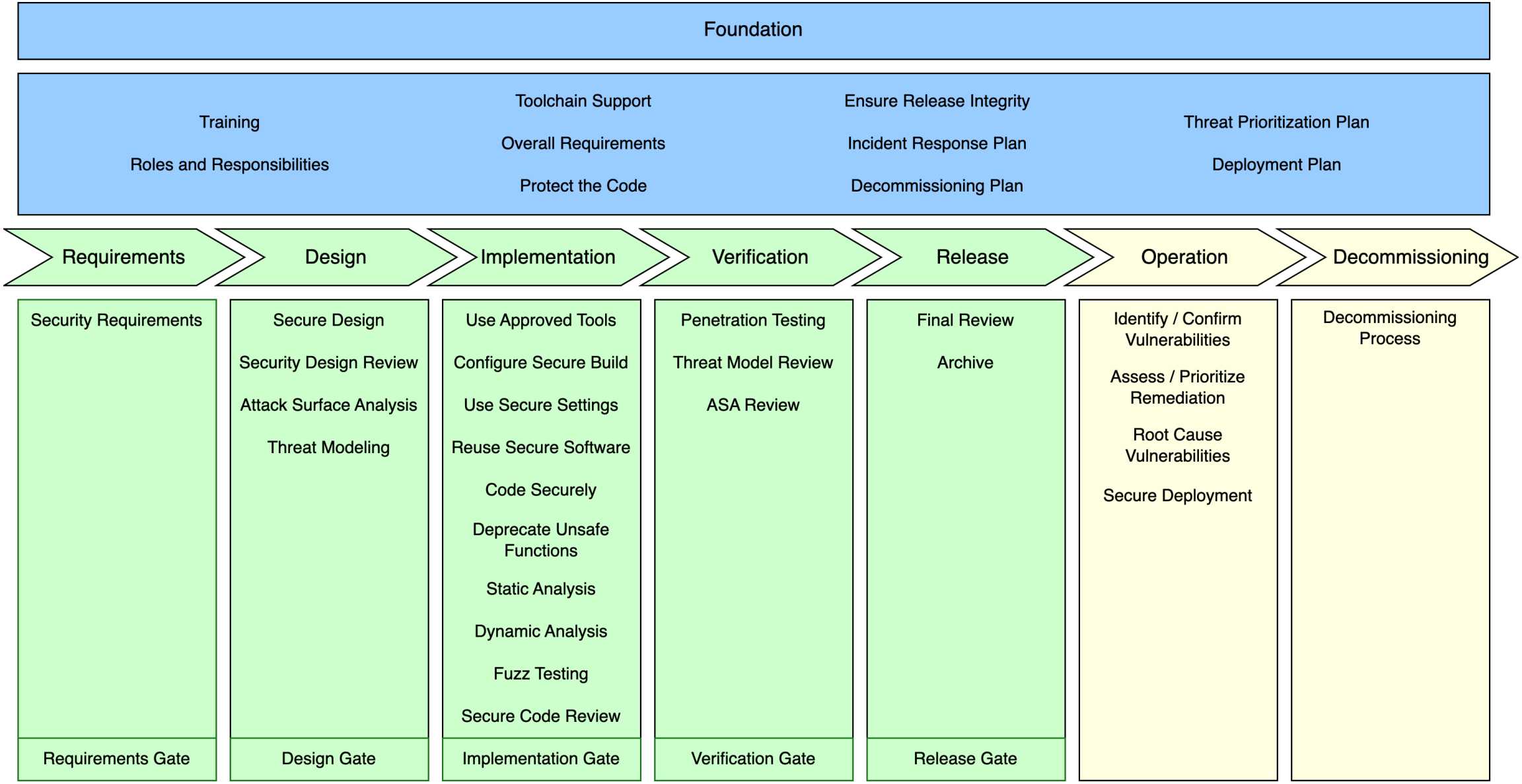
Supply Chain Cybersecurity

Charles Wilson
Technical Fellow, Cybersecurity Engineering
Motional

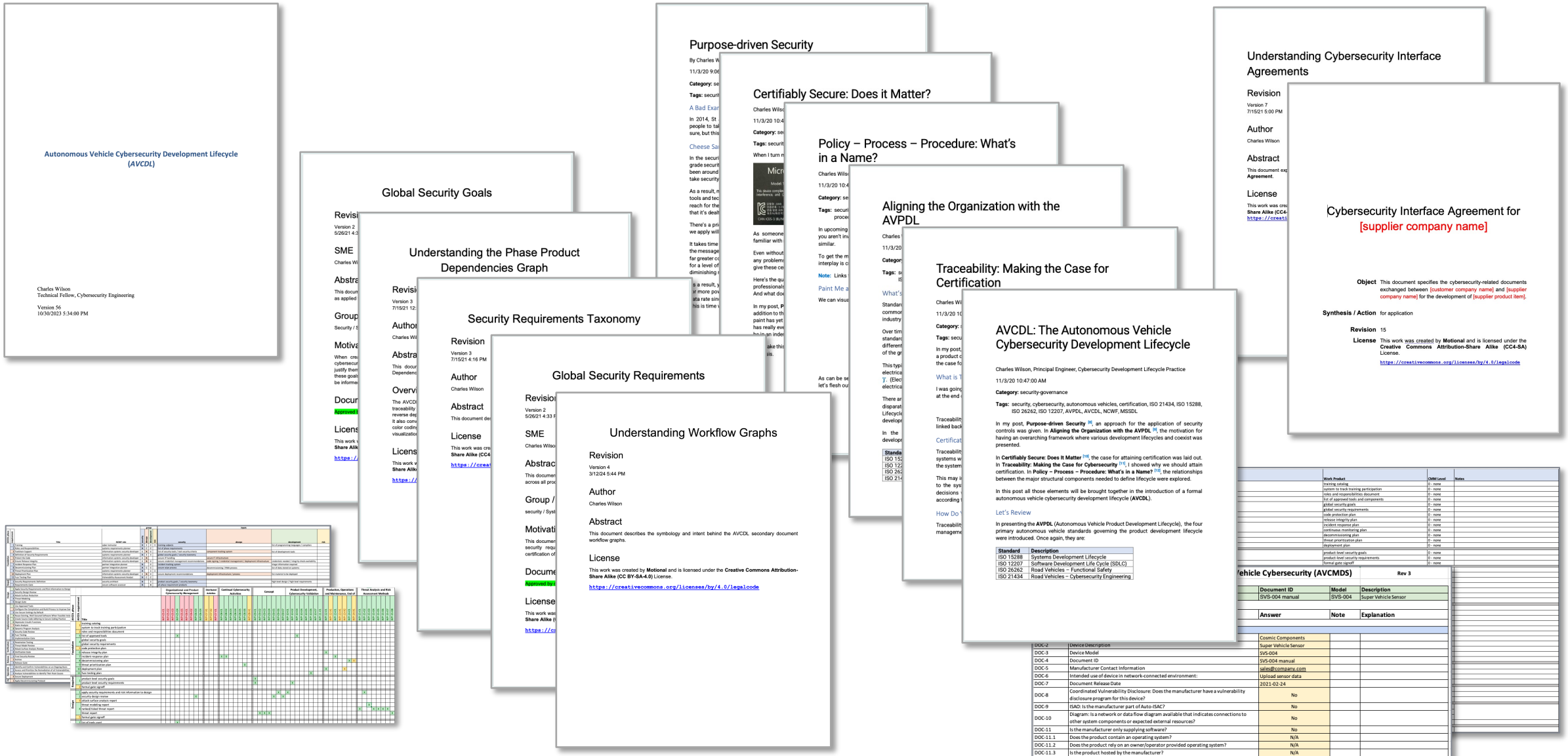
version 3
2024-03-12

AVCDL

AVCDL Framework



AVCDL Materials



Autonomous Vehicle Cybersecurity Development Lifecycle
(*AVCDL*)

Charles Wilson
Technical Fellow, Cybersecurity Engineering

Version 56
10/30/2023 5:34:00 PM

Global Security Goals

Understanding the Phase Product Dependencies Graph

Security Requirements Taxonomy

Global Security Requirements

Understanding Workflow Graphs

Revision
Version 4
3/12/24 5:44 PM

Author
Charles Wilson

Abstract
This document describes the symbology and intent behind the AVCDL secondary document workflow graphs.

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

Purpose-driven Security

Certifiably Secure: Does it Matter?

Policy – Process – Procedure: What's in a Name?

Aligning the Organization with the AVPDL

Traceability: Making the Case for Certification

AVCDL: The Autonomous Vehicle Cybersecurity Development Lifecycle

Charles Wilson, Principal Engineer, Cybersecurity Development Lifecycle Practice

11/3/20 10:47:00 AM

Category: security-governance

Tags: security, cybersecurity, autonomous vehicles, certification, ISO 21434, ISO 15288, ISO 26262, ISO 12207, AVPDL, AVCDL, NCWF, MSSDL

In my post, **Purpose-driven Security** [9], an approach for the application of security controls was given. In **Aligning the Organization with the AVPDL** [8], the motivation for having an overarching framework where various development lifecycles and coexist was presented.

In **Certifiably Secure: Does It Matter** [10], the case for attaining certification was laid out. In **Traceability: Making the Case for Cybersecurity** [11], I showed why we should attain certification. In **Policy – Process – Procedure: What's in a Name?** [12], the relationships between the major structural components needed to define lifecycle were explored.

In this post all those elements will be brought together in the introduction of a formal autonomous vehicle cybersecurity development lifecycle (**AVCDL**).

Let's Review

In presenting the **AVPDL** (Autonomous Vehicle Product Development Lifecycle), the four primary autonomous vehicle standards governing the product development lifecycle were introduced. Once again, they are:

Standard	Description
ISO 15288	Systems Development Lifecycle
ISO 12207	Software Development Life Cycle (SDLC)
ISO 26262	Road Vehicles – Functional Safety
ISO 21434	Road Vehicles – Cybersecurity Engineering

Understanding Cybersecurity Interface Agreements

Revision
Version 7
7/15/21 5:00 PM

Author
Charles Wilson

Abstract
This document exp
Agreement.

License
This work was cre
Share Alike (CC4-
https://creati

Cybersecurity Interface Agreement for
[supplier company name]

Object This document specifies the cybersecurity-related documents exchanged between [customer company name] and [supplier company name] for the development of [supplier product item].

Synthesis / Action for application

Revision 15

License This work was created by **Motional** and is licensed under the **Creative Commons Attribution-Share Alike (CC4-SA)** License.
https://creativecommons.org/licenses/by/4.0/legalcode

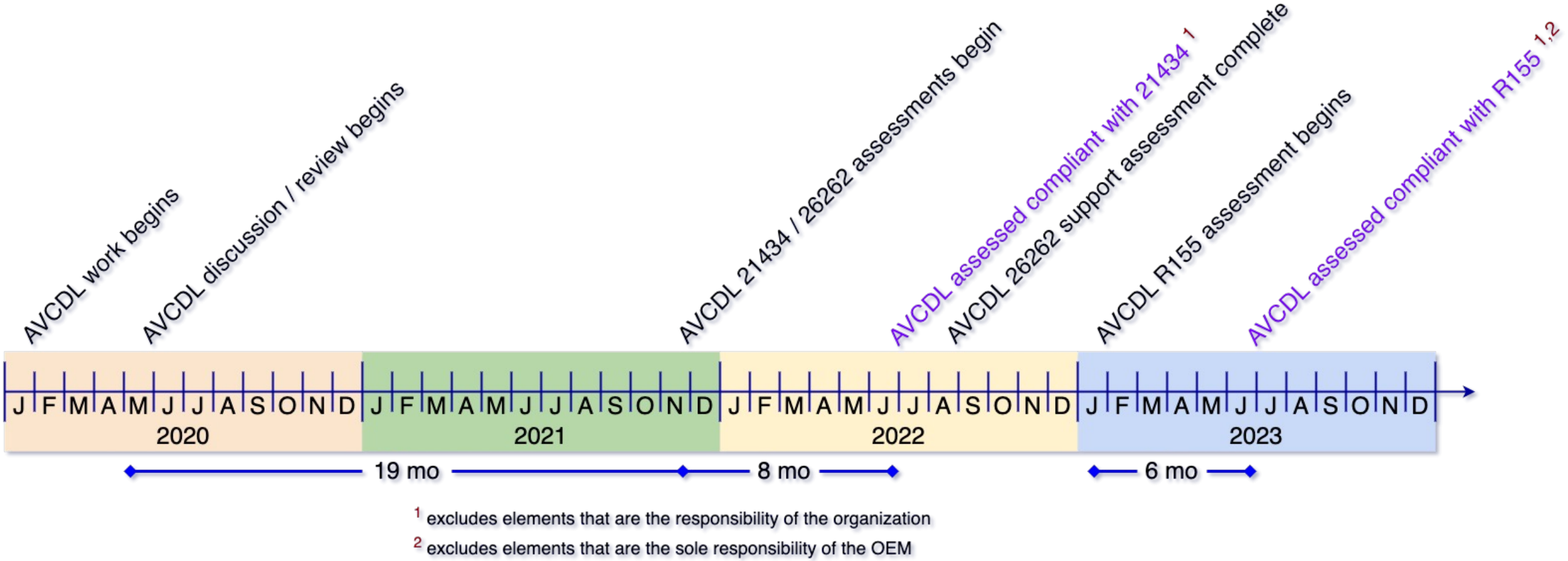
Work Product	CMM Level	Notes
training catalog	0 - none	
system to track training participation	0 - none	
roles and responsibilities document	0 - none	
list of approved tools and components	0 - none	
global security goals	0 - none	
global security requirements	0 - none	
code protection plan	0 - none	
release integrity plan	0 - none	
incident response plan	0 - none	
continuous monitoring plan	0 - none	
decommissioning plan	0 - none	
threat prioritization plan	0 - none	
deployment plan	0 - none	
product-level security goals	0 - none	
product-level security requirements	0 - none	
formal gate signoff	0 - none	

Vehicle Cybersecurity (AVCMDS) Rev 3

Document ID	Model	Description
SVS-004 manual	SVS-004	Super Vehicle Sensor

	Answer	Note	Explanation
Cosmic Components			
Super Vehicle Sensor			
DOC-3 Device Model	SVS-004		
DOC-4 Document ID	SVS-004 manual		
DOC-5 Manufacturer Contact Information	sales@company.com		
DOC-6 Intended use of device in network-connected environment:	Upload sensor data		
DOC-7 Document Release Date	2021-02-24		
DOC-8 Coordinated Vulnerability Disclosure: Does the manufacturer have a vulnerability disclosure program for this device?	No		
DOC-9 ISAO: Is the manufacturer part of Auto-ISAC?	No		
DOC-10 Diagram: Is a network or data flow diagram available that indicates connections to other system components or expected external resources?	No		
DOC-11 Is the manufacturer only supplying software?	No		
DOC-11.1 Does the product contain an operating system?	N/A		
DOC-11.2 Does the product rely on an owner/operator provided operating system?	N/A		
DOC-11.3 Is the product hosted by the manufacturer?	N/A		
DOC-11.4 Is the product hosted by the customer?	N/A		

Assessment Timeline

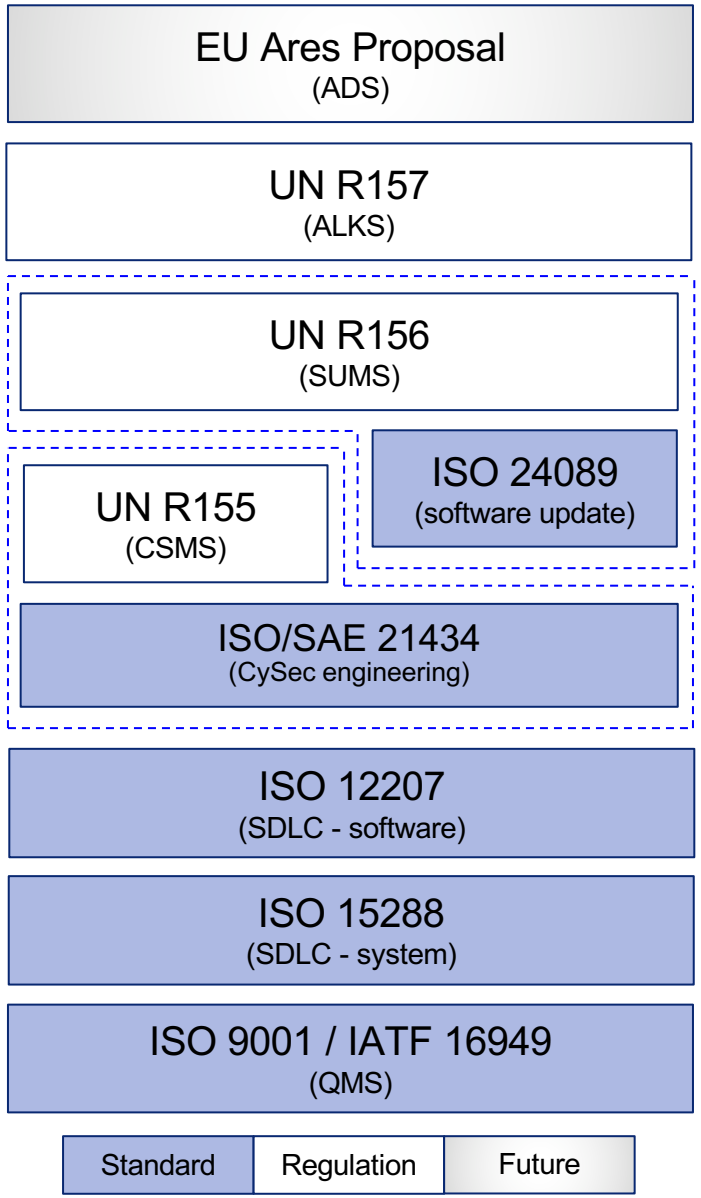


[1] excludes elements that are the responsibility of the organization

[2] excludes elements that are the sole responsibility of the OEM

Standard and Regulations

Standards and Regulations Ecosystem



Automated Driving Systems will require conformance to R155 and R156

Auto Lane Keeping Systems must conform to R155 and R156

Software Update Management Systems aligned with 24089 and 21434

Cybersecurity Management Systems aligned with 21434

System and software development lifecycles

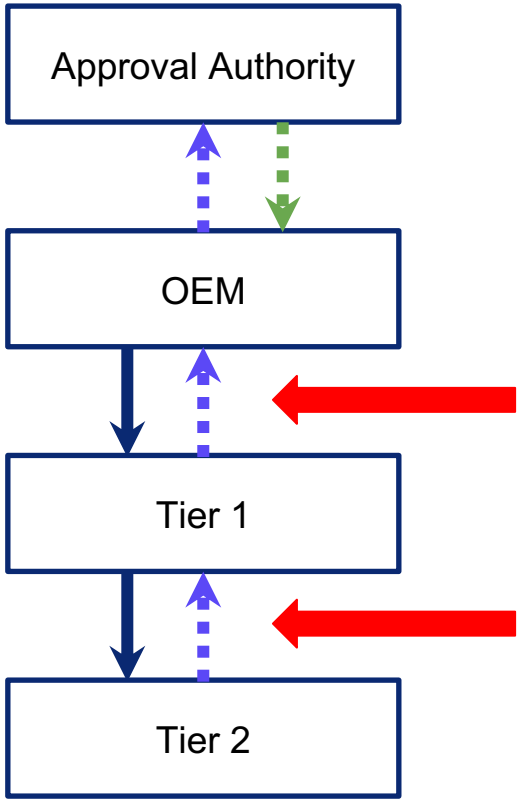
A certified QMS is the basis for compliance

R155 At a Glance

Category	Description	Responsibility	
		OEM	Supplier
General	UN regulation boilerplate	N/A	
CSMS *	Product creation processes	Owner	Support
Vehicle Type	Product operation processes		
Reporting	Product issue processes		

* CyberSecurity Management System

R155 Supply Chain Scope



distribution of work and data sharing through agreed upon ISO/SAE 21434-compliant cybersecurity interface agreements

Requirements Evidence Approval

R155 Requirements

Fundamentals

- development phase CSMS
- production phase CSMS
- post-production CSMS

Operation

- adaptable monitoring and response
- cybersecurity controls tracking
- timely risk mitigation
- threat extraction from vehicle logs
- supplier deficiency management

Product Development

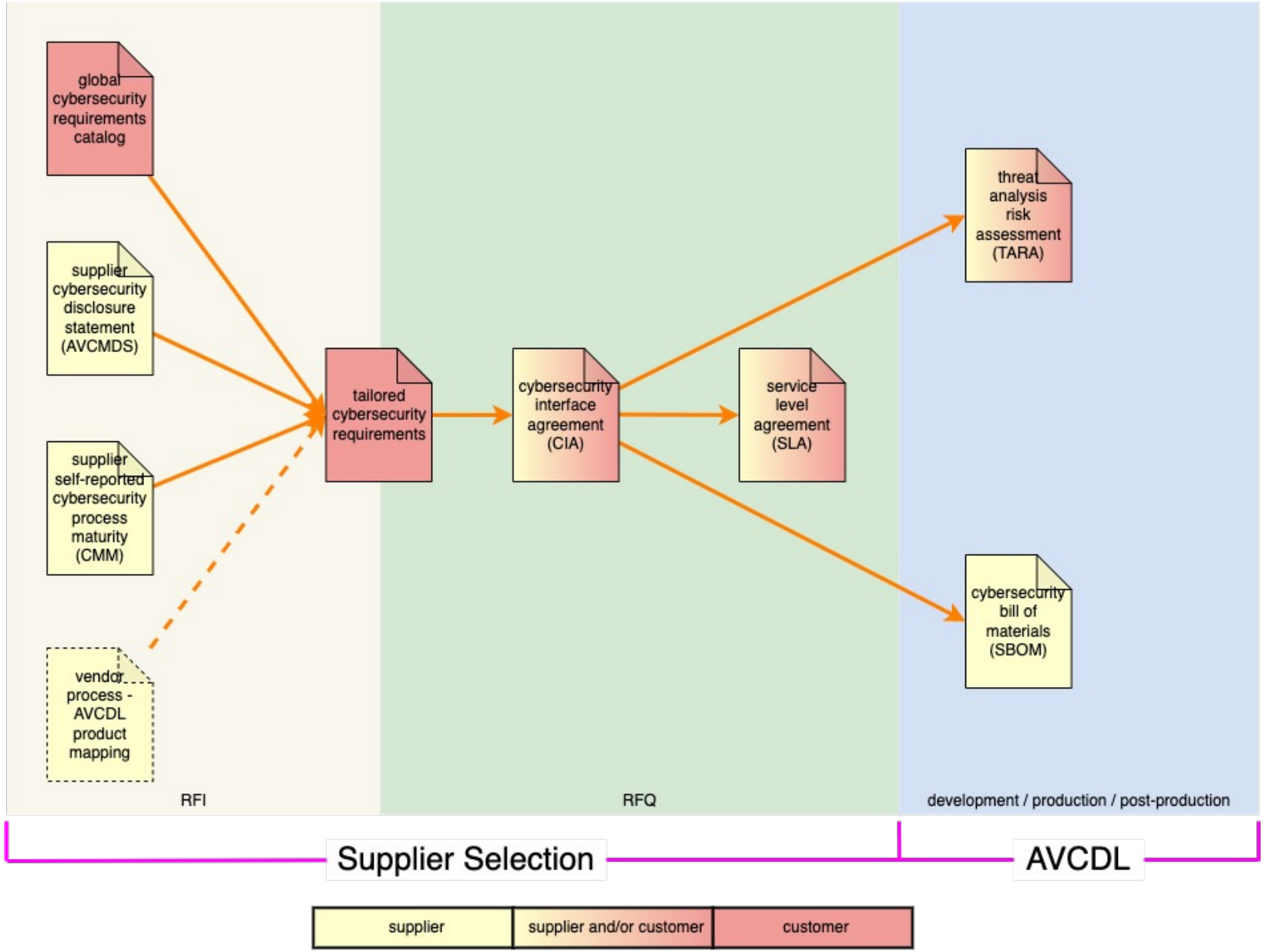
- risk identification
- risk assessment and treatment
- verification of risk management
- cybersecurity testing
- risk assessment kept current

OEM Support

- critical element risk assessment
- type risk protection
- type risk countermeasures
- sufficient testing
- detect and prevent cyber attacks
- vehicle cybersecurity monitoring
- provide forensic capability

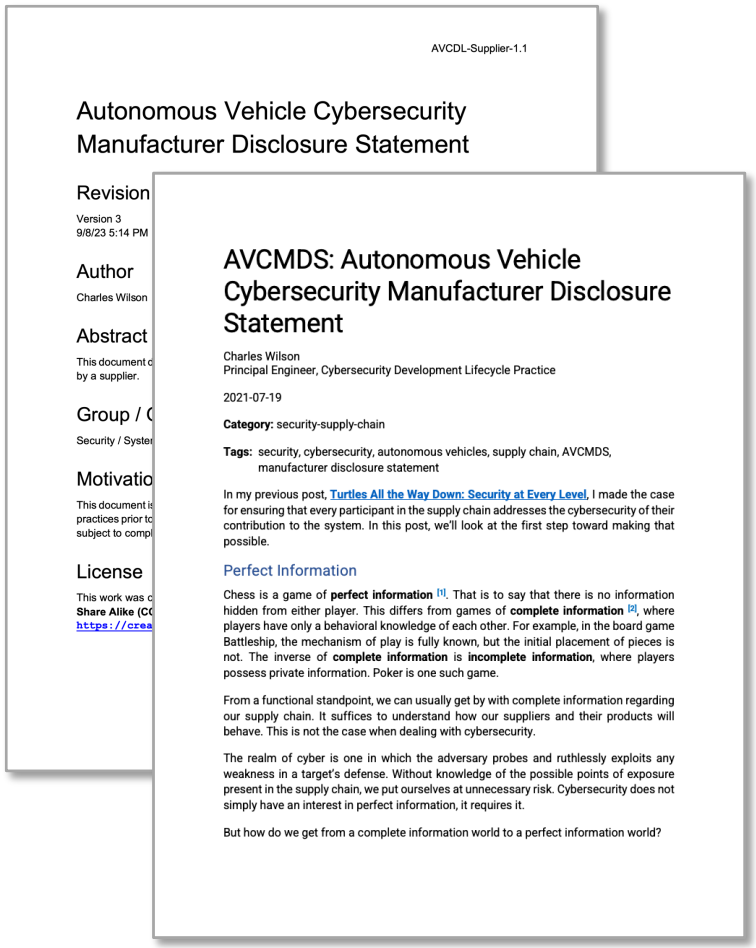
Supplier Selection

Supplier Selection



Supplier Cybersecurity Manufacturer Disclosure Statement

AVCMDS Material



AVCDL-Supplier-1.1

Autonomous Vehicle Cybersecurity Manufacturer Disclosure Statement

Revision

Version 3
9/8/23 5:14 PM

Author

Charles Wilson

Abstract

This document c
by a supplier.

Group / C

Security / Syster

Motivatio

This document is
practices prior to
subject to compl

License

This work was c
Share Alike (CC
https://crea

AVCMDS: Autonomous Vehicle Cybersecurity Manufacturer Disclosure Statement

Charles Wilson
Principal Engineer, Cybersecurity Development Lifecycle Practice

2021-07-19

Category: security-supply-chain

Tags: security, cybersecurity, autonomous vehicles, supply chain, AVCMDS, manufacturer disclosure statement

In my previous post, Turtles All the Way Down: Security at Every Level, I made the case for ensuring that every participant in the supply chain addresses the cybersecurity of their contribution to the system. In this post, we'll look at the first step toward making that possible.

Perfect Information

Chess is a game of **perfect information** [1]. That is to say that there is no information hidden from either player. This differs from games of **complete information** [2], where players have only a behavioral knowledge of each other. For example, in the board game Battleship, the mechanism of play is fully known, but the initial placement of pieces is not. The inverse of **complete information** is **incomplete information**, where players possess private information. Poker is one such game.

From a functional standpoint, we can usually get by with complete information regarding our supply chain. It suffices to understand how our suppliers and their products will behave. This is not the case when dealing with cybersecurity.

The realm of cyber is one in which the adversary probes and ruthlessly exploits any weakness in a target's defense. Without knowledge of the possible points of exposure present in the supply chain, we put ourselves at unnecessary risk. Cybersecurity does not simply have an interest in perfect information, it requires it.

But how do we get from a complete information world to a perfect information world?

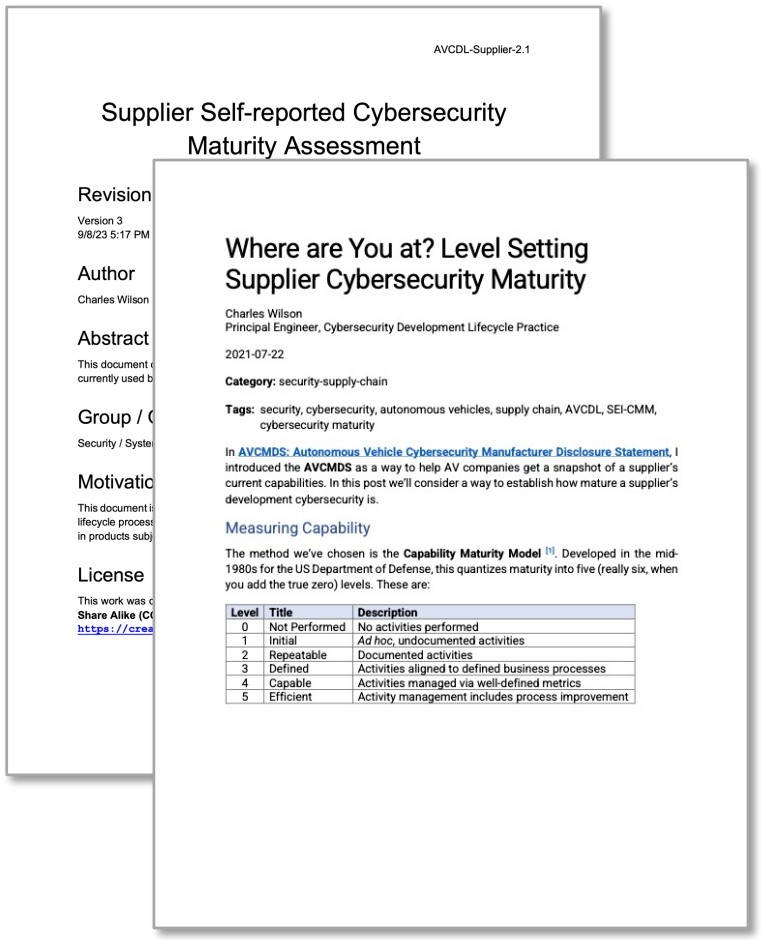
Manufacturer Disclosure Statement for Autonomous Vehicle Cybersecurity (AVCMDS)				Rev 4
Date	**Company**	**Document ID**	**Model**	**Description**
2021-02-24	Cosmic Components	SVS-004 manual	SVS-004	Super Vehicle Sensor
ID	**Question**	**Answer**	**Note**	**Explanation**
DOCUMENTATION (DOC)				
DOC-1	Manufacturer Name	Cosmic Components		
DOC-2	Device Description	Super Vehicle Sensor		
DOC-3	Device Model	SVS-004		
DOC-4	Document ID	SVS-004 manual		
DOC-5	Manufacturer Contact Information	sales@company.com		
DOC-6	Intended use of device in network-connected environment:	Upload sensor data		
DOC-7	Document Release Date	2021-02-24		
DOC-8	Coordinated Vulnerability Disclosure: Does the manufacturer have a vulnerability disclosure program for this device?	No		
DOC-9	ISAO: Is the manufacturer part of Auto-ISAC?	No		
DOC-10	Diagram: Is a network or data flow diagram available that indicates connections to other system components or expected external resources?	No		
DOC-11	Is the manufacturer only supplying software?	No		
DOC-11.1	Does the product contain an operating system?	N/A		
DOC-11.2	Does the product rely on an owner/operator provided operating system?	N/A		
DOC-11.3	Is the product hosted by the manufacturer?	N/A		
DOC-11.4	Is the product hosted by the customer?	N/A		
MANAGEMENT OF PERSONALLY IDENTIFIABLE INFORMATION (MPII)				
MPII-1	Can this device display, transmit, store, or modify personally identifiable information (PII)?	Yes		
MPII-2	Does the device maintain personally identifiable information?	Yes		
MPII-2.1	Does the device maintain personally identifiable information temporarily in volatile memory (i.e., until cleared by power-off or reset)?	N/A		
MPII-2.2	Does the device store personally identifiable information persistently on internal media?	Yes		
MPII-2.3	Is personally identifiable information preserved in the device's non-volatile memory until explicitly erased?	Yes		
MPII-2.4	Does the device store personally identifiable information in a database?	No		
MPII-2.5	Does the device allow configuration to automatically delete local personally identifiable information after it is stored to a long term solution?	No		
MPII-2.6	Does the device import/export personally identifiable information with other systems (e.g., video/audio system device that exports private feeds to other devices or a server)?	Yes		
MPII-2.7	Does the device maintain personally identifiable information when powered off, or during power service interruptions?	Yes		

Worksheet Topics

- Documentation
- PII management
- Automatic logoff
- Audit controls
- Access controls
- Product upgrading
- Data de-identification
- Data backup
- Disaster recovery
- Data integrity / authenticity
- Malware handling
- Device authentication
- Device connectivity
- User authentication
- Physical security
- Device lifecycle management
- Software bill-of-materials (SBOM)
- Hardening
- Security guidance
- Data storage confidentiality
- Data transmission confidentiality
- Data transmission integrity
- Connectivity / remote access
- Other

Supplier Cybersecurity Maturity

Supplier Self-reported Maturity Material



AVCDL-Supplier-2.1

Supplier Self-reported Cybersecurity Maturity Assessment

Revision

Version 3
9/8/23 5:17 PM

Author

Charles Wilson

Abstract

This document
currently used b

Group /

Security / Syste

Motivatic

This document i
lifecycle process
in products subj

License

This work was
Share Alike (C
https://crea

Where are You at? Level Setting Supplier Cybersecurity Maturity

Charles Wilson
Principal Engineer, Cybersecurity Development Lifecycle Practice

2021-07-22

Category: security-supply-chain

Tags: security, cybersecurity, autonomous vehicles, supply chain, AVCDL, SEI-CMM, cybersecurity maturity

In AVCMDS: Autonomous Vehicle Cybersecurity Manufacturer Disclosure Statement, I introduced the **AVCMDS** as a way to help AV companies get a snapshot of a supplier's current capabilities. In this post we'll consider a way to establish how mature a supplier's development cybersecurity is.

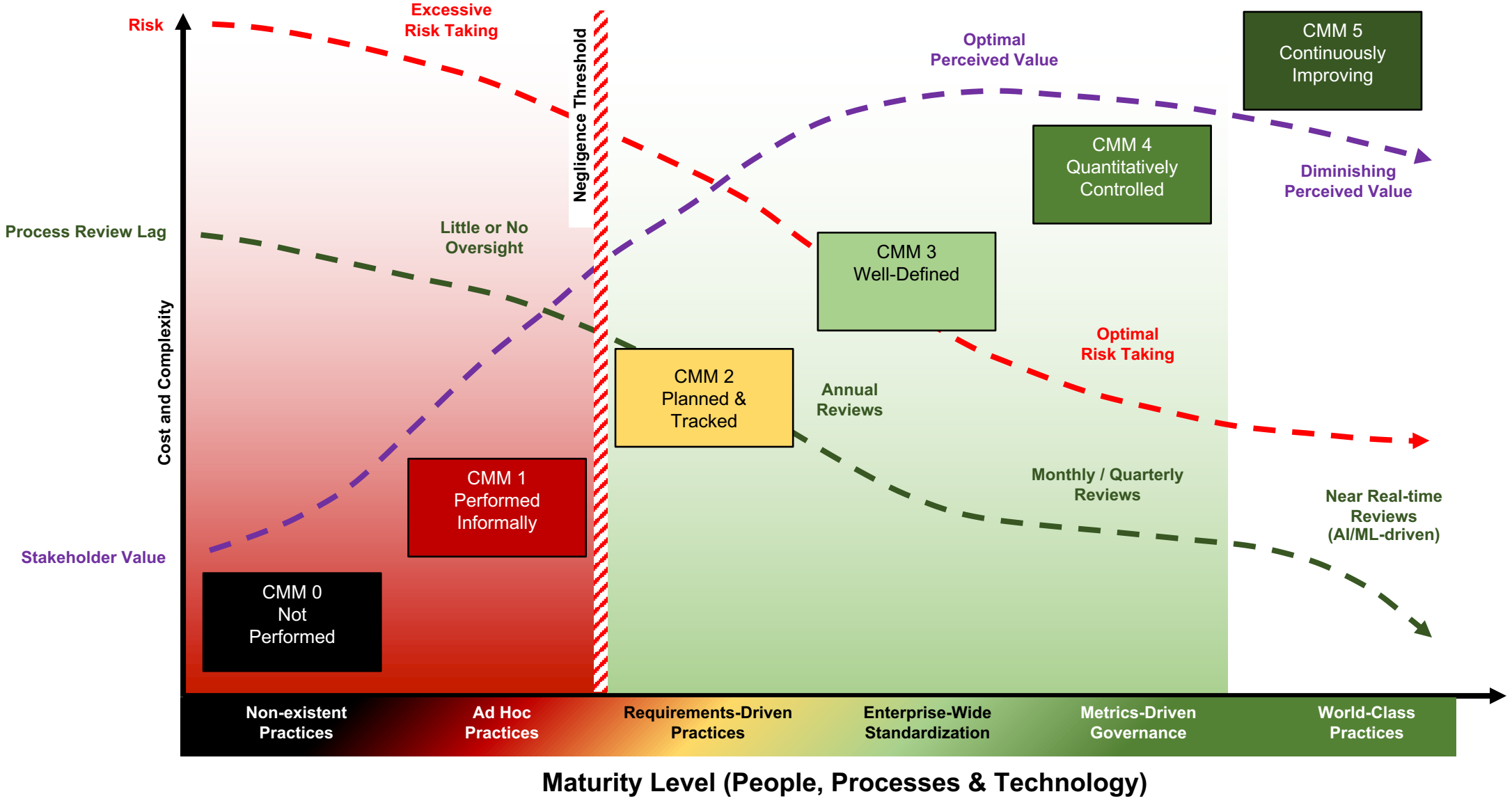
Measuring Capability

The method we've chosen is the **Capability Maturity Model** [1]. Developed in the mid-1980s for the US Department of Defense, this quantizes maturity into five (really six, when you add the true zero) levels. These are:

Level	Title	Description
0	Not Performed	No activities performed
1	Initial	*Ad hoc*, undocumented activities
2	Repeatable	Documented activities
3	Defined	Activities aligned to defined business processes
4	Capable	Activities managed via well-defined metrics
5	Efficient	Activity management includes process improvement

Phase	Phase Requirement	Description	Work Product	CMM Level	Notes
Foundation	Foundation-1	Training	training catalog	0 - none	
			system to track training participation	0 - none	
	Foundation-2	Roles and Responsibilities	roles and responsibilities document	0 - none	
	Foundation-3	Toolchain Support	list of approved tools and components	0 - none	
	Foundation-4	Definition of Security Requirements	global security goals	0 - none	
			global security requirements	0 - none	
	Foundation-5	Protect the Code	code protection plan	0 - none	
	Foundation-6	Ensure Release Integrity	release integrity plan	0 - none	
	Foundation-7	Incident Response Plan	incident response plan	0 - none	
			continuous monitoring plan	0 - none	
	Foundation-8	Decommissioning Plan	decommissioning plan	0 - none	
	Foundation-9	Threat Prioritization Plan	threat prioritization plan	0 - none	
	Foundation-10	Deployment Plan	deployment plan	0 - none	
Requirer	Requirements-1	Definition of Security Requirements	product-level security goals	0 - none	
			product-level security requirements	0 - none	
	Requirements-2	Requirements Gate	formal gate signoff	0 - none	
Design	Design-1	Take Security Requirements and Risk Information into Account During Software Design	design showing security considerations	0 - none	
	Design-2	Review the Software Design to Verify Compliance with Security Requirements and Risk Information	security design review report	0 - none	
	Design-3	Attack Surface Reduction	attack surface analysis report	0 - none	
	Design-4	Threat Modeling	threat modeling report	0 - none	
			ranked/risked threat report	0 - none	
			threat report	0 - none	
	Design-5	Design Gate	formal gate signoff	0 - none	
Implementation	Implementation-1	Use Approved Tools	list of tools and components used	0 - none	
	Implementation-2	Configure the Compilation and Build Process to Improve Executable Security	build process documentation	0 - none	
	Implementation-3	Configure the Software to Have Secure Settings by Default	secure setting document	0 - none	
	Implementation-4	Reuse Existing, Well-Secured Software When Feasible Instead of Duplicating Functionality	component/version - product/version cross-reference document	0 - none	
	Implementation-5	Create Source Code Adhering to Secure Coding Practice	secure development	0 - none	
	Implementation-6	Deprecate Unsafe Functions	currently used deprecated functions document	0 - none	
	Implementation-7	Static Analysis	static analysis report	0 - none	
	Implementation-8	Dynamic Program Analysis	dynamic analysis report	0 - none	
	Implementation-9	Security Code Review	secure code review summary	0 - none	
	Implementation-10	Fuzz Testing	fuzz testing report	0 - none	
	Implementation-11	Implementation Gate	formal gate signoff	0 - none	
Verification	Verification-1	Penetration Testing	penetration testing report	0 - none	
	Verification-2	Threat Model Review	updated threat model	0 - none	
	Verification-3	Attack Surface Analysis Review	updated attack surface analysis	0 - none	
	Verification-4	Verification Gate	formal gate signoff	0 - none	
Release	Release-1	Final Security Review	final security review report	0 - none	
	Release-2	Archive	archive manifest	0 - none	
	Release-3	Release Gate	formal gate signoff	0 - none	
Operation	Operation-1	Identify and Confirm Vulnerabilities on an Ongoing Basis		0 - none	
	Operation-2	Assess and Prioritize the Remediation of all Vulnerabilities	cybersecurity incident report	0 - none	
	Operation-3	Analyze Vulnerabilities to Identify Their Root Causes		0 - none	
	Operation-4	Secure Deployment	software deployment report	0 - none	
De	Decommissioning-1	Apply Decommissioning Protocol	decommissioning report	0 - none	

Not Enough vs. Too Much *

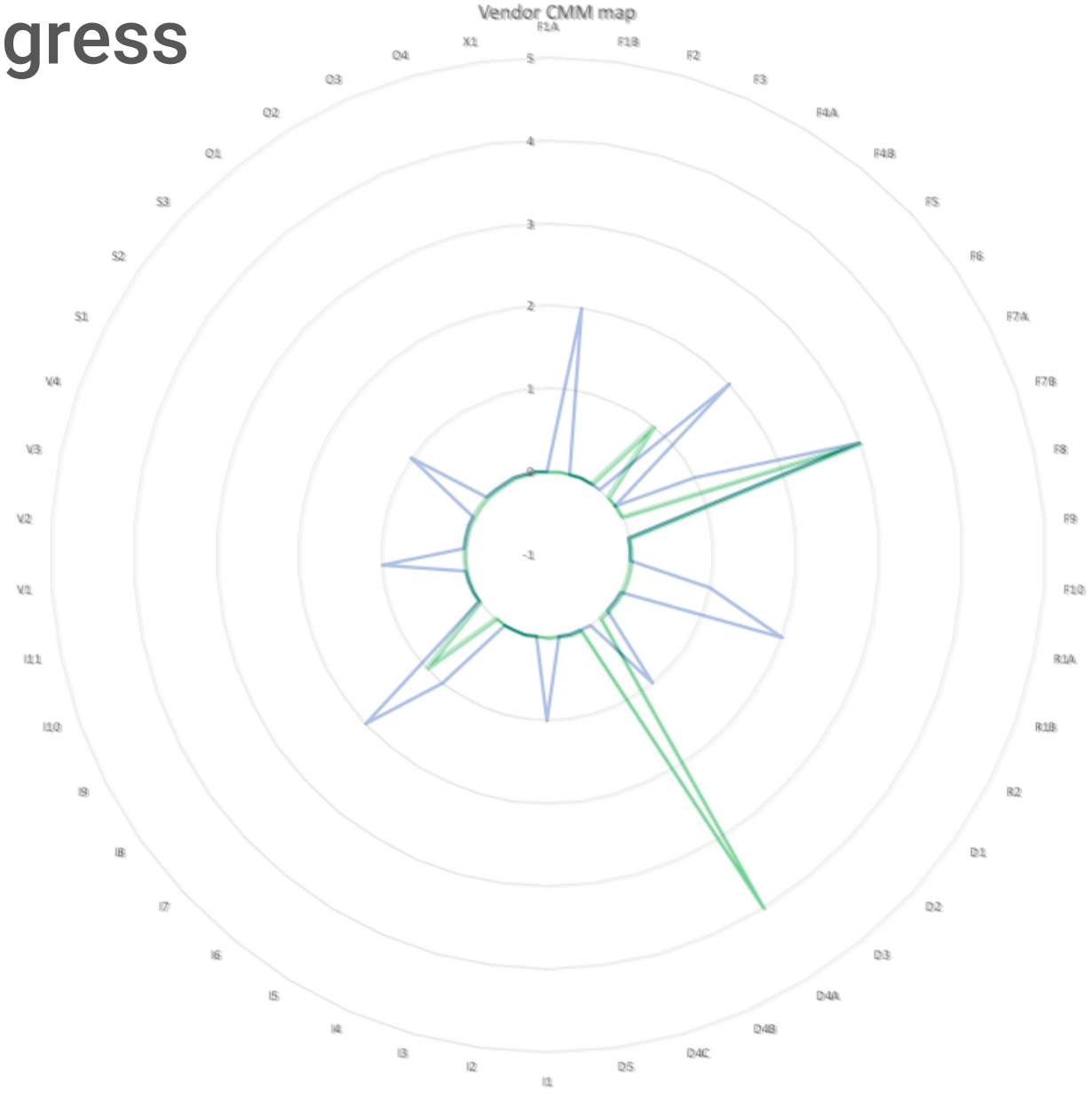


* **CMM level and CMM Sweet Spot images** (link in references)

Maturity Summary

Phase	Phase Requirement	Description	Work Product	Primary RASIC		Confidentiality Level	CMM Level
				Supplier	Customer		
Foundation	Foundation-1	Training	training catalog	Responsible	Responsible	Public	0 - none
			system to track training participation	Responsible	Responsible	Confidential with Third Parties	0 - none
	Foundation-2	Roles and Responsibilities	roles and responsibilities document	Responsible	Responsible	Public	0 - none
	Foundation-3	Toolchain Support	list of approved tools and components			Confidential with Third Parties	0 - none
	Foundation-4	Definition of Security Requirements	global security goals	Inform	Responsible	Confidential	0 - none
			global security requirements	Inform	Responsible	Confidential	0 - none
	Foundation-5	Protect the Code	code protection plan			Confidential	0 - none
	Foundation-6	Ensure Release Integrity	release integrity plan			Confidential	0 - none
	Foundation-7	Incident Response Plan	incident response plan	Responsible	Responsible	Confidential with Third Parties	0 - none
			continuous monitoring plan	Responsible	Responsible	Confidential with Third Parties	0 - none
	Foundation-8	Decommissioning Plan	decommissioning plan	Responsible	Responsible	Confidential	0 - none
	Foundation-9	Threat Prioritization Plan	threat prioritization plan			Confidential	0 - none
	Foundation-10	Deployment Plan	deployment plan			Confidential	0 - none
Requirer	Requirements-1	Definition of Security Requirements	product-level security goals	Inform	Responsible	Confidential	0 - none
			product-level security requirements	Support	Responsible	Confidential	0 - none
	Requirements-2	Requirements Gate	formal gate signoff	Support	Responsible	Confidential	0 - none
Design	Design-1	Take Security Requirements and Risk Information into Account During Software Design	design showing security considerations			Confidential	0 - none
	Design-2	Review the Software Design to Verify Compliance with Security Requirements and Risk Information	security design review report			Confidential	0 - none
	Design-3	Attack Surface Reduction	attack surface analysis report			Confidential	0 - none
	Design-4	Threat Modeling	threat modeling report			Highly Confidential	0 - none
			ranked/risked threat report			Highly Confidential	0 - none
			threat report			Highly Confidential	0 - none
	Design-5	Design Gate	formal gate signoff	Support	Responsible	Confidential	0 - none
Implementation	Implementation-1	Use Approved Tools	list of tools and components used	Responsible	Consult	Confidential	0 - none
	Implementation-2	Configure the Compilation and Build Process to Improve Executable Security	build process documentation	Responsible	Consult	Highly Confidential	0 - none
	Implementation-3	Configure the Software to Have Secure Settings by Default	secure setting document	Responsible	Consult	Confidential	0 - none
	Implementation-4	Reuse Existing, Well-Secured Software When Feasible Instead of Duplicating Functionality	component/version - product/version cross-reference document	Responsible	Consult	Confidential	0 - none
	Implementation-5	Create Source Code Adhering to Secure Coding Practice	secure development	Responsible	Consult	Confidential	0 - none
	Implementation-6	Deprecate Unsafe Functions	currently used deprecated functions document	Responsible	Consult	Confidential	0 - none
	Implementation-7	Static Analysis	static analysis report	Responsible	Consult	Highly Confidential	0 - none
	Implementation-8	Dynamic Program Analysis	dynamic analysis report	Responsible	Consult	Highly Confidential	0 - none
	Implementation-9	Security Code Review	secure code review summary	Responsible	Consult	Highly Confidential	0 - none
	Implementation-10	Fuzz Testing	fuzz testing report	Responsible	Consult	Highly Confidential	0 - none
	Implementation-11	Implementation Gate	formal gate signoff	Support	Responsible	Highly Confidential	0 - none
Verification	Verification-1	Penetration Testing	penetration testing report			Confidential with Third Parties	0 - none
	Verification-2	Threat Model Review	updated threat model			Highly Confidential	0 - none
	Verification-3	Attack Surface Analysis Review	updated attack surface analysis			Confidential	0 - none
	Verification-4	Verification Gate	formal gate signoff	Support	Responsible	Confidential	0 - none
Release	Release-1	Final Security Review	final security review report	Inform	Responsible	Confidential	0 - none
	Release-2	Archive	archive manifest	Responsible	Inform	Confidential	0 - none
	Release-3	Release Gate	formal gate signoff	Support	Responsible	Confidential	0 - none
Operation	Operation-1	Identify and Confirm Vulnerabilities on an Ongoing Basis	cybersecurity incident report	Support	Responsible	Confidential with Third Parties	0 - none
	Operation-2	Assess and Prioritize the Remediation of all Vulnerabilities		Support	Responsible	Confidential with Third Parties	0 - none
	Operation-3	Analyze Vulnerabilities to Identify Their Root Causes				Confidential with Third Parties	0 - none
	Operation-4	Secure Deployment	software deployment report			Confidential	0 - none
De	Decommissioning-1	Apply Decommissioning Protocol	decommissioning report	Support	Responsible	Confidential	0 - none

Visualizing Progress



Supplier Cybersecurity Process Mapping

Process Mapping Material

Understanding Supplier Cybersecurity Process Mapping

Revision

Version 4
3/12/24 5:37 PM

Author

Charles Wilson

Abstract

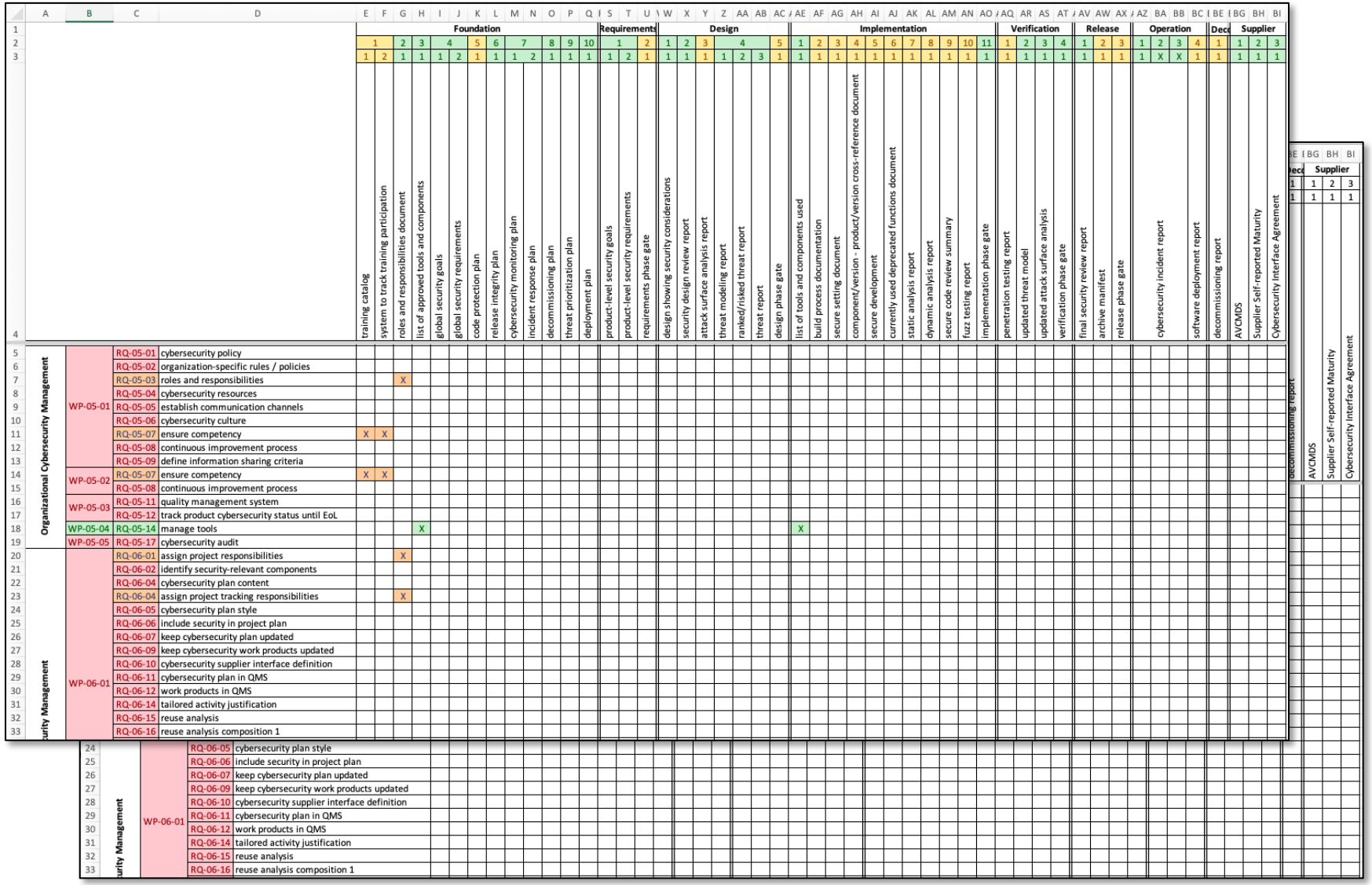
This document explains the means by which a supplier's cybersecurity processes can be mapped onto the **AVCDL** phase requirements and products.

Audience

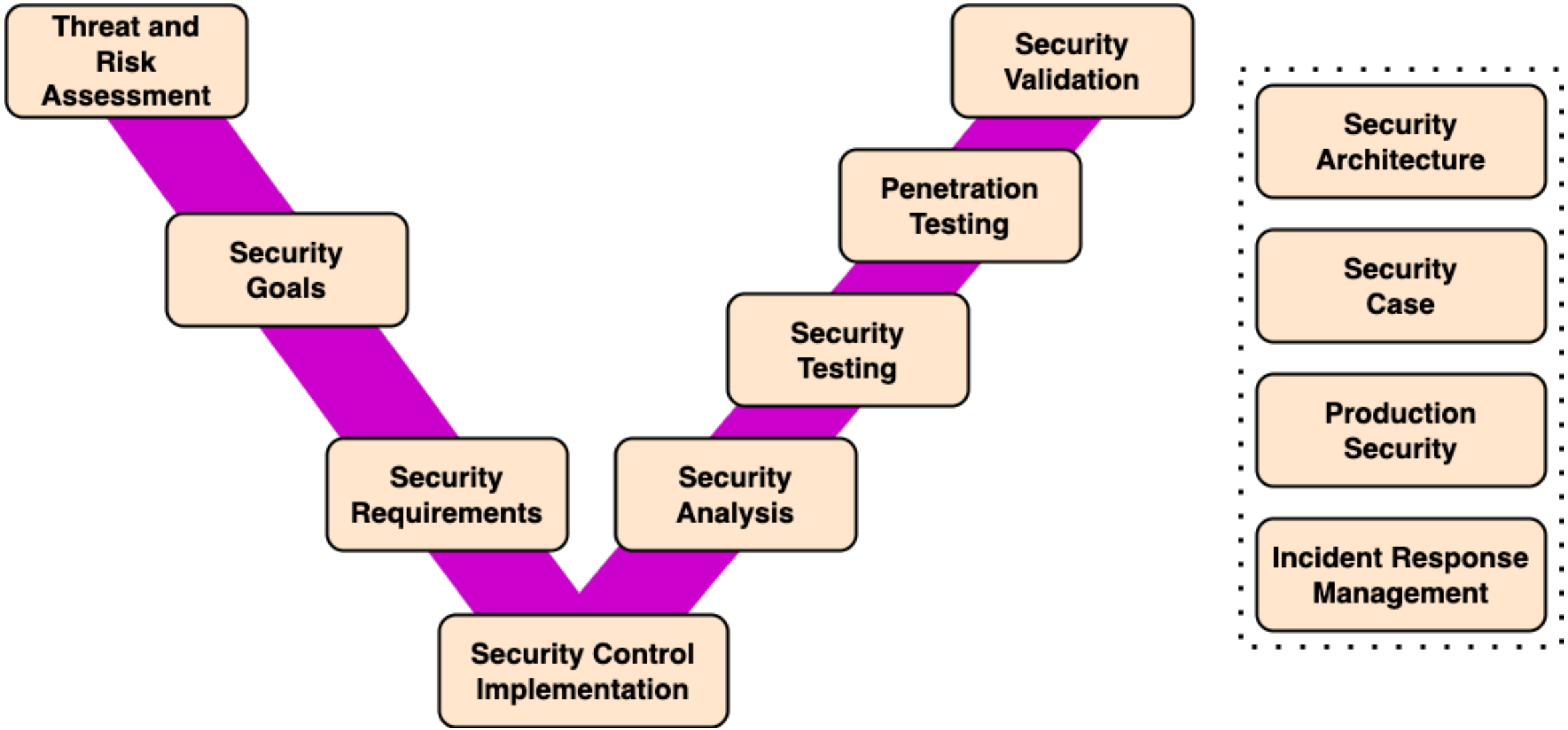
The audience of this document are those supplier cybersecurity SMEs tasked with interfacing to customers using the **AVCDL** as the basis for their product cybersecurity lifecycle.

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

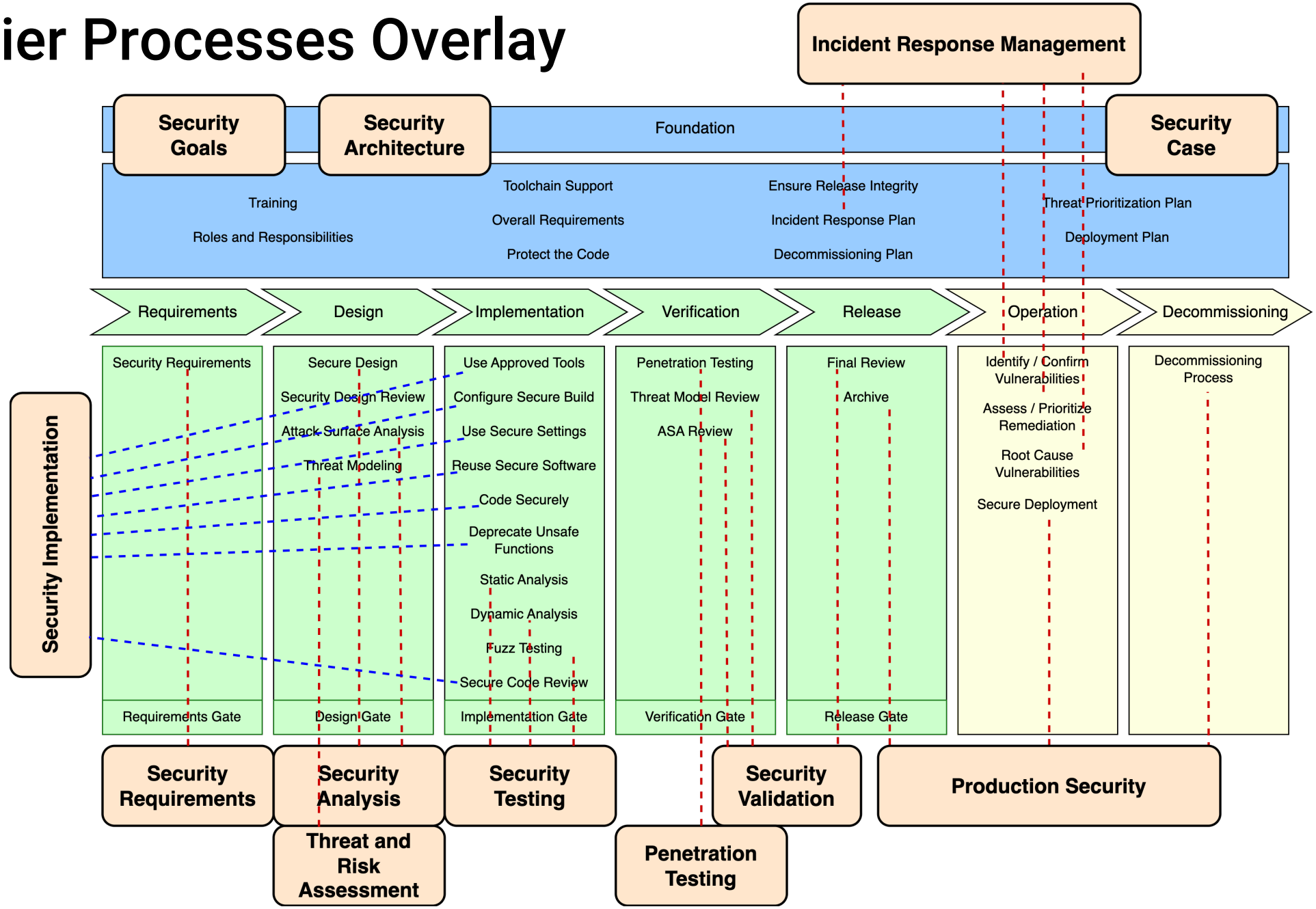
License



Supplier Processes

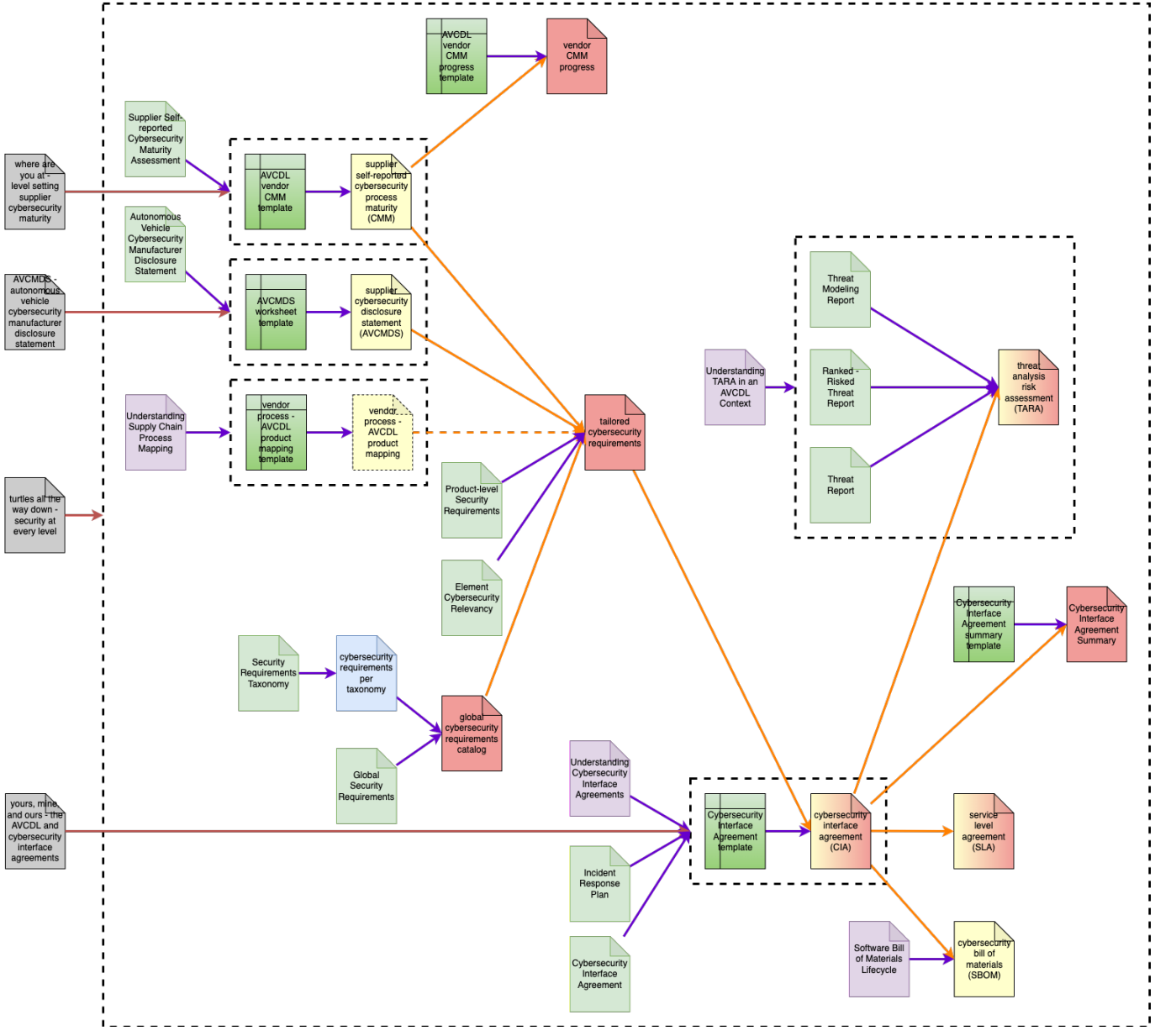


Supplier Processes Overlay



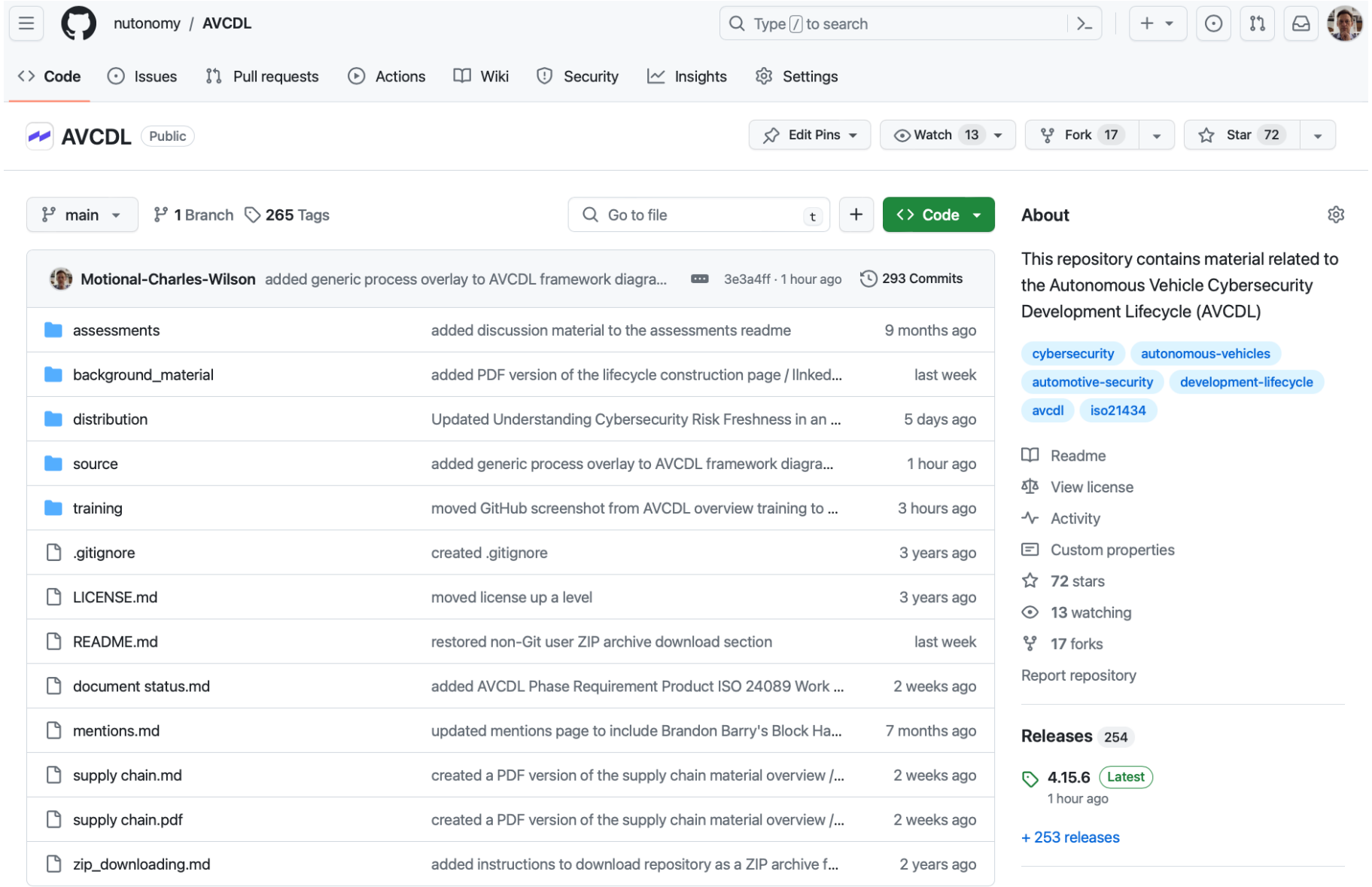
Where to Go From Here

Supply Chain Guidance Documents

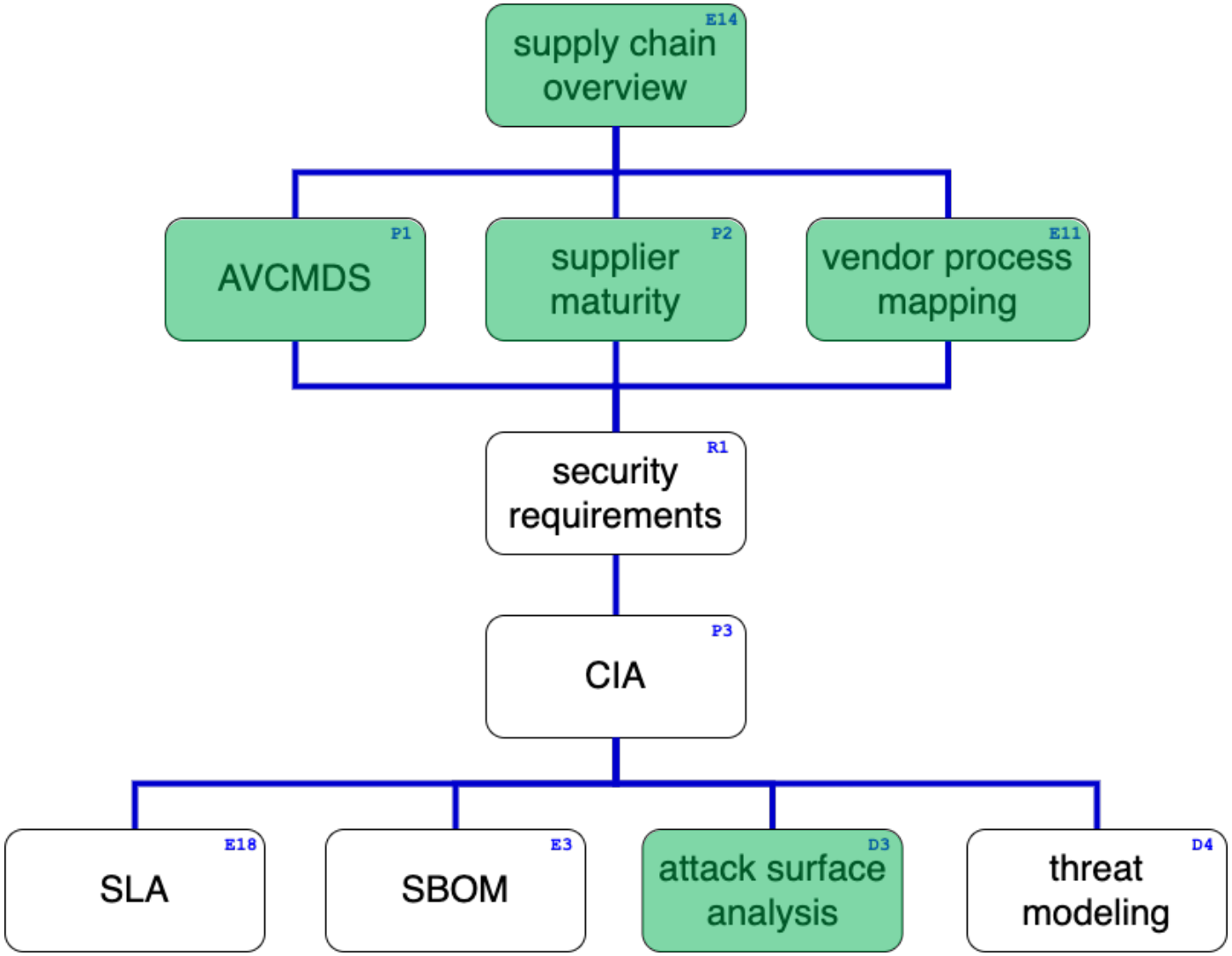


AVCDL on GitHub

https://github.com/nutonomy/AVCDL

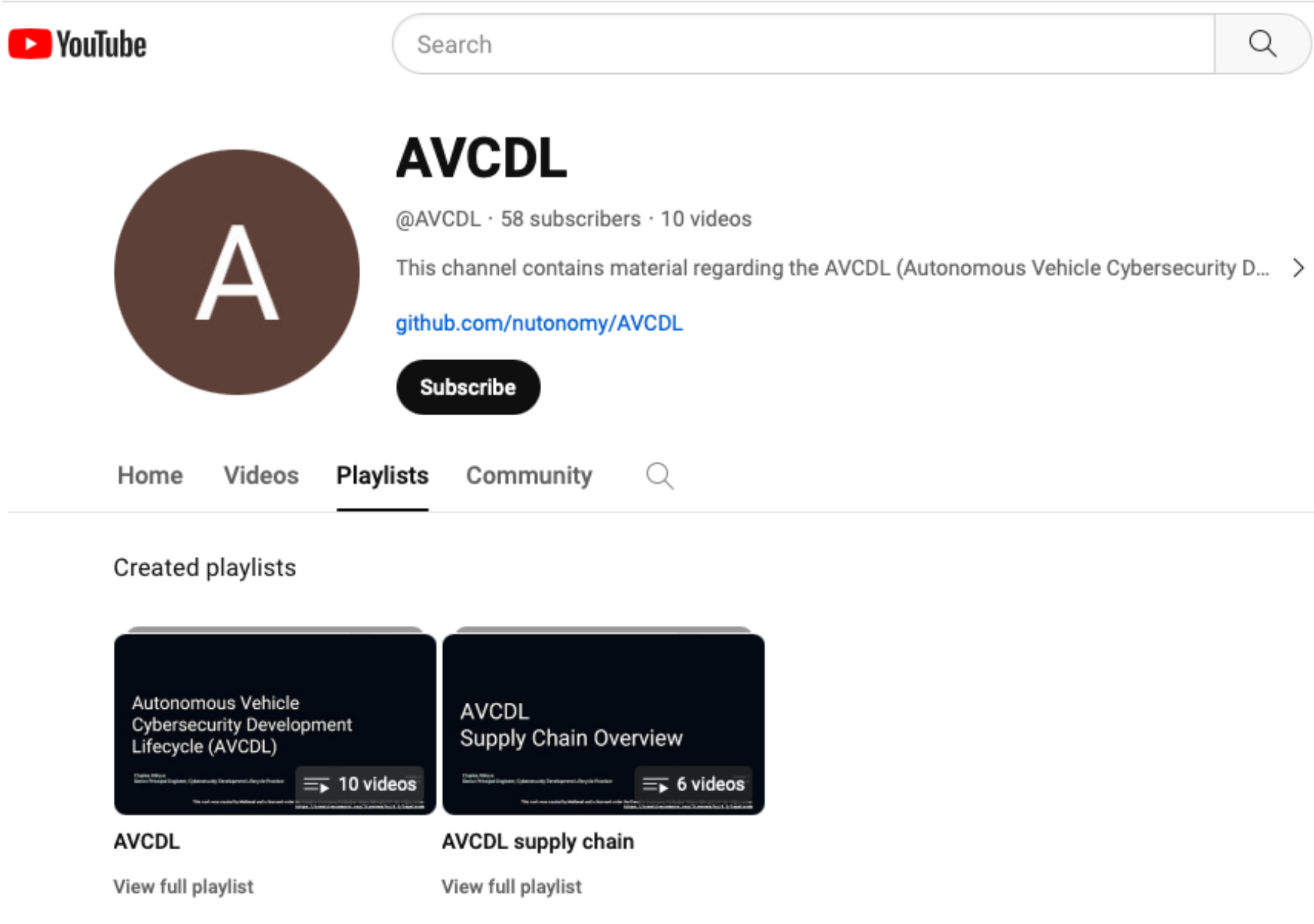


Supply Chain Training Path



AVCDL on YouTube

https://youtube.com/@AVCDL/playlists



Questions

References (1 of 3)

AVCDL (GitHub)
https://github.com/nutonomy/AVCDL

AVCDL (YouTube)
https://youtube.com/@AVCDL

Autonomous Vehicle Cybersecurity Manufacturer Disclosure Statement (AVCDL secondary document)

Supplier Self-reported Cybersecurity Maturity Assessment (AVCDL secondary document)

vendor process - AVCDL product mapping template (AVCDL template document)

Understanding Supplier Cybersecurity Process Mapping (AVCDL elaboration document)

Understanding Supply Chain Interaction in an AVCDL Context (AVCDL elaboration document)

AVCMDS: Autonomous Vehicle Cybersecurity Manufacturer Disclosure Statement (AVCDL blog post)

AVCDL CMM template (AVCDL template document)

AVCDL cybersecurity interface agreement summary template (AVCDL template document)

References (2 of 3)

Road vehicles – Cybersecurity engineering
https://www.sae.org/standards/content/iso/sae21434/

Road vehicles – Software update engineering
https://www.iso.org/standard/77796.html

UN Regulation No. 155 - Cyber security and cyber security management system
https://unece.org/transport/documents/2021/03/standards/un-regulation-no-155-cyber-security-and-cyber-security

UN Regulation No. 156 – Software update and software update management system
https://unece.org/transport/documents/2021/03/standards/un-regulation-no-156-software-update-and-software-update

UN Regulation No. 157 – Automated Lane Keeping Systems (ALKS)
https://unece.org/transport/documents/2021/03/standards/un-regulation-no-157-automated-lane-keeping-systems-alks

laying down rules for the application of Regulation (EU) 2019/2144 of the European Parliament and of the Council as regards uniform procedures and technical specifications for the type-approval of the automated driving system (ADS) of fully automated motor vehicles
https://eur-lex.europa.eu/legal-content/DA/TXT/?uri=PI_COM:Ares(2022)2667391

References (3 of 3)

Capability Maturity Model
https://en.wikipedia.org/wiki/Capability_Maturity_Model

ISO/IEC 21827 - Information technology — Security techniques — Systems Security Engineering — Capability Maturity Model® (SSE-CMM®)
https://www.iso.org/standard/44716.html

CMM level and CMM Sweet Spot images (CC BY-ND 4.0)
https://www.securecontrolsframework.com/sp-cmm