Third-Party Risk Management (TPRM) and Cybersecurity maturiteitseisen

Doel

Dit beleid beschrijft de reikwijdte en de richtlijnen voor het beheren van risico's die gepaard gaan met het gebruik van derde partijen die digitale diensten of producten leveren binnen Port of Antwerp-Bruges. Het doel is om ervoor te zorgen dat alle interacties met deze derde partijen, inclusief leveranciers, dienstverleners, consultants en andere externe entiteiten, voldoen aan onze normen voor cyberveiligheid, compliance, en operationele integriteit.

Veiligheidsclassificatie

Dit document heeft een veiligheidsclassificatie "**Publiek**", wat betekent dat er geen beperkingen zijn op distributie.

Version history

Nr.	Beschrijving	Bewerker	Datum
1.0	Final version	Yannick Herrebaut	30 augustus 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

Toepassingsgebied

Port of Antwerp-Bruges is geclassificeerd als een 'essentiële' entiteit' onder de Belgische NIS2-wetgeving. Het doel van de wet is het versterken van maatregelen op het gebied van cyberbeveiliging, incidentbeheer en het toezicht op entiteiten die diensten leveren die essentieel zijn voor het in stand houden van kritieke maatschappelijke of economische activiteiten. Daarenboven verbetert de wet de coördinatie van overheidsbeleid op het gebied van cyberbeveiliging.

Als NIS2-entiteit is de Haven van Antwerpen-Brugge, hierna POAB genoemd, wettelijk verplicht om de beveiliging van haar toeleveringsketen te waarborgen, inclusief de cybersecurity gerelateerde aspecten van haar directe leveranciers of dienstverleners.

Het Third-Party Risk Management (TPRM) beleid dat door POAB wordt gehanteerd, is ontworpen om risico's te identificeren, beheren en beperken die verband houden met het gebruik door derde partijen van onze digitale diensten en/of derde partijen die digitale diensten of producten leveren, en dit in overeenstemming met de vereisten van de NIS2-richtlijn. Het is van toepassing op alle derden die digitale diensten of producten leveren.

Daarom adviseert POAB alle organisaties binnen de toeleveringsketen van POAB om zich minimaal te conformeren aan de maatregelen zoals uiteengezet in het CyberFundamentals (CyFun®) Framework **level Basic**.

TPRM Programma

1. **Classificatie en Triage**

Elke leverancier van digitale diensten of producten draagt een verschillend belang en ook een verschillend risiconiveau met zich mee. Daarom classificeert en trieert POAB al deze leveranciers om ervoor te zorgen dat de gepaste focus wordt gelegd en de juiste prioriteiten worden gesteld. Om de inherente risico's van leveranciers voor POAB te prioriteren wordt, naast de algemene context van POAB, een risicowegingsmatrix gebruikt. Alle leveranciers worden ingedeeld in vier Tiers:

Tier 1	Zeer hoog risico
Tier 2	Hoog risico
Tier 3	Gemiddeld risico
Tier 4	Laag risico

Op basis van deze classificatie worden verschillende elementen, afzonderlijk of gecombineerd, gebruikt om het risico te analyseren:

- ISO/IEC 27001-certificering met relevant toepassingsgebied of CyberFundamentals (CyFun®) verificatie (niveau Important of Basic)
- Cybersecurity Questionnaire
- Security rating

Daarenboven zal, afhankelijk van de diensten of producten en gelet op de classificatie, de link gelegd worden naar de door de leverancier te respecteren richtlijnen en policies, waaronder:

- Non-functional requirements
- Verklaring externe toegang
- Cybersecurity policy voor externen
- Verwerkersovereenkomst

Overzicht voor vereisten en maatregelen:

Tier	Requirements

Tier 1	- **NIS2 compliance** (ISO/IEC 27001 certified or CyFun Important Verified)
	  o Uitgebreide vragenlijst (Indien geen ISO/IEC 27001 of CyberFundamentals Important Verified kan worden voorgelegd)
	  o Standaard vragenlijst (Indien ISO/IEC 27001 of CyberFundamentals Important Verified kan worden voorgelegd)
	- **Security rating**[1]
	- **Non-Functional Requirements**
	- **Cybersecurity policy voor externen** (indien van toepassing)
	- **Verklaring externe toegang** (indien van toepassing)

Tier 2	- **NIS2 compliance** (ISO/IEC27001 certified of CyFun Basic Verified)
	  o Uitgebreide vragenlijst (Indien geen ISO/IEC 27001 of CyberFundamentals Basic Verified kan worden voorgelegd)
	  o Standaard vragenlijst (Indien ISO/IEC 27001 of CyberFundamentals Basic Verified kan worden voorgelegd)
	- **Security rating**
	- **Non-Functional Requirements**
	- **Cybersecurity policy voor externen** (indien van toepassing)
	- **Verklaring externe toegang** (indien van toepassing)

Tier 3	- **Security rating** - **Non-Functional Requirements** - **Cybersecurity policy voor externen** (indien van toepassing) - **Verklaring externe toegang** (indien van toepassing)
Tier 4	- **Non-Functional Requirements** - **Cybersecurity policy voor externen** (indien van toepassing) - **Verklaring externe toegang** (indien van toepassing)

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

Leveranciers worden periodiek beoordeeld. Bij iedere herbeoordeling worden de prestaties, naleving van contractuele verplichtingen en cybersecuritymaatregelen geëvalueerd.

De frequentie van deze herbeoordeling is gebaseerd op de risicocategorie waartoe de dienstverlener behoort:

- **Tier 1:** Jaarlijkse herbeoordeling
- **Tier 2:** Herbeoordeling om de 3 jaar
- **Tier 3:** Herbeoordeling om de 5 jaar
- **Tier 4:** Herbeoordeling ad hoc

Naast de periodieke herbeoordelingen voert POAB ook herbeoordelingen uit op basis van specifieke triggers die wijzen op een verhoogd risico:

- **Incidenten of beveiligingsinbreuken:**
  Indien een dienstverlener betrokken is bij een datalek, operationele storing of ander incident dat impact heeft op POAB.
- **Structurele wijzigingen bij de dienstverlener:**
  Bij fusies, overnames of significante veranderingen in eigendom of bedrijfsstrategie.
- **Contractuele of operationele wijzigingen:**
  Indien er wijzigingen plaatsvinden in de dienstverlening of contractvoorwaarden.
- **Negatieve rapportages of signalen:**
  Indien externe bronnen (zoals audits, nieuwsberichten of toezichthouders) waarschuwen voor verhoogde risico's bij een dienstverlener.

2. **Engagement**

Op basis van de classificatie die toegewezen is in stap 1, legt POAB de overeenkomstige maatregelen op aan de (potentiële) leverancier, die zich dient te verbinden tot het naleven van deze maatregelen.

Voor Tier 1, Tier 2 en Tier 3 wordt een 'security rating score' gehanteerd om een appreciatie van de cybersecurity maturiteit van de (potentiële) leverancier te maken.

Voor Tier 1 en Tier 2 leveranciers dient daarenboven een (online) vragenlijst, die ter beschikking wordt gesteld door POAB, ingevuld te worden door de (potentiële) leverancier. Enkel indien POAB de security rating score alsook de antwoorden op de vragenlijst positief beoordeelt kan er verder gegaan worden met deze (potentiële) leverancier.

3. **Remediëring**

In een aantal gevallen, zowel in de contractuele als pre-contractuele fase, kan een remediëring worden opgestart wanneer:

- de security rating scoring niet positief beoordeeld wordt door POAB, of
- de vragenlijst niet adequaat wordt ingevuld, of
- indien de (potentiële) leverancier niet aan onze voorwaarden voldoet.

Geïdentificeerde aandachtspunten worden aangekaart bij de (potentiële) leverancier door POAB. Hierbij kan een remediëringsperiode toegekend worden, waarbij de potentiële leverancier zich schriftelijk verbindt om de maatregelen binnen deze periode te implementeren.

Indien de potentiële leverancier niet in staat is om bijkomende maatregelen binnen de afgesproken periode te implementeren, wordt de dienstverlener geweerd of wordt de samenwerking beëindigd.

4. **Monitoring**

Tier 1, 2 en 3 leveranciers worden permanent gemonitord door POAB gedurende de looptijd van het contract. Hierbij wordt gebruik gemaakt van threat intel en security rating scores. Auditverslagen of certificeringen kunnen opgevraagd worden indien nodig. Wanneer de leverancier op een gegeven moment niet meer voldoet aan de eisen van POAB, zal hij daarop aangesproken worden en dient hij binnen een redelijke periode actie te ondernemen om de geïdentificeerde problemen op te lossen. De lengte van deze remediëringsperiode wordt, afhankelijk van de context, bepaald in samenspraak met de leverancier.

Uitzonderingen

Aanvragen voor uitzonderingen op deze policy, dienen schriftelijk gericht te worden aan en formeel goedgekeurd te worden door de Cyber Resilience Manager van POAB, met de specifieke reden waarom er een uitzondering gevraagd wordt. Bij elke uitzondering op deze policy zal de verzoekende afdeling de verantwoordelijkheid aanvaarden om de security controles te bewaken. Goedgekeurde uitzonderingen weerhouden de Cyber Resilience Manager er evenwel niet van om deze eenzijdig in te trekken, indien er een onacceptabel risico ontstaat of zou ontstaan voor de vertrouwelijkheid, beschikbaarheid of integriteit van data, applicaties of systemen.