Smart Freight Centre Think-it bsi.

SFC Exchange Network

Proof of Concept Evaluation Report

August 2023

SFC Exchange Network

Proof of Concept Evaluation Report

August 2023

Suggested citation: Smart Freight Centre, Think-it and British Standards Institution. SFC Exchange Network – Proof of Concept Evaluation Report. 2023.

Disclaimer

The views expressed in this publication are those of Smart Freight Centre and its staff, consultants and management, and do not necessarily reflect the views of the Board of Trustees of Smart Freight Centre. Smart Freight Centre is not responsible for the consequence of the use of data included in this publication.

About Smart Freight Centre

Smart Freight Centre is an international non-profit organization focused on reducing greenhouse gas emissions from freight transportation. Smart Freight Centre's vision is an efficient and zero emission global logistics sector. Smart Freight Centre's mission is to collaborate with the organization's global partners to quantify impacts, identify solutions, and propagate logistics decarbonization strategies. Smart Freight Centre's goal is to guide the global logistics industry in tracking and reducing the industry's greenhouse gas emissions by one billion tonnes by 2030 and to reach zero emissions by 2050 or earlier, consistent with a 1.5°C future.

Contact

Smart Freight Centre
Keizersgracht 560, 1017 EM, Amsterdam, Netherlands
P.O. Box 11772, 1001 GT, Amsterdam, Netherlands
Tel office: +31 6 4695 4405
www.smartfreightcentre.org
info@smartfreightcentre.org

Technology Partner

Think-it is a software engineering collective. Their mission is to leverage technology to regenerate our planet and advance human potential. They are pioneers in the operationalization of data space connectors, making sovereign data exchange a reality. Their cutting-edge cross-disciplinary approach is advancing a more sustainable future.

Knowledge Partners

BSI (British Standards Institution) is a non-profit distributing organization and offers global services in the linked fields of standardization, systems assessment, product certification, training and advisory services. BSI has worked with SFC and the SFC Exchange Network consortia in advising on an initial risk-based controls framework for the PoC phase.

McKinsey Sustainability is the firm's client-service platform with the goal of helping all industry sectors reach net zero carbon emissions by 2050 and to cut emissions by half by 2030.

The SINE Foundation is a tech for good non-profit which supports global organizations in establishing and maintaining data collaboration initiatives within complex multi-stakeholder environments through ready-to-use governance tools and open-source software.

Acknowledgements

This Proof of Concept evaluation report about the SFC Exchange Network project was written by Smart Freight Centre with contributions by Think-it and BSI. The authors wish to thank partners from the logistics industry, representing shippers, logistics service providers, carriers and technology solution providers who collaborated on the development of the evaluation report for their valuable insights, expertise, and contributions. We would also like to thank The Climate Pledge for its partnership and support of this publication.

Participants and contributors

Contents

List of tables

List of figures

Executive Summary

The logistics industry faces numerous challenges attaining overall visibility on greenhouse gas (GHG) related information from transport chains. Starting with siloed data, limited availability and the difficulties in the exchange of data, these challenges are structural and known within the industry. Another major challenge is the lack of trust. This creates a huge barrier in the shift towards the decarbonization, as transport value chains are highly interdependent and intertwined across the many stakeholders within.

To alleviate this, the SFC Exchange Network was initiated with the aim to facilitate emissions data exchange based on data space principles through collective efforts. The SFC Exchange Network is a sociotechnical project composed of multi-stakeholders with the aim to encourage and promote data sharing between transport value chain actors & strive towards carbon transparency. The first major stride towards this target is completed with the Proof of Concept (PoC). This inaugural phase delivered a working technology prototype with ingrained key pillars of governance, technology and assurance.

As a sociotechnical project, the SFC Exchange Network is defined by its governance and assurance characteristics to ensure data space principles such as data sovereignty and security are upheld and maintained. An exploration of potential governance structures and a suggestion for current and future options is conducted. In terms of technological development, a technological prototype was developed and tested, based on principles for decentralized exchanges and previous work on semantics by SFC. Lastly, a preliminary assurance framework is proposed for an assurance process to meet the objectives of such a network while ensuring trust in the data exchange.

The contribution from this Proof of Concept to the logistics industry is three-fold. Firstly, the project has been collaboratively formulated by the project stakeholders proving the need to strengthen collaboration within the transport value chains. Secondly, the technological development was based on an evaluation survey and feedback gathered throughout the project workshops addressing three key criteria. The key takeaways were feasibility of the technical implementation and peer-to-peer data exchange to be 70% and 80% respectively. In terms of willingness to share data, participants rated 6.4 out of 10. In addition, the theoretical work utilized existing knowledge and explored options for future governance and assurance frameworks within the domain of environment-related data spaces. Finally, the results of this project prove the need for future efforts in an industry with colossal effects on the environment such as logistics.

The Proof of Concept provided a momentum and promising results to continue towards a full build. Moving forward, a considerable amount of work is required to improve and scale towards maturity. A few key improvements for the future of the SFC Exchange Network are improving semantics, handling of large datasets and designing a user interface. This vision cannot be achieved by a single entity; it requires collective efforts of all stakeholders. Therefore, joint action is both necessary and impactful in reducing GHG emissions and strengthening resiliency for planet earth and future generations.

1 Business Value

The need for companies to improve their understanding on carbon impact continues to be more relevant than ever. This is coming at an unprecedented time of transparent and actionable corporate social responsibility targets. The shift towards addressing carbon footprint for products and services is contingent upon the availability and the accessibility of data for a sound overview. Thus, SFC Exchange Network is a sociotechnical project aimed to demonstrate the strength of collaborative efforts to harmonize data sharing on the premises of dataspace principles.

The collaboration of diverse actors to report better quality data allows consumers to take informed action and signal the shift towards decarbonization with their choices. In addition, a methodological approach to corporate reporting which relies less on manual input can catalyze the shift towards decarbonization as complying with regulations from local and international governmental agencies are becoming non-negotiable.

The focus of the PoC phase has been set on large corporate to corporate exchange. Initially, two use cases were prioritized; carbon reporting and identification of carbon hotspots. However, due to resource limitations from the participants, only the use case of improving accuracy of reporting emissions is the focus of the PoC. Improving accuracy of reporting emissions is an important use case for all stakeholders working to gain a better overview on their data and inform sustainability-led decision-making. In today's business world, the extent of a company's profitability is contingent upon the climate impact of its operations, legal compliance and brand identity regarding carbon emissions. Thus, choosing this use-case is a first step towards supporting granular logistics emissions reporting. The Proof of Concept was evaluated based on the data exchange for the chosen use case which provided the context of the exchange. The evaluation of this phase is assessed against three key criteria of:

- Willingness to share data
- Feasible peer-to-peer data exchange
- Feasible technical implementation

Looking beyond the PoC phase, dataspaces provide immense opportunities to foster carbon transparency. Currently within the logistics industry, carbon reporting levels are within business-to-business (B2B) or business-to-consumer (B2C) exchanges. In the future, enabling business-to-anyone (B2X) reporting is key so that any use case can be addressed through data exchange. Therefore, this work is preparatory to achieve the grander vision of B2X reporting for multi-faceted objectives towards decarbonization.

1.1 Project Team

The project team consisted of Smart Freight Centre as the main project management team as well as external support teams. The external support teams contributed within their realm of subject matter thereby providing expertise and valuable inputs to the shaping of the PoC phase. The teams consisted of Think-it, British Standards Institution (BSI) and McKinsey Sustainability. Think-it headed the IT development and technology implementation. McKinsey Sustainability contributed a fact-based analysis towards developing the Business Value Proposition and Full Build development assessment. BSI advised on an initial risk-based assurance framework to be audited. Additionally, drawing upon the already existing working relations with the Partnership for Carbon Transparency (PACT) - a consortium managed by WBCSD, numerous brainstorming exchanges were conducted to share best practices on consortia. Finally, the SINE Foundation has aided in the data semantics segment and provided guidance on industry practices in sovereign data sharing.

1.2 Project Participants

Moreover, this project would not have started and progressed further without the unwavering contributions of the participants. The participants were a combination of shippers, carriers, logistics service providers (LSP's) and tool providers. The PoC participants were composed of two groups, advisory and core members. The advisory members have been supportive in the project initiation. Additionally, they provided feedback on key decisions of the project through their participation in plenary workshops.

The core members are participants who have been continuously providing input and feedback throughout the project. From the project initiation, starting with the kick-off period, progressing thus far in the project to support testing until the end of the PoC. The core members have formed PoC value chain groups to test the use case of: Improving accuracy of reporting emissions. The value chain participants fulfilled one of the two main roles of: data providers and data consumers. Lastly, one tool provider asynchronously supported the work given their resource availability and expertise in API development. They exchanged dummy data with a hypothetical data consumer, being Think-it.

2 Governance

Governance is a term that defines any interaction in a social setting. It is particularly crucial to be defined in a very complex project that comprises of multiple stakeholders. Hence, governance is one of the main pillars of SFC Exchange Network. Considering dataspaces are an open ecosystem of data sharing based on adherence to set guidelines, it is of utmost importance to determine the governance structure. A governance structure in dataspaces mandates a playbook of how participants conduct themselves and interact with one another in a level playing field. This is important as dataspaces are self-governing and complex in nature hence a playbook with guidelines on participants' roles and obligations, legal obedience and conflict resolution scenarios must be determined. These guidelines are the dictation of the dataspace as it is set forth, agreed upon and monitored by all participants of the dataspace.

According to Reference Architecture Model v.3 report by (International Data Spaces Association, 2019), the strength of dataspaces is drawn from the fact that it is an ecosystem which leverages the federation of participants for the mutual benefit of all. As a result, dataspaces enable participants the ability to contribute while maintaining accountability to fulfil secure and trusted data sharing mechanisms. In general, governance structures in dataspaces consist of two components:

- Organizational governance
- Data governance

For the scope of the PoC, governance within this section is reflected as organizational governance defined by Cairney (2019) as the "range of practices or conditions to ensure integrity and accountability in a social setting". Whilst the data governance as emphasized by the International Data Spaces Association is crucial as well—this part is embedded in greater details within the technology section of this report (see section 3).

2.1 Organizational Governance

Organizational governance can take many forms and shapes depending on the context and envisioned aim of the congregation. SFC Exchange Network's PoC phase aims to provide an industry wide automated and decentralized exchange of logistics GHG emissions thereby enabling a use case to improve accuracy of reporting emissions. Refining the accuracy of emissions allows for better transparency within the logistics sector that is significant to decarbonize. In relation to this, the organizational governance structure is to be based on environment-related data space principles to drive the work towards decarbonization. According to the Governing the Environment-Related Data Space report from the GovLab, three criteria are essential in achieving an effective governance structure as seen in below Figure 1 which depicts Data Governance Components (Fritzenkötter, et al., n.d.).

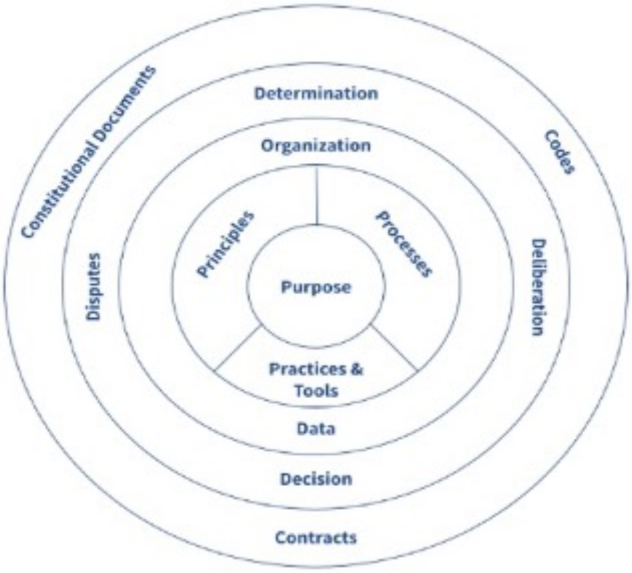


Figure 1: "The 3 Ps of Data Governance" by (Verhulst & Young , Governing the Environment-Related Data Space, n.d.)

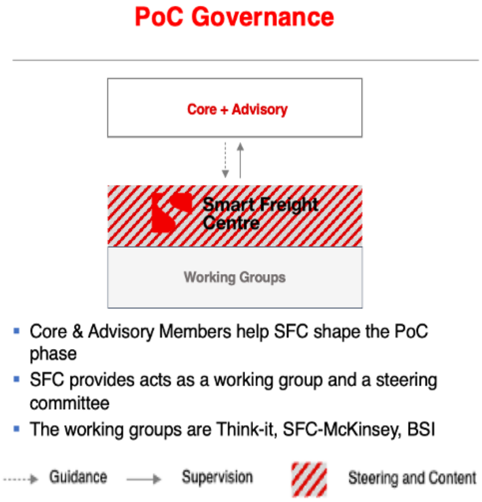
The criteria are composed of the "3 Ps": principles, processes, and practices thereby cumulatively making up the purpose (Verhulst, Hudson, & Zacharzewski, Governing the Environment-Related Data Space, 2022):

- Principles are the core characters to guide and establish activities
- Processes are systematic methods in which decision making is taken and implemented
- Practices & Tools are the actions and resources needed to bring the structure alive

The 3 P's relate to various aspects which are closely and broadly related to overall Data Governance components. This framework by Stefaan G. Verhulst and Andrew Young showcases the complexity of governance and the ever-present multi-layers (Verhulst, Hudson, & Zacharzewski, Governing the Environment-Related Data Space, 2022). With the SFC Exchange Network being a complex project composed of various stakeholders, it was evident to define the organizational governance to ensure fair and robust structure that upholds responsibility and accountability amongst participants.

2.2 PoC Governance

During the PoC phase, SFC oversaw the organizational governance of the project with input from the core and advisory members. This decision was due to two reasons. Firstly, guidance was needed given the short time period and members' limited conceptual understanding of the project. Therefore, having SFC as a centralized decision-making body was efficient to be agile and propel the work given the very ambitious timeline. SFC is a neutral entity amongst the actors with the intermediary role to act as a guide was a needed approach. Secondly, the PoC is the initiation of a decentralized, dataspace effort. Thus, as the grounding work was created, a successful PoC delivery with tangible results was needed before exploring any governance structure with higher member involvement.



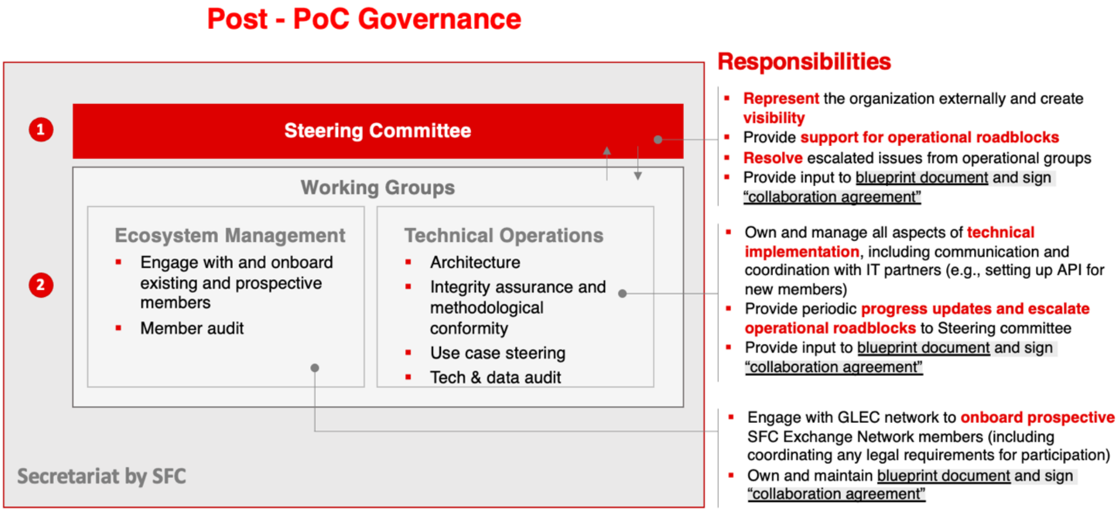
- Core & Advisory Members help SFC shape the PoC phase
- SFC provides acts as a working group and a steering committee
- The working groups are Think-it, SFC-McKinsey, BSI

Figure 2: PoC Governance

In Figure 2, a depiction of the PoC governance structure is laid out. As seen, the PoC governance is made up of core and advisory participants who guide SFC through critical feedback and engagements. In turn, SFC “steers” the overall structure by incorporating the input from participants as well as completing content and project management tasks. This dual role resulted in SFC acting both as a working group and a steering committee. Further working groups include the external support teams who are instrumental in the project. Since this governance structure was undertaken during the PoC, it is temporary.

2.3 Intermediate Post-PoC Governance

In between the PoC phase and the fully scaled solution, is the intermediate post-PoC phase. In terms of organizational governance, the post-PoC phase will be marked by increasing participants, amidst other objectives, who will join SFC Exchange Network to pilot the technology further. This is a growth projection that requires SFC to be involved as the project adapts to the expanding members and other objectives such as increased use cases. Therefore, SFC will act as a secretariat to help with “nurturing” the project towards further maturity.



Post - PoC Governance

1 Steering Committee

2 Working Groups

Ecosystem Management
- Engage with and onboard existing and prospective members
- Member audit

Technical Operations
- Architecture
- Integrity assurance and methodological conformity
- Use case steering
- Tech & data audit

Secretariat by SFC

Responsibilities

- **Represent** the organization externally and create **visibility**
- Provide **support for operational roadblocks**
- **Resolve** escalated issues from operational groups
- Provide input to blueprint document and sign "collaboration agreement"

- Own and manage all aspects of **technical implementation**, including communication and coordination with IT partners (e.g., setting up API for new members)
- Provide periodic **progress updates and escalate operational roadblocks** to Steering committee
- Provide input to blueprint document and sign "collaboration agreement"

- Engage with GLEC network to **onboard prospective** SFC Exchange Network members (including coordinating any legal requirements for participation)
- Own and maintain blueprint document and sign "collaboration agreement"

Figure 3: Post - PoC Governance

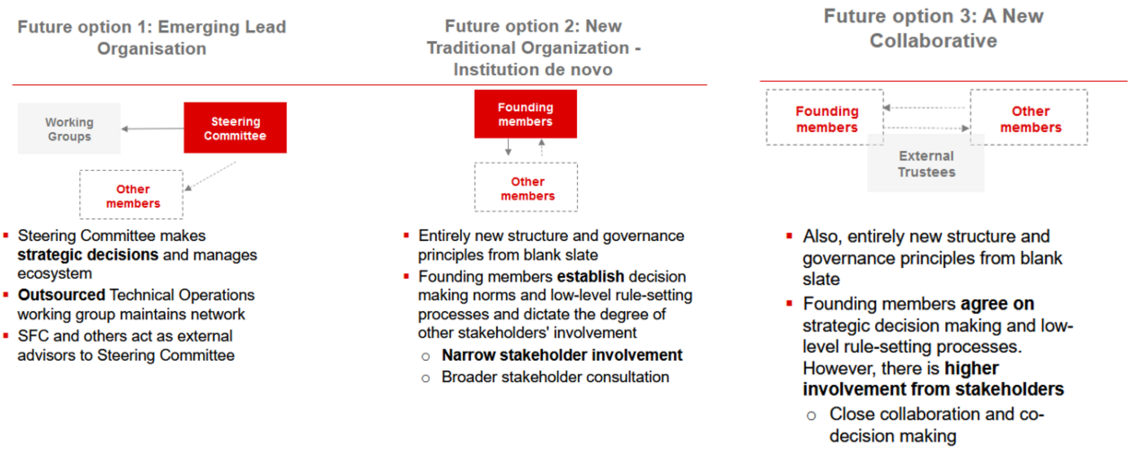
Figure 3 above displays the immediate post PoC governance structure which is chosen. A few of the main “nurturing” tasks include SFC to make decisions on the working groups of the project. Such working groups will be organized into two parts, the ecosystem management and technical operations. One of the main changes that is expected is the official Steering Committee group which will provide overall visibility and support the operations. This group will be composed of the various company participants and voted in by a participatory process. SFC as a secretariat joined by the Steering Committee and working groups, the SFC Exchange Network can continue to develop in project structure and establish itself further in dataspace efforts.

2.4 Future Governance

Since the previous phases are considered provisional, moving from a temporary governance structure to an established governance structure requires the need to collect input from participants and follow guidance from IDSA and other related decentralized dataspace knowledge streams. Although there may be various working definitions of governance, when it comes to defining the structure--majority emphasize the importance of collecting input from participants so that all opinions are voiced.

Considering this key aspect of governance, consequently, a hybrid workshop on Governance and Assurance was held during the Smart Freight Week in April, 2023. The goal of this workshop was to gauge understanding on governance as well as discuss and collect input regarding future governance options. During this workshop, SFC presented governance options based on *Governing the Environment-Related Data Space* report (Fritzenkötter, et al., n.d.).

After a group brainstorm session and related discussions on the governance options, the participants voted for their favorite option on the premise that the SFC Exchange Network is moving past the scale-up phase. The options are seen in Figure 4.



Future option 1: Emerging Lead Organisation

- Steering Committee makes **strategic decisions** and manages ecosystem
- **Outsourced** Technical Operations working group maintains network
- SFC and others act as external advisors to Steering Committee

Future option 2: New Traditional Organization - Institution de novo

- Entirely new structure and governance principles from blank slate
- Founding members **establish** decision making norms and low-level rule-setting processes and dictate the degree of other stakeholders' involvement
  - **Narrow stakeholder involvement**
  - Broader stakeholder consultation

Future option 3: A New Collaborative

- Also, entirely new structure and governance principles from blank slate
- Founding members **agree on** strategic decision making and low-level rule-setting processes. However, there is **higher involvement from stakeholders**
  - Close collaboration and co-decision making

Figure 4: Future Governance Options

The voting results concluded the favorite option to be Future option 1: Emerging Lead Organization. The three options displayed in Figure 4 are based on the work of (Fritzenkötter, et al., n.d.). from the GovLab. Discussing and brainstorming on the future governance structure is useful to understand what participants think and identify where progress can be made to move towards advanced and a resilient governance structure although it is a far-fetched task considering there will be many modifications.

Based on continuous feedback and discussions regarding future governance structure, there are a few open-ended questions which can help guide the choice of a governance scheme. At this stage, it is difficult to address them but these questions and points will be taken aboard for future developments. Some examples include:

- How are decisions made in the Network? Is the philosophy of the work reflected in the decision making?
- How participatory is the decision making?
- Is there a voting mechanism? If yes, how does it work?
- How will the Network interact with similar consortia?
- How will the governance change when i.e., 1000 members are on board?

3 Technology

The project is built upon key principles that prioritize data ownership, security, control, interoperability, and adaptability. By adhering to these principles, the project fosters trust, enhances data governance, and facilitates valuable insights from shared data.

- **Data sovereignty:** Participants keep ownership rights over their data, ensuring that they **retain control and autonomy** over its use. Data is not stored in any intermediary system; it is shared directly from participants' systems to the recipient.
- **Security:** We prioritize the security of the data through **encryption**, ensuring confidentiality even in the event of unauthorized access.
- **Control:** Participants have the ability to **revoke access** to their data at **any time**, providing them with control over who can view their information.
- **Interoperability:** Consistent formatting and nomenclature enable seamless **integration** of disparate data sources, enhance **data interoperability**, and simplify **data governance**. Ensuring that participants can trust the accuracy and reliability of the data they interact with, fostering trust and enabling meaningful insights to be derived from the data.
- **Adaptability:** The system is designed to be versatile and adaptable, capable of **accommodating diverse technologies, use cases, and industries**. By remaining flexible and **agnostic** to specific technological or industry requirements, we ensure our solution can seamlessly **integrate into different systems** and cater to a wide range of use cases.

3.1 SFC Exchange Network – API

In the project, an API has been developed with the objective of streamlining data sharing, enforcing data model compliance, and enabling integration with participants' existing systems. These features empower participants to easily collaborate, maintain data consistency, and adapt to changing needs as the project evolves, following the project’s principles of **adaptability, control, interoperability, and security.**

First, the API simplifies the process of sharing data with other participants by abstracting the complexities of the Eclipse Dataspace Connector (EDC). This streamlined approach fosters efficient data exchange and enhances collaboration among all participants.

Furthermore, the API ensures seamless data model compliance. It enforces the standardized data model across all participants, allowing each participant to align their data with the specified model. At this stage, the data model which is used is a subset of the data model published as part of the Data Access for Logistics Emissions Project. This eliminates inconsistencies and promotes data quality. The uniformity in data structures and formats enhances interoperability, facilitating smooth data integration and analysis.

The API offers flexibility, enabling participants to integrate it into their existing systems, regardless of the platforms or technologies they currently employ. This compatibility ensures a smooth transition and allows participants to leverage their existing infrastructure. Additionally, the API is designed to support automation, empowering participants to automate data management processes when needed. This adaptability ensures that participants can optimize their workflows and achieve operational efficiencies as the project evolves.

Tags: Data sovereignty, interoperability, control, security, adaptability

3.2 The Eclipse Dataspace Components (EDC) Connector at the heart

A connector provides a generic way to express, negotiate, and document the rules for sharing data, as well as with whom it is shared. These rules are not only in plain text but also machine-readable and enforceable. To guarantee consistency and interoperability in policy definition, the rules or “policies” are formulated using the ODRL (Open Digital Rights Language).

The Eclipse Dataspace Components (EDC) project, governed by the Eclipse Foundation, offers a comprehensive set of open-source components for building data spaces (Eclipse Foundation, 2022). Its main component, the Connector, enables secure and sovereign inter-organizational data exchange based on the International Data Spaces (IDS) standard. This extensible framework supports multiple clouds and protocols, including those associated with the GAIA-X project, empowering organizations to establish trusted data sharing environments. With decentralized design and support for various data transfer protocols, the Eclipse Dataspace Connector ensures enterprise-grade scalability and performance for organizations of any size.

The most important facts about the Eclipse Dataspace Components Connector

- The connector is **completely FOSS** (free and open-source software) supported by various companies
- The connector (through Eclipse Foundation) has clear and **accepted governance** structure and community processes
- The connector is **more than connecting a database**
- The connector manages **data transfer and flow inclusive management of contract and policy management** in cloud-native environments
- The connector follows **a modular system** to serve as a facilitator
- Running **code available** on GitHub

Tags: Data sovereignty, interoperability, control, security, adaptability

3.3 Testing Process

The participants were actively engaged in the testing process, which involved the preparation and exchange of a set of data within the provided infrastructure. Pairs were derived based on the existing contractual relationships participants had to ensure data confidentiality and simulate a realistic scenario of data sharing. Carriers acted as data providers sharing information related to the activity of the freight and its emissions back to shippers, the data consumers. To ensure a realistic testing environment, the pairs were asked to prepare a set of data that closely resembled real-world data, although it could be dummy data.

During the Proof of Concept (PoC), participants were presented with two options: they can either have the deployment handled by the Think-it technical team utilizing the infrastructure provided by SFC or receive support and deploy the solution themselves. Participants were also presented with a range of data source options, providing them with flexibility and catering to their individual preferences. They could choose between utilizing data from HTTP sources, S3 buckets, or Azure blob storage. This was intended to offer a variety of options that allowed them to select the one that aligned best with their specific requirements and existing infrastructure.

Before testing began, Think-it conducted a workshop which served as an initial introduction to the API and a demonstration on how to use it, ensuring that participants gain a clear understanding of its capabilities. To facilitate the testing of data exchange, the participants were also provided with detailed documentation that serves as a valuable resource, offering support and guidance throughout the testing process.

Considering the time constraints and availability during the testing phase, all the participants decided to have the deployment handled by Think-it on SFC's infrastructure. This technology choice in simple terms is the "SME plug-in option" and it can be classified as Software as a Service (SaaS). The main benefits are that the technology is configured and deployed easily for the participants and the software updates can be automatically rolled out. However, choosing such an option has its respective considerations. It is worth mentioning that it can be restrictive for companies in terms of flexibility as there is a separation between this SaaS choice and company's IT infrastructure.

A second option for companies was also developed which was the "deploy it yourself" choice. All participants could use their own cloud infrastructure and deploy the API. This choice allows for a higher degree of control. Thus, participants can decide how to shape the API and integrate in within their IT systems. This option requires maintenance responsibility and higher resource commitments from participants. A few benefits are clear with such a choice: each company has a higher degree of flexibility for customisation thus achieving higher interoperability with own existing environment for internal processes.

All in all, the project concluded with all participants choosing the SaaS solution using the SFC infrastructure deployed on AWS. This was justifiable given the time and resources available for the PoC. For future testing, corporate needs should be identified in terms of carbon reporting obligations and IT procedures. In addition, participants would have to agree on a set of technological features that the API would have to cater to. This requires prioritisation and ranking of the most important criteria to navigate between the two technology choices upon joining the SFC Exchange Network.

3.4 SFC Exchange Network PoC Architecture – Showcasing the exchange of data

The participants were grouped in pairs of data providers and data consumers. These pairs reflected their contractual relationships in real life and guided the data exchange. In the project, the data providers were carriers and the consumers were the respective shippers they provide services to. In the data exchange process, there are two main phases: "Preparing the data exchange", details at Figure 5 and " The consumer requests data from a provider " with more details at Figure 6.

In Figure 5, the provider initiates the process by sending a request that includes details about the data they want to share (1), such as its location and the intended recipient. The API then communicates with the connector (2), which creates an asset linked to the data source. This asset is configured with the appropriate policies to enable secure sharing with the chosen participant.

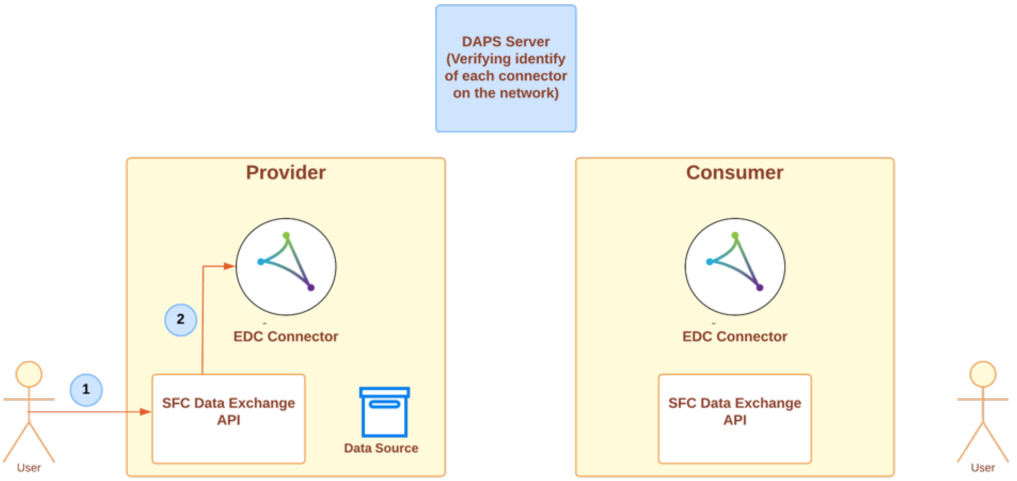


Figure 5: Preparing the data exchange

Once the data is prepared, the data exchange can happen as seen in Figure 6. In this phase, the consumer sends a request to the API (1), specifying the data they want to consume. The API then communicates with the connector (2) to initiate the exchange process. The consumer's connector establishes communication with the provider's connector (3), which retrieves the requested data from the provider's data source. The retrieved data is then passed back to the API (4), which finally delivers it to the consumer.

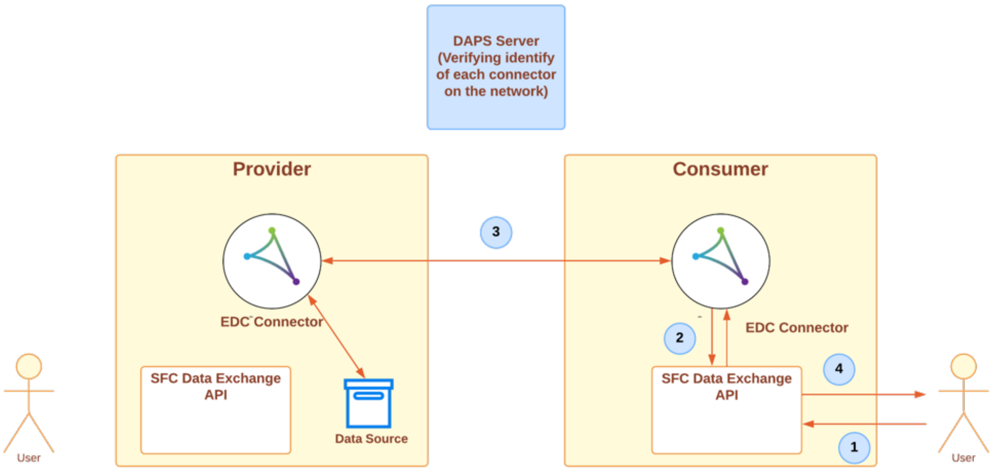


Figure 6: The consumer requests data from a provider

4 Assurance Framework and Approach

As part of the Proof of Concept, SFC has identified the need to establish trust in the SFC Exchange Network. To achieve this, an assurance framework needs to be established, embedded and monitored to mitigate risks relating to trust in the data exchange. Within the assurance framework, a set of controls needs to be iteratively defined. The output of this assurance framework should ensure that controls are firstly identified and present and secondly are operating as intended.

This framework has been structured into three pillars to address the key categories of risks identified:

Table 1: Overview of the assurance framework

	Pillar 1	Pillar 2	Pillar 3
	Member	Technology	Data
Description	Member's management of emissions data.	The software and hardware supporting the exchange.	Data flow and processing within the exchange.
Risk	The controls supporting the pillars (i.e. Risk categories) are not aligned to best practice which may result in a loss of trust in the data exchange.		
Focus	Are the members business practices, data management, accounting and reporting practices carried out appropriately?	How can we place reliance on a decentralized technology solution? Can it accommodate the variances in size, security, maturity and complexity of the key stakeholders?	Does the data being submitted by members adhere to predefined parameters?
Output	Out of scope as this is part of another work stream and it is expected these requirements will be adhered to by members.	To define the controls expected to mitigate the risk and document these requirements so that they can be embedded and monitored.	

An initial subset of this assurance framework is described in this section. The assurance framework is based on internationally recognized frameworks that are widely accepted and used internationally. Key terminology to remember:

Table 2: Key terms

Term	Description
Controls	These are the controls that need to be put in place to make sure that the respective process achieves its objectives.
Assurance Framework	Establishing the process of monitoring these controls to ensure they have been embedded and are working effectively i.e. the assurance protocol, criteria, frequency, roles and responsibilities etc. This should incorporate an

	independent audit of the assurance framework by an external auditor with appropriate competencies.

4.1 Pillar 1: Member

Best Practice Identified

A core foundational requirement of maintaining a high degree of trust in the data exchange is that all parties are confident that emissions data submitted into the ecosystem are produced based on best practice guidance on emissions management and calculation, and that data represents all relevant business activity. The existing GLEC guidelines and ISO 14083 standard provide the most relevant best practice foundations at this point, and organizations can opt to be verified or certified against these by qualified auditors. Such verification and certification schemes will eventually form the foundational basis for enabling members to participate in the data exchange, with relevant information about third-party verification/certification and the status of individual members being recorded in the SFC Exchange Network.

Critical Controls

The purpose of the Member Assurance scheme is to evaluate and verify that member practices and organizational controls are in alignment with key guiding principles described in ISO 14083 of Completeness, Consistency, Accuracy, Transparency, and Conservativeness. This pillar should also define the scope / system boundaries that companies will be exposing within the SFC Exchange Network, for example the number of business units including data at any given time, or the number/percentage of suppliers participating in sharing data.

Post-PoC Steps

In the next post-PoC phase – as a core part of defining the wider member onboarding procedures, conformity of members to both the relevant ISO 14083 and SFC CAS schemes as part of these procedures will be more deeply considered, with data integrity and quality beyond manual inputs being a core requirement of members participating in the Data Exchange.

4.2 Pillar 2: Technology

Best Practice Identified

Providing assurance over a decentralized technology solution requires a tailored approach that is both meaningful and practical. The approaches proposed here are grounded in international best practice, but have been designed to provide flexibility of choice in specific criteria against which the key cybersecurity principles of (1) Confidentiality, (2) Integrity and (3) Availability can be assessed.

The use of v1.1 of the NIST Cybersecurity Framework (CSF)[1] or similar is proposed. The Framework provides a common language for understanding, managing and expressing cybersecurity and broader technology risk both internally and externally, and can be used to help identify and prioritize actions for risk reduction. Selection of NIST CSF for use within this project is more advantageous than a specific international cybersecurity or information security standard.

NIST CSF is a flexible framework under which we can:

- Consider the decentralized nature of the data exchange, ensuring that risks are identified and assigned to data exchange custodians (e.g. SFC/Think-It) or individual members in an appropriate manner.
- Identify controls using NIST's functions to define an overarching set of assurance criteria that can be applied and assessed, while considering the size and risk profile of the different exchange members.

- Identify controls at the exchange design phase, assign appropriate mitigations to be implemented throughout the development phase to ensure the controls objectives are met, assign ownership and accountability, and track any observations through to operationalization.

Critical Controls

NIST CSF is an activity or capability focused framework, which means the basic activities or capabilities required to manage information security risk, enable risk management decisions, address threats and continuous improvement, are organized using a set of 5 Functions – namely:

- *Identify: "Develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities."* The activities in the Identify function are foundational for effective use of the Framework. Understanding the business context, the resources that support critical functions, and the related cybersecurity risks enables an organization to focus and prioritize its efforts, consistent with its risk management strategy and business needs.
- *Protect: "Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services"* The Protect Function supports the ability to limit or contain the impact of a potential cybersecurity event.
- *Detect: "Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event"* The Detect function enables timely discovery of cybersecurity events.
- *Respond: "Develop and implement the appropriate activities to take action regarding a detected cybersecurity event"* The Respond Function supports the ability to contain the impact of a potential cybersecurity event.
- *Recover: "Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event."* The Recover function supports timely recovery to normal operations to reduce the impact from a cybersecurity event.

A detailed list of the NIST CSF control categories and subcategories is provided as a separate appendix.

Post-PoC Steps

A Technology Assurance scheme will be developed during the next phases of this work and then incorporated into this Assurance Framework.

4.3 Pillar 3: Data

Best Practice Identified

SFC has a number of separate set of initiatives around developing consistent understanding of data semantics around parameters relevant to the data exchange which support the data validation goals required here. To support the scale and speed needed by an exchange network of this size, key optimal elements of data integrity and assurance should be automated and built into checks of data as they are submitted into the system. Therefore, the data validation element of the assurance framework is designed as system-managed semantic validation of data submitted by members (in-line as data is submitted) to ensure that specific data adheres to predefined parameters - data types, feasible ranges of data, accurate outputs of data calculations, etc. A prerequisite of good exchange data validation rules is the activities highlighted in Pillar 1 above in relation to upstream assurance of member practices.

Critical Controls

This pillar focuses on ensuring that data being submitted into the SFC Exchange Network system adheres to a number of key principles described in the ISO 14083 standard[2] - or put more simply, “what good input data to the exchange should be”. These principles, in the context of good data validation rules are:

- **Completeness:** Data submissions should include all relevant GHG emissions specific data to the allocated business activity. Although this principle will be fully verified via the next Member Practices Assurance element of the assurance framework, opportunities to implement completeness checks of member data submitted into the system will be implemented where feasible, to ensure that submitted data reflects all applicable business activity and GHG emissions specific to appropriately allocated business activity.
- **Consistency:** Data submissions should enable meaningful comparisons in GHG-related information, ensuring that submitted data is only permissible within specific ranges or based on consistent units. Any data not adhering to required ranges/units will flag a system error and will not be accepted by the SFC system, which supports meaningful comparisons across submissions.
- **Accuracy:** Accuracy in business activity data and/or calculated GHG emissions will reduce bias and uncertainties as far as is practical, for primary, modelled or other data formats. The data validation element of the Framework supports this principle by ensuring that submitted data falls within ranges that reflect typical or feasible business activity and greenhouse gas emissions, and that data associated with multiple units of business activity produce accurate outputs (e.g., GHG calculations), where feasible and where input/output data are available.
- **Transparency:** This principle aims to ensure that sufficient and appropriate GHG-related information is disclosed, allowing intended users to make decisions with reasonable confidence. In practice, this means that the assumptions and methodologies used in creating a data inventory should be clearly explained to facilitate replication and assessment of the inventory by the intended users of the reported data. Although the Member pillar of this framework will evaluate methods and assumptions, the Data pillar will support this principle by preventing omissions of required information, such as:
    - Business activity data
    - Disclosure of use of primary or secondary data
    - Disclosure of estimations or modeling used to produce calculations
- **Conservativeness:** This element of the framework will support the principle of conservativeness by rejecting data or calculations that are disproportionately small or large, and fall outside of the range of feasible volumes of business activity and/or associated GHG emissions associated with transport activity.

Post-PoC Steps

Note that initial data validation criteria have been implemented for an initial set of input data parameters supported by the PoC, with an intent to expand the data validation checks as the number of supported input data parameters increase. The SFC Exchange Network project team will continue to seek member input and technical assistance in the definition and application of the expanding validation requirements post-PoC.

5 Evaluation

The goal of the Proof of Concept was to verify the feasibility and value proposition of the SFC Exchange Network, while also identifying critical and sensitive elements that need to be addressed in future scale-up.

The evaluation focused on the following key elements to determine the success of the PoC:

- **Willingness to share data:** The primary component of the evaluation process centers around assessing participants' willingness to share data under the given **data sovereignty, control, security, interoperability, and adaptability principles**. This criterion was specifically selected to gauge participants' acceptance and adherence to the established data governance framework and robust security principles.
- **Feasible peer-to-peer data exchange:** The PoC aimed to demonstrate the practical implementation of data sharing and exchange functionalities within the proposed project. Participants should be able to effectively share and exchange data, showcasing the system's ability to facilitate seamless data transfer.
- **Feasible technical implementation given the nature of the project:** Data sovereignty and security are paramount in any data-sharing initiative. The PoC evaluated the implementation of robust measures to ensure that each participant maintains control over their data and that the data remains secure throughout the sharing process. This includes encryption protocols, access controls, authentication mechanisms, and other relevant security measures that align with the project principles of **security, control, and data sovereignty.**

5.1 Evaluation Outcomes

To assess the PoC results an evaluation survey was designed and shared with all project participants post the testing phase. Participants' feedback was gathered to assess the effectiveness and viability of the POC in achieving its objectives. The outcomes provided valuable insights and drew meaningful conclusions for the future of this initiative. The key takeaways are summarized in the tables below.

- **Willingness to share data**: The average willingness of participants to share data under given data governance and security principles is **6.4 out of 10.** This figure is partially attributed to the value chain partnership which defined the resource availability spent and the efforts put forward in the exchange.
- **Feasible peer-to-peer data exchange**: **80%** of the participants were able to exchange data within their designated partner. This figure is justified due to reasons such as misalignment of value chain capacity and short testing phase. The aforementioned reasons will be addressed in the future.
- **Feasible technical implementation given the nature of the project**: **70%** of the participants believed that data sovereignty and security were maintained. Considering the PoC deployments were hosted on a temporary cloud infrastructure, this figure is reassuring to continue scaling for full integration.

Table 3: Overall impression and experience

Overall Impression of the PoC	Data Exchange
The average rating for the overall impression of the PoC was around 7 to 8, indicating a positive and favorable response from most participants	Most participants were able to exchange data with their designated partner, although some encountered challenges with data models and parameter acceptance

Table 4: API documentation and testing

Experience Testing the PoC	API Documentation	API Responses	Testing Difficulties
Overall, participants had a positive experience testing the POC with a rating of was 7.6 out of 10, with favorable comments about the documentation and support provided	Participants found the API documentation generally easy to understand and sufficient to test the necessary steps, but some suggested improvements to provide more detailed information on the API endpoints	Most participants reported consistent and accurate API responses, but some encountered communication issues	Participants faced challenges related to access issues, the data model, and aligning with it

Table 5: Security and performance

Security Measures Effectiveness	Data Sovereignty and Security	API Performance, Responsiveness, and Reliability
Participants found the security measures, including authentication and access control mechanisms, to be robust and effective	Maintained for most participants, although the testing was not extensive. Participants requested additional transparency and documentation for GDPR compliance	The overall performance, responsiveness, and reliability of the API during testing received an average rating of 7.6 out of 10

Table 6: PoC Evaluation and Expectations

Alignment with Expectations and Objectives	Appealing Aspects	Data Model Alignment
While the PoC aligned with participants' expectations and objectives to some extent, there were suggestions for improvements in user-friendliness and clarity on the role of tool providers	Participants were most interested in the technology aspect of the PoC, including governance and assurance considerations, and the validated data model	The alignment of the data model with existing data structures varied, with ratings ranging from 3 to 10 out of 10. Participants mentioned significant work required to match the data and ensure consistency

Table 7: Post PoC and Implementation

Scalability Confidence	**Post-PoC Use Cases**	**Enhancements**	**Implementation Obstacles**	**Alignment with Goals**	**Likelihood of Implementation**
Participants expressed moderate confidence in the scalability of the PoC API to handle larger volumes of data or users, with an average rating of **5.8 out of 10**	Participants envisioned various use cases and business scenarios after the PoC, including optimizing networks for CO2e minimization, identifying carbon hotspots, monitoring corporate targets, and sharing parcel-level emissions with end customers	Participants recommended mass upload capabilities, improved UX, and additional data source types as primary enhancements	Potential obstacles included data quality, IT infrastructure complexity, and compliance of carriers to the data model	The PoC aligned well with most organizations' long-term strategies and goals, receiving an average rating of 8.8 out of 10	Participants showed a positive inclination towards moving forward with the implementation, with an average score of **8.6 out of 10**

6 Conclusion

Based on the evaluations of insights and feedback from the participants, the PoC has successfully demonstrated the feasibility and potential of data exchange. As participants continue to collaborate and contribute insights, the PoC can evolve into a transformative solution with far-reaching impacts on the industry's sustainability efforts.

For starters, participants demonstrated the ability to exchange data with their designated partners, showcasing the PoC's ability to facilitate smooth and valuable information flow. In terms of support, participants appreciated the well-structured API documentation with comprehensive information on testing and the process of integrating and utilizing the API. With this, the participants stated confidence in the API for real-world application as the API consistently delivered accurate responses during testing. Finally, participants expressed confidence in the security measures, authentication, and access control mechanisms, ensuring data sovereignty and adherence to governance principles.

While there were promising outcomes in certain parts, areas of improvement will need to be identified, prioritized and addressed moving forward. For example, participants encountered challenges aligning their existing data structures with the PoC's data model. Standardization and data model improvements are needed to ensure seamless data integration. In addition, participants requested transparent documentation on GDPR compliance, security measures, and governance aspects to bolster trust. There was moderate confidence in scalability, a comprehensive analysis is necessary to assess performance with larger data volumes and user loads. Lastly, participants stated the need for better user experience and front-end design, aiming to strengthen user adoption and engagement.

Given the aforementioned points and key takeaways from the PoC justified by the participants' evaluation and complemented by the value proposition of the project, pursuit of further work is needed to accelerate transparency in the logistics industry and fast-track decarbonization.

7 Recommendations

Based on the valuable experience and feedback from the PoC, these recommendations address both new insights and aspects that were previously known but left out of the scope in the initial iteration.

Table 8: Recommendations

Technical Challenges and Opportunities	**Scalability and Performance:** Evaluate and enhance the system's scalability to accommodate a larger user base effectively, along with increasing the capacity to handle larger volumes of data, higher frequency of data sharing, or the number of use cases supported. The scalability of the system is crucial to ensure its seamless operation and optimal performance.
	Advanced Data Integrity Layer: Add value restrictions, handling units of measure, and implement validations when retrieving data to maintain data integrity and consistency across the platform.
	More Support for Authentication Methods and Data Sources: Expand the range of authentication methods and data sources to accommodate diverse user needs and preferences.
	Logging and Monitoring: Implement comprehensive logging and monitoring mechanisms to ensure system stability and security and provide insights about performance.
User Experience and Interface	Despite being initially considered a lower priority in the PoC phase, it is now evident that focusing on UX development and creating a user-friendly interface is crucial. A well-designed interface will encourage wider adoption and active engagement among both business and technical teams, making it essential for the project's success moving forward.
Technical Support for Participants	Ensure seamless project adoption by offering tailored technical support catering to different levels of technical expertise/needs from the participants. Providing accessible documentation, establishing a responsive support team, offering guidance through trusted technical partners, helping participants understand the existing ecosystem of applications and software, etc. Enhancing technical support empowers participants, fostering collaboration and project success.
Data Governance and Compliance	Strengthen alignment with SFC and participants to facilitate the rollout of PACT-compliant features and better adherence to established standards and requirements. Continuously assess and refine the data governance and security principles to align with evolving regulations and industry best practices. Additionally, address feedback related to the data model, consider technical ways to standardize formats and ensure consistent labeling of fields to match the data model.
Consider Different Company Profiles	Considering the wide range of participating companies and different profiles, it is key to understand their unique ways of using the

	platform and their distinct requirements is essential for successful project implementation.
Agile & User-Centric Development	Adopt an agile approach for continuous improvement, iterating based on real scenarios feedback, and embracing user-centric insights. Engage participants to better understand their needs, identify pain points, and incorporate these valuable insights into the system's design. By fostering a collaborative platform for knowledge sharing, we ensure collective growth, success, and seamless communication.
Collaboration in a Diverse Participant Landscape and Clear Expectations	Acknowledging the varying levels of maturity and capacity among participants to follow standards, fit project requirements, and collaborate in terms of insights, testing, and support is crucial. As the project progresses and more participants join, establishing clear roles and responsibilities alongside a robust communication and collaboration model becomes essential. Adapting to these differences and defining clear expectations and commitments based on each participant's context and availability will play a pivotal role in ensuring the scalability and success of the project.
Creating an Engaging Onboarding Experience	Developing a robust onboarding experience holds significant importance in successfully integrating new participants into the project. It involves providing comprehensive resources that enable individuals to become acquainted with the project's objectives, values, and key aspects from both business and technical perspectives. A well-designed onboarding experience not only facilitates the newcomers' integration but also plays a pivotal role in fostering knowledge sharing, collaboration, and overall project success.
Effective Communication and Transparent Documentation	One key aspect moving forward is coordination, clear documentation, and transparent communication among diverse participants. Regular updates, documented decisions, and shared guidelines build trust and understanding. Providing easy access to essential information through a centralized platform, collaboration & trust are fostered.
Envisioned Valuable Business Use Cases	Participants various use cases and business scenarios that could add value to their organizations. These include optimizing networks for CO2e minimization, identifying carbon hotspots, monitoring corporate targets, and sharing parcel-level emissions with end customers, underscoring the PoC's potential for significant business impact.

8 Bibliography

Cairney, P. (2019). *Understanding Public Policy: Theories and Issues (2nd ed.).* Bloomsbury Publishing.

Fritzenkötter, J., Hohoff, L., Pierri, P., Verhulst, S. G., Young, A., & Zacharzewski, A. (n.d.). *GOVERNING THE ENVIRONMENT-RELATED DATA SPACE.* TheGovLab.

International Data Spaces Association. (2019). *REFERENCE ARCHITECTURE MODEL.* Berlin: International Data Spaces Association.

Verhulst, S. G., & Young , A. (n.d.). *Governing the Environment-Related Data Space.* Retrieved from TheGovLab: https://blog.thegovlab.org/post/governing-the-environment-related-data-space

Verhulst, S. G., Hudson, C., & Zacharzewski, A. (2022, October 04). *Governing the Environment-Related Data Space*. Retrieved from TheGovLab: https://blog.thegovlab.org/post/governing-the-environment-related-data-space

Eclipse Foundation. (2022, July). *Eclipse Dataspace Components* . Retrieved from https://projects.eclipse.org/projects/technology.edc

The React Framework for the Web. (n.d.). Retrieved from NEXT.js: https://nextjs.org/

Koa next generation web framework for node.js. (n.d.). Retrieved from Koa: https://koajs.com/

Redis. (n.d.). Retrieved from Redis: https://redis.io/

Automate infrastructure on any cloud with Terraform. (n.d.). Retrieved from Terraform: https://www.terraform.io/

Production-Grade Container Orchestration. (n.d.). Retrieved from Kubernetes: https://kubernetes.io/

Dynamic Attribute Provisioning Service (DAPS). (n.d.). Retrieved from Github: https://github.com/International-Data-Spaces-Association/IDS-G/blob/main/Components/IdentityProvider/DAPS/README.md

Identity Provider. (n.d.). Retrieved from Fraunhofer International Data Spaces: https://www.dataspaces.fraunhofer.de/en/software/identity_provider.html

Keycloak. (n.d.). Retrieved from Open Source Identity and Access Management: https://www.keycloak.org/

NIST. (2023, March 13). *Framework Documents*. Retrieved from Cybersecurity framework: https://www.nist.gov/cyberframework/framework

9 Appendix

9.1 Technology choices

9.1.1 SFC Exchange Network – API Tech Stack

The SFC Exchange Network API is built upon a robust and secure tech stack that ensures the reliability, scalability, and protection of data exchanged between participants. By selecting these technologies for the project's tech stack, we ensure that the implementation adheres to the principles of data ownership, security, control, interoperability, and adaptability.

Frontend

Next.js is a powerful web development framework that offers a range of benefits (The React Framework for the Web, n.d.). With its automatic server-side rendering, Next.js enhances the performance and load time of web pages. The inclusion of built-in routing eliminates the need for a separate routing library, resulting in a simplified code base. Additionally, Next.js enables static site generation, creating static versions of pages for improved performance and reduced server costs. Furthermore, Next.js boasts a thriving ecosystem of plugins and libraries, facilitating the discovery of solutions to common challenges and the seamless integration of new features into applications.

Tags: interoperability, control, security, adaptability

Backend

KOA was selected as the backend framework due to its efficiency and modern web development practices, aligning mainly with the project's principles of adaptability and security (Koa next generation web framework for node.js, n.d.). Its streamlined code structure and modular design enable faster development and easy addition/removal of functionality. KOA also provides robust error handling, ensuring a reliable user experience. It provides tools like Helmet middleware to protect against common web vulnerabilities and measures such as CSRF protection and JWT authentication can be implemented to enhance security further. Overall, By utilizing KOA, we ensure a secure and efficient backend that aligns with the project's principles and ensures high performance and reliability.

Tags: interoperability, control, security, adaptability

Redis Cache is an in-memory data structure store that provides multiple functionalities, including high-performance cache, database storage, and message broker (Redis, n.d.). It leverages its in-memory storage mechanism to enable fast access to data, significantly improving data retrieval speed. In the project, it plays a crucial role in managing tokens required for data retrieval. Furthermore, Redis Cache offers robust security features that align with the project's **security principle** and ensures the confidentiality and integrity of the cached data. By leveraging the capabilities of Redis Cache, we **optimize data storage and retrieval**, enhance system performance, and prioritize the security and integrity of the cached data.

Tags: security

Infrastructure

Infrastructure as code: Terraform was chosen as the infrastructure management tool due to its ability to define infrastructure in a code-based format, ensuring consistent reproducibility across different environments (Automate infrastructure on any cloud with Terraform, n.d.). With Terraform, changes to the infrastructure configurations can be tracked and managed, and changes can be easily rolled back when necessary. Collaboration is also made more effective using version control tools. Additionally, Terraform's cloud-agnostic nature allows you to write infrastructure code for multiple cloud providers, providing the flexibility to adapt to different environments and take advantage of various cloud offerings. By utilizing Terraform, we adhere to the project's **adaptability principle**, allowing **consistent infrastructure deployment and easy scalability**.

Tags: adaptability

Orchestration: Kubernetes has been selected as the orchestration tool because it allows to **effortlessly scale the application** to accommodate **increased traffic and workload** (Production-Grade Container Orchestration, n.d.). With its platform-agnostic nature, Kubernetes allows to deploy and manage our application across various cloud providers, on-premises setups, or hybrid environments, providing greater **flexibility** for the participants, aligning with the **adaptability principle**.

Tags: adaptability

Security

Encryption: Ensuring the security of the project is a paramount concern. Robust encryption measures are implemented to safeguard data both at rest and in transit. AWS S3 and other supported data sources offer built-in encryption features, with the option to define custom encryption keys if necessary. Similarly, encryption for databases connected to our instances is enforced. For secure data transmission, HTTPS encryption over SSL/TLS protocols is employed. These encryption practices provide a strong layer of protection for sensitive information, ensuring the project maintains a secure environment for all users, aligning with the security principle.

Tags: security

Network: Network security is another crucial aspect for the project. Encryption is used to safeguard all network traffic, both between the application and users and among different components within the application. By encrypting the communication channels, we ensure that sensitive data remains secure and inaccessible to unauthorized parties. Additionally, secure network architectures like demilitarized zones (DMZ) are applied to create a clear separation between internal and external networks, minimizing the risk of unauthorized access. To further fortify the network, firewalls are implemented to actively monitor network traffic and block potential threats, providing an additional layer of protection against malicious activities. These measures collectively contribute to maintaining a secure network environment, safeguarding the project from potential security risks, and aligning with the security principle.

Tags: security

Authentication - Connector to Connector: DAPS (Data Authorization and Provisioning Service) serves as an attribute server. It issues OAuth2 access tokens to International Data Spaces connectors, enabling them to access services and data from other connectors securely (Identity Provider, n.d.). The DAPS server implements JWT bearer client authentication for OAuth2, allowing connectors to authenticate themselves using their certificates (Dynamic Attribute Provisioning Service (DAPS), n.d.). In return, they receive an access token that grants them authorized access to other connectors within the network. This mechanism ensures secure authentication and facilitates seamless communication between connectors thus aligning with the project's security principle.

Tags: security

Authentication - Application: Keycloak is an open-source identity and access management solution that offers a comprehensive set of features for authentication (Keycloak, n.d.). It provides a centralized platform for managing user identities, securing applications, and enforcing fine-grained access control policies. It offers customizable authentication flows, allowing organizations to adapt the authentication process according to their specific requirements. Overall, it aligns with the security, control and adaptability principles.

Tags: security, control & adaptability

9.1.2 Limitations

During the Proof of Concept phase, certain requirements and features were intentionally excluded from implementation. This deliberate decision aimed to achieve a more efficient and timely delivery of a functional solution, while gaining a thorough understanding of the diverse business requirements and participant needs. By focusing on a simplified approach, valuable insights were gathered to inform the development of more complex features in future phases. This strategic approach minimized the risk of rework and reduced the need for significant adjustments to the initial implementation. These limitations and out-of-scope features should be considered in the context of the short-term nature of the PoC. They can be addressed and expanded upon as the foundation has been set for the project to accommodate these new features in the upcoming phases.

- **Time & resource constraints:** This is a main key factor and to optimize efficiency and meet the project's objectives within the ambitious time available & diverse responsibilities to fulfill, the team had to make strategic decisions regarding resource allocation and project scope. The primary focus was on delivering a functional solution within the defined timeframe, which required adopting a streamlined approach with a strong emphasis on essential functionalities. By focusing on a simplified & agile approach, the objective was to gather valuable insights to inform the value of the project, as well as what would be the best strategy to move it forward as well as identify the needs & requirements to consider for future phases. It also enabled the team to effectively allocate their efforts to understand and develop the solution, create comprehensive documentation, and support materials, actively participate in workshops, communicate & support participants, etc.
- **Use cases:** From the very beginning of the project it became evident that attempting to address a vast array of use cases was not feasible. Consequently, the goal shifted from an initial proposed set of use cases to demonstrate the effectiveness of the data

exchange solution, which possesses the versatility to accommodate various use cases. This deliberate choice allowed the technical team to gain familiarity with the specific business requirements used on the PoC and the participants to do just the necessary adjustments for this stage of the project and align with other use cases in the future.

- **Technology**: The project posed significant technical challenges in integrating various complex components within the PoC timeframe. The EDC, the PACT framework, and the diversity of systems from potential participants, all brought their distinct requirements, making it challenging to create a cohesive solution that could effectively bring them together in the amount of time available. As already stated on previously mentioned factors, this reinforced the decision on the primary goal being the delivery of a functional and operational initial version of the data exchange solution, also from a technical perspective. This approach prioritizes the successful implementation of a working solution, avoiding the risk of non-delivery in time, or developing a solution that would not adequately meet the requirements of a broad range of participants, limiting the options to test and provide valuable input which will inform the development of enhanced functionalities in future phases.

9.1.3 Out of Scope Reflection

It is important to acknowledge that certain items are currently considered out of scope during the Proof of Concept phase due to timeline constraints. However, it should be noted that these items are not limited to future feature phases but encompass key features of the overall project. While they may not be addressed immediately, they hold significant importance and will be carefully considered in subsequent stages of development.

- Support for **batch requests**, allowing users to share multiple shipments simultaneously for improved efficiency
- Support **all** the nine different **use cases** currently identifies
- Handling **large volumes of data**
- All features are fully **PACT compliant**
- Deployment on participant’s systems
- **Advanced data integrity layer:** add values restrictions, handle units of measure, add validations when retrieving data, etc.
- Offer **more** support for **authentication methods and data sources**
- A **user interface** to facilitate interaction with the API
- **Logging and monitoring**

9.2 Assurance Framework and Approach – NIST details

Some details on the NIST framework (NIST, 2023) can be found in the table below.

Function	Category	Subcategory	Informative References
IDENTIFY (ID)	**Asset Management (ID.AM):** The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy.	**ID.AM-1:** Physical devices and systems within the organization are inventoried	· **CIS CSC** 1
			· **COBIT 5** BAI09.01, BAI09.02
			· **ISA 62443-2-1:2009** 4.2.3.4
			· **ISA 62443-3-3:2013** SR 7.8
			· **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2
			· **NIST SP 800-53 Rev. 4** CM-8, PM-5
		ID.AM-2: Software platforms and applications within the organization are inventoried	· **CIS CSC** 2
			· **COBIT 5** BAI09.01, BAI09.02, BAI09.05
			· **ISA 62443-2-1:2009** 4.2.3.4
			· **ISA 62443-3-3:2013** SR 7.8
			· **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2, A.12.5.1
			· **NIST SP 800-53 Rev. 4** CM-8, PM-5
		ID.AM-3: Organizational communication and data flows are mapped	· **CIS CSC** 12
			· **COBIT 5** DSS05.02
			· **ISA 62443-2-1:2009** 4.2.3.4
			· **ISO/IEC 27001:2013** A.13.2.1, A.13.2.2
			· **NIST SP 800-53 Rev. 4** AC-4, CA-3, CA-9, PL-8
		ID.AM-4: External information systems are catalogued	· **CIS CSC** 12
			· **COBIT 5** APO02.02, APO10.04, DSS01.02
			· **ISO/IEC 27001:2013** A.11.2.6
			· **NIST SP 800-53 Rev. 4** AC-20, SA-9
		ID.AM-5: Resources (e.g., hardware, devices, data, time, personnel, and software) are prioritized based on their classification, criticality, and business value	· **CIS CSC** 13, 14
			· **COBIT 5** APO03.03, APO03.04, APO12.01, BAI04.02, BAI09.02
			· **ISA 62443-2-1:2009** 4.2.3.6
			· **ISO/IEC 27001:2013** A.8.2.1
			· **NIST SP 800-53 Rev. 4** CP-2, RA-2, SA-14, SC-6
		ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g.,	· **CIS CSC** 17, 19
			· **COBIT 5** APO01.02, APO07.06, APO13.01, DSS06.03
			· **ISA 62443-2-1:2009** 4.3.2.3.3
			· **ISO/IEC 27001:2013** A.6.1.1

		suppliers, customers, partners) are established	· **NIST SP 800-53 Rev. 4** CP-2, PS-7, PM-11
	Business Environment (ID.BE): The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.	**ID.BE-1:** The organization's role in the supply chain is identified and communicated	· **COBIT 5** APO08.01, APO08.04, APO08.05, APO10.03, APO10.04, APO10.05
			· **ISO/IEC 27001:2013** A.15.1.1, A.15.1.2, A.15.1.3, A.15.2.1, A.15.2.2
			· **NIST SP 800-53 Rev. 4** CP-2, SA-12
		ID.BE-2: The organization's place in critical infrastructure and its industry sector is identified and communicated	· **COBIT 5** APO02.06, APO03.01
			· **ISO/IEC 27001:2013** Clause 4.1
			· **NIST SP 800-53 Rev. 4** PM-8
		ID.BE-3: Priorities for organizational mission, objectives, and activities are established and communicated	· **COBIT 5** APO02.01, APO02.06, APO03.01
			· **ISA 62443-2-1:2009** 4.2.2.1, 4.2.3.6
			· **NIST SP 800-53 Rev. 4** PM-11, SA-14
		ID.BE-4: Dependencies and critical functions for delivery of critical services are established	· **COBIT 5** APO10.01, BAI04.02, BAI09.02
			· **ISO/IEC 27001:2013** A.11.2.2, A.11.2.3, A.12.1.3
			· **NIST SP 800-53 Rev. 4** CP-8, PE-9, PE-11, PM-8, SA-14
		ID.BE-5: Resilience requirements to support delivery of critical services are established for all operating states (e.g. under duress/attack, during recovery, normal operations)	· **COBIT 5** BAI03.02, DSS04.02
			· **ISO/IEC 27001:2013** A.11.1.4, A.17.1.1, A.17.1.2, A.17.2.1
			· **NIST SP 800-53 Rev. 4** CP-2, CP-11, SA-13, SA-14
	Governance (ID.GV): The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.	**ID.GV-1:** Organizational cybersecurity policy is established and communicated	· **CIS CSC** 19
			· **COBIT 5** APO01.03, APO13.01, EDM01.01, EDM01.02
			· **ISA 62443-2-1:2009** 4.3.2.6
			· **ISO/IEC 27001:2013** A.5.1.1
			· **NIST SP 800-53 Rev. 4** -1 controls from all security control families
		ID.GV-2: Cybersecurity roles and responsibilities are coordinated and aligned with internal roles and external partners	· **CIS CSC** 19
			· **COBIT 5** APO01.02, APO10.03, APO13.02, DSS05.04
			· **ISA 62443-2-1:2009** 4.3.2.3.3
			· **ISO/IEC 27001:2013** A.6.1.1, A.7.2.1, A.15.1.1
			· **NIST SP 800-53 Rev. 4** PS-7, PM-1, PM-2
			· **CIS CSC** 19

		ID.GV-3: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed	· **COBIT 5** BAI02.01, MEA03.01, MEA03.04 · **ISA 62443-2-1:2009** 4.4.3.7 · **ISO/IEC 27001:2013** A.18.1.1, A.18.1.2, A.18.1.3, A.18.1.4, A.18.1.5 · **NIST SP 800-53 Rev. 4** -1 controls from all security control families
		ID.GV-4: Governance and risk management processes address cybersecurity risks	· **COBIT 5** EDM03.02, APO12.02, APO12.05, DSS04.02 · **ISA 62443-2-1:2009** 4.2.3.1, 4.2.3.3, 4.2.3.8, 4.2.3.9, 4.2.3.11, 4.3.2.4.3, 4.3.2.6.3 · **ISO/IEC 27001:2013** Clause 6 · **NIST SP 800-53 Rev. 4** SA-2, PM-3, PM-7, PM-9, PM-10, PM-11
	Risk Assessment (ID.RA): The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.	**ID.RA-1:** Asset vulnerabilities are identified and documented	· **CIS CSC** 4 · **COBIT 5** APO12.01, APO12.02, APO12.03, APO12.04, DSS05.01, DSS05.02 · **ISA 62443-2-1:2009** 4.2.3, 4.2.3.7, 4.2.3.9, 4.2.3.12 · **ISO/IEC 27001:2013** A.12.6.1, A.18.2.3 · **NIST SP 800-53 Rev. 4** CA-2, CA-7, CA-8, RA-3, RA-5, SA-5, SA-11, SI-2, SI-4, SI-5
		ID.RA-2: Cyber threat intelligence is received from information sharing forums and sources	· **CIS CSC** 4 · **COBIT 5** BAI08.01 · **ISA 62443-2-1:2009** 4.2.3, 4.2.3.9, 4.2.3.12 · **ISO/IEC 27001:2013** A.6.1.4 · **NIST SP 800-53 Rev. 4** SI-5, PM-15, PM-16
		ID.RA-3: Threats, both internal and external, are identified and documented	· **CIS CSC** 4 · **COBIT 5** APO12.01, APO12.02, APO12.03, APO12.04 · **ISA 62443-2-1:2009** 4.2.3, 4.2.3.9, 4.2.3.12 · **ISO/IEC 27001:2013** Clause 6.1.2 · **NIST SP 800-53 Rev. 4** RA-3, SI-5, PM-12, PM-16
		ID.RA-4: Potential business impacts and likelihoods are identified	· **CIS CSC** 4 · **COBIT 5** DSS04.02 · **ISA 62443-2-1:2009** 4.2.3, 4.2.3.9, 4.2.3.12 · **ISO/IEC 27001:2013** A.16.1.6, Clause 6.1.2 · **NIST SP 800-53 Rev. 4** RA-2, RA-3, SA-14, PM-9, PM-11
			· **CIS CSC** 4

		ID.RA-5: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk	· **COBIT 5** APO12.02 · **ISO/IEC 27001:2013** A.12.6.1 · **NIST SP 800-53 Rev. 4** RA-2, RA-3, PM-16
		ID.RA-6: Risk responses are identified and prioritized	· **CIS CSC** 4 · **COBIT 5** APO12.05, APO13.02 · **ISO/IEC 27001:2013** Clause 6.1.3 · **NIST SP 800-53 Rev. 4** PM-4, PM-9
	Risk Management Strategy (ID.RM): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.	**ID.RM-1:** Risk management processes are established, managed, and agreed to by organizational stakeholders	· **CIS CSC** 4 · **COBIT 5** APO12.04, APO12.05, APO13.02, BAI02.03, BAI04.02 · **ISA 62443-2-1:2009** 4.3.4.2 · **ISO/IEC 27001:2013** Clause 6.1.3, Clause 8.3, Clause 9.3 · **NIST SP 800-53 Rev. 4** PM-9
		ID.RM-2: Organizational risk tolerance is determined and clearly expressed	· **COBIT 5** APO12.06 · **ISA 62443-2-1:2009** 4.3.2.6.5 · **ISO/IEC 27001:2013** Clause 6.1.3, Clause 8.3 · **NIST SP 800-53 Rev. 4** PM-9
		ID.RM-3: The organization's determination of risk tolerance is informed by its role in critical infrastructure and sector specific risk analysis	· **COBIT 5** APO12.02 · **ISO/IEC 27001:2013** Clause 6.1.3, Clause 8.3 · **NIST SP 800-53 Rev. 4** SA-14, PM-8, PM-9, PM-11
	Supply Chain Risk Management (ID.SC): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support risk decisions associated with managing supply chain risk. The organization has established and implemented the processes to identify, assess and manage supply chain risks.	**ID.SC-1:** Cyber supply chain risk management processes are identified, established, assessed, managed, and agreed to by organizational stakeholders	· **CIS CSC** 4 · **COBIT 5** APO10.01, APO10.04, APO12.04, APO12.05, APO13.02, BAI01.03, BAI02.03, BAI04.02 · **ISA 62443-2-1:2009** 4.3.4.2 · **ISO/IEC 27001:2013** A.15.1.1, A.15.1.2, A.15.1.3, A.15.2.1, A.15.2.2 · **NIST SP 800-53 Rev. 4** SA-9, SA-12, PM-9
		ID.SC-2: Suppliers and third party partners of information systems, components, and services are identified, prioritized, and assessed using a cyber supply	· **COBIT 5** APO10.01, APO10.02, APO10.04, APO10.05, APO12.01, APO12.02, APO12.03, APO12.04, APO12.05, APO12.06, APO13.02, BAI02.03 · **ISA 62443-2-1:2009** 4.2.3.1, 4.2.3.2, 4.2.3.3, 4.2.3.4, 4.2.3.6, 4.2.3.8, 4.2.3.9, 4.2.3.10, 4.2.3.12, 4.2.3.13, 4.2.3.14 · **ISO/IEC 27001:2013** A.15.2.1, A.15.2.2

		chain risk assessment process	· **NIST SP 800-53 Rev. 4** RA-2, RA-3, SA-12, SA-14, SA-15, PM-9
		ID.SC-3: Contracts with suppliers and third-party partners are used to implement appropriate measures designed to meet the objectives of an organization's cybersecurity program and Cyber Supply Chain Risk Management Plan.	· **COBIT 5** APO10.01, APO10.02, APO10.03, APO10.04, APO10.05 · **ISA 62443-2-1:2009** 4.3.2.6.4, 4.3.2.6.7 · **ISO/IEC 27001:2013** A.15.1.1, A.15.1.2, A.15.1.3 · **NIST SP 800-53 Rev. 4** SA-9, SA-11, SA-12, PM-9
		ID.SC-4: Suppliers and third-party partners are routinely assessed using audits, test results, or other forms of evaluations to confirm they are meeting their contractual obligations.	· **COBIT 5** APO10.01, APO10.03, APO10.04, APO10.05, MEA01.01, MEA01.02, MEA01.03, MEA01.04, MEA01.05 · **ISA 62443-2-1:2009** 4.3.2.6.7 · **ISA 62443-3-3:2013** SR 6.1 · **ISO/IEC 27001:2013** A.15.2.1, A.15.2.2 · **NIST SP 800-53 Rev. 4** AU-2, AU-6, AU-12, AU-16, PS-7, SA-9, SA-12
		ID.SC-5: Response and recovery planning and testing are conducted with suppliers and third-party providers	· **CIS CSC** 19, 20 · **COBIT 5** DSS04.04 · **ISA 62443-2-1:2009** 4.3.2.5.7, 4.3.4.5.11 · **ISA 62443-3-3:2013** SR 2.8, SR 3.3, SR.6.1, SR 7.3, SR 7.4 · **ISO/IEC 27001:2013** A.17.1.3 · **NIST SP 800-53 Rev. 4** CP-2, CP-4, IR-3, IR-4, IR-6, IR-8, IR-9
PROTECT (PR)	**Identity Management, Authentication and Access Control (PR.AC):** Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.	**PR.AC-1:** Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes	· **CIS CSC** 1, 5, 15, 16 · **COBIT 5** DSS05.04, DSS06.03 · **ISA 62443-2-1:2009** 4.3.3.5.1 · **ISA 62443-3-3:2013** SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.7, SR 1.8, SR 1.9 · **ISO/IEC 27001:2013** A.9.2.1, A.9.2.2, A.9.2.3, A.9.2.4, A.9.2.6, A.9.3.1, A.9.4.2, A.9.4.3 · **NIST SP 800-53 Rev. 4** AC-1, AC-2, IA-1, IA-2, IA-3, IA-4, IA-5, IA-6, IA-7, IA-8, IA-9, IA-10, IA-11
		PR.AC-2: Physical access to assets is managed and protected	· **COBIT 5** DSS01.04, DSS05.05 · **ISA 62443-2-1:2009** 4.3.3.3.2, 4.3.3.3.8 · **ISO/IEC 27001:2013** A.11.1.1, A.11.1.2, A.11.1.3, A.11.1.4, A.11.1.5, A.11.1.6, A.11.2.1, A.11.2.3, A.11.2.5, A.11.2.6, A.11.2.7, A.11.2.8

			· **NIST SP 800-53 Rev. 4** PE-2, PE-3, PE-4, PE-5, PE-6, PE-8
		PR.AC-3: Remote access is managed	· **CIS CSC** 12
			· **COBIT 5** APO13.01, DSS01.04, DSS05.03
			· **ISA 62443-2-1:2009** 4.3.3.6.6
			· **ISA 62443-3-3:2013** SR 1.13, SR 2.6
			· **ISO/IEC 27001:2013** A.6.2.1, A.6.2.2, A.11.2.6, A.13.1.1, A.13.2.1
			· **NIST SP 800-53 Rev. 4** AC-1, AC-17, AC-19, AC-20, SC-15
		PR.AC-4: Access permissions and authorizations are managed, incorporating the principles of least privilege and separation of duties	· **CIS CSC** 3, 5, 12, 14, 15, 16, 18
			· **COBIT 5** DSS05.04
			· **ISA 62443-2-1:2009** 4.3.3.7.3
			· **ISA 62443-3-3:2013** SR 2.1
			· **ISO/IEC 27001:2013** A.6.1.2, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4, A.9.4.5
			· **NIST SP 800-53 Rev. 4** AC-1, AC-2, AC-3, AC-5, AC-6, AC-14, AC-16, AC-24
		PR.AC-5: Network integrity is protected (e.g., network segregation, network segmentation)	· **CIS CSC** 9, 14, 15, 18
			· **COBIT 5** DSS01.05, DSS05.02
			· **ISA 62443-2-1:2009** 4.3.3.4
			· **ISA 62443-3-3:2013** SR 3.1, SR 3.8
			· **ISO/IEC 27001:2013** A.13.1.1, A.13.1.3, A.13.2.1, A.14.1.2, A.14.1.3
			· **NIST SP 800-53 Rev. 4** AC-4, AC-10, SC-7
		PR.AC-6: Identities are proofed and bound to credentials and asserted in interactions	· **CIS CSC**, 16
			· **COBIT 5** DSS05.04, DSS05.05, DSS05.07, DSS06.03
			· **ISA 62443-2-1:2009** 4.3.3.2.2, 4.3.3.5.2, 4.3.3.7.2, 4.3.3.7.4
			· **ISA 62443-3-3:2013** SR 1.1, SR 1.2, SR 1.4, SR 1.5, SR 1.9, SR 2.1
			· **ISO/IEC 27001:2013**, A.7.1.1, A.9.2.1
			· **NIST SP 800-53 Rev. 4** AC-1, AC-2, AC-3, AC-16, AC-19, AC-24, IA-1, IA-2, IA-4, IA-5, IA-8, PE-2, PS-3
		PR.AC-7: Users, devices, and other assets are authenticated (e.g., single-factor, multi-factor) commensurate with the risk of the	· **CIS CSC** 1, 12, 15, 16
			· **COBIT 5** DSS05.04, DSS05.10, DSS06.10
			· **ISA 62443-2-1:2009** 4.3.3.6.1, 4.3.3.6.2, 4.3.3.6.3, 4.3.3.6.4, 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.3.3.6.8, 4.3.3.6.9

		transaction (e.g., individuals' security and privacy risks and other organizational risks)	· **ISA 62443-3-3:2013** SR 1.1, SR 1.2, SR 1.5, SR 1.7, SR 1.8, SR 1.9, SR 1.10
			· **ISO/IEC 27001:2013** A.9.2.1, A.9.2.4, A.9.3.1, A.9.4.2, A.9.4.3, A.18.1.4
			· **NIST SP 800-53 Rev. 4** AC-7, AC-8, AC-9, AC-11, AC-12, AC-14, IA-1, IA-2, IA-3, IA-4, IA-5, IA-8, IA-9, IA-10, IA-11
	Awareness and Training (PR.AT): The organization's personnel and partners are provided cybersecurity awareness education and are trained to perform their cybersecurity-related duties and responsibilities consistent with related policies, procedures, and agreements.	**PR.AT-1:** All users are informed and trained	· **CIS CSC** 17, 18
			· **COBIT 5** APO07.03, BAI05.07
			· **ISA 62443-2-1:2009** 4.3.2.4.2
			· **ISO/IEC 27001:2013** A.7.2.2, A.12.2.1
			· **NIST SP 800-53 Rev. 4** AT-2, PM-13
		PR.AT-2: Privileged users understand their roles and responsibilities	· **CIS CSC** 5, 17, 18
			· **COBIT 5** APO07.02, DSS05.04, DSS06.03
			· **ISA 62443-2-1:2009** 4.3.2.4.2, 4.3.2.4.3
			· **ISO/IEC 27001:2013** A.6.1.1, A.7.2.2
			· **NIST SP 800-53 Rev. 4** AT-3, PM-13
		PR.AT-3: Third-party stakeholders (e.g., suppliers, customers, partners) understand their roles and responsibilities	· **CIS CSC** 17
			· **COBIT 5** APO07.03, APO07.06, APO10.04, APO10.05
			· **ISA 62443-2-1:2009** 4.3.2.4.2
			· **ISO/IEC 27001:2013** A.6.1.1, A.7.2.1, A.7.2.2
			· **NIST SP 800-53 Rev. 4** PS-7, SA-9, SA-16
		PR.AT-4: Senior executives understand their roles and responsibilities	· **CIS CSC** 17, 19
			· **COBIT 5** EDM01.01, APO01.02, APO07.03
			· **ISA 62443-2-1:2009** 4.3.2.4.2
			· **ISO/IEC 27001:2013** A.6.1.1, A.7.2.2
			· **NIST SP 800-53 Rev. 4** AT-3, PM-13
		PR.AT-5: Physical and cybersecurity personnel understand their roles and responsibilities	· **CIS CSC** 17
			· **COBIT 5** APO07.03
			· **ISA 62443-2-1:2009** 4.3.2.4.2
			· **ISO/IEC 27001:2013** A.6.1.1, A.7.2.2
			· **NIST SP 800-53 Rev. 4** AT-3, IR-2, PM-13
	Data Security (PR.DS): Information and records (data) are managed consistent with the organization's risk	**PR.DS-1:** Data-at-rest is protected	· **CIS CSC** 13, 14
			· **COBIT 5** APO01.06, BAI02.01, BAI06.01, DSS04.07, DSS05.03, DSS06.06
			· **ISA 62443-3-3:2013** SR 3.4, SR 4.1

	strategy to protect the confidentiality, integrity, and availability of information.		· **ISO/IEC 27001:2013** A.8.2.3
			· **NIST SP 800-53 Rev. 4** MP-8, SC-12, SC-28
		PR.DS-2: Data-in-transit is protected	· **CIS CSC** 13, 14
			· **COBIT 5** APO01.06, DSS05.02, DSS06.06
			· **ISA 62443-3-3:2013** SR 3.1, SR 3.8, SR 4.1, SR 4.2
			· **ISO/IEC 27001:2013** A.8.2.3, A.13.1.1, A.13.2.1, A.13.2.3, A.14.1.2, A.14.1.3
			· **NIST SP 800-53 Rev. 4** SC-8, SC-11, SC-12
		PR.DS-3: Assets are formally managed throughout removal, transfers, and disposition	· **CIS CSC** 1
			· **COBIT 5** BAI09.03
			· **ISA 62443-2-1:2009** 4.3.3.3.9, 4.3.4.4.1
			· **ISA 62443-3-3:2013** SR 4.2
			· **ISO/IEC 27001:2013** A.8.2.3, A.8.3.1, A.8.3.2, A.8.3.3, A.11.2.5, A.11.2.7
			· **NIST SP 800-53 Rev. 4** CM-8, MP-6, PE-16
		PR.DS-4: Adequate capacity to ensure availability is maintained	· **CIS CSC** 1, 2, 13
			· **COBIT 5** APO13.01, BAI04.04
			· **ISA 62443-3-3:2013** SR 7.1, SR 7.2
			· **ISO/IEC 27001:2013** A.12.1.3, A.17.2.1
			· **NIST SP 800-53 Rev. 4** AU-4, CP-2, SC-5
		PR.DS-5: Protections against data leaks are implemented	· **CIS CSC** 13
			· **COBIT 5** APO01.06, DSS05.04, DSS05.07, DSS06.02
			· **ISA 62443-3-3:2013** SR 5.2
			· **ISO/IEC 27001:2013** A.6.1.2, A.7.1.1, A.7.1.2, A.7.3.1, A.8.2.2, A.8.2.3, A.9.1.1, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4, A.9.4.5, A.10.1.1, A.11.1.4, A.11.1.5, A.11.2.1, A.13.1.1, A.13.1.3, A.13.2.1, A.13.2.3, A.13.2.4, A.14.1.2, A.14.1.3
			· **NIST SP 800-53 Rev. 4** AC-4, AC-5, AC-6, PE-19, PS-3, PS-6, SC-7, SC-8, SC-13, SC-31, SI-4
		PR.DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity	· **CIS CSC** 2, 3
			· **COBIT 5** APO01.06, BAI06.01, DSS06.02
			· **ISA 62443-3-3:2013** SR 3.1, SR 3.3, SR 3.4, SR 3.8
			· **ISO/IEC 27001:2013** A.12.2.1, A.12.5.1, A.14.1.2, A.14.1.3, A.14.2.4
			· **NIST SP 800-53 Rev. 4** SC-16, SI-7
		PR.DS-7: The development and testing	· **CIS CSC** 18, 20
			· **COBIT 5** BAI03.08, BAI07.04

		environment(s) are separate from the production environment	· **ISO/IEC 27001:2013** A.12.1.4
			· **NIST SP 800-53 Rev. 4** CM-2
		PR.DS-8: Integrity checking mechanisms are used to verify hardware integrity	· **COBIT 5** BAI03.05
			· **ISA 62443-2-1:2009** 4.3.4.4.4
			· **ISO/IEC 27001:2013** A.11.2.4
			· **NIST SP 800-53 Rev. 4** SA-10, SI-7
	Information Protection Processes and Procedures (PR.IP): Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.	**PR.IP-1:** A baseline configuration of information technology/industrial control systems is created and maintained incorporating security principles (e.g. concept of least functionality)	· **CIS CSC** 3, 9, 11
			· **COBIT 5** BAI10.01, BAI10.02, BAI10.03, BAI10.05
			· **ISA 62443-2-1:2009** 4.3.4.3.2, 4.3.4.3.3
			· **ISA 62443-3-3:2013** SR 7.6
			· **ISO/IEC 27001:2013** A.12.1.2, A.12.5.1, A.12.6.2, A.14.2.2, A.14.2.3, A.14.2.4
			· **NIST SP 800-53 Rev. 4** CM-2, CM-3, CM-4, CM-5, CM-6, CM-7, CM-9, SA-10
		PR.IP-2: A System Development Life Cycle to manage systems is implemented	· **CIS CSC** 18
			· **COBIT 5** APO13.01, BAI03.01, BAI03.02, BAI03.03
			· **ISA 62443-2-1:2009** 4.3.4.3.3
			· **ISO/IEC 27001:2013** A.6.1.5, A.14.1.1, A.14.2.1, A.14.2.5
			· **NIST SP 800-53 Rev. 4** PL-8, SA-3, SA-4, SA-8, SA-10, SA-11, SA-12, SA-15, SA-17, SI-12, SI-13, SI-14, SI-16, SI-17
		PR.IP-3: Configuration change control processes are in place	· **CIS CSC** 3, 11
			· **COBIT 5** BAI01.06, BAI06.01
			· **ISA 62443-2-1:2009** 4.3.4.3.2, 4.3.4.3.3
			· **ISA 62443-3-3:2013** SR 7.6
			· **ISO/IEC 27001:2013** A.12.1.2, A.12.5.1, A.12.6.2, A.14.2.2, A.14.2.3, A.14.2.4
			· **NIST SP 800-53 Rev. 4** CM-3, CM-4, SA-10
		PR.IP-4: Backups of information are conducted, maintained, and tested	· **CIS CSC** 10
			· **COBIT 5** APO13.01, DSS01.01, DSS04.07
			· **ISA 62443-2-1:2009** 4.3.4.3.9
			· **ISA 62443-3-3:2013** SR 7.3, SR 7.4
			· **ISO/IEC 27001:2013** A.12.3.1, A.17.1.2, A.17.1.3, A.18.1.3
			· **NIST SP 800-53 Rev. 4** CP-4, CP-6, CP-9
			· **COBIT 5** DSS01.04, DSS05.05

		PR.IP-5: Policy and regulations regarding the physical operating environment for organizational assets are met	· **ISA 62443-2-1:2009** 4.3.3.3.1 4.3.3.3.2, 4.3.3.3.3, 4.3.3.3.5, 4.3.3.3.6
			· **ISO/IEC 27001:2013** A.11.1.4, A.11.2.1, A.11.2.2, A.11.2.3
			· **NIST SP 800-53 Rev. 4** PE-10, PE-12, PE-13, PE-14, PE-15, PE-18
		PR.IP-6: Data is destroyed according to policy	· **COBIT 5** BAI09.03, DSS05.06
			· **ISA 62443-2-1:2009** 4.3.4.4.4
			· **ISA 62443-3-3:2013** SR 4.2
			· **ISO/IEC 27001:2013** A.8.2.3, A.8.3.1, A.8.3.2, A.11.2.7
			· **NIST SP 800-53 Rev. 4** MP-6
		PR.IP-7: Protection processes are improved	· **COBIT 5** APO11.06, APO12.06, DSS04.05
			· **ISA 62443-2-1:2009** 4.4.3.1, 4.4.3.2, 4.4.3.3, 4.4.3.4, 4.4.3.5, 4.4.3.6, 4.4.3.7, 4.4.3.8
			· **ISO/IEC 27001:2013** A.16.1.6, Clause 9, Clause 10
			· **NIST SP 800-53 Rev. 4** CA-2, CA-7, CP-2, IR-8, PL-2, PM-6
		PR.IP-8: Effectiveness of protection technologies is shared	· **COBIT 5** BAI08.04, DSS03.04
			· **ISO/IEC 27001:2013** A.16.1.6
			· **NIST SP 800-53 Rev. 4** AC-21, CA-7, SI-4
		PR.IP-9: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed	· **CIS CSC** 19
			· **COBIT 5** APO12.06, DSS04.03
			· **ISA 62443-2-1:2009** 4.3.2.5.3, 4.3.4.5.1
			· **ISO/IEC 27001:2013** A.16.1.1, A.17.1.1, A.17.1.2, A.17.1.3
			· **NIST SP 800-53 Rev. 4** CP-2, CP-7, CP-12, CP-13, IR-7, IR-8, IR-9, PE-17
		PR.IP-10: Response and recovery plans are tested	· **CIS CSC** 19, 20
			· **COBIT 5** DSS04.04
			· **ISA 62443-2-1:2009** 4.3.2.5.7, 4.3.4.5.11
			· **ISA 62443-3-3:2013** SR 3.3
			· **ISO/IEC 27001:2013** A.17.1.3
			· **NIST SP 800-53 Rev. 4** CP-4, IR-3, PM-14
		PR.IP-11: Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening)	· **CIS CSC** 5, 16
			· **COBIT 5** APO07.01, APO07.02, APO07.03, APO07.04, APO07.05
			· **ISA 62443-2-1:2009** 4.3.3.2.1, 4.3.3.2.2, 4.3.3.2.3

			· **ISO/IEC 27001:2013** A.7.1.1, A.7.1.2, A.7.2.1, A.7.2.2, A.7.2.3, A.7.3.1, A.8.1.4
			· **NIST SP 800-53 Rev. 4** PS-1, PS-2, PS-3, PS-4, PS-5, PS-6, PS-7, PS-8, SA-21
		PR.IP-12: A vulnerability management plan is developed and implemented	· **CIS CSC** 4, 18, 20
			· **COBIT 5** BAI03.10, DSS05.01, DSS05.02
			· **ISO/IEC 27001:2013** A.12.6.1, A.14.2.3, A.16.1.3, A.18.2.2, A.18.2.3
			· **NIST SP 800-53 Rev. 4** RA-3, RA-5, SI-2
	Maintenance (PR.MA): Maintenance and repairs of industrial control and information system components are performed consistent with policies and procedures.	**PR.MA-1:** Maintenance and repair of organizational assets are performed and logged, with approved and controlled tools	· **COBIT 5** BAI03.10, BAI09.02, BAI09.03, DSS01.05
			· **ISA 62443-2-1:2009** 4.3.3.3.7
			· **ISO/IEC 27001:2013** A.11.1.2, A.11.2.4, A.11.2.5, A.11.2.6
			· **NIST SP 800-53 Rev. 4** MA-2, MA-3, MA-5, MA-6
		PR.MA-2: Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access	· **CIS CSC** 3, 5
			· **COBIT 5** DSS05.04
			· **ISA 62443-2-1:2009** 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.3.3.6.8
			· **ISO/IEC 27001:2013** A.11.2.4, A.15.1.1, A.15.2.1
			· **NIST SP 800-53 Rev. 4** MA-4
	Protective Technology (PR.PT): Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.	**PR.PT-1:** Audit/log records are determined, documented, implemented, and reviewed in accordance with policy	· **CIS CSC** 1, 3, 5, 6, 14, 15, 16
			· **COBIT 5** APO11.04, BAI03.05, DSS05.04, DSS05.07, MEA02.01
			· **ISA 62443-2-1:2009** 4.3.3.3.9, 4.3.3.5.8, 4.3.4.4.7, 4.4.2.1, 4.4.2.2, 4.4.2.4
			· **ISA 62443-3-3:2013** SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12
			· **ISO/IEC 27001:2013** A.12.4.1, A.12.4.2, A.12.4.3, A.12.4.4, A.12.7.1
			· **NIST SP 800-53 Rev. 4** AU Family
		PR.PT-2: Removable media is protected and its use restricted according to policy	· **CIS CSC** 8, 13
			· **COBIT 5** APO13.01, DSS05.02, DSS05.06
			· **ISA 62443-3-3:2013** SR 2.3
			· **ISO/IEC 27001:2013** A.8.2.1, A.8.2.2, A.8.2.3, A.8.3.1, A.8.3.3, A.11.2.9
			· **NIST SP 800-53 Rev. 4** MP-2, MP-3, MP-4, MP-5, MP-7, MP-8
		PR.PT-3: The principle of least functionality is	· **CIS CSC** 3, 11, 14
			· **COBIT 5** DSS05.02, DSS05.05, DSS06.06

		incorporated by configuring systems to provide only essential capabilities	· **ISA 62443-2-1:2009** 4.3.3.5.1, 4.3.3.5.2, 4.3.3.5.3, 4.3.3.5.4, 4.3.3.5.5, 4.3.3.5.6, 4.3.3.5.7, 4.3.3.5.8, 4.3.3.6.1, 4.3.3.6.2, 4.3.3.6.3, 4.3.3.6.4, 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.3.3.6.8, 4.3.3.6.9, 4.3.3.7.1, 4.3.3.7.2, 4.3.3.7.3, 4.3.3.7.4
			· **ISA 62443-3-3:2013** SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.6, SR 1.7, SR 1.8, SR 1.9, SR 1.10, SR 1.11, SR 1.12, SR 1.13, SR 2.1, SR 2.2, SR 2.3, SR 2.4, SR 2.5, SR 2.6, SR 2.7
			· **ISO/IEC 27001:2013** A.9.1.2
			· **NIST SP 800-53 Rev. 4** AC-3, CM-7
		PR.PT-4: Communications and control networks are protected	· **CIS CSC** 8, 12, 15
			· **COBIT 5** DSS05.02, APO13.01
			· **ISA 62443-3-3:2013** SR 3.1, SR 3.5, SR 3.8, SR 4.1, SR 4.3, SR 5.1, SR 5.2, SR 5.3, SR 7.1, SR 7.6
			· **ISO/IEC 27001:2013** A.13.1.1, A.13.2.1, A.14.1.3
			· **NIST SP 800-53 Rev. 4** AC-4, AC-17, AC-18, CP-8, SC-7, SC-19, SC-20, SC-21, SC-22, SC-23, SC-24, SC-25, SC-29, SC-32, SC-36, SC-37, SC-38, SC-39, SC-40, SC-41, SC-43
		PR.PT-5: Mechanisms (e.g., failsafe, load balancing, hot swap) are implemented to achieve resilience requirements in normal and adverse situations	· **COBIT 5** BAI04.01, BAI04.02, BAI04.03, BAI04.04, BAI04.05, DSS01.05
			· **ISA 62443-2-1:2009** 4.3.2.5.2
			· **ISA 62443-3-3:2013** SR 7.1, SR 7.2
			· **ISO/IEC 27001:2013** A.17.1.2, A.17.2.1
			· **NIST SP 800-53 Rev. 4** CP-7, CP-8, CP-11, CP-13, PL-8, SA-14, SC-6
DETECT (DE)	**Anomalies and Events (DE.AE):** Anomalous activity is detected and the potential impact of events is understood.	**DE.AE-1:** A baseline of network operations and expected data flows for users and systems is established and managed	· **CIS CSC** 1, 4, 6, 12, 13, 15, 16
			· **COBIT 5** DSS03.01
			· **ISA 62443-2-1:2009** 4.4.3.3
			· **ISO/IEC 27001:2013** A.12.1.1, A.12.1.2, A.13.1.1, A.13.1.2
			· **NIST SP 800-53 Rev. 4** AC-4, CA-3, CM-2, SI-4
		DE.AE-2: Detected events are analyzed to understand attack targets and methods	· **CIS CSC** 3, 6, 13, 15
			· **COBIT 5** DSS05.07
			· **ISA 62443-2-1:2009** 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8
			· **ISA 62443-3-3:2013** SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12, SR 3.9, SR 6.1, SR 6.2
			· **ISO/IEC 27001:2013** A.12.4.1, A.16.1.1, A.16.1.4
			· **NIST SP 800-53 Rev. 4** AU-6, CA-7, IR-4, SI-4
			· **CIS CSC** 1, 3, 4, 5, 6, 7, 8, 11, 12, 13, 14, 15, 16

		DE.AE-3: Event data are collected and correlated from multiple sources and sensors	· **COBIT 5** BAI08.02
			· **ISA 62443-3-3:2013** SR 6.1
			· **ISO/IEC 27001:2013** A.12.4.1, A.16.1.7
			· **NIST SP 800-53 Rev. 4** AU-6, CA-7, IR-4, IR-5, IR-8, SI-4
		DE.AE-4: Impact of events is determined	· **CIS CSC** 4, 6
			· **COBIT 5** APO12.06, DSS03.01
			· **ISO/IEC 27001:2013** A.16.1.4
			· **NIST SP 800-53 Rev. 4** CP-2, IR-4, RA-3, SI-4
		DE.AE-5: Incident alert thresholds are established	· **CIS CSC** 6, 19
			· **COBIT 5** APO12.06, DSS03.01
			· **ISA 62443-2-1:2009** 4.2.3.10
			· **ISO/IEC 27001:2013** A.16.1.4
			· **NIST SP 800-53 Rev. 4** IR-4, IR-5, IR-8
	Security Continuous Monitoring (DE.CM): The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.	**DE.CM-1:** The network is monitored to detect potential cybersecurity events	· **CIS CSC** 1, 7, 8, 12, 13, 15, 16
			· **COBIT 5** DSS01.03, DSS03.05, DSS05.07
			· **ISA 62443-3-3:2013** SR 6.2
			· **NIST SP 800-53 Rev. 4** AC-2, AU-12, CA-7, CM-3, SC-5, SC-7, SI-4
		DE.CM-2: The physical environment is monitored to detect potential cybersecurity events	· **COBIT 5** DSS01.04, DSS01.05
			· **ISA 62443-2-1:2009** 4.3.3.3.8
			· **ISO/IEC 27001:2013** A.11.1.1, A.11.1.2
			· **NIST SP 800-53 Rev. 4** CA-7, PE-3, PE-6, PE-20
		DE.CM-3: Personnel activity is monitored to detect potential cybersecurity events	· **CIS CSC** 5, 7, 14, 16
			· **COBIT 5** DSS05.07
			· **ISA 62443-3-3:2013** SR 6.2
			· **ISO/IEC 27001:2013** A.12.4.1, A.12.4.3
			· **NIST SP 800-53 Rev. 4** AC-2, AU-12, AU-13, CA-7, CM-10, CM-11
		DE.CM-4: Malicious code is detected	· **CIS CSC** 4, 7, 8, 12
			· **COBIT 5** DSS05.01
			· **ISA 62443-2-1:2009** 4.3.4.3.8
			· **ISA 62443-3-3:2013** SR 3.2
			· **ISO/IEC 27001:2013** A.12.2.1
			· **NIST SP 800-53 Rev. 4** SI-3, SI-8
			· **CIS CSC** 7, 8

		DE.CM-5: Unauthorized mobile code is detected	· **COBIT 5** DSS05.01
			· **ISA 62443-3-3:2013** SR 2.4
			· **ISO/IEC 27001:2013** A.12.5.1, A.12.6.2
			· **NIST SP 800-53 Rev. 4** SC-18, SI-4, SC-44
		DE.CM-6: External service provider activity is monitored to detect potential cybersecurity events	· **COBIT 5** APO07.06, APO10.05
			· **ISO/IEC 27001:2013** A.14.2.7, A.15.2.1
			· **NIST SP 800-53 Rev. 4** CA-7, PS-7, SA-4, SA-9, SI-4
		DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed	· **CIS CSC** 1, 2, 3, 5, 9, 12, 13, 15, 16
			· **COBIT 5** DSS05.02, DSS05.05
			· **ISO/IEC 27001:2013** A.12.4.1, A.14.2.7, A.15.2.1
			· **NIST SP 800-53 Rev. 4** AU-12, CA-7, CM-3, CM-8, PE-3, PE-6, PE-20, SI-4
		DE.CM-8: Vulnerability scans are performed	· **CIS CSC** 4, 20
			· **COBIT 5** BAI03.10, DSS05.01
			· **ISA 62443-2-1:2009** 4.2.3.1, 4.2.3.7
			· **ISO/IEC 27001:2013** A.12.6.1
			· **NIST SP 800-53 Rev. 4** RA-5
	Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure awareness of anomalous events.	**DE.DP-1:** Roles and responsibilities for detection are well defined to ensure accountability	· **CIS CSC** 19
			· **COBIT 5** APO01.02**,** DSS05.01, DSS06.03
			· **ISA 62443-2-1:2009** 4.4.3.1
			· **ISO/IEC 27001:2013** A.6.1.1, A.7.2.2
			· **NIST SP 800-53 Rev. 4** CA-2, CA-7, PM-14
		DE.DP-2: Detection activities comply with all applicable requirements	· **COBIT 5** DSS06.01, MEA03.03, MEA03.04
			· **ISA 62443-2-1:2009** 4.4.3.2
			· **ISO/IEC 27001:2013** A.18.1.4, A.18.2.2, A.18.2.3
			· **NIST SP 800-53 Rev. 4** AC-25, CA-2, CA-7, SA-18, SI-4, PM-14
		DE.DP-3: Detection processes are tested	· **COBIT 5** APO13.02, DSS05.02
			· **ISA 62443-2-1:2009** 4.4.3.2
			· **ISA 62443-3-3:2013** SR 3.3
			· **ISO/IEC 27001:2013** A.14.2.8
			· **NIST SP 800-53 Rev. 4** CA-2, CA-7, PE-3, SI-3, SI-4, PM-14
		DE.DP-4: Event detection information is communicated	· **CIS CSC** 19
			· **COBIT 5** APO08.04, APO12.06, DSS02.05
			· **ISA 62443-2-1:2009** 4.3.4.5.9

			· **ISA 62443-3-3:2013** SR 6.1
			· **ISO/IEC 27001:2013** A.16.1.2, A.16.1.3
			· **NIST SP 800-53 Rev. 4** AU-6, CA-2, CA-7, RA-5, SI-4
		DE.DP-5: Detection processes are continuously improved	· **COBIT 5** APO11.06, APO12.06, DSS04.05
			· **ISA 62443-2-1:2009** 4.4.3.4
			· **ISO/IEC 27001:2013** A.16.1.6
			· **NIST SP 800-53 Rev. 4**, CA-2, CA-7, PL-2, RA-5, SI-4, PM-14
RESPOND (RS)	**Response Planning (RS.RP):** Response processes and procedures are executed and maintained, to ensure response to detected cybersecurity incidents.	**RS.RP-1:** Response plan is executed during or after an incident	· **CIS CSC** 19
			· **COBIT 5** APO12.06, BAI01.10
			· **ISA 62443-2-1:2009** 4.3.4.5.1
			· **ISO/IEC 27001:2013** A.16.1.5
			· **NIST SP 800-53 Rev. 4** CP-2, CP-10, IR-4, IR-8
	Communications (RS.CO): Response activities are coordinated with internal and external stakeholders (e.g. external support from law enforcement agencies).	**RS.CO-1:** Personnel know their roles and order of operations when a response is needed	· **CIS CSC** 19
			· **COBIT 5** EDM03.02, APO01.02, APO12.03
			· **ISA 62443-2-1:2009** 4.3.4.5.2, 4.3.4.5.3, 4.3.4.5.4
			· **ISO/IEC 27001:2013** A.6.1.1, A.7.2.2, A.16.1.1
			· **NIST SP 800-53 Rev. 4** CP-2, CP-3, IR-3, IR-8
		RS.CO-2: Incidents are reported consistent with established criteria	· **CIS CSC** 19
			· **COBIT 5** DSS01.03
			· **ISA 62443-2-1:2009** 4.3.4.5.5
			· **ISO/IEC 27001:2013** A.6.1.3, A.16.1.2
			· **NIST SP 800-53 Rev. 4** AU-6, IR-6, IR-8
		RS.CO-3: Information is shared consistent with response plans	· **CIS CSC** 19
			· **COBIT 5** DSS03.04
			· **ISA 62443-2-1:2009** 4.3.4.5.2
			· **ISO/IEC 27001:2013** A.16.1.2, Clause 7.4, Clause 16.1.2
			· **NIST SP 800-53 Rev. 4** CA-2, CA-7, CP-2, IR-4, IR-8, PE-6, RA-5, SI-4
		RS.CO-4: Coordination with stakeholders occurs consistent with response plans	· **CIS CSC** 19
			· **COBIT 5** DSS03.04
			· **ISA 62443-2-1:2009** 4.3.4.5.5
			· **ISO/IEC 27001:2013** Clause 7.4
			· **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-8
			· **CIS CSC** 19

		RS.CO-5: Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness	· **COBIT 5** BAI08.04 · **ISO/IEC 27001:2013** A.6.1.4 · **NIST SP 800-53 Rev. 4** SI-5, PM-15
	Analysis (RS.AN): Analysis is conducted to ensure effective response and support recovery activities.	**RS.AN-1:** Notifications from detection systems are investigated	· **CIS CSC** 4, 6, 8, 19 · **COBIT 5** DSS02.04, DSS02.07 · **ISA 62443-2-1:2009** 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8 · **ISA 62443-3-3:2013** SR 6.1 · **ISO/IEC 27001:2013** A.12.4.1, A.12.4.3, A.16.1.5 · **NIST SP 800-53 Rev. 4** AU-6, CA-7, IR-4, IR-5, PE-6, SI-4
		RS.AN-2: The impact of the incident is understood	· **COBIT 5** DSS02.02 · **ISA 62443-2-1:2009** 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8 · **ISO/IEC 27001:2013** A.16.1.4, A.16.1.6 · **NIST SP 800-53 Rev. 4** CP-2, IR-4
		RS.AN-3: Forensics are performed	· **COBIT 5** APO12.06, DSS03.02, DSS05.07 · **ISA 62443-3-3:2013** SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12, SR 3.9, SR 6.1 · **ISO/IEC 27001:2013** A.16.1.7 · **NIST SP 800-53 Rev. 4** AU-7, IR-4
		RS.AN-4: Incidents are categorized consistent with response plans	· **CIS CSC** 19 · **COBIT 5** DSS02.02 · **ISA 62443-2-1:2009** 4.3.4.5.6 · **ISO/IEC 27001:2013** A.16.1.4 · **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-5, IR-8
		RS.AN-5: Processes are established to receive, analyze and respond to vulnerabilities disclosed to the organization from internal and external sources (e.g. internal testing, security bulletins, or security researchers)	· **CIS CSC** 4, 19 · **COBIT 5** EDM03.02, DSS05.07 · **NIST SP 800-53 Rev. 4** SI-5, PM-15
	Mitigation (RS.MI): Activities are performed to prevent expansion of an event, mitigate its	**RS.MI-1:** Incidents are contained	· **CIS CSC** 19 · **COBIT 5** APO12.06 · **ISA 62443-2-1:2009** 4.3.4.5.6 · **ISA 62443-3-3:2013** SR 5.1, SR 5.2, SR 5.4

	effects, and resolve the incident.		· **ISO/IEC 27001:2013** A.12.2.1, A.16.1.5 · **NIST SP 800-53 Rev. 4** IR-4
		RS.MI-2: Incidents are mitigated	· **CIS CSC** 4, 19 · **COBIT 5** APO12.06 · **ISA 62443-2-1:2009** 4.3.4.5.6, 4.3.4.5.10 · **ISO/IEC 27001:2013** A.12.2.1, A.16.1.5 · **NIST SP 800-53 Rev. 4** IR-4
		RS.MI-3: Newly identified vulnerabilities are mitigated or documented as accepted risks	· **CIS CSC** 4 · **COBIT 5** APO12.06 · **ISO/IEC 27001:2013** A.12.6.1 · **NIST SP 800-53 Rev. 4** CA-7, RA-3, RA-5
	Improvements (RS.IM): Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.	**RS.IM-1:** Response plans incorporate lessons learned	· **COBIT 5** BAI01.13 · **ISA 62443-2-1:2009** 4.3.4.5.10, 4.4.3.4 · **ISO/IEC 27001:2013** A.16.1.6, Clause 10 · **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-8
		RS.IM-2: Response strategies are updated	· **COBIT 5** BAI01.13, DSS04.08 · **ISO/IEC 27001:2013** A.16.1.6, Clause 10 · **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-8
RECOVER (RC)	**Recovery Planning (RC.RP):** Recovery processes and procedures are executed and maintained to ensure restoration of systems or assets affected by cybersecurity incidents.	**RC.RP-1:** Recovery plan is executed during or after a cybersecurity incident	· **CIS CSC** 10 · **COBIT 5** APO12.06, DSS02.05, DSS03.04 · **ISO/IEC 27001:2013** A.16.1.5 · **NIST SP 800-53 Rev. 4** CP-10, IR-4, IR-8
	Improvements (RC.IM): Recovery planning and processes are improved by incorporating lessons learned into future activities.	**RC.IM-1:** Recovery plans incorporate lessons learned	· **COBIT 5** APO12.06, BAI05.07, DSS04.08 · **ISA 62443-2-1:2009** 4.4.3.4 · **ISO/IEC 27001:2013** A.16.1.6, Clause 10 · **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-8
		RC.IM-2: Recovery strategies are updated	· **COBIT 5** APO12.06, BAI07.08 · **ISO/IEC 27001:2013** A.16.1.6, Clause 10 · **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-8
	Communications (RC.CO): Restoration activities are coordinated with internal and external parties (e.g.	**RC.CO-1:** Public relations are managed	· **COBIT 5** EDM03.02 · **ISO/IEC 27001:2013** A.6.1.4, Clause 7.4
		RC.CO-2: Reputation is repaired after an incident	· **COBIT 5** MEA03.02 · **ISO/IEC 27001:2013** Clause 7.4

	coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors).	**RC.CO-3:** Recovery activities are communicated to internal and external stakeholders as well as executive and management teams	· **COBIT 5** APO12.06 · **ISO/IEC 27001:2013** Clause 7.4 · **NIST SP 800-53 Rev. 4** CP-2, IR-4

Contact

Smart Freight Centre
Keizersgracht 560, 1017 EM
Amsterdam, Netherlands

P.O. Box 11772, 1001 GT
Amsterdam, Netherlands

Tel. office: +31 6 4695 4405
www.smartfreightcentre.org
info@smartfreightcentre.org

Join our journey towards efficient and zero-emission global freight and logistics

Contact

Smart Freight Centre
Keizersgracht 560, 1017 EM
Amsterdam, Netherlands

P.O. Box 11772, 1001 GT
Amsterdam, Netherlands

Tel. office: +31 6 4695 4405
www.smartfreightcentre.org
info@smartfreightcentre.org