Understanding Supply Chain Interaction in an AVCDL Context

Revision

Version 6
4/22/24 2:20 PM

Author

Charles Wilson

Abstract

This document provides an overview of how a supplier is integrated into an **AVCDL**-based product development lifecycle.

Motivation

This document is motivated by the need to ensure sufficient cybersecurity across the entire supply chain.

Note: This document is not intended as a replacement for the processes and commentary materials it references.

Audience

The audience of this document are those supplier cybersecurity SMEs tasked with interfacing to customers using the **AVCDL** as the basis for their product cybersecurity lifecycle.

Note: This document is not subject to certification body review.

License

Overview

The **AVCDL** [1] is primarily intended for application to an individual organization's product development. It does, however, provide guidance and resources for handling the interaction between the organization (as a customer) and a vendor (as a supplier) within the overall supply chain. This document provides an overview of both the supplier-specific materials and how the supplier is integrated into the overall product cybersecurity lifecycle.

Criticality of Integrated Supply Chain Cybersecurity

The **AVCDL** does not call out supplier-provided elements in every process and document within its corpus. It is presumed that every element of the product be held to the same standards, regardless of source. As such, it is critical that customers ensure that their suppliers are providing elements that meet the customer's cybersecurity requirements. This includes undertaking activities described in the **AVCDL** phase requirements. There is an expectation that the supplier will provide evidence that these activities were conducted according to industry best practices.

Both international standards and regulations have requirements mandating the integration of the supply chain into the cybersecurity aspect of product development. These can be seen in the **AVCDL mappings** [5] **AVCDL** reference document.

Extraordinary Supplier Understanding

Given the nature of cybersecurity attacks it is necessary to take into consideration supply chain aspects that are outside the cybersecurity domain. Both the breadth and depth of the supply chain must be considered when making supplier selection and risk assessment decisions.

Supplier-specific factors needing explicit consideration include (but are not limited to):

- partnerships
- competitors
- nationality
- supply chain

Verifying Supplier Conformance

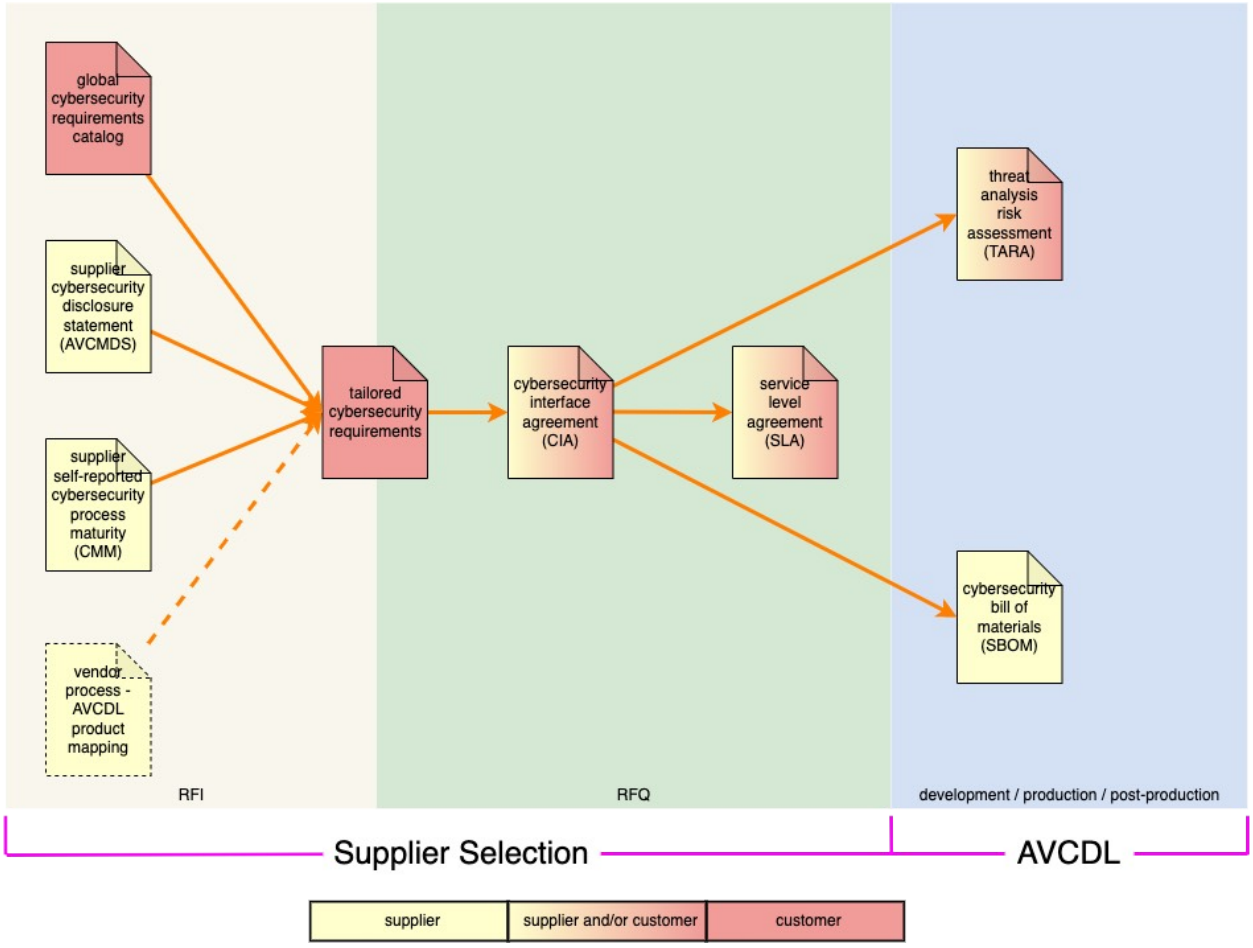
There are many activities enumerated throughout this document, and those referenced by it. Many of them provide information which needs to be kept current. Others are the subject of on-demand review (audit). Typically, descriptions of these are provided throughout the referenced AVCDL documentation. Specific mechanisms for ensuring the accuracy of the information provided by the supplier should be established in the cybersecurity elements of the supplier's service level agreement. It is recognized that service level agreement oversight is an organizational level responsibility.

Additional discussion regarding service level agreements is provided in the elaboration document, **Understanding Service Level Agreements in an AVCDL Context** [29].

Supplier Selection

In cases where the supplier has few or no formal cybersecurity processes, the **AVCDL** may be adopted by the supplier directly. In cases where the supplier has established cybersecurity processes, it is necessary to create a mapping from those to the corresponding **AVCDL** processes and evaluate whether the vendor processes are sufficient or require augmentation in order to achieve compliance.

The following is the overview of the workflow to be applied to make these determinations.

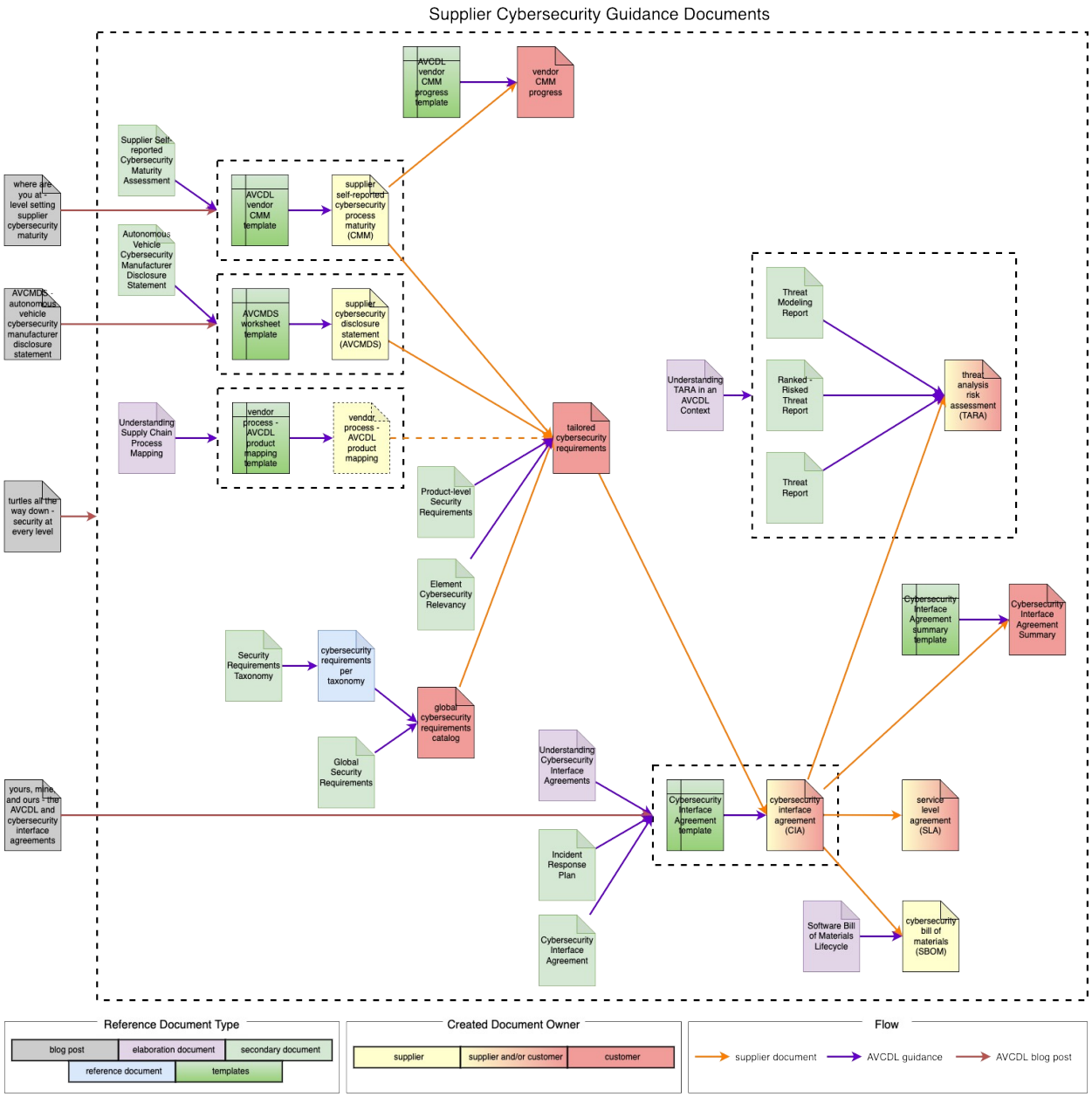


There are two supplier selection phases: request for information (RFI) and request for quote (RFQ). In order for the cybersecurity requirements of a product to be fulfilled, it is critical to ensure that all supplied elements of the product be capable of supporting those requirements. As can be seen above, multiple pieces of information (in yellow) provided by the supplier are used to establish each element's cybersecurity requirements, and also the inter-organization cybersecurity interface agreement (CIA) and service level agreement (SLA).

During the product's development, suppliers will be expected to provide a threat analysis / risk assessment (TARA) and software bill of materials (SBOM) for their element.

Guidance Documents and Dependencies

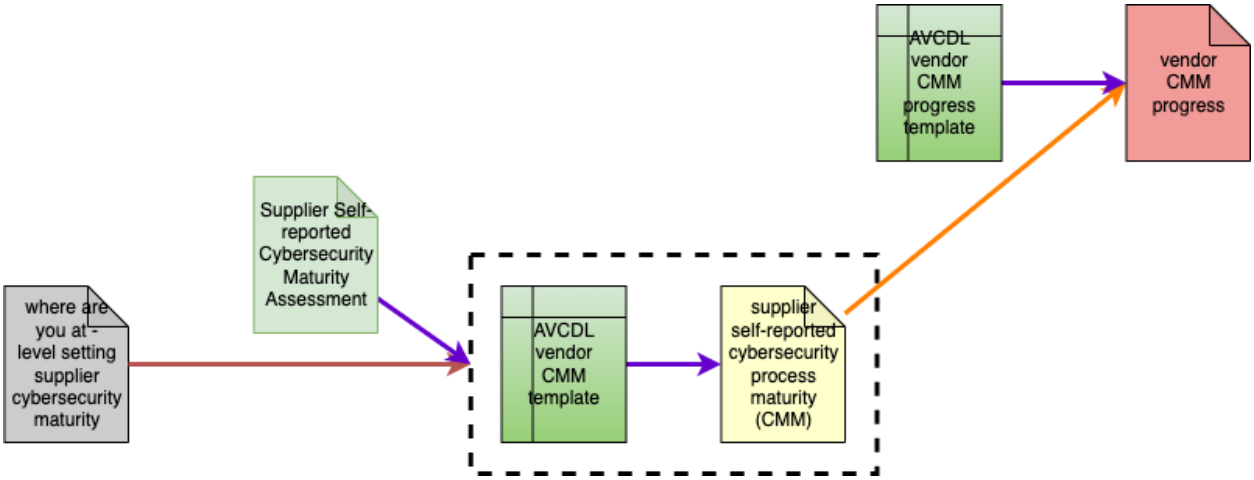
The following diagram shows the overall relationship between the various documents (reference and created) directly applicable to supplier-customer interactions.



Note: The blog post **Turtles All the Way Down: Security at Every Level** [2], which provides the motivation for application of cybersecurity across the supply chain, will not be covered here. It is provided for completeness only.

Supplier Cybersecurity Maturity Metrics (CMM)

The following diagram shows the documents related to the creation and tracking of supplier cybersecurity maturity.

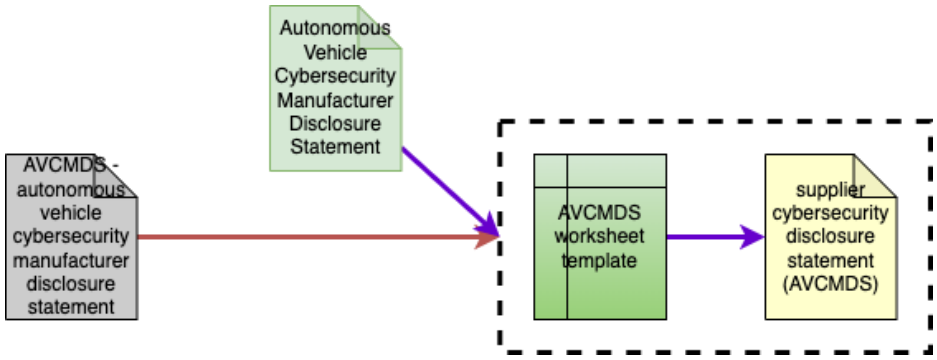


Guided by the **Supplier Self-reported Cybersecurity Maturity Assessment** [3] **AVCDL** secondary document, the supplier uses the **AVCDL vendor CMM template** [4] to create their **supplier self-reported cybersecurity process maturity** document. The blog post **Where are You at? Level Setting Supplier Cybersecurity Maturity** [6] provides a background for this document.

Using the **AVCDL vendor CMM progress template** [7] the customer creates a **vendor CMM progress** document to track the evolution of the supplier over time. This supports the desire to improve an element's cybersecurity posture over time.

Manufacturer Disclosure Statement (AVCMDS)

The following diagram shows the documents related to the creation of the supplier's cybersecurity disclosure statement.

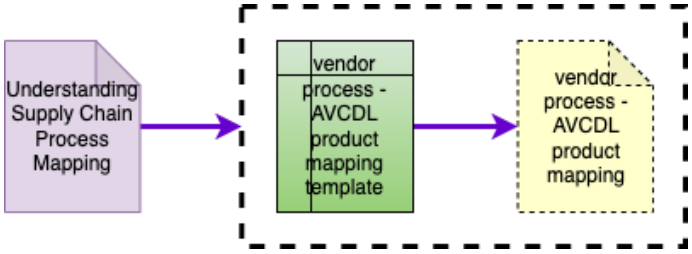


Guided by the **Autonomous Vehicle Cybersecurity Manufacturer Disclosure Statement** [8] **AVCDL** secondary document, the supplier uses the **AVCMDS worksheet template** [9] to create their **supplier cybersecurity disclosure statement (AVCMDS)** document. The blog post **AVCMDS: Autonomous Vehicle Cybersecurity Manufacturer Disclosure Statement** [10] provides a background for this document.

Note: The **AVCMDS** contains material of interest to the IT and OT groups within the customer's organization.

Supplier Process Mapping

The following diagram shows the documents related to the creation of supplier cybersecurity process to AVCDL process mapping.

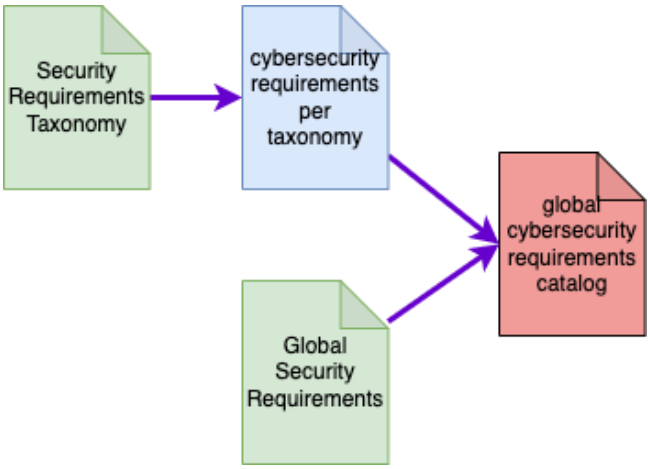


Guided by the **Understanding Supply Chain Process Mapping** [11] **AVCDL** elaboration document, the supplier uses the **vendor process – AVCDL product mapping template** [12] to create their **vendor process – AVCDL product mapping** document.

Note: This document is optional. Its creation is required when the supplier has a pre-existing set of cybersecurity lifecycle processes.

Global Cybersecurity Requirements Catalog

The following diagram shows the documents related to the creation of the customer's global cybersecurity requirements catalog.



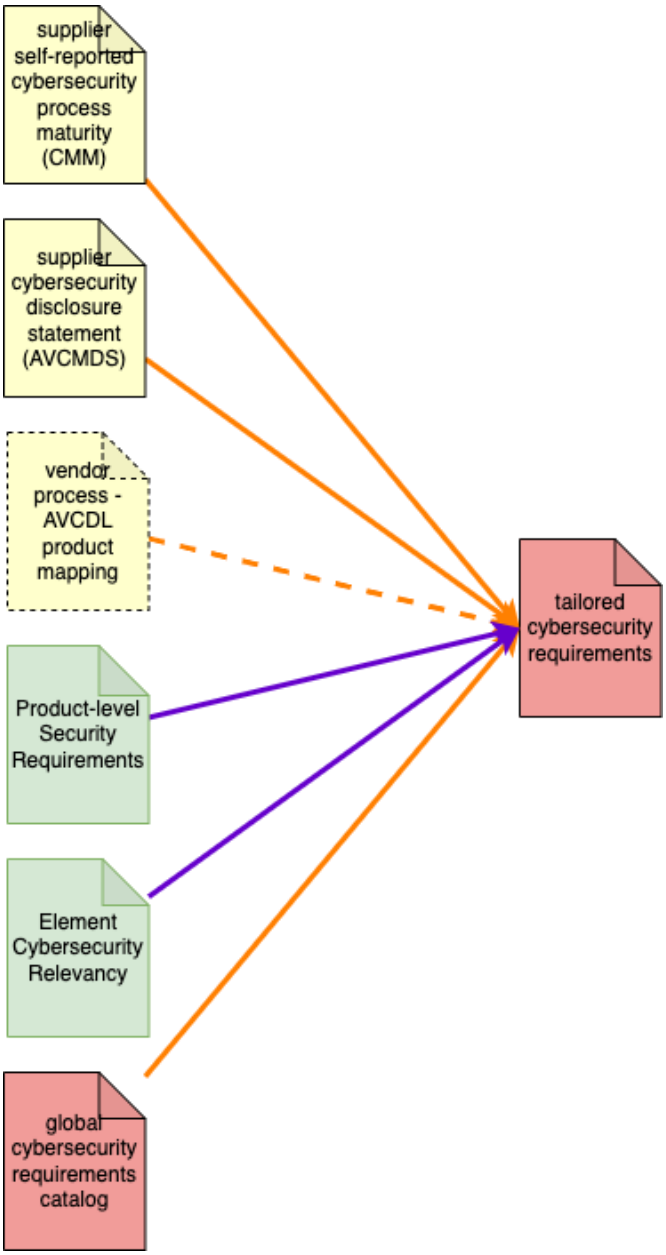
Guided by the **Security Requirements Taxonomy** [13] **AVCDL** secondary document, the customer creates their **cybersecurity requirements per taxonomy** [14]. Guided by the **Global Security Requirements** [15] **AVCDL** secondary document, the customer creates a global cybersecurity requirements catalog.

Note: The AVCDL provides an exemplar of the **cybersecurity requirements per taxonomy** document.

Note: This material is included for reference purposes as the creation of the **global cybersecurity requirements catalog** is presumed to have been completed prior to engagement with suppliers.

Tailored Requirements

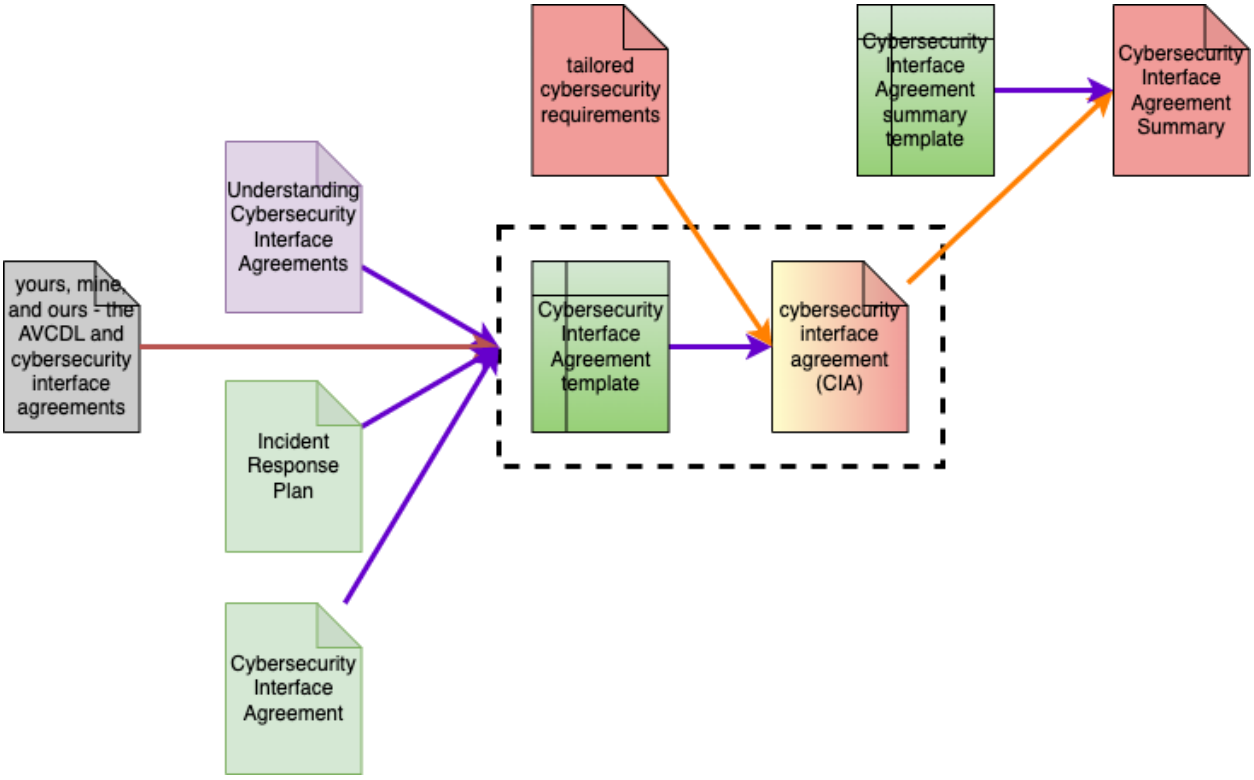
The following diagram shows the documents related to the creation of cybersecurity requirements tailored to the supplier's element.



Guided by the **Product-level Security Requirements** [16] and **Element Cybersecurity Relevancy** [17] **AVCDL** secondary documents, the customer uses information in the **supplier self-reported cybersecurity process maturity**, **supplier cybersecurity disclosure statement**, and where applicable **vendor process - AVCDL product mapping** documents to tailor a subset of the **global cybersecurity requirements catalog** to create a **tailored cybersecurity requirements** document.

Cybersecurity Interface Agreement (CIA)

The following diagram shows the documents related to the creation of the supplier – customer cybersecurity interface agreement and related customer summary.

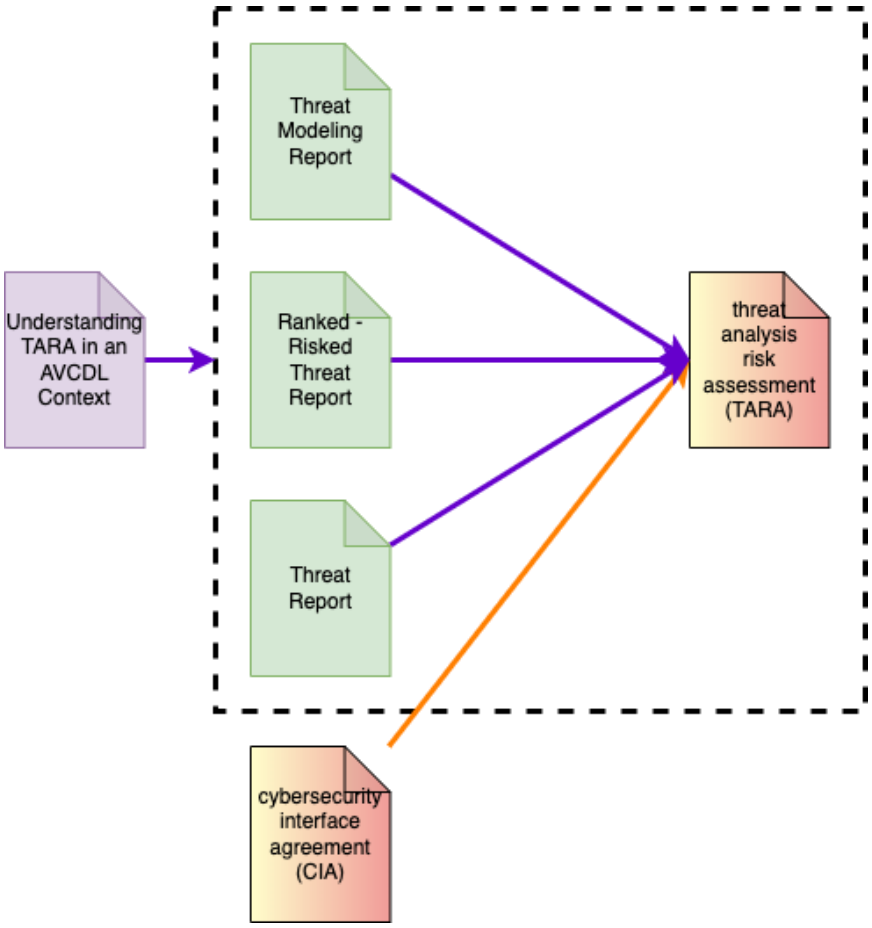


Guided by the **Understanding Cybersecurity Interface Agreements** [18] **AVCDL** elaboration document, as well as the **Cybersecurity Interface Agreement** [19] and **Incident Response Plan** [20] **AVCDL** secondary documents, the customer and supplier use the **Cybersecurity Interface Agreement template** [21] and **tailored cybersecurity requirements** (see previous section) to create a **cybersecurity interface agreement** document. The blog post, **Yours, Mine, and Ours: The AVCDL and Cybersecurity Interface Agreements** [22] provides a background for this.

Using the **Cybersecurity Interface Agreement summary template** [23] the customer creates a **Cybersecurity Interface Agreement Summary** document to capture the high-level information for consumption by customer project management.

Threat Analysis and Risk Assessment (TARA)

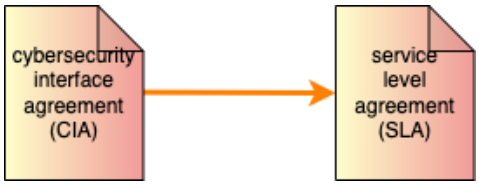
The following diagram shows the documents related to the creation of the supplier element TARA.



Guided by the **Understanding TARA in an AVCDL Context** [24] **AVCDL** elaboration document, as well as the **Threat Modeling Report** [25], **Ranked-Risked Threat Report** [26] and **Threat Report** [27] **AVCDL** secondary documents, the customer and/or supplier create a **threat analysis and risk assessment (TARA)** document, where the participants are specified in the **Cybersecurity Interface Agreement**.

Service Level Agreement (SLA)

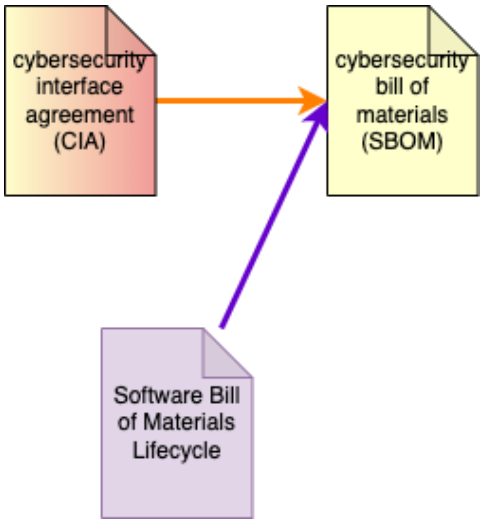
The following diagram shows the documents related to the creation of the supplier service level agreement.



Guided by the **Cybersecurity Interface Agreement**, the customer and supplier create a **service level agreement (SLA)** document.

Software Bill of Materials (SBOM)

The following diagram shows the documents related to the creation of the supplier element SBOM.



Guided by the **Software Bill of Materials Lifecycle** [28] **AVCDL** elaboration document, and as specified in the **Cybersecurity Interface Agreement**, the supplier creates a **cybersecurity bill of materials (SBOM)**.

References

1. **AVCDL** (primary document)
2. **Turtles All the Way Down: Security at Every Level (AVCDL** blog post**)**
3. **Supplier Self-reported Cybersecurity Maturity Assessment** (**AVCDL** secondary document)
4. **AVCDL vendor CMM template** (**AVCDL** template document**)**
5. **AVCDL mappings** (**AVCDL** reference document)
6. **Where are You at? Level Setting Supplier Cybersecurity Maturity (AVCDL** blog post**)**
7. **AVCDL vendor CMM progress template** (**AVCDL** template document**)**
8. **Autonomous Vehicle Cybersecurity Manufacturer Disclosure Statement** (**AVCDL** secondary document)
9. **AVCMDS worksheet template** (**AVCDL** template document**)**
10. **AVCMDS: Autonomous Vehicle Cybersecurity Manufacturer Disclosure Statement (AVCDL** blog post**)**
11. **Understanding Supply Chain Process Mapping** (**AVCDL** elaboration document**)**
12. **vendor process – AVCDL product mapping template** (**AVCDL** template document**)**
13. **Security Requirements Taxonomy** (**AVCDL** secondary document)
14. **cybersecurity requirements per taxonomy** (**AVCDL** exemplar**)**
15. **Global Security Requirements** (**AVCDL** secondary document)
16. **Product-level Security Requirements** (**AVCDL** secondary document)
17. **Element Cybersecurity Relevancy** (**AVCDL** secondary document)
18. **Understanding Cybersecurity Interface Agreements** (**AVCDL** elaboration document**)**
19. **Cybersecurity Interface Agreement** (**AVCDL** secondary document)
20. **Incident Response Plan** (**AVCDL** secondary document)
21. **Cybersecurity Interface Agreement template** (**AVCDL** template document**)**
22. **Yours, Mine, and Ours: The AVCDL and Cybersecurity Interface Agreements (AVCDL** blog post**)**
23. **Cybersecurity Interface Agreement summary template** (**AVCDL** template document**)**
24. **Understanding TARA in an AVCDL Context** (**AVCDL** elaboration document**)**
25. **Threat Modeling Report** (**AVCDL** secondary document**)**
26. **Ranked-Risked Threat Report** (**AVCDL** secondary document**)**
27. **Threat Report** (**AVCDL** secondary document**)**
28. **Software Bill of Materials Lifecycle** (**AVCDL** elaboration document**)**
29. **Understanding Service Level Agreements in an AVCDL Context** (**AVCDL** elaboration document**)**