CYLUS


# Typical Buying Process for Rail Security Uplift Projects

A general overview of the steps global rail operators use in purchasing cybersecurity for operational environments

# Table of Contents

# Introduction

This document summarizes the buying or purchase process Cylus has seen prior customers use successfully in efficiently purchasing rail cybersecurity platforms for existing rail security uplift projects. This document does not cover the purchase of rail security platforms as part of a more extensive greenfield rolling stock or infrastructure tender process. This typical buying process breaks down into four straightforward steps, three of which are covered in this document. The final step, the security platform deployment, is not covered here. Below are the high-level steps of the typical buying process for rail security uplift projects:

## Phase 1

Project Identification

## Phase 2

Vendor Review and Partner Identification

## Phase 3

Optional: Tender Process

## Phase 4

Deployment

# Phase 1
## Project Identification

The Project Identification phase of the project can vary considerably, but for most operators that Cylus have observed, this portion of the project typically takes 1-3 months with many of the activities happening internally and in parallel.

In most cases, the rail security uplift project begins with the rail operator identifying an internal cybersecurity need. Cylus sometimes communicates with the rail operator during the project phase, but not always. Typically the early stage of the project involves various activities often conducted internally including:

1. Documenting the project triggers
2. Identifying the initial project team
3. Conducting basic needs research
4. Identifying vendors and creating a shortlist
5. Developing budget parameters
6. Scoping possible project timelines

Below are a few notes on each activity that we have observed that can contribute to a more frictionless and timely project.

### 1.1 Documenting the Project Triggers

In the early stages of the process, it can be important for the project team to understand what triggered or may trigger this project to move forward. Understanding the driving motive and project objectives early helps focus steps later in the process such as documenting proof of value success criteria. And having clear and documented project reasons helps bring on new team members as well. Below are a few rail security uplift project triggers we see regularly.

#### Regulatory Pressure

In many cases, changing regulatory requirements or guidance triggers new cybersecurity investigations. The regulatory environment for the rail industry has been quickly evolving and as such is driving a desire to show ‘progress’ in cybersecurity maturity toward existing and emerging regulations and guidelines.

#### Cybersecurity Risk Assessment

Risk assessments, whether conducted for regulatory reasons or for internal purposes, typically reveal security weaknesses, vulnerabilities, and substantial risks to critical areas such as safety and service availability. The documentation of these risks then triggers projects to investigate methods to address identified vulnerabilities.

### Security Incident

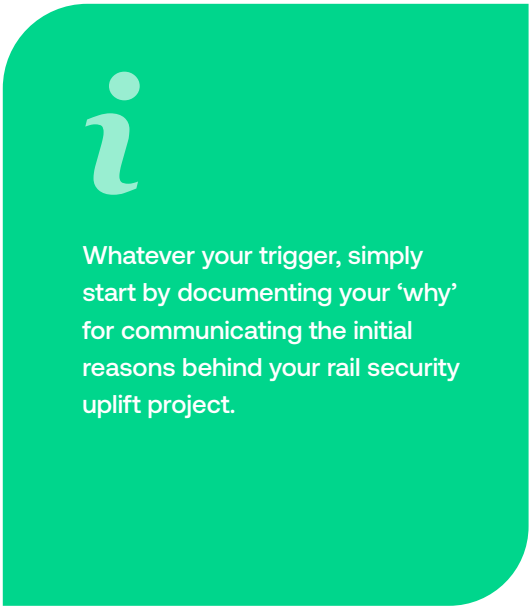
Whether internal or to another rail operator, security incidents can fuel urgency and action. The outcome of any such incident is often a new security project of the nature discussed herein.

### Changes and Upgrades

Non-cyber changes/upgrades into which a cyber upgrade can be incorporated (i.e., signaling upgrades, rolling stock upgrade, etc.) often serve as the ideal time and trigger for operators to kick off projects to add cybersecurity with limited additional disruption.

### Executive Pressure

Executive mandates can also sometimes trigger a new cybersecurity project.




## 1.2 Identifying the Initial Project Team

Rail security uplift projects are almost always owned by the Chief Information Security Officer (CISO) or equivalent role, who assigns members of his/her team to explore options, vendors, and processes for a cybersecurity upgrade. This stage of the project is then led by a member of the IT Security team. Though in some cases, it may be a partner or external organization who conducts this analysis; however, the rail operator is still driving the definition of the project and the need to proceed.

One best practice in this early stage is to get the rail operations team involved sooner rather than later. This eases and makes future stages of the project more efficient.

## 1.3 Conducting Basic Needs Research

At this stage in the process, market research is conducted to determine how the need can be met, how other organizations are addressing the need, and whether best practices guidance exists. This activity typically consists of a combination of online research, speaking to peers, reading relevant whitepapers and case studies, and reviewing technical and industry sites. Items to consider include:

- Who else has this need?
- How are they addressing the need?
- Are there documented case studies or best practices that can help?
- What are the typical benefits and outcomes of addressing the need?

## 1.4 Identifying Vendors and Creating a Shortlist

The next step involves identifying who can provide the security products or services and what options already exist in the marketplace. Online research and peer references usually help produce a short list of vendors to evaluate in the project's next phase. At this stage, items to consider are:

- Who can provide a product or service to address the need?
- Is the solution standard versus custom?
- Do they have strong reference customers?
- Collect useful information from suppliers and questions to address.

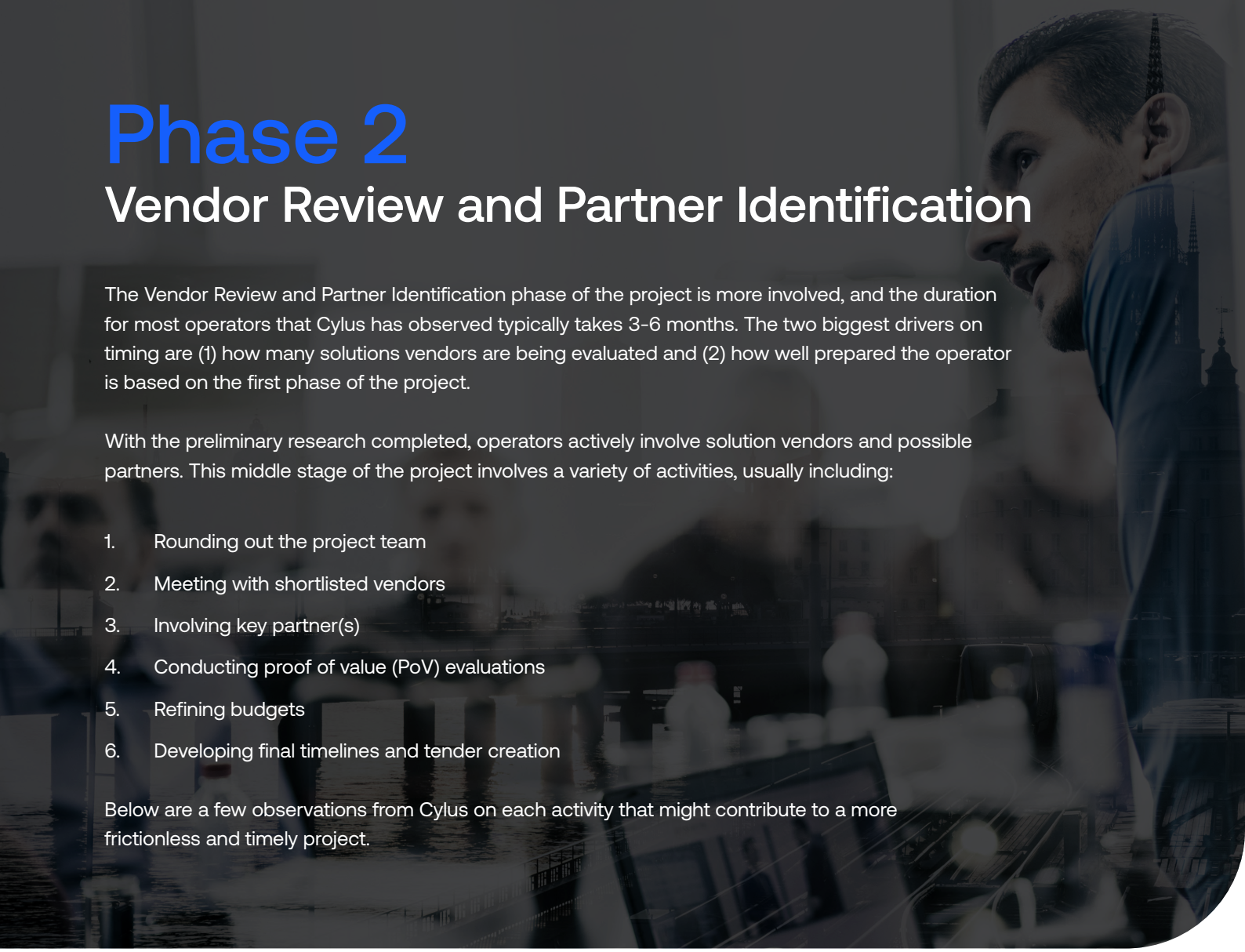
## 1.5 Developing Budget Parameters

At this point in the project, customers typically look to estimate an overall budget for an initial purchase as well as specific constraints and requirements that must be considered. This often involves consulting with key stakeholders and taking into account the expected contract term and/or solution lifespan.

## 1.6 Scoping Possible Project Timelines

Lastly, taking into account the project triggers and objectives at this point, the project team members usually begin to think through initial project scope considerations that might work best for initial deployments. The initial budget parameters are considered, and high-level future project milestones are documented for the remainder of the purchase process.

It is also at this point that most operators have clearly documented both future project expectations and key questions that need to be addressed. This can help to ensure the purchase is completed efficiently and effectively and can help to minimize delays and disruptions.



# Phase 2

# Vendor Review and Partner Identification

The Vendor Review and Partner Identification phase of the project is more involved, and the duration for most operators that Cylus has observed typically takes 3-6 months. The two biggest drivers on timing are (1) how many solutions vendors are being evaluated and (2) how well prepared the operator is based on the first phase of the project.

With the preliminary research completed, operators actively involve solution vendors and possible partners. This middle stage of the project involves a variety of activities, usually including:

1. Rounding out the project team
2. Meeting with shortlisted vendors
3. Involving key partner(s)
4. Conducting proof of value (PoV) evaluations
5. Refining budgets
6. Developing final timelines and tender creation

Below are a few observations from Cylus on each activity that might contribute to a more frictionless and timely project.

## 2.1 Rounding Out the Project Team

By this point, the full operator buying team is involved in the project and usually consists of:

- The CISO or equivalent as the initiator and decision maker.
- The head of operations who jointly works the project with the CISO.
- The IT security team who manages much of the project and leads the solution/vendor discussions and evaluations.
- The operations team members who are jointly involved in vendor discussions and evaluations.
- Key company executives that serve as stakeholders and provide top-down support and funding.
- Key partner(s) that will be involved in vendor evaluations and may serve as technical influencers.
- Other team members we see that get involved in this phase include finance, governance, and/or procurement.

## 2.2 Meeting with Shortlisted Vendors

Rail operators have a variety of approaches to how they conduct this stage of the process. Most often, it starts with an initial sales meeting and product demonstration if this wasn't completed in the prior phase of the project. Generally, we find the following objectives are part of every rail operator's desires during this short evaluation process:

- Product Information: Confirm the accuracy and veracity of the vendor's product information claims - does the product seem to do what they say it does?
- Expertise: Establish the depth of the vendor's rail expertise and experience and how that is reflected in the product tailored for their rail environment.
- Integrations: Understand how the vendor's solution can and will integrate into the operator's security and/or operations technology ecosystem (e.g., SIEM integration, etc.).
- Bridging Security and Operations: Understand exactly how the vendor solution serves the needs of both the IT security team and the involved operations team.
- Deployment Support: Understand the deployment support and training that the vendor provides and the team they have in place to do so.
- References: Identify and speak with relevant reference customers.
- Q&A: Answer all open questions for the early vendor review process.

This is not an exhaustive list but summarizes the key evaluation points that Cylus has seen repeatedly in rail operator's purchase processes.



## 2.3 Involving Key Partner(s)

If they haven't been involved from the early stages of the project research, Cylus has observed that key equipment manufacturers and/or security service providers are usually brought into the rail security uplift project at this point in the process. Other partners like systems integrators and consultants may also be involved.

## 2.4 Conducting Proof of Value (PoV) Evaluations

The proof of value evaluations may involve all shortlisted vendors. The most timely and successful PoVs Cylus have seen include but are not limited to:

- Clear Success Criteria: PoVs start with documenting success criteria, mapping them back to the initial project triggers and objectives, and clearly defining expected outcomes.
- Deployed in Live Rail Environment: While it can be more involved, PoV's conducted in live rail environments, in our experience, give the operator much greater experience with the solution and vendor, allows team members to more accurately demonstrate vendor success or failure, and ultimately reduces the risk of unknowns with the actual deployments later on.
- PoV Preparations: Operators jointly involve key partners in the set-up and execution of the PoV, and vendors are provided with the necessary technical prerequisites and information to efficiently deploy and conduct the proof of the value of their solution.

Given the importance of an efficient PoV, Cylus provides below an outline developed as a result of many PoVs with rail operators.

### PoV Journey

| PoV Agreement | Pre-Planning | Deployment | PoV Results | PoV Conclusion |
|---|---|---|---|---|
| • Establish PoV success criteria<br>• Coordinate with vendor technical and commercial teams | • Plan PoV internal resources<br>• Establish PoV timeframes<br>• Present network topology<br>• Provide an interface to live networks (if a live PoV is to be conducted) | • Ensure vendor solution is functioning as expected with PoV network interfaces | • Examine full functionality of the vendor solution<br>• Evaluate against success criteria<br>• Look for additional unexpected benefits/use cases<br>• Identify potential challenges<br>• Prepare PoV results summary | • Agree on success or failure with vendor<br>• Move to next steps |

## 2.5 Refining Budgets

During the meetings with the shortlisted vendors, rail operators usually ask for early scoping budgets based on the desired scope of the project. These scoping numbers help refine the project's projected scope and the early budget estimates prepared in phase 1 of the research. The information can also help understand pricing models and how to refine project scopes to clearly understand what a full deployment across the entire environment might eventually cost.

## 2.6 Developing Final Timelines and Tender Creation

At this stage, the rail operator has finished evaluating the vendor solutions, and all project team members are in agreement on the next steps. The next steps from our observations usually go in one of two directions. Either the rail operator moves to single source a solution from one vendor based on the performance of solutions in the PoV, or the rail operator moves to a competitive tendering process. Either way, the project team prepares refined and final project timelines and begins commercial preparations for vendor negotiations or tender preparations.

# Phase 3
## Optional: Tender Process

If the rail operator moves to use a single source vendor solution instead of a competitive tendering process, some level of internal justification is typically needed, and this project phase becomes unnecessary.

However, many rail operators being public entities, require a public tender process. The Tender Process phase of the project is often conducted in 1-3 months. It can go longer, but most rail operators we've experienced are driven to shorten this process at this project stage.

The tender process is a formal and structured invitation to suppliers to submit competitive bids to supply the security solution or services in question. These processes are typically well-defined and governed to ensure fair competition among vendor bidders and are thus not covered in detail in this document.

However, at a high level, the tender process steps generally include a call for submissions, the bid submission(s), the selection process, and the formation of the contract. Once these steps are complete, the vendor starts the project and sees it through to completion.

# Phase 4
## Deployment

The purchase process for the rail security uplift project is now complete. While critically important, the security solution deployment entails an entirely different process than the purchase process described above, often with different project team representatives, and is not covered in this document.

# About

Cylus is the global leader in rail cybersecurity. Cylus provides rail operators with a specialized cybersecurity solution to ensure service availability and safety. Combining deep rail and cybersecurity expertise, Cylus pioneered a real-time asset visibility and threat detection platform across heterogeneous rail operating technology environments. With customers across the globe, Cylus leads with a comprehensive cybersecurity solution enabling compliance and reducing risks in the face of escalating cyber threats.

CYLUS