# Title

I'm Charles Wilson, senior principal engineer at motional responsible for cybersecurity development lifecycle practice.

This presentation will cover the supplier self-report maturity documentation.

# Supply Chain Training Path

# This diagram shows the overall AVCDL supply chain training path.

# If you're taking this training, it's assumed that you've already completed the supply chain overview training.

# This training covers the supplier self-report cybersecurity maturity documentation.

# Additional trainings will cover:

# manufacturer disclosure statement (AVCMDS),

# vendor cybersecurity process to AVCDL mapping,

# cybersecurity requirements,

# tailoring the cybersecurity interface agreement,

# service level agreements (SLAs),

# software bill of materials (SBOM),

# attack surface analysis,

# and threat modeling.

# Introduction

Let's say your country has just decided that they want to go to the moon and you're responsible for getting them there.

Everyone knows what the moon looks like.

Everyone knows where the moon is.

But how are you going to get there?

Let's consider some of the aspects from the Apollo program and see how they fit into supplier maturity.

# Introduction – Flight Profile

The first thing you're going to need is an overall plan.

Something that tells you how to get from where you are to where you want to go, establishes terminology, and sets the ground rules.

# Introduction – Spacecraft

You’ll need to establish an architecture that lays out the major pieces of the system that you're going to build.

# Introduction – Camera

You'll need to break down each subsystem, component and device until you've established the smallest unit to be used in the system.

# Introduction – Training

Because this is a highly technical and safety critical activity, you're going to want to ensure that everyone is appropriately trained, whether they be those building the system or those using it.

# Introduction – Simulator

Because of the risks involved, you’ll need to ensure that there's been adequate testing and simulation to identify and eliminate any issues in the system.

# Introduction – Documentation

System procedures will be both detailed and well documented.

# Introduction – Egress System

Emergency situations must be identified, considered and their risks mitigated.

# Introduction – TV Schedule

The operational phase must be given the same level of attention as the design and the production phases.

<pause>

So how does the preparation for a mission to the moon relate to the AVCDL?

And how does it relate to supplier maturity?

# AVCDL

The AVCDL is a framework that covers all the points from our Apollo example, as well as many others.

Because of its scope, detail and availability, we will use the AVCDL as the basis for evaluating the maturity of our suppliers.

For more details on the framework, refer to the AVCDL overview training.

# Supplier Self-reported Maturity Use in Supplier Selection

There are three documents within the AVCDL document set that support the creation of the AVCMDS.

# AVCMDS Documentation

This diagram shows the major documents used in both the supplier selection request for information (RFI) and request for quote (RFQ) activities, as well as the development production and post-production activities.

The **supplier self-reported maturity** and the **supplier cybersecurity manufacturer's disclosure statement** are the two primary documents which enable us to create **tailored cybersecurity requirements**

and the **cybersecurity interface agreement.**

The CMM and AVCMDS are key to establishing the **cybersecurity interface agreement** because they allow us to identify gaps in the supplier's cybersecurity posture,

so that they can be addressed before implementation begins.

As-Is Assessment

It's important to emphasize that for the **supplier self-reported maturity** to be a useful source of information, it has to be done as an as-is assessment.

It shows where the maturity of the supplier stands today, not what the ideal will be someday.

The point of this is not to be punitive, but rather as stated earlier, to identify gaps so that those gaps can be addressed ensuring the cybersecurity posture of the end product.

Supplier Self-reported Maturity Material

There are three documents within the AVCDL document set that support the creation of the supplier’s self-report maturity.

These are

* the **Supplier Self-reported Cybersecurity Maturity Assessment** secondary document
* the blog post **Where are You at? Level Setting Supplier Cybersecurity Maturity**
* and the **AVCDL vendor CMM template** spreadsheet.

Supplier Self-reported Maturity Documentation

Here you can see the relationship between the various AVCDL documents covering the supplier’s self-report maturity.

We can see that the **AVCDL vendor CMM template** is used to create the **supplier self-reported cybersecurity process maturity** document. A specific instance of the CMM template.

Once completed, the supplier’s maturity is tracked over time via a **vendor CMM progress** spreadsheet.

The dotted lines surrounding those two documents Is used to indicate that both the **Supplier Self-reported Cybersecurity Maturity Assessment** secondary document and the **Where are You at? Level Setting Supplier Cybersecurity Maturity** blog posts refer to both of those documents taken together.

Maturity Level vs. Cost and Complexity

Let's consider process maturity level versus its cost and complexity.

On the X axis, we can see the maturity level.

This can represent processes, people, or technology.

On the Y axis, we show the cost and complexity of implementation.

Maturity Level vs. Cost and Complexity – CMM 0

At maturity level zero (here noted as CMM zero), nothing is done.

There are no practices in place for the particular activity, unless otherwise specifically indicated.

This is going to be our base assumption.

Maturity Level vs. Cost and Complexity – CMM 1

At level one, there are some cybersecurity practices being done but they're being done informally.

Either they're not documented or they're just tribal knowledge.

There are at least some cybersecurity activity happening.

Maturity Level vs. Cost and Complexity – CMM 2

At level two, we see cybersecurity activities are being planned and tracked.

This takes things beyond tribal knowledge.

Cybersecurity activities are being done intentionally. They tend to be requirements-driven and reviewed for results.

Now, a thing you'll note here is that there's a black connecting line which says that this incorporates the capabilities from CMM level one.

You never lose anything as processes mature.

You're merely making the process more sophisticated.

Maturity Level vs. Cost and Complexity – CMM 3

An organization that has level three processes is applying them consistently across the organization.

It’s no longer just a single team or group using them.

The process is used consistent manner in all of the products.

Maturity Level vs. Cost and Complexity – CMM 4

At CMM Level four, cybersecurity activities are being quantitatively controlled.

There is consistent process usage across the organization with the processes being planned, track, and driven by requirements.

And then the metrics being tracked are used to make decisions as to refining and updating of the processes.

Maturity Level vs. Cost and Complexity – CMM 5

A CMM Level five process is one which undergoes continuous improvement.

This is a process doing everything right.

It's being tracked, is well defined, planned, and metrics are used to keep things up-to-date.

This is an absolutely best-in-class process.

Not Enough vs. Too Much

As you can imagine, the more sophisticated your processes are the higher the cost and the complexity of implementing them is going to be.

So, let's step back and consider a couple of different pieces of information that we can overlay onto these and get an idea of how to set our expectations.

Not Enough vs. Too Much – Shareholder Value

First, we'll look at shareholder value.

This is a perceptual issue.

When we have no processes, there’s no perceived ROI.

As we implement more and more sophisticated processes, we can show that we have greater value.

However, at a certain point, somewhere around the CMM level three and 4 area, we reach peak perceived value.

Beyond that point, it's really difficult for an outside observer to appreciate the value add being contributed.

Not Enough vs. Too Much – Process Review Lag

Now let’s consider process review lag.

This is our ability to track and to adjust the processes themselves.

At CMM levels zero and one, we have little to no oversight and so little to no visibility as to the effectiveness of the process.

At around CMM level three, we're applying annual reviews.

By CMM level four, we're looking at processes on a quarterly or monthly basis.

Finally, at CMM level five, we're doing near real-time reviews. Here you'll see things like AI- and ML-driven reviews that are processing things for you.

Not Enough vs. Too Much – Risk

The final aspect to look at, and arguably the most important, is risk.

At the low end of the maturity scale there's an excessive amount of risk being taken because the processes aren't in place to apply cybersecurity controls.

At around CMM level four, you've reached an optimal risk-taking level.

And from there on out it, risk basically plateaus again because we're not adding additional controls, we’re merely tweaking the processes themselves.

Not Enough vs. Too Much – Negligence Threshold

In fact, we can establish a negligence threshold between CMM level one and two because the amount of risk is so high.

Any objective third-party would look at the lack of processes in place to ensure that cybersecurity controls are applied

and say that there is simply no reason why they're not being used and tracked.

Not Enough vs. Too Much – Sweet Spot

This brings us to the maturity sweet spot.

It's above the negligence threshold.

It's below the diminished perceived value area.

It doesn't rely on using AI and ML to drive things.

It's within the bounds of optimal risk taking.

Generally speaking, preforming at CMM levels two, three, or four, gets the best return on investment.

Supplier Self-reported Maturity Workflow

With the background material covered, let’s turn our attention to the assessment process.

Here's the workflow used to create the supplier’s self-reported maturity.

This diagram is taken from the **Supplier Self-reported Cybersecurity Maturity Assessment** secondary document.

As you can see, there are two activities that take place, the processes assessment and the assessment review.

In the processes assessment activity, the supplier’s cybersecurity SME uses the supplier’s cybersecurity processes to complete the **AVCDL vendor CMM template**.

This results in the creation of a **supplier self-reported cybersecurity maturity draft** document specific to the supplier.

This draft is then reviewed by the customer’s cybersecurity SME.

Any deficiencies found are fed back to the supplier to create an update of the draft.

Once it's been determined that there are no deficiencies the document is considered to be final and is entered into the customer's document tracking system.

Supplier Self-reported Maturity Worksheet

Now let's go over some general information that you'll need in order to fill out the **supplier self-reported maturity** worksheet.

Worksheet Columns

Each AVCDL phase requirement product is listed on its own line, and each line has six columns associated with it.

The first three columns roll up the phase requirement products into their corresponding phase requirement and phase.

The fields specific to each phase requirement product include

* the phase requirement product’s description (typically, the corresponding AVCDL secondary document’s name)
* the CMM level
* And a note (should one be necessary)

Answer Options

The CMM level is entered via drop-down (as shown here).

The options are listed as the CMM level and a short description

These are:

* 0 - none
* 1 - performed
* 2 - documented
* 3 - managed
* 4 - reviewed
* 5 - optimizing

Legend

The template workbook contains a legend sheet that provides a longer description for each of the CMM levels.

For greater detail, review the SEI CMM documentation.

Understanding the AVCDL Phase Requirements

In order to complete the maturity assessment, it's necessary that the supplier review the AVCDL documentation.

The starting point for this is the AVCDL primary document itself.

This provides the overview of the cybersecurity development lifecycle and establishes the framework upon which both the phases and the phase requirements exist.

Understanding the AVCDL Phase Requirements - 2

Within the AVCDL primary document each of the phase requirements is listed.

For each of the phase requirements, summary information and a list of secondary documents elaborating on that material is provided.

Understanding the AVCDL Phase Requirements - 3

The secondary documents referred to in the phase requirements shown in the AVCDL primary document contain detailed information as to the processes that are expected to take place in order to satisfy the phase requirement.

Always Verify

Once the supplier returns the self-reported maturity document, it's important that the customer verify the CMM levels provided for each of the phase requirement products.

This is true regardless of CMM level.

This information should be used to inform the amount of support that a supplier may need in order to satisfy the cybersecurity requirements and posture necessary for the product.

Whenever a CMM level is called out which would have associated evidence, the customer should feel comfortable in requesting samples of this evidence in order to verify that the level specified is justified.

Supplier Self-reported Maturity Progress Tracking

As mentioned earlier,

Once completed, the supplier’s maturity is tracked over time via a **vendor CMM progress** spreadsheet.

Let’s see that spreadsheet looks like.

Maturity Summary

We can track the maturity using the **AVCDL cybersecurity interface agreement summary** template, spreadsheet.

This spreadsheet includes is a column for the CMM level.

Additional information of the RASICs and confidentiality level can be ignored in the context of the supplier’s cybersecurity maturity.

To track this information over time, the sheet can be duplicated with each new sheet having the time stamp of the assessment being included on it.

This material can then be used to form a series of charts depicting visually how the cybersecurity posture of the supplier is changing over time.

Visualizing Maturity

The **AVCDL cybersecurity interface Agreement summary** template also provides a sheet which visualizes the maturity information.

Here we can see a sample visualization.

Around the circumference are listed each of the AVCDL phase requirement product IDs, and radially depicted is the CMM level.

The use of negative one as the center simply allows us to have zero in a way which is more visually impactful.

This representation gives us a visual fingerprint that allows us to very rapidly take in the state of the supplier’s cybersecurity maturity.

Visualizing Progress

Over time, we can take these data series and overlay them to get a good idea of the dynamics of the progress that an organization is making,

both advancing and regressing in terms of their cybersecurity posture.

AVCDL on GitHub

All AVCDL materials, both in source and distribution forms, are available on our GitHub site, as shown here.

Because of the size of the repository, it's recommended that you either clone the repository or download a ZIP archive of it, if you're not familiar with using git.

Instructions for downloading a ZIP archive are linked to on the repository’s front page.

Supply Chain Training Path – Next Steps

The next step in this training sequence is to complete the two other courses at this level, if you haven’t already.

The **AVCMDS** training, covers the supplier’s cybersecurity manufacturer disclosure statement.

The **vendor process mapping** training covers how to take established vendor processes and map them to the corresponding AVCDL processes.

This helps to ensure that no gaps will exist between the vendor and the customer in the area of cybersecurity.

Once the three trainings at this level are complete, you should proceed to the **security requirements** training.

References

Here are references to the source material used in the creation of this presentation.

They'll also be included in the video description.

Additionally, this presentation’s source material will be provided on the AVCDL GitHub repository.