively evaluates the answers, the process can continue with this potential supplier.

3. **Remediation**

In some cases, both during the contractual or pre-contractual phase, remediation may be initiated when:

- The security rating score is not positively assessed by POAB, or
- The questionnaire is not adequately completed, or
- The (potential) supplier does not meet our requirements.

Identified points of concern are addressed with the (potential) supplier by POAB. Subsequently, a remediation period can be granted, during which the potential supplier commits in writing to implement the necessary measures within this period. If the potential supplier is unable to implement the additional measures within the agreed period, the service provider will be excluded or the collaboration will be terminated.

4. **Monitoring**

Tier 1, 2, and 3 suppliers are continuously monitored by POAB throughout the duration of the contract. This is done using threat intelligence and security rating scores. Audit reports or certifications can be requested if necessary. If, at any point, the supplier no longer meets POAB's requirements, they will be addressed and action must be taken within a reasonable period to resolve the identified issues. The length of this remediation period will be determined, depending on the context, in consultation with the supplier.

Exceptions

Requests for exceptions to this policy must be submitted in writing and formally approved by the Cyber Resilience Manager of Port of Antwerp-Bruges, along with the specific reason for the exception request. For each exception to this policy, the relevant department will accept responsibility for maintaining security controls. The approval of exceptions does not prevent the Cyber Resilience Manager from unilaterally revoking approved exceptions if an unacceptable risk to the confidentiality, availability, or integrity of data, applications, or systems arises.