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

We can visualize this (and show relative cost / complexity) as follows:

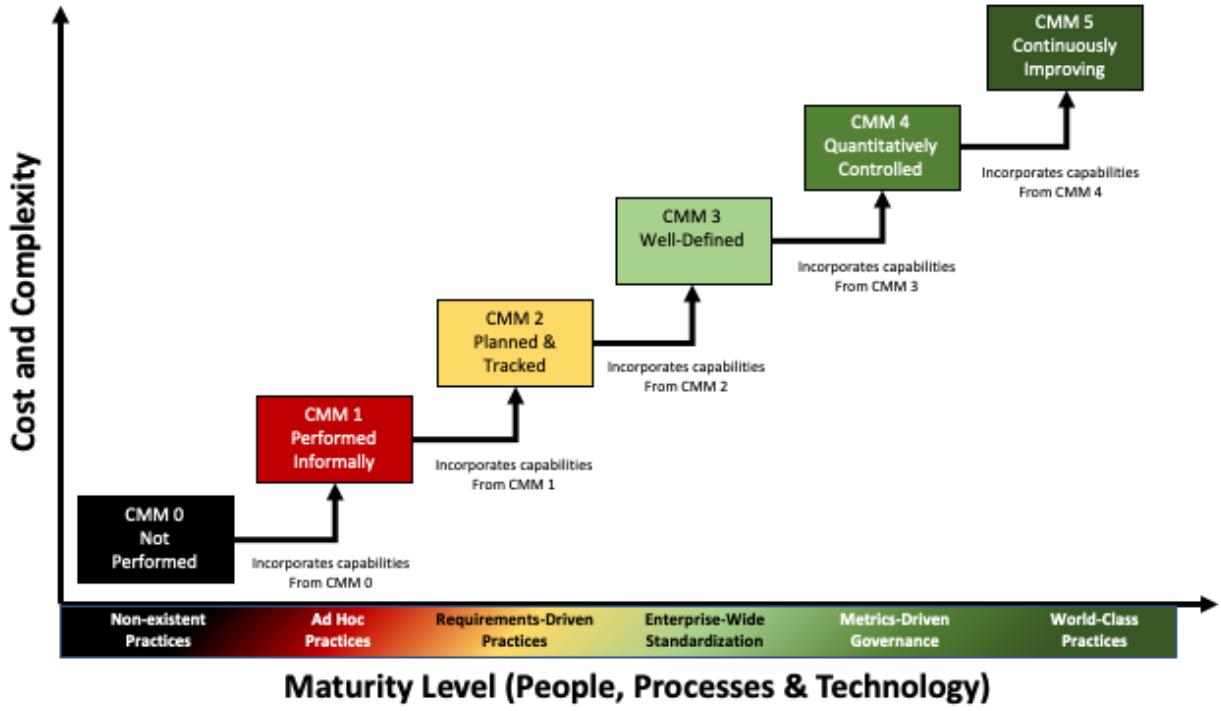

Figure 1 - Capability Maturity Levels [5]

We can enhance this diagram with information showing the interplay between the CMM levels and risk, process review lag, and shareholder value.

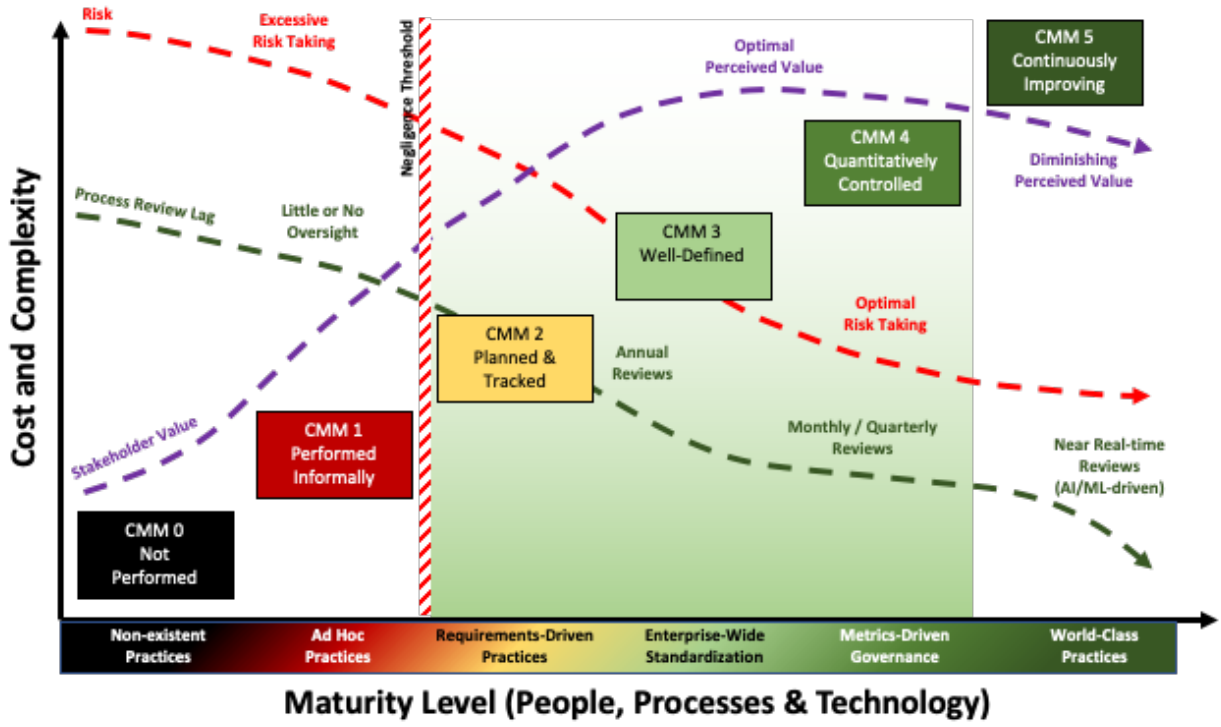

Figure 2 - Capability Maturity Sweet Spot [5]

Here we see a “sweet spot,” where perceived shareholder value is high, and both risk and process review lag are low. We can also see a negligence threshold between levels 1 and 2. This gives us an effective floor for desired maturity. At the other end of the spectrum, we can see that beyond level 4 the perceived value and risk level off. This is not to say that it is not desirable to attain level 5, but that one should recognize that there will likely be a high level of internal friction involved given the associated cost and complexity increase.

Covering Your Basis

With an understanding of how we’re going to quantify maturity, we turn to what we will measure. We will use the **AVCDL** [2] as the basis for evaluation. We use the AVCDL because it is built around the development lifecycle rather than any specific certification standard. This is because the **AVCDL** generalizes the cybersecurity needs of standards such as ISO 21434, ISO 26262, and UNECE WP.29 R155. So long as the **AVCDL** can be shown to satisfy any arbitrary certification standard, the maturity information will be transferable.

Know Thy Self

The maturity information is gathered via a simple spreadsheet (AVCDL CMM) [6].

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	

This spreadsheet covers all **AVCDL** phase requirements and their associated products. Suppliers are asked to self-report their maturity for each of the phase requirement products. They may also provide notes for each.

We can then take the provided information a render a radar diagram of the answers.

Trust, but Verify

It's really important to sanity-check the self-reported maturity values. If a supplier asserts that they are at level 1 (*ad hoc* activity), ask to see the products. If the supplier asserts that an activity has a maturity of level 2 (documented activity), ask to see the documentation. These are things that will come up in an audit, so suppliers should have no excuse in producing material to support their claims. Additionally, this information will be used in the creation of the cybersecurity interface agreement, so accuracy matters. An activity with a maturity level of 0 would necessitate that either the customer or a third party be used in order to ensure that the activity is properly handled.

How the AVCMDS and AVCDL CMM Differ

Where the AVCMDS gave us a snapshot of cybersecurity technical posture, the AVCDL CMM gives us insight into the cybersecurity process posture. It shows us supplier strengths and weaknesses with respect to supporting their cybersecurity efforts. This is critical in determining whether a supplier is capable of undertaking the activities necessary to ensure the cybersecurity of the element they would provide. It is also a major input into the cybersecurity interface agreement.

Bringing Things Together

In the next post in this series, we'll consider how to establish the division of responsibilities using a cybersecurity interface agreement. We'll also show how the AVCMDS and AVCDL CMM inform the completion of that document.

References

1. **Capability Maturity Model**
   https://en.wikipedia.org/wiki/Capability_Maturity_Model
2. **Autonomous Vehicle Cybersecurity Development Lifecycle (AVCDL)**
   https://github.com/nutonomy/AVCDL
3. **ISO/IEC 21827 - Information technology — Security techniques — Systems Security Engineering — Capability Maturity Model® (SSE-CMM®)**
   https://www.iso.org/standard/44716.html
4. **Systems Security Engineering Capability Maturity Model – Model Description Document Version 2.0 (1999-01-04)**
   https://apps.dtic.mil/dtic/tr/fulltext/u2/a393329.pdf
5. **CMM level and CMM Sweet Spot images (CC BY-ND 4.0)**
   https://www.securecontrolsframework.com/sp-cmm
6. **AVCDL CMM template**
   https://github.com/nutonomy/AVCDL/blob/main/distribution/reference_documents/templates/AVCDL%20vendor%20CMM%20template.xlsx