

Understanding Supplier Cybersecurity Process Mapping

Revision

Version 6
4/14/25 4:23 PM

Author

Charles Wilson

Abstract

This document explains the means by which a supplier's cybersecurity processes can be mapped onto the **AVCDL** phase requirements and products.

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

This work was created by **Motional** and is licensed under the **Creative Commons Attribution-Share Alike (CC BY-SA-4.0)** License.

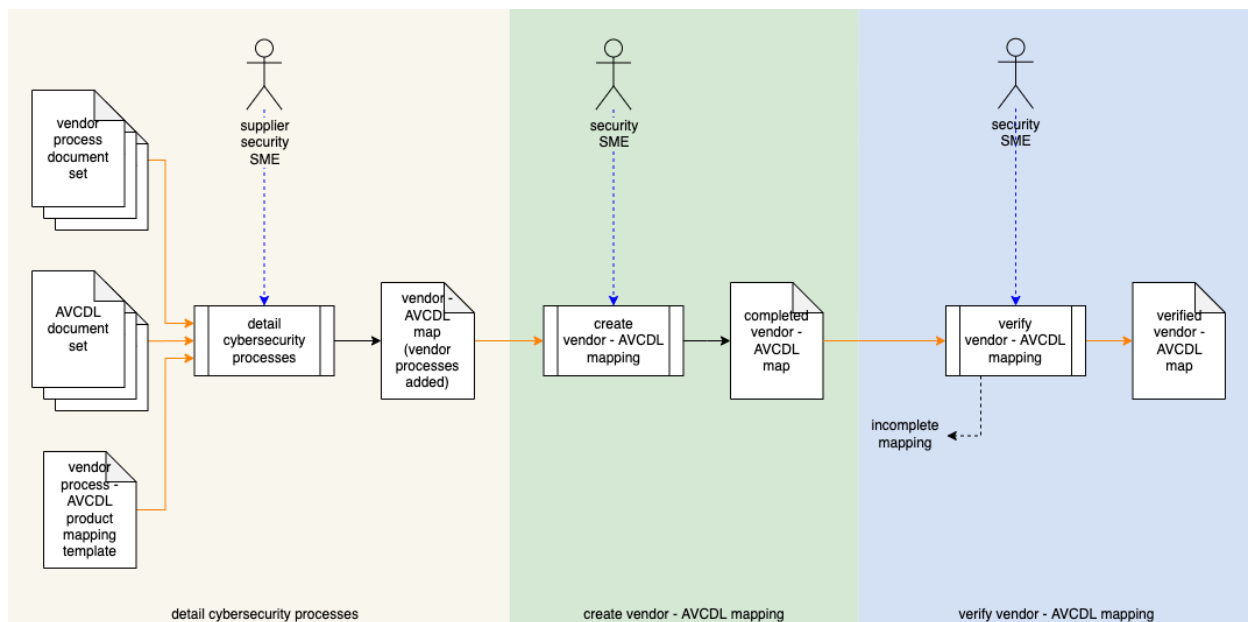
<https://creativecommons.org/licenses/by/4.0/legalcode>

Overview

Within the context of an organization using the **AVCDL** ^[1] as the basis for their product cybersecurity development, the **AVCDL Cybersecurity Interface Agreement** ^[2] is the instrument used to codify the supplier – customer relationship from a cybersecurity standpoint. Key to the process of completing the cybersecurity interface agreement is the establishment of a basis for determining whether the supplier cybersecurity processes are sufficient to achieve compliance with applicable regulatory standards. Since the **AVCDL** is compliant with all known standards, it is the basis to be used.

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.

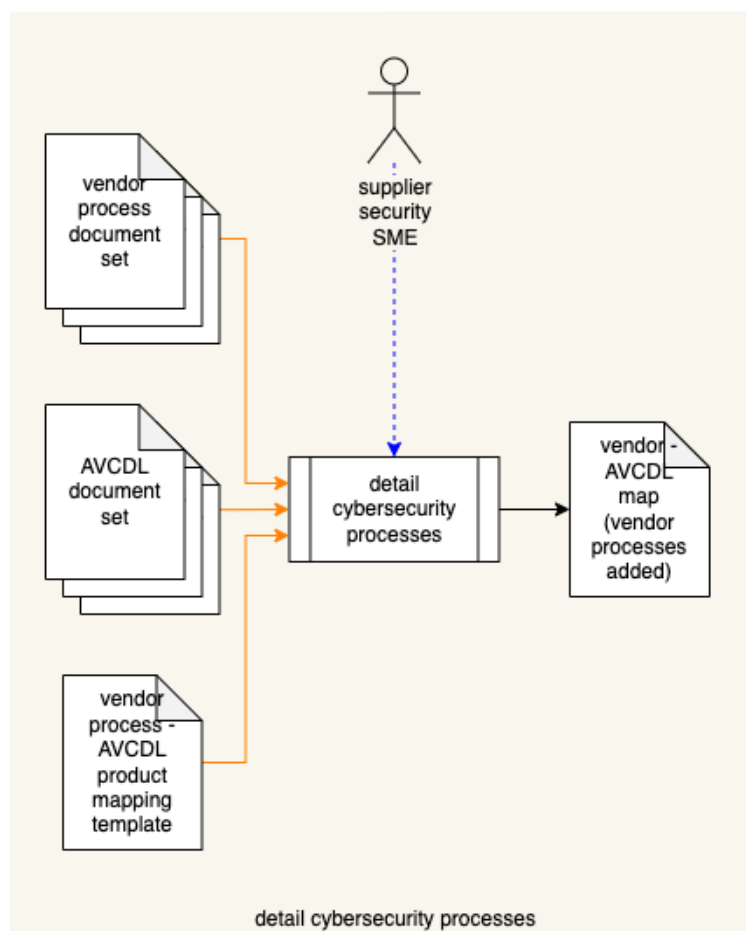
The following is the overview of the workflow to be applied to make these determinations.



Process

Detail Cybersecurity Processes

Inputs	Vendor process document set AVCDL document set Vendor process – AVCDL product mapping template
Outputs	Vendor – AVCDL map (vendor processes added)
Participants	Supplier security SME

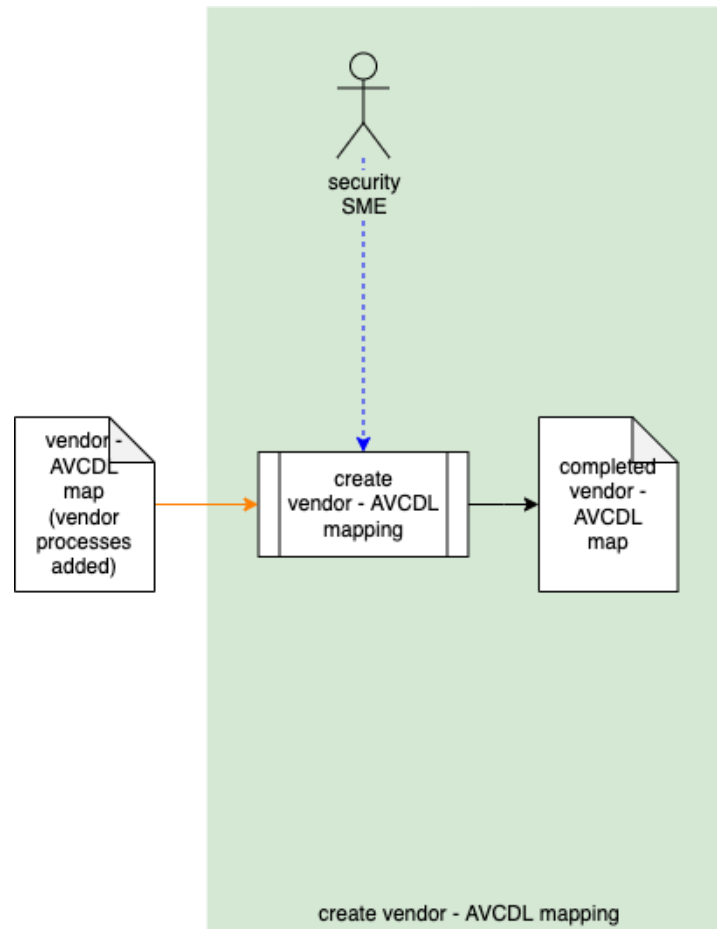


Using the **AVCDL document set** and **vendor process document set**, the supplier security SME details their cybersecurity processes in an instantiation of the **vendor process – AVCDL product mapping template** ^[3]. More specifically, the supplier security SME will use the template's [434 req-AVCDL product](#) sheet as a baseline and adjust the [434 req-vendor process](#) sheet to show their processes across the top in place of the **AVCDL** ones.

Then using the same information, the supplier security SME will complete the **434 req-vendor process** sheet's matrix to indicate the **ISO 21434** requirements they satisfy with their processes. The resultant completed instantiation is a **vendor – AVCDL map (vendor processes added)**.

Create Vendor – AVCDL mapping

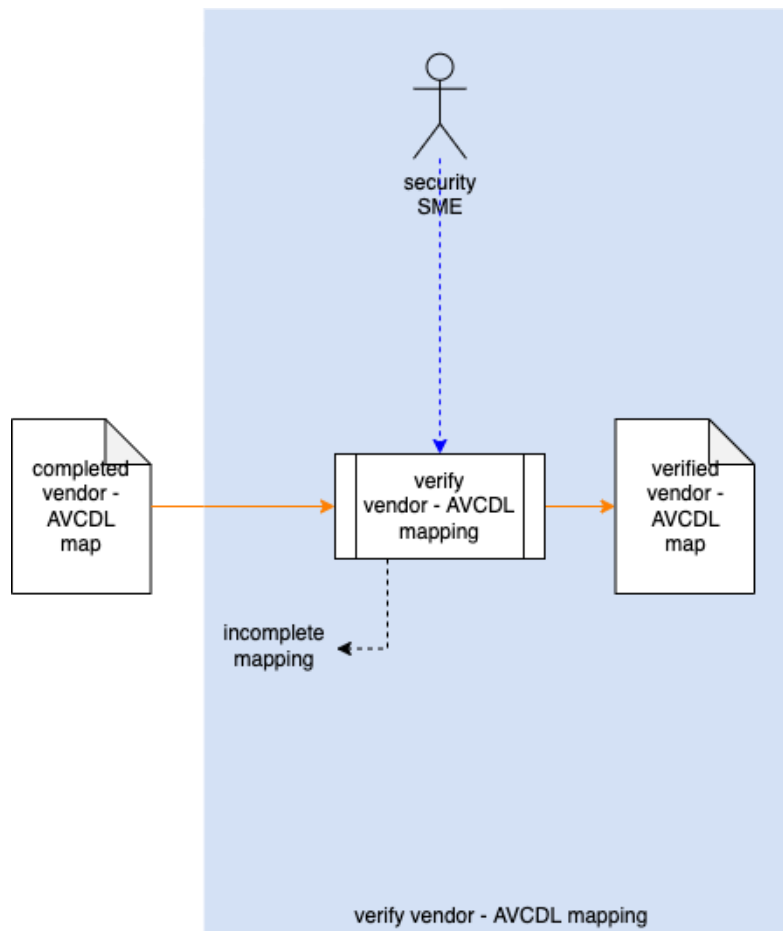
Inputs	Vendor – AVCDL map
Outputs	Completed vendor – AVCDL map
Participants	Security SME



Using the **vendor – AVCDL map (vendor processes added)**, the security SME uses the information populated in the [434 req-vendor process](#) sheet to construct a mapping in the [AVCDL-vendor process](#) sheet. The security SME will fill out the [AVCDL-vendor process](#) sheet's matrix to show process coverage with respect to the **AVCDL**. The result will be a **completed vendor – AVCDL map**.

Verify Vendor – AVCDL Mapping

Inputs	Completed vendor – AVCDL map
Outputs	Verified vendor – AVCDL map
Participants	Security SME



The security SME will review **completed vendor – AVCDL map**'s [AVCDL-vendor process](#) sheet. If there is a lack of coverage in the supplier processes this is documented and returned to the supplier noting that their coverage has an incomplete mapping. Otherwise, the document will be a **verified vendor – AVCDL map**.

Note: Deficiencies in vendor process coverage against the **AVCDL** should be handled in the same manner as with suppliers adopting the **AVCDL**.

Template

There are three sheets to the **vendor process - AVCDL product mapping template**. We'll examine each in turn.

434 req-AVCDL product

This **434 req-AVCDL product** sheet is copied from the **AVCDL mappings** workbook sheet by the same name.

			Foundation										Requirement	Design				Implementation										Verification				Release		Operation				Dec	Supplier																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																													
			1	2	3	4	5	6	7	8	9	10	1	2	1	2	3	4	5	1	2	3	4	5	6	7	8	9	10	11	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																						
			1	2	1	1	1	2	1	1	1	1	1	2	1	1	1	1	2	3	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																			
Organizational Cybersecurity Management	WP-05-01	RQ-05-01	cybersecurity policy																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																	
		RQ-05-02	organization-specific rules / policies																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																	
		RQ-05-03	roles and responsibilities			X																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																																														

Rows are **ISO 21434** requirements and associated work products. Columns are **AVCDL** phase requirements, products, and associated phases.

Note: The **AVCDL Cybersecurity Interface Agreement** should be used as a source of summary information regarding the **AVCDL** phases, requirements, and products.

434 req-vendor process

This **434 req-vendor process** sheet is intended to document the vendor cybersecurity processes and show **ISO 21434** requirements coverage of the same.

		Foundation										Requirement		Design					Implementation										Verification				Release			Operation			Dec		Supplier		
		1	2	3	4	5	6	7	8	9	10	1	2	1	2	3	4	5	1	2	3	4	5	6	7	8	9	10	11	1	2	3	4	1	2	3	4	1	2	3			
		1	2	1	1	1	2	1	1	1	1	1	2	1	1	1	1	2	3	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	
Organizational Cybersecurity Management	WP-05-01	RQ-05-01	cybersecurity policy																																								
		RQ-05-02	organization-specific rules / policies																																								
		RQ-05-03	roles and responsibilities																																								
		RQ-05-04	cybersecurity resources																																								
		RQ-05-05	establish communication channels																																								
	WP-05-02	RQ-05-06	cybersecurity culture																																								
		RQ-05-07	ensure competency																																								
		RQ-05-08	continuous improvement process																																								
		RQ-05-09	define information sharing criteria																																								
	WP-05-03	RQ-05-07	ensure competency																																								
		RQ-05-08	continuous improvement process																																								
		RQ-05-11	quality management system																																								
	WP-05-04	RQ-05-12	track product cybersecurity status until EoL																																								
		RQ-05-14	manage tools																																								
	WP-05-05	RQ-05-17	cybersecurity audit																																								
Product Cybersecurity Management	WP-06-01	RQ-06-01	assign project responsibilities																																								
		RQ-06-02	identify security-relevant components																																								
		RQ-06-04	cybersecurity plan content																																								
		RQ-06-04	assign project tracking responsibilities																																								
		RQ-06-05	cybersecurity plan style																																								
		RQ-06-06	include security in project plan																																								
		RQ-06-07	keep cybersecurity plan updated																																								
		RQ-06-09	keep cybersecurity work products updated																																								
		RQ-06-10	cybersecurity supplier interface definition																																								
		RQ-06-11	cybersecurity plan in QMS																																								
		RQ-06-12	work products in QMS																																								
		RQ-06-14	tailored activity justification																																								
		RQ-06-15	reuse analysis																																								
		RQ-06-16	reuse analysis composition 1																																								

Rows are **ISO 21434** requirements and associated work products. Columns are **AVCDL** requirements, products, and associated phases. These need to be replaced with the appropriate vendor processes aligned to the AVCDL phases as described in the [Detail Cybersecurity Processes](#) activity.

This **AVCDL-vendor process** sheet is intended to show the mapping from the **AVCDL** phase requirement products to the vendor processes.

[illegible]

Rows are **AVCDL** requirements, products, and associated phases. Columns are vendor processes aligned to the **AVCDL** phases. These need to be replaced with the appropriate vendor processes aligned to the **AVCDL** phases as described in the [Detail Cybersecurity Processes](#) activity. This is accomplished in the [Create Vendor – AVCDL Mapping](#) activity. The columns are copied from the [AVCDL-vendor process](#) sheet updated in that activity.

References

1. **AVCDL** (primary document)
2. **Cybersecurity Interface Agreement (AVCDL secondary document)**
3. **vendor process – AVCDL product mapping template** (AVCDL template document)