Understanding Supplier Cybersecurity Process Mapping

Revision

Version 4
3/12/24 5:37 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.

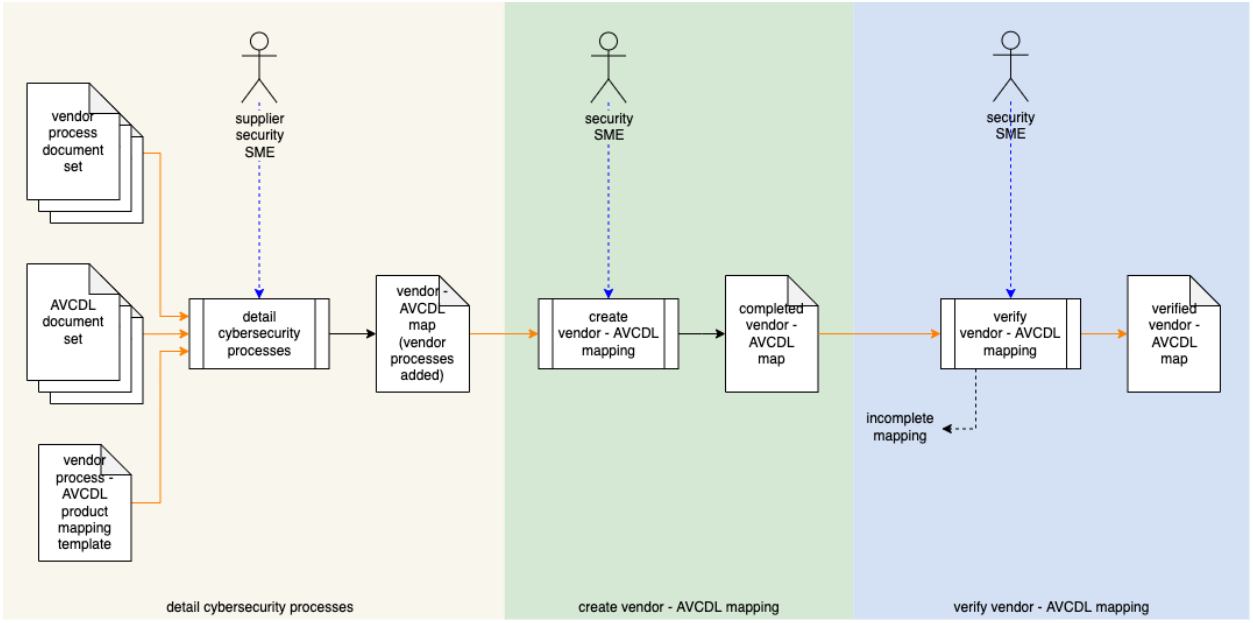
License

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.

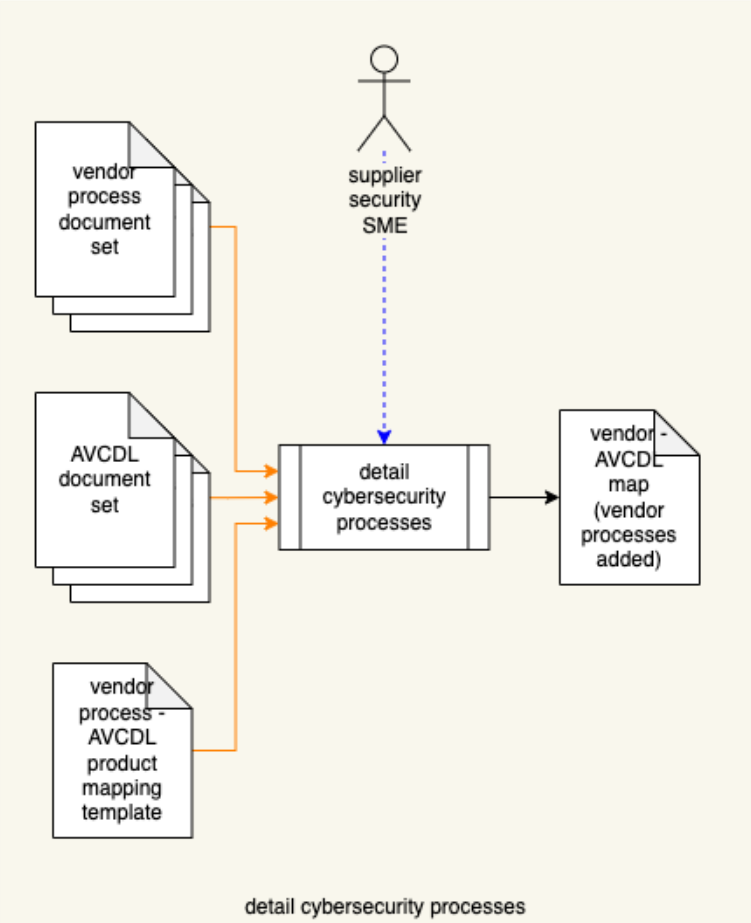
The following is the overview of the workflow to be applied to make these determinations.



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

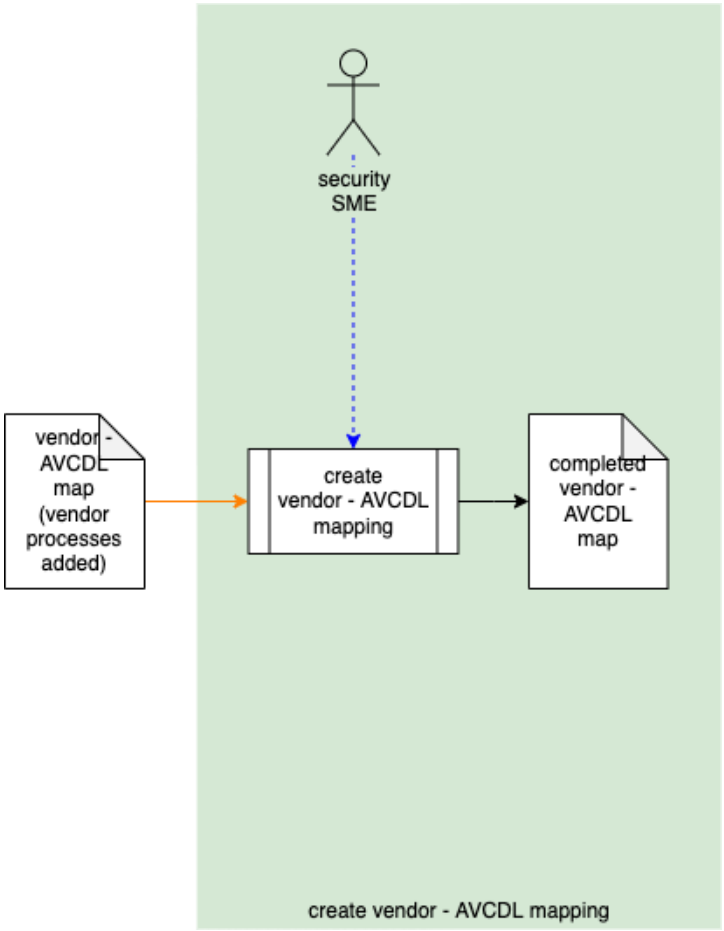


Using the **AVCDL document set** and **vendor process document set**, the supplier security SME details their cybersecurity processes in an instantiation of the **vendor process – AVCDL product mapping template** [3]. More specifically, the supplier security SME will use the template's **434 req-AVCDL 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

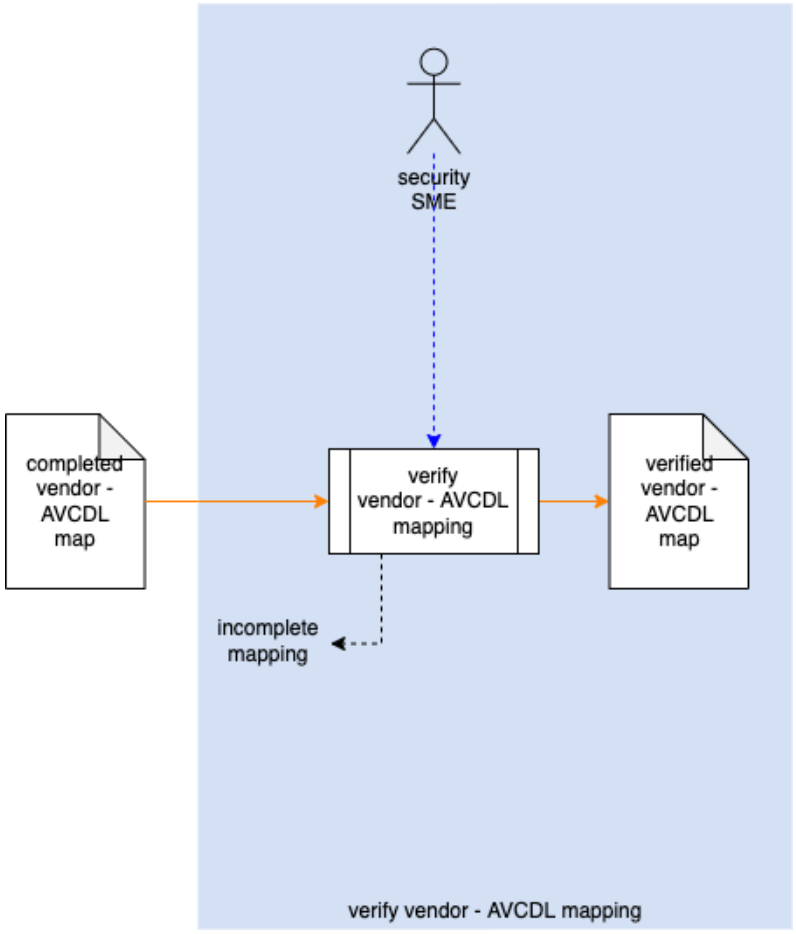
Inputs	Vendor – AVCDL map
Outputs	Completed vendor – AVCDL map
Participants	Security SME



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**.

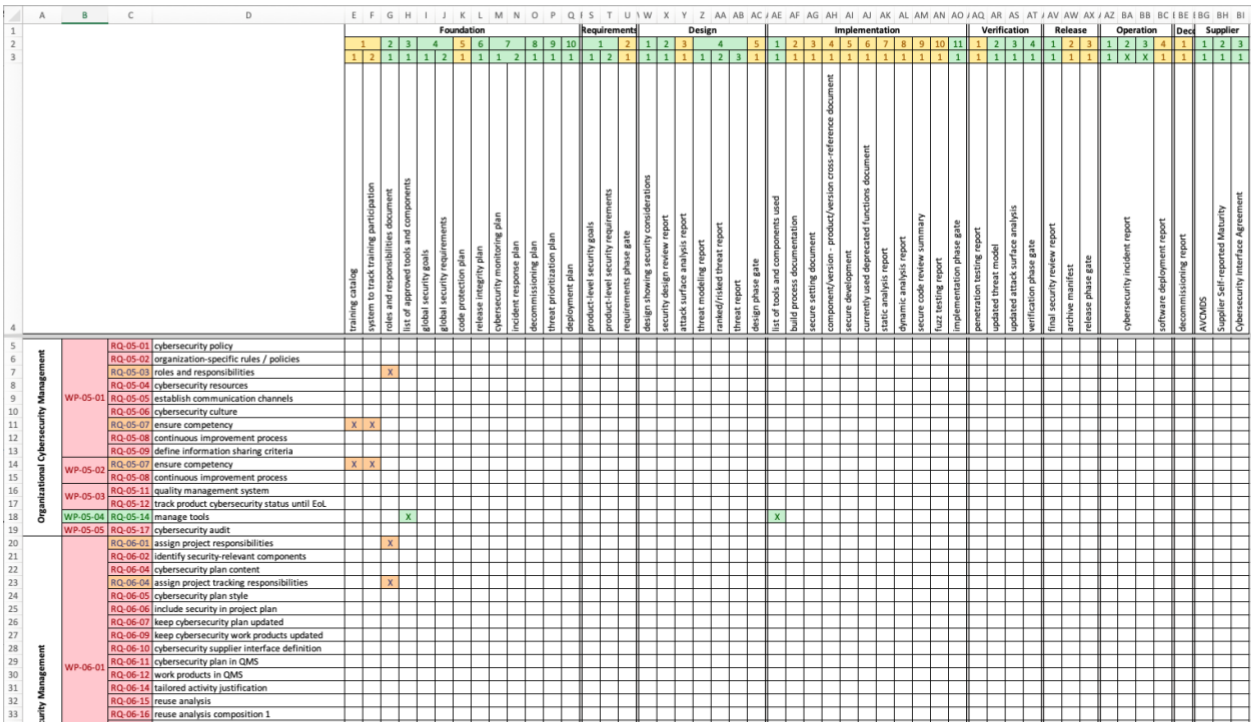
Note: Deficiencies in vendor process coverage against the **AVCDL** should be handled in the same manner as with suppliers adopting the **AVCDL**.

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.

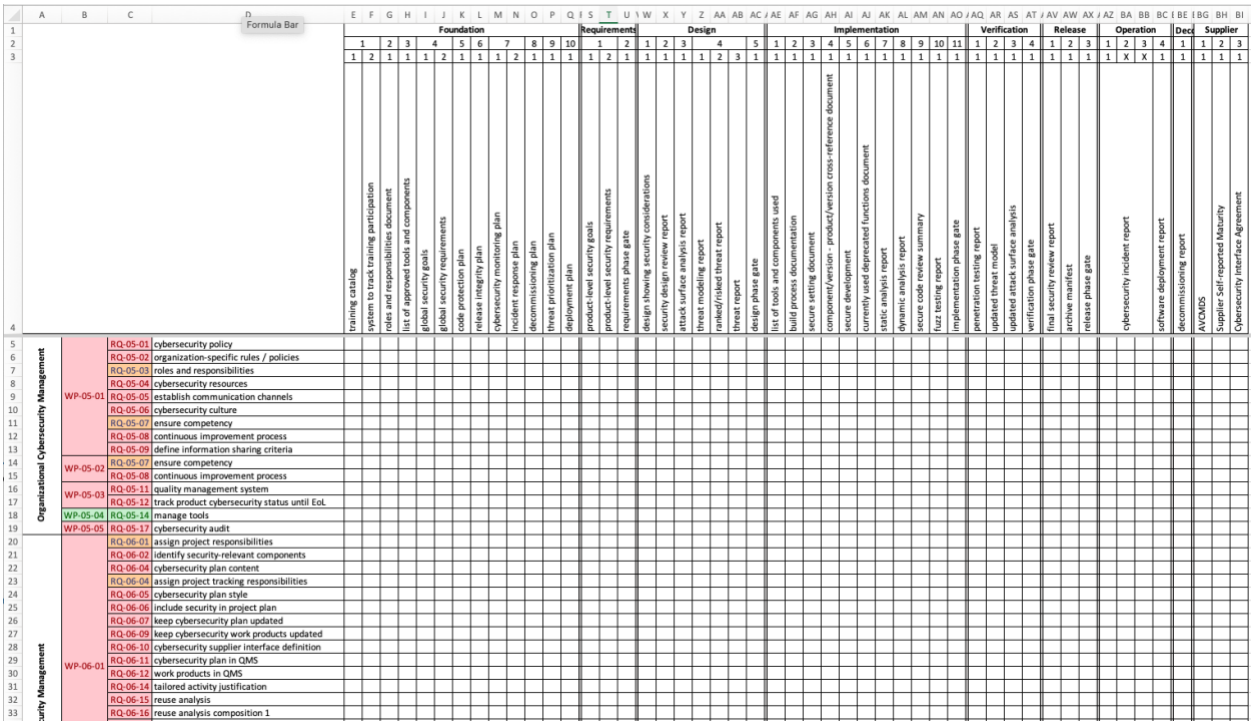


Rows are **ISO 21434** requirements and associated work products. Columns are **AVCDL** phase requirements, products, and associated phases.

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.



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.

AVCDL-vendor process

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

AVCDL phase	Foundation													
vendor requirement	1		2	3	4		5	6	7		8	9	10
vendor product	1	2	1	1	1	2	1	1	1	2	1	1	1
Title	training catalog	system to track training participation	roles and responsibilities document	list of approved tools and components	global security goals	global security requirements	code protection plan	release integrity plan	cybersecurity monitoring plan	incident response plan	decommissioning plan	threat prioritization plan	deployment plan

AVCDL phase	Requirements			Design						
vendor requirement	1		2	1	2	3	4			5
vendor product	1	2	1	1	1	1	1	2	3	1
Title	product-level security goals	product-level security requirements	requirements phase gate	design showing security considerations	security design review report	attack surface analysis report	threat modeling report	ranked/risked threat report	threat report	design phase gate

AVCDL phase	Implementation										
vendor requirement	1	2	3	4	5	6	7	8	9	10	11
vendor product	1	1	1	1	1	1	1	1	1	1	1
Title	list of tools and components used	build process documentation	secure setting document	component/version - product/version cross-reference document	secure development	currently used deprecated functions document	static analysis report	dynamic analysis report	secure code review summary	fuzz testing report	implementation phase gate

AVCDL phase	Verification				Release			Operation				Deco	Supplier		
vendor requirement	1	2	3	4	1	2	3	1	2	3	4	1	1	2	3
vendor product	1	1	1	1	1	1	1	1	X	X	1	1	1	1	1
Title	penetration testing report	updated threat model	updated attack surface analysis	verification phase gate	final security review report	archive manifest	release phase gate		cybersecurity incident report		software deployment report	decommissioning report	AVCMDS	Supplier Self-reported Maturity	Cybersecurity Interface Agreement

AVCDL phase	AVCDL requirement	AVCDL product	Title
Foundation	1	1	training catalog
		2	system to track training participation
	2	1	roles and responsibilities document
	3	1	list of approved tools and components
	4	1	global security goals
		2	global security requirements
	5	1	code protection plan
	6	1	release integrity plan
	7	1	cybersecurity monitoring plan
		2	incident response plan
	8	1	decommissioning plan
	9	1	threat prioritization plan
	10	1	deployment plan
Requiren	1	1	product-level security goals
		2	product-level security requirements
	2	1	requirements phase gate
Design	1	1	design showing security considerations
	2	1	security design review report
	3	1	attack surface analysis report
	4	1	threat modeling report
		2	ranked/risked threat report
		3	threat report
	5	1	design phase gate
	1	1	list of tools and components used
	2	1	build process documentation

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. **Autonomous Vehicle Cybersecurity Development Lifecycle**
2. **Cybersecurity Interface Agreement** (**AVCDL** secondary document**)**
3. **vendor process – AVCDL product mapping template** (AVCDL template document)