309 SWEG Supply Chain Risk Management Center of Excellence

A System Engineer's Approach to Software SCRM

Alexander Wright
Parker Bauer

BLUF

- **Supply Chain Risk Management (SCRM) as related to software, firmware, and cyber physical systems is about eliminating vulnerabilities that adversaries may attack in DoD, Federal, and private sector critical infrastructure systems. As system engineers, we need to learn how to integrate SCRM into our processes and increase the likelihood that:**
  - **software and firmware is secure**
  - **the supply chains producing it is secure**
  - **the final customer is shielded from lower tiers of the supply chain where vetting is difficult**

Who We Are

Parker Bauer

- Computer Scientist/Mechanical Engineer
- Six Sigma Black Belt
- Private industry supplier quality auditor
- Director of USAF Software Technology Support Center
- Hill AFB
- Co-lead of USAF 309 SWEG C-SCRM CoE

Alexander Wright

- Computer scientist and a member of the 309 Software Engineering Group.
- Worked on a number of air and space systems and became involved in SCRM in 2018
- Peterson AFB
- Co-lead of USAF 309 SWEG C-SCRM CoE

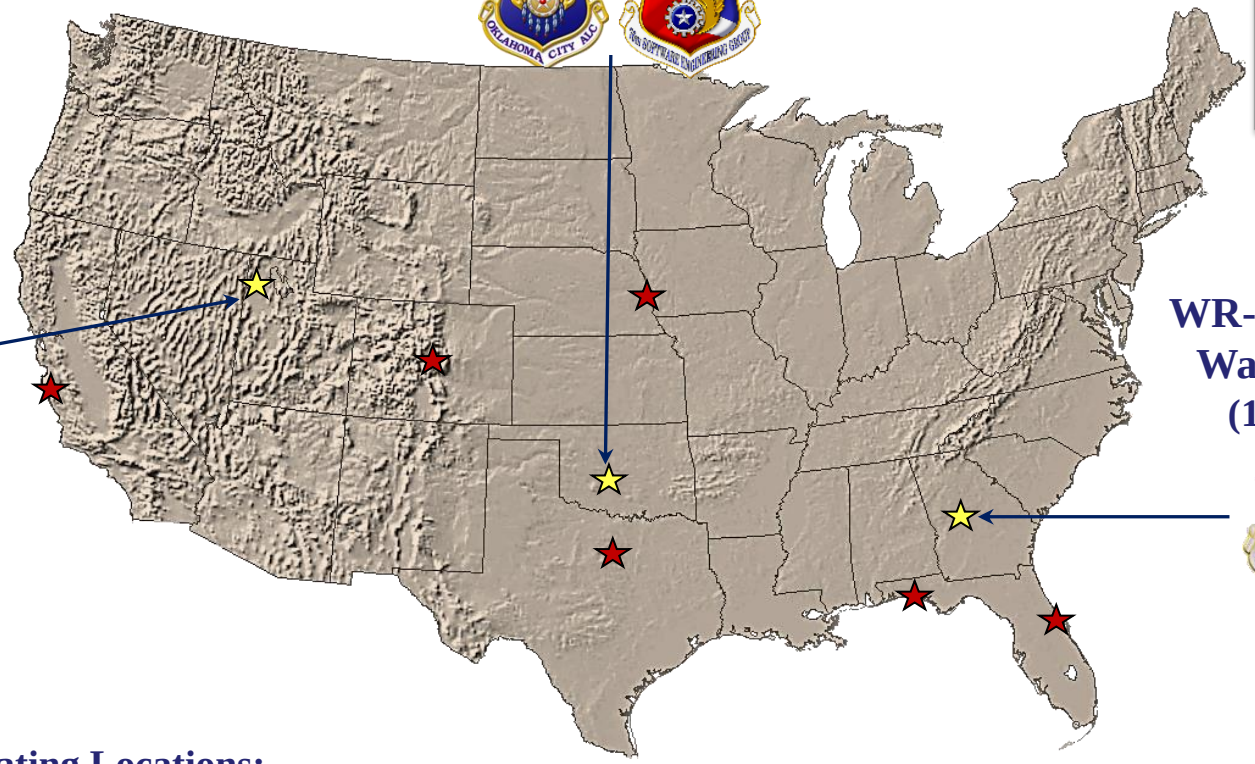
Who We Are
Software Enterprise: Three Partners – One Mission

~4,500 Software Professionals Combined

OC-ALC, Tinker AFB
Oklahoma City, OK
(1300+ Personnel)

Specializing in Operational Programs, C4I, Mission Support, Test Program Sets and Training Systems

OO-ALC, Hill AFB
Ogden, UT
(1900+ Personnel)



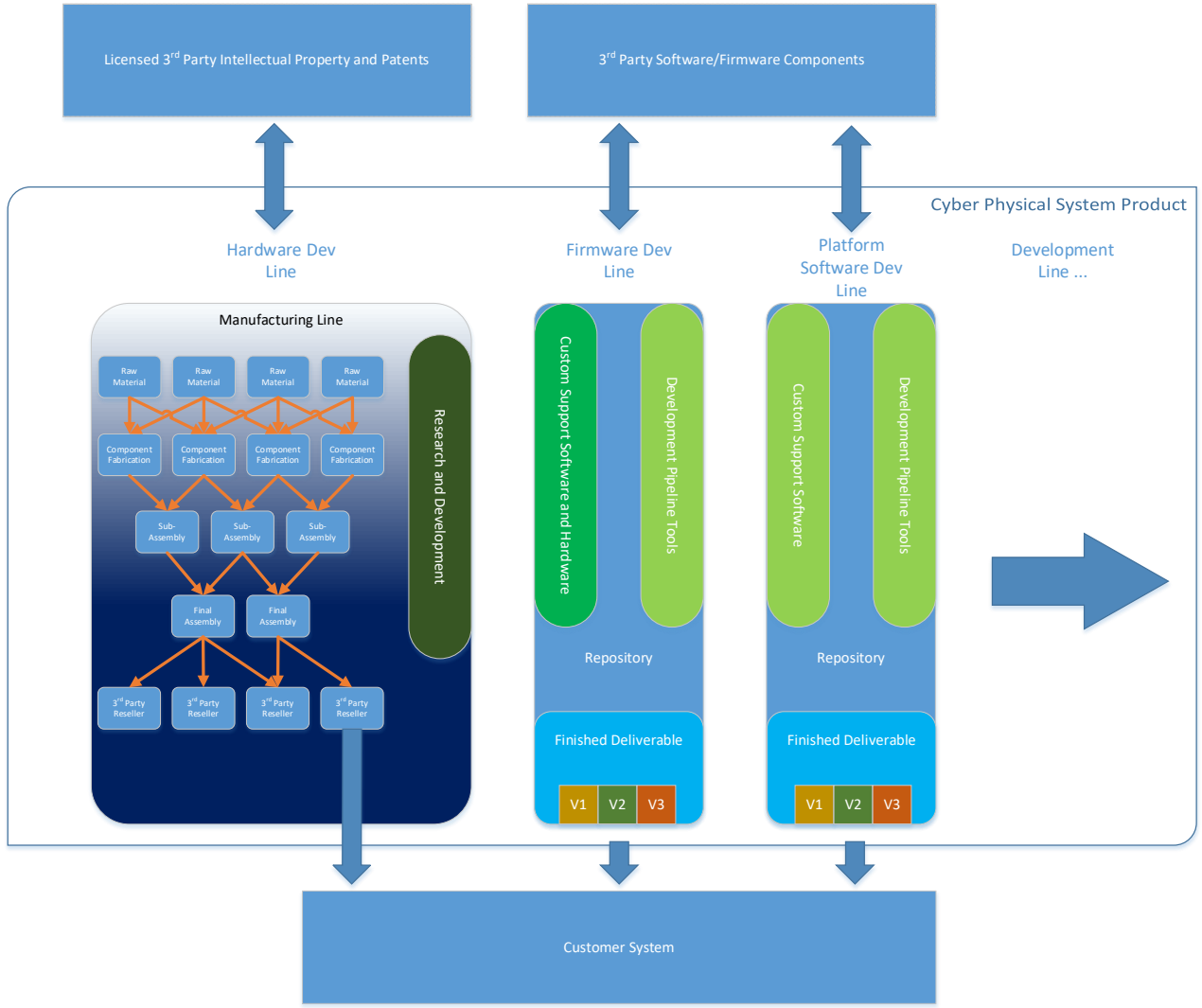
WR-ALC, Robins AFB
Warner Robins, GA
(1300+ Personnel)

★ **Six (6) Current Operating Locations:**
Vandenberg AFB, CA – Peterson AFB, CO – NAS-JRB, TX – Offutt AFB, NE – NAS Pensacola, FL – Patrick AFB, FL

The Technical Illumination of an Information Technology Supplier

WHAT MAKES UP A COMPONENT?

Cyber Physical Systems



Real Life Example: Dell PowerEdge r950

Image Credit DellEMC

Product Breakdown

Hardware

- CPU
- DRAMM Module
- Motherboard
- Discrete Graphics
- iDRAC
- SSD/HDD

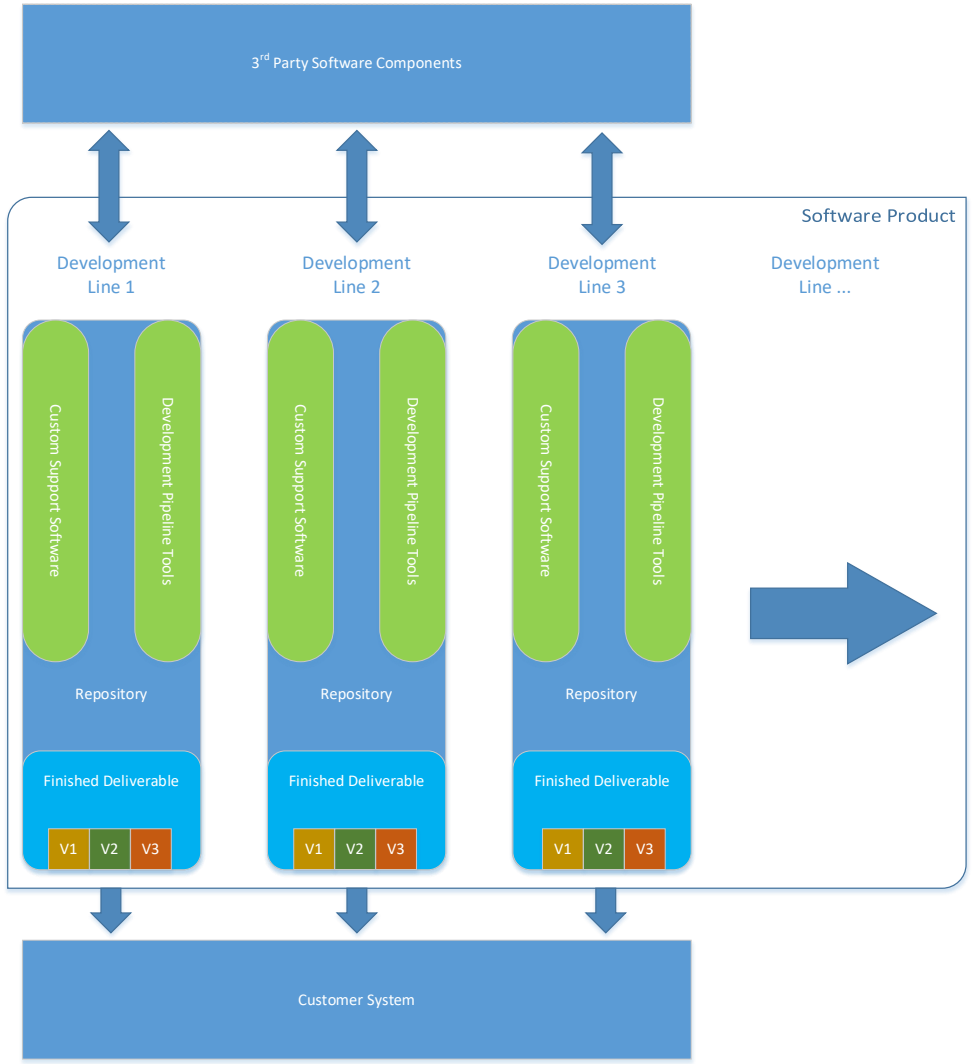
Firmware

- UEFI (motherboard)
- UEFI (iDRAC)
- SSD/HDD
- RAID Controller

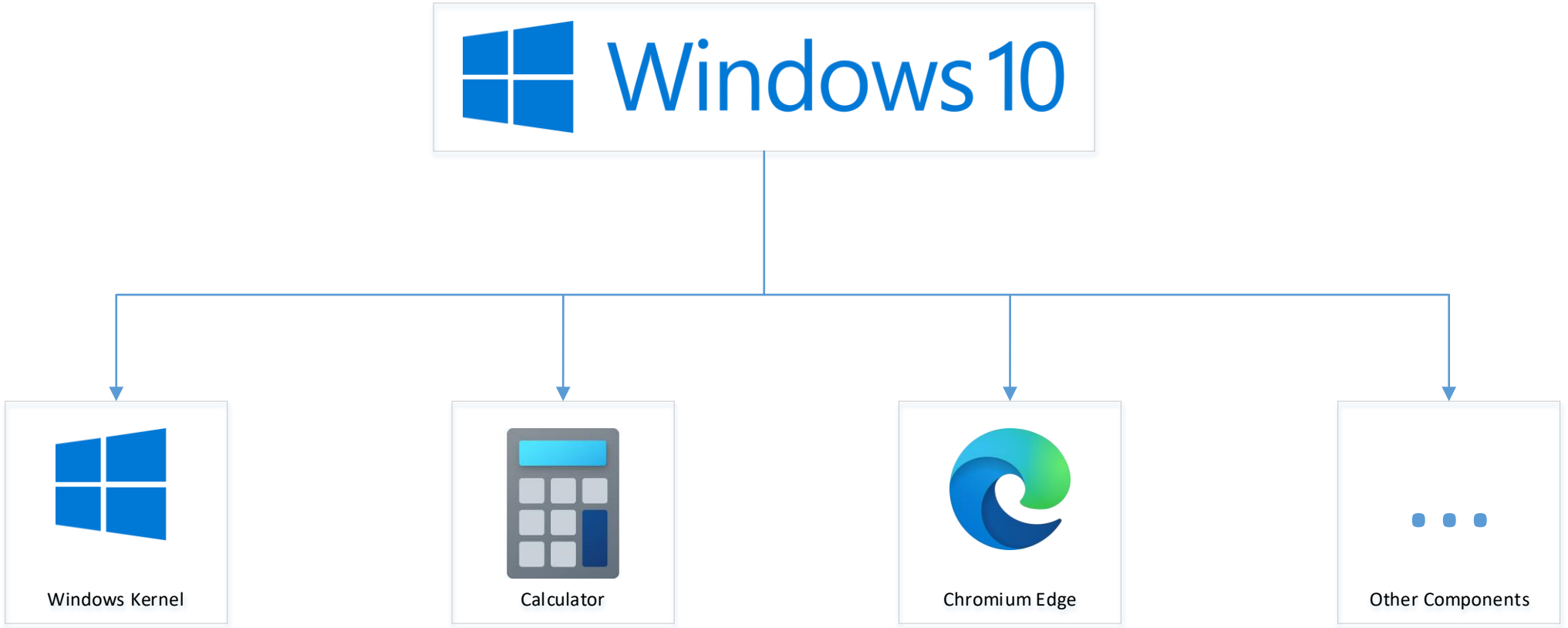
Software

- Installed OS
- iDRAC
  - OS
  - Webserver
  - Database

Software Centric Product

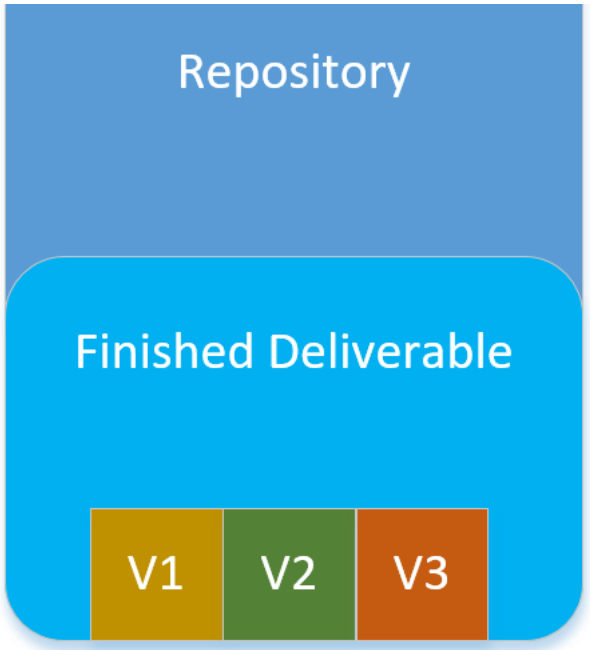


Real Life Example: Windows 10



Software Versioning

- Versioning
  - Software and firmware can have many versions being maintained simultaneously
    - Different SKUs
    - Different versions
    - Different Platforms
    - Different Regions
  - Processes can be different for each version
    - Tooling
    - Culture
    - Technology



Real Life Example: Windows 10

V • T • E

Windows 10 versions

Version	Codename	Marketing name	Build	Release date	Supported until (and support status by color)			
					Home, Pro, Pro Education, Pro for Workstations	Enterprise, Education	LTSC[a]	Mobile
1507	Threshold 1	N/A	10240	July 29, 2015	May 9, 2017		October 14, 2025[b]	N/A
1511	Threshold 2	November Update	10586	November 10, 2015	October 10, 2017	April 10, 2018	N/A	January 9, 2018
1607	Redstone 1	Anniversary Update	14393	August 2, 2016	April 10, 2018[c]	April 9, 2019[c]	October 13, 2026[d]	October 9, 2018
1703	Redstone 2	Creators Update	15063	April 5, 2017[e]	October 9, 2018	October 8, 2019	N/A	June 11, 2019
1709	Redstone 3	Fall Creators Update	16299[f]	October 17, 2017	April 9, 2019	October 13, 2020[g]		January 14, 2020
1803	Redstone 4	April 2018 Update	17134	April 30, 2018	November 12, 2019	May 11, 2021[h]		N/A
1809	Redstone 5	October 2018 Update	17763	November 13, 2018[i]	November 10, 2020[j]		**January 9, 2029**[k]	
1903	19H1	May 2019 Update	18362	May 21, 2019	December 8, 2020		N/A	
1909	19H2	November 2019 Update	18363	November 12, 2019	May 11, 2021	May 10, 2022		
2004	20H1	May 2020 Update	19041	May 27, 2020	December 14, 2021			
20H2	20H2	October 2020 Update	19042	October 20, 2020	May 10, 2022	May 9, 2023		
21H1	21H1	May 2021 Update	19043	May 18, 2021	**December 13, 2022**			
21H2	21H2	November 2021 Update	19044	TBA	18 months	30 months	5 years	

Legend: Old version, not maintained[l] Older version, still maintained[m] **Current stable version**[n] Latest preview version[o]

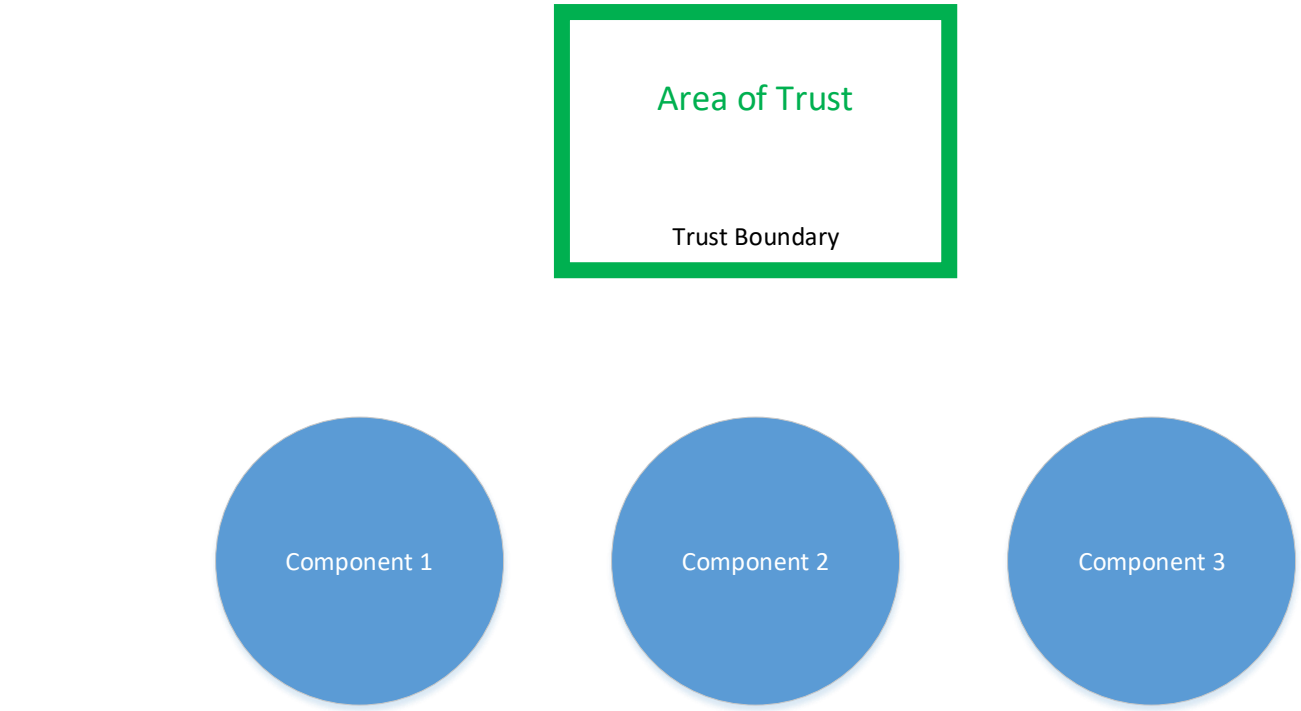
[show]

Image Credit Wikipedia

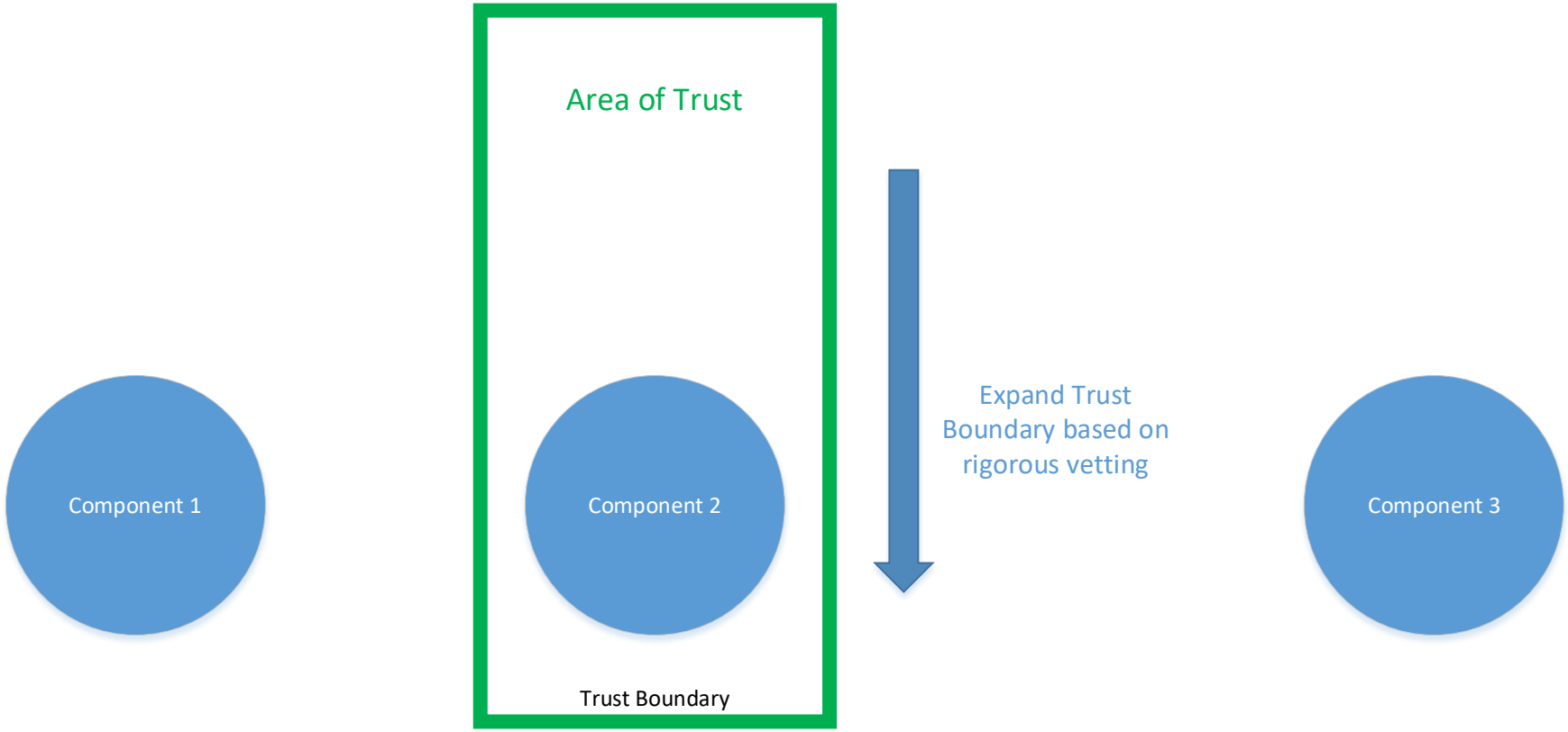
Moving from automatic trust to distrust

ZERO TRUST MODEL

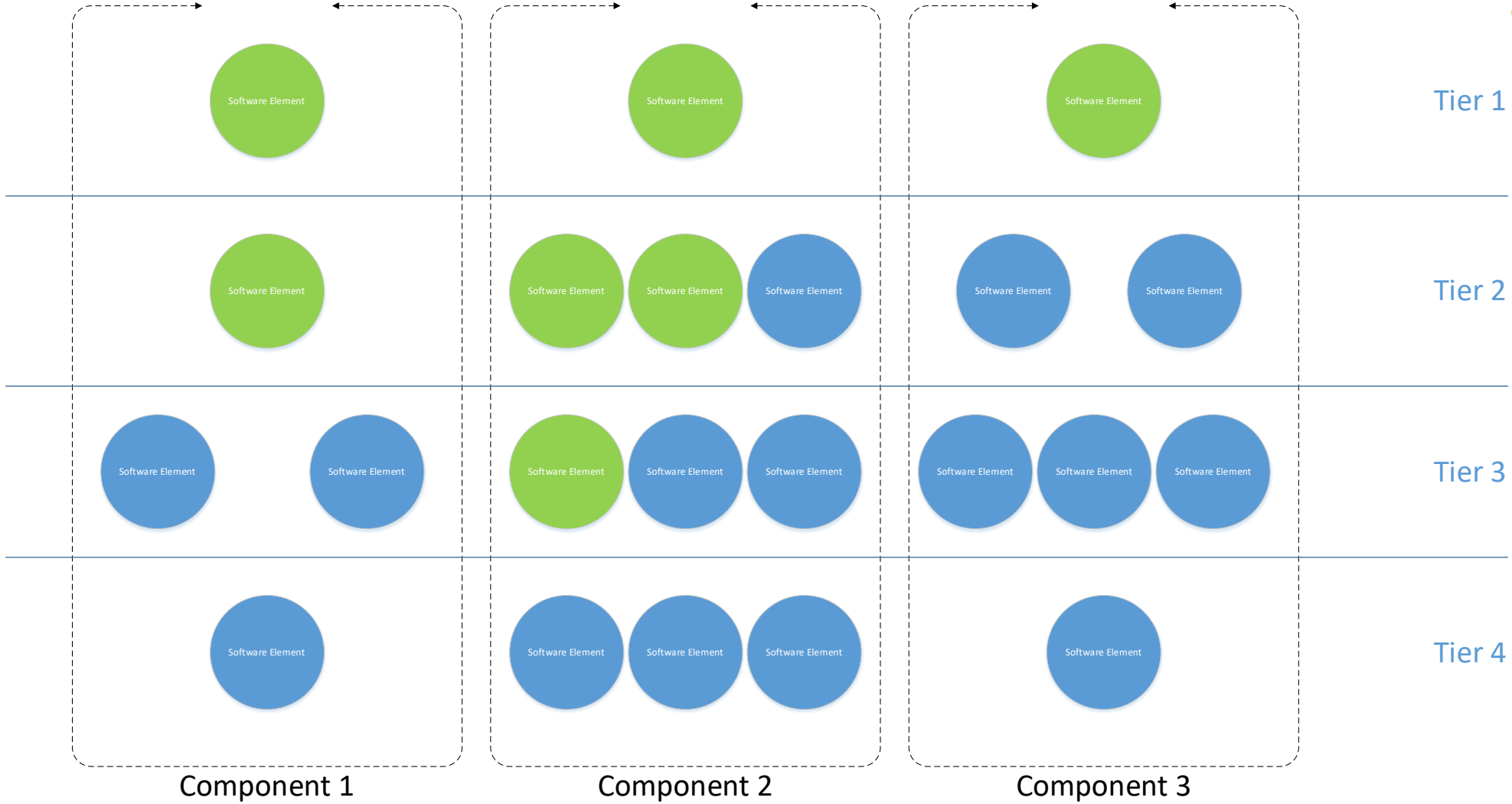
Zero Trust Model



Adding Components to our Trust Area



The Verify/Trust Boundary



Order of Component Inclusion

- **Many systems contain too many components/suppliers to assess all at once**
  - **Determine order based on a completed Criticality Analysis**
  - **Apply the Risk Management Framework**

Probability \ Severity		1 Negligable	2 Minor	3 Moderate	4 Significant	5 Severe
5	Very Likely					
4	Likely					
3	Possible					
2	Unlikely					
1	Very Unlikely					

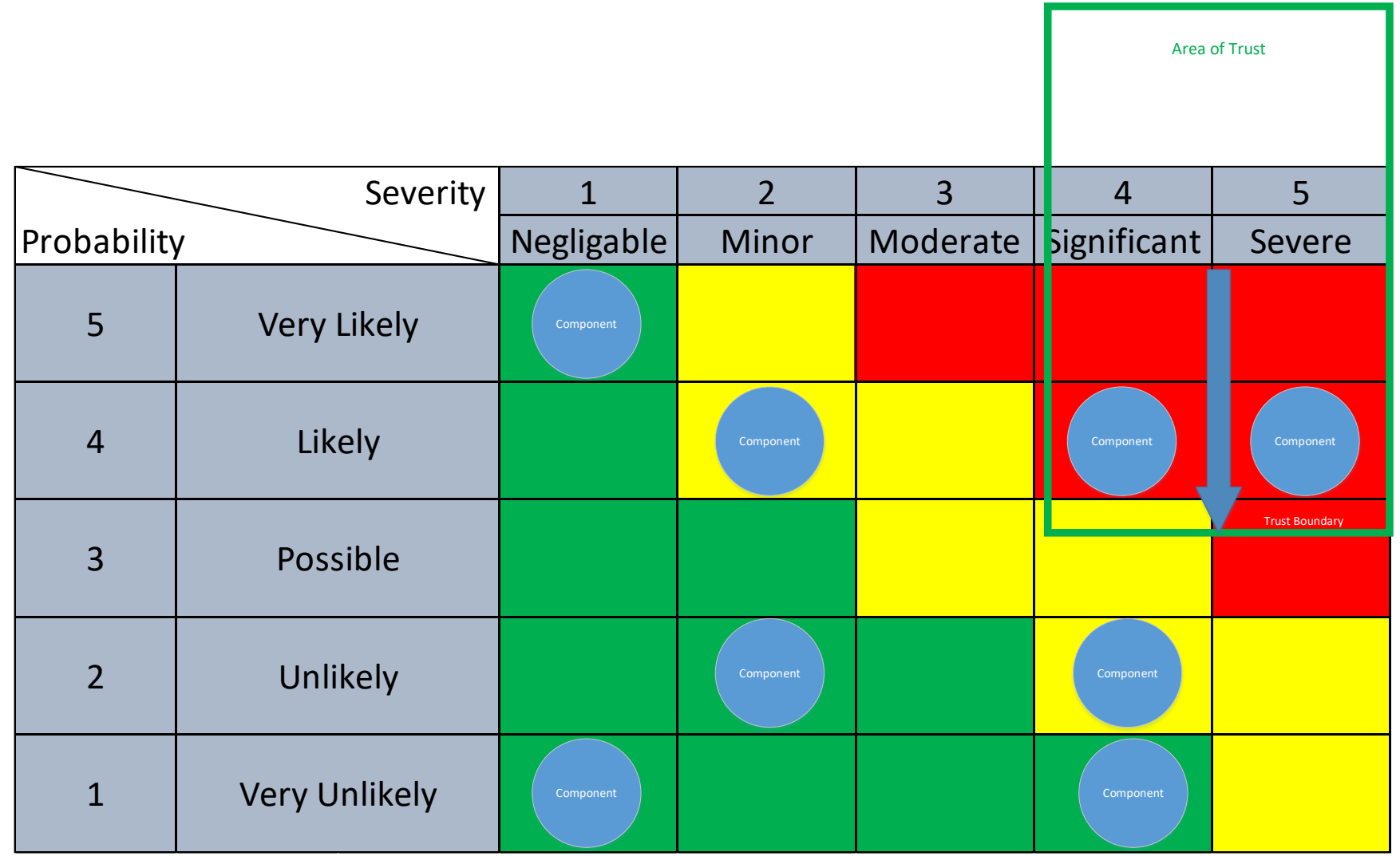
Order of Component Inclusion

Area of Trust

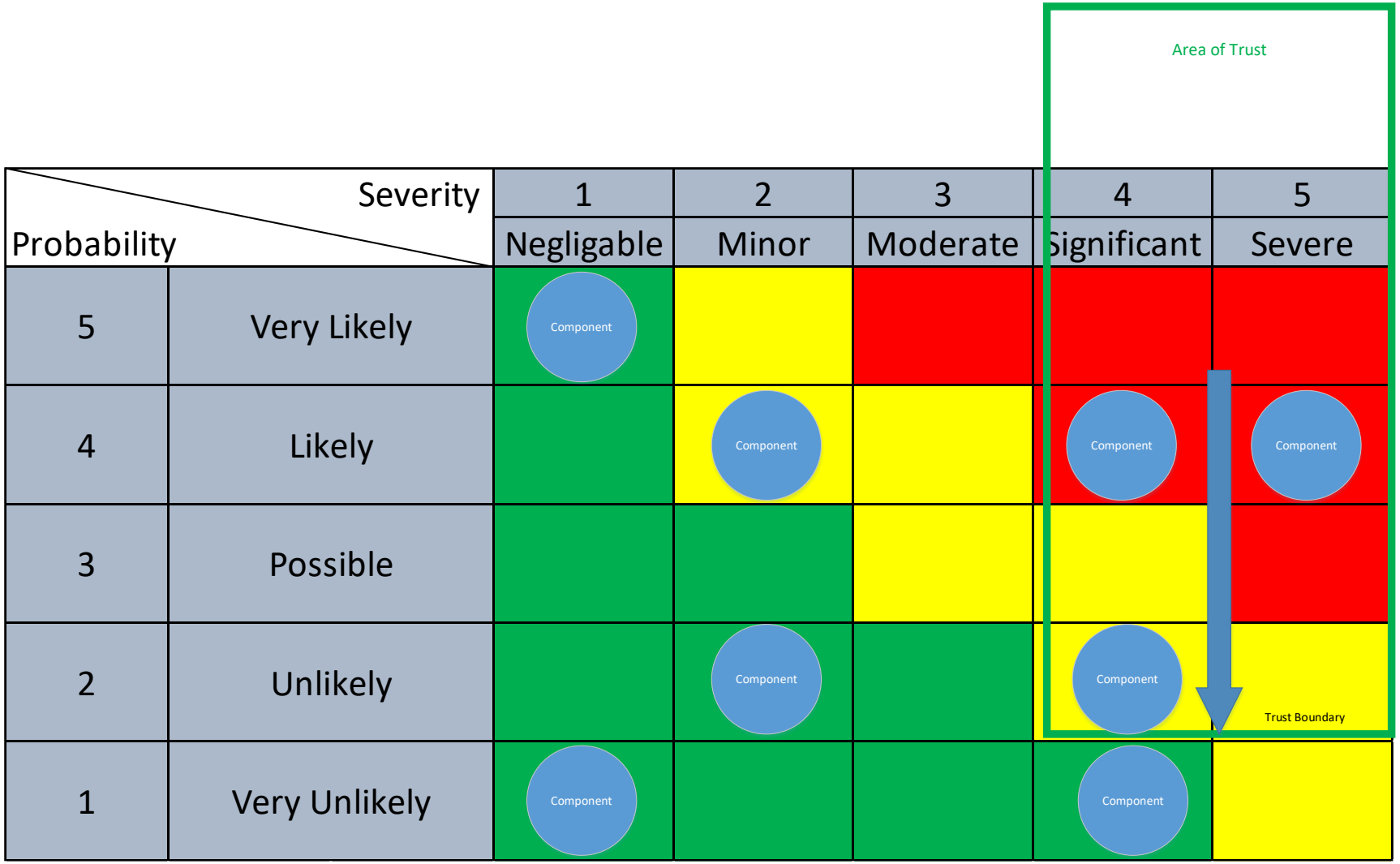
Trust Boundary

Probability \ Severity		1 Negligable	2 Minor	3 Moderate	4 Significant	5 Severe
5	Very Likely	Component				
4	Likely		Component		Component	Component
3	Possible					
2	Unlikely		Component		Component	
1	Very Unlikely	Component			Component	

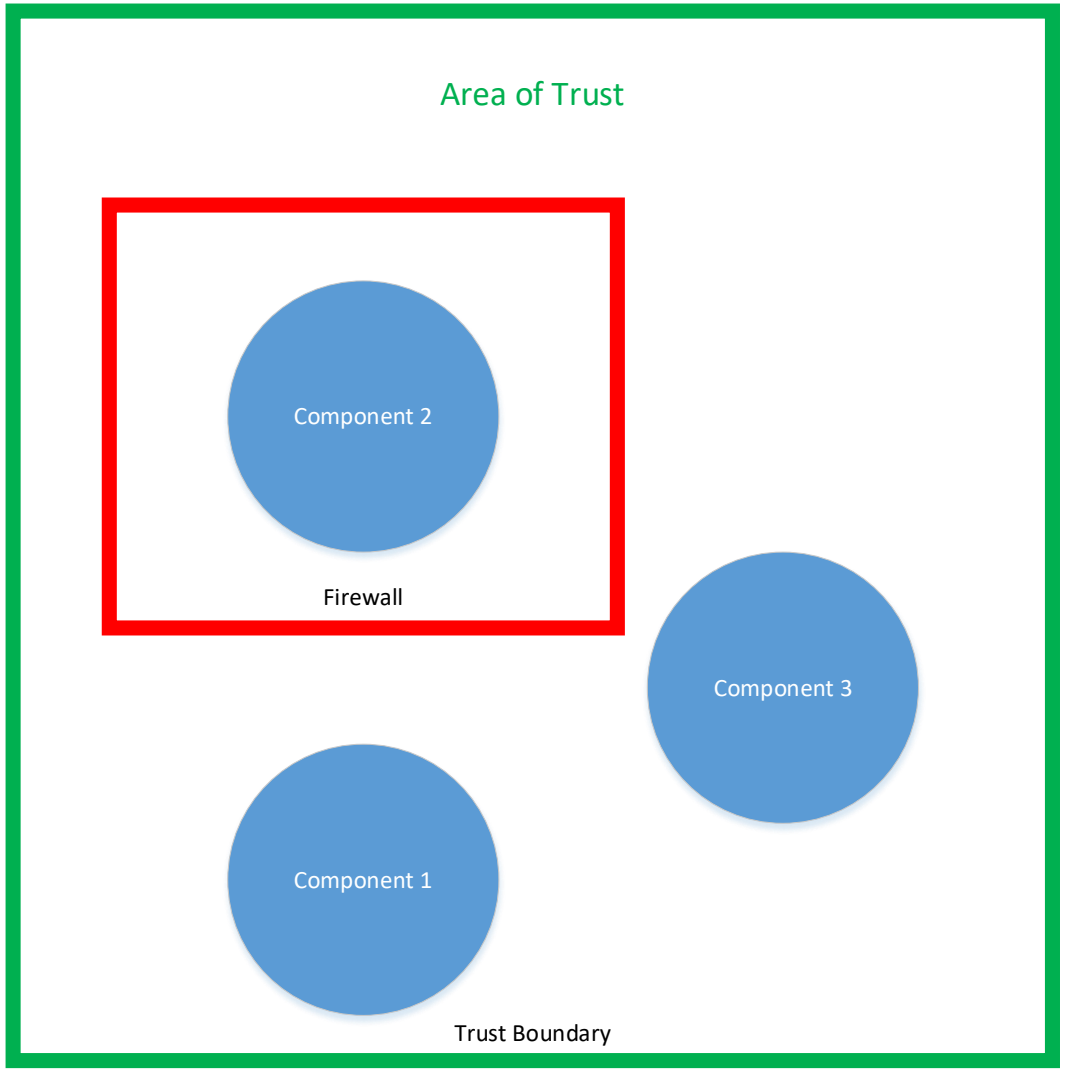
Order of Component Inclusion



Order of Component Inclusion

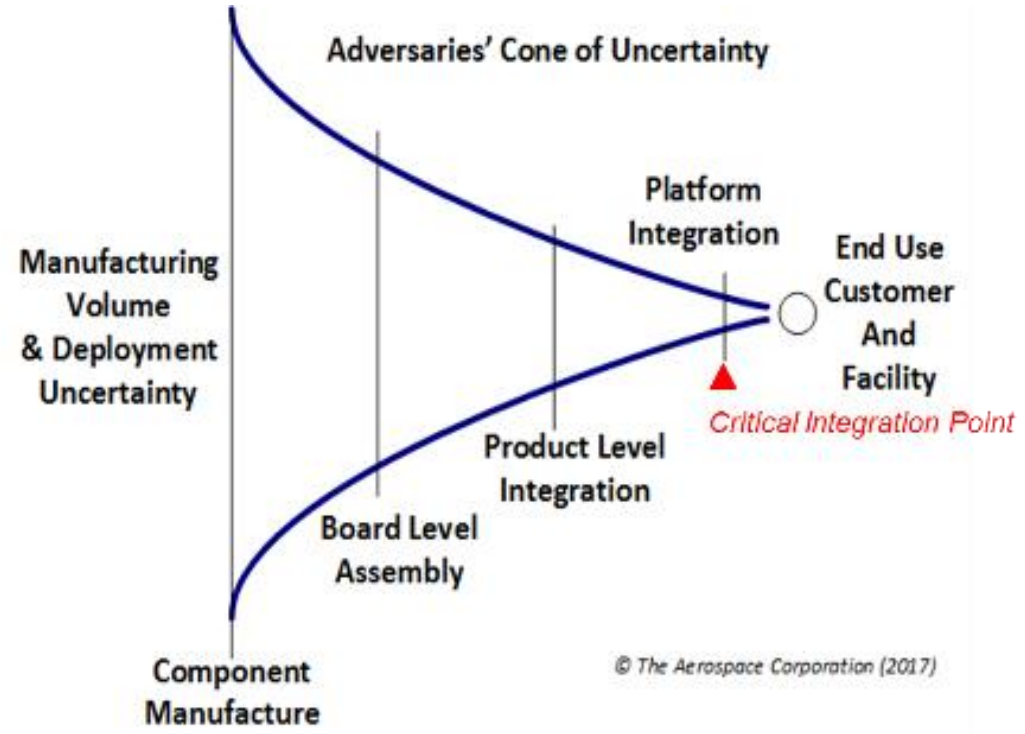


If C-SCRM Posture Degrades, Consider Isolating Components



The Trust/Verify Boundary

- How far back into the suppply chain should we go?
  - At least 1st tier
  - Maybe 2nd and 3rd tier as needed
- There are risks to going back too far and identifying that component is part of a weapon system



The Three types of assessments

SCRM ASSESSMENTS

Three Types of Assessments

Intelligence Reports

Business Analytic Reports

Technical Field C-SCRM Assessments

Pre-Procurement

Traditional Assurance Practices

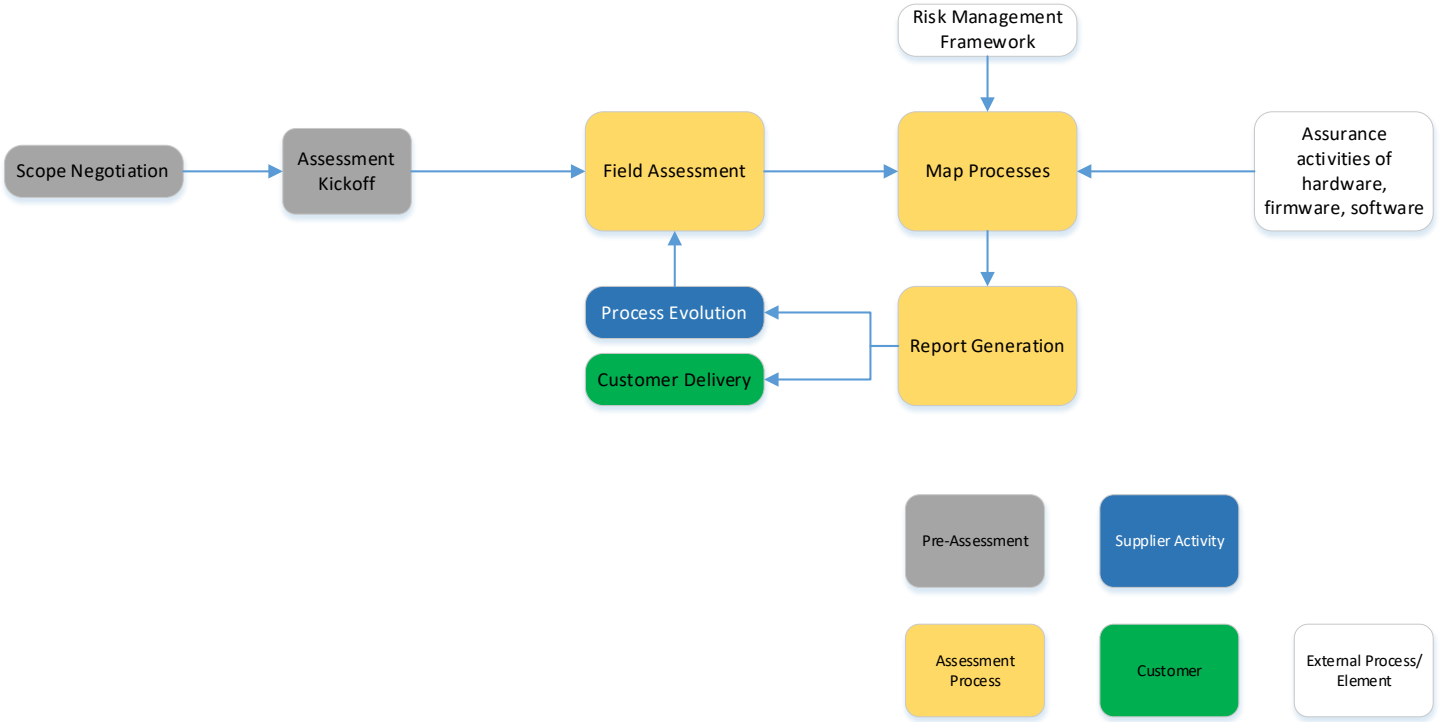
Post-Procurement

Adapting Space Force SMC SCRM Process

THE TECHNICAL ASSESSMENT PROCESS

C-SCRM Assessment Process

1. **Define scope with supplier and Government Organization and determine contract vehicle**
2. **Assessment kickoff with initial information exchange**
3. **Conduct field assessments, identify processes, and collect artifacts**
4. **Map and compare against best practices and document risks**
5. **Report generation with identified risks**
6. **Deliver report to customer and supplier**



Questionnaire Assessment Categories

- General Organizational Practices
- Hardware Centric Products
  - Design & Test
  - Integration
  - Platform Firmware
  - Platform Software
- Software Centric Products
- Cloud Centric Products

Sample Questions

General Organizational Practices

- How does continuous SCRM threat assessment factor into your organization's design, integration, test and support strategy? Can you cite an example where you have responded to or altered your business process based on the threat assessment?
- How has your SCRM strategy evolved over the past five years? What changes do you anticipate in the next five years?

Platform Management Software Development and Controls

- What processes are used internally to develop, build, test and release software? Do you maintain continuous integration, continuous deployment pipelines for this software? If so how are releases made available to customers?
- What types of platform management software do you provide to data center customers? Is it internally developed or contracted from a third party?

How Responses are Evaluated

- **A score is not assigned to each question, instead the assessment process looks for specific observations of policies and practices which are mapped to a SCRM threat level shown below**
- **These threat levels directly map to the risk levels in the RMF framework (DoDi 8510.01)**

Level 0	Level 1	Level 2	Level 3
Does Not Meet the Standards of Common Practice or Cyber Needs	Consistent with common Practice but not Current Industry Standards	Consistent with Standard Practice for Current Industry Standards	Best in Class Practice and Targets Future Cyber Threats/Risks

How Risks are Identified

- **Observations are rated by risk level and compiled by category.**

Category	L0	L1	L2	L3
General				
Organizational SCRM Practicies		2	4	3
Hardware Centric Products				
Organizational Practices in Acquiring, Integrating and Controlling Materials			5	4
Organizational Practices for Sourcing, Integrating and Controlling Platform Firmware		4	3	1
Design, Integration, and Test of Data Center Platforms		3		2
Development, Software Assurance, and Cyber Controls of Platform Control Software		4	4	
Software Centric Products				
Development, Software Assurance, and Cyber Controls of Application Software			2	3
Cloud Centric Products				
Development, Software Assurance, and Cyber Controls of Cloud Infrastructure		2	1	2

- **Identified risk for PPP: If Supplier X signing servers are not separated from the development network, then there is the risk of insider threats being able to pass a malware payload as legitimate.**

C-SCRM Assessments Across the Acquisition Lifecycle

- MDD-MS B: Best time to perform C-SCRM supplier assessments – prior to selecting a Prime.
- MS B - FOC: If C-SCRM assessments not performed prior to Prime contract award, assess suppliers during development of firmware and software to ensure secure C-SCRM posture.
- Sustainment: Never too late to assess a supplier even in Sustainment to understand C-SCRM posture. A program may take advantage of contracting for new capabilities to perform C-SCRM assessments.
- In all cases, continue working with suppliers to improve their C-SCRM posture/ensure no backsliding.

In Conclusion

- DoD programs need input from three different kinds of SCRM assessments
  - Program Offices need more information and deeper technical expertise to illuminate their software and hardware supply chains
- Once supply chains are illuminated, understanding the depth that a program office should validate and which level to trust is key
- Programs need to establish a zero-trust model for critical components and be able to validate supply chain trust on a per component bases

QUESTIONS AND COMMENTS

Contact Us

- **Alexander Wright**
  - **alexander.wright.4@us.af.mil**
  - **(719) 556-9314**
- **Parker Bauer**
  - **parker.bauer@us.af.mil**
  - **(801) 777-5308**

THANK YOU!