Intel's Product Security Maturity Model (PSMM)

8 Mar 2016

Harold Toomey | Sr. Product Security Architect & PSIRT Manager, Intel Security
James Ransome | Sr. Director Product Security, Intel Security

Introduction

Responsibilities

- PSIRT Manager
- Manage a team of 72 Sr. Security Architects (PSCs)
- Manage the PSG program, Agile SDL and policies
- Training program
- Metrics / Reporting

Experience

- 4 Years: Software / Application Security
- 2 Years: IT Operational Security
- 11 Years: Product Management
- 10 Years: Software Development (C++)

CVSS Special Interest Group (SIG)

ISSA North Texas Chapter, Past President

CISSP, CISA, CISM, CRISC, CGEIT, …

Harold Toomey
Sr. Product Security Architect

Agenda

- SDLC / SDL
- Maturity Models
- PSMM Reports
- PSMM Design Criteria
- Org. Structure
- 20 PSMM Parameters
- MS Excel / Word
- Metrics

SDLCs / SDLs

Waterfall

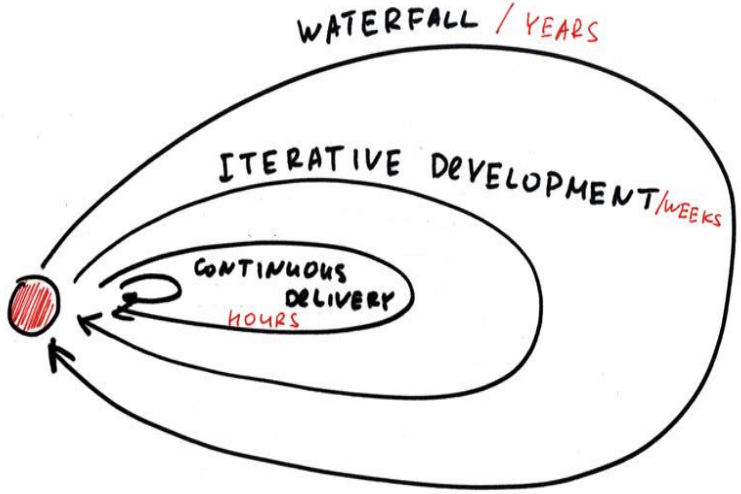
- Current methodology for Hardware side of Intel
- Was used by McAfee 5 years ago

Agile

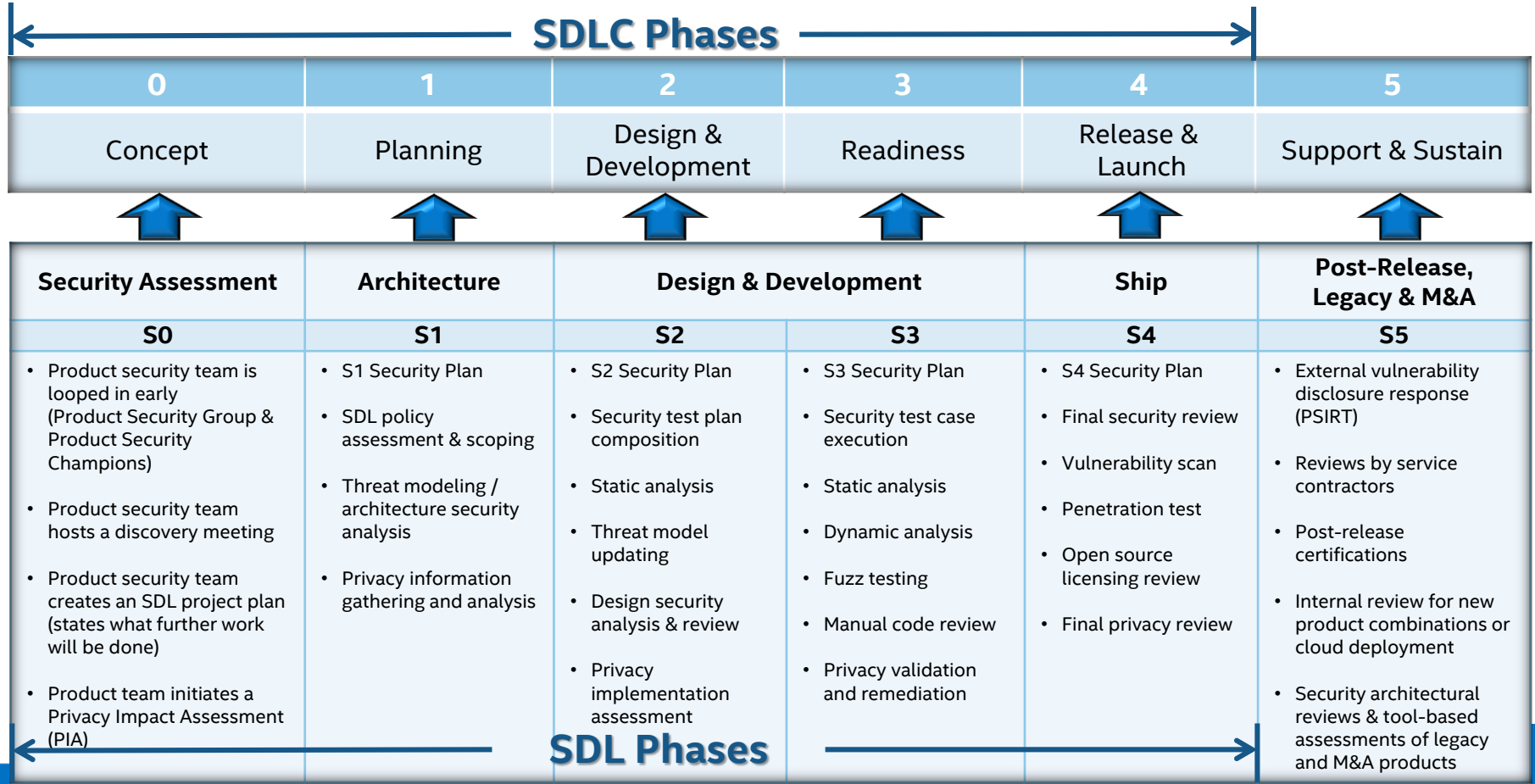
- Current methodology for Software side of Intel
- 95% of Intel Security (McAfee) uses

Continuous Delivery

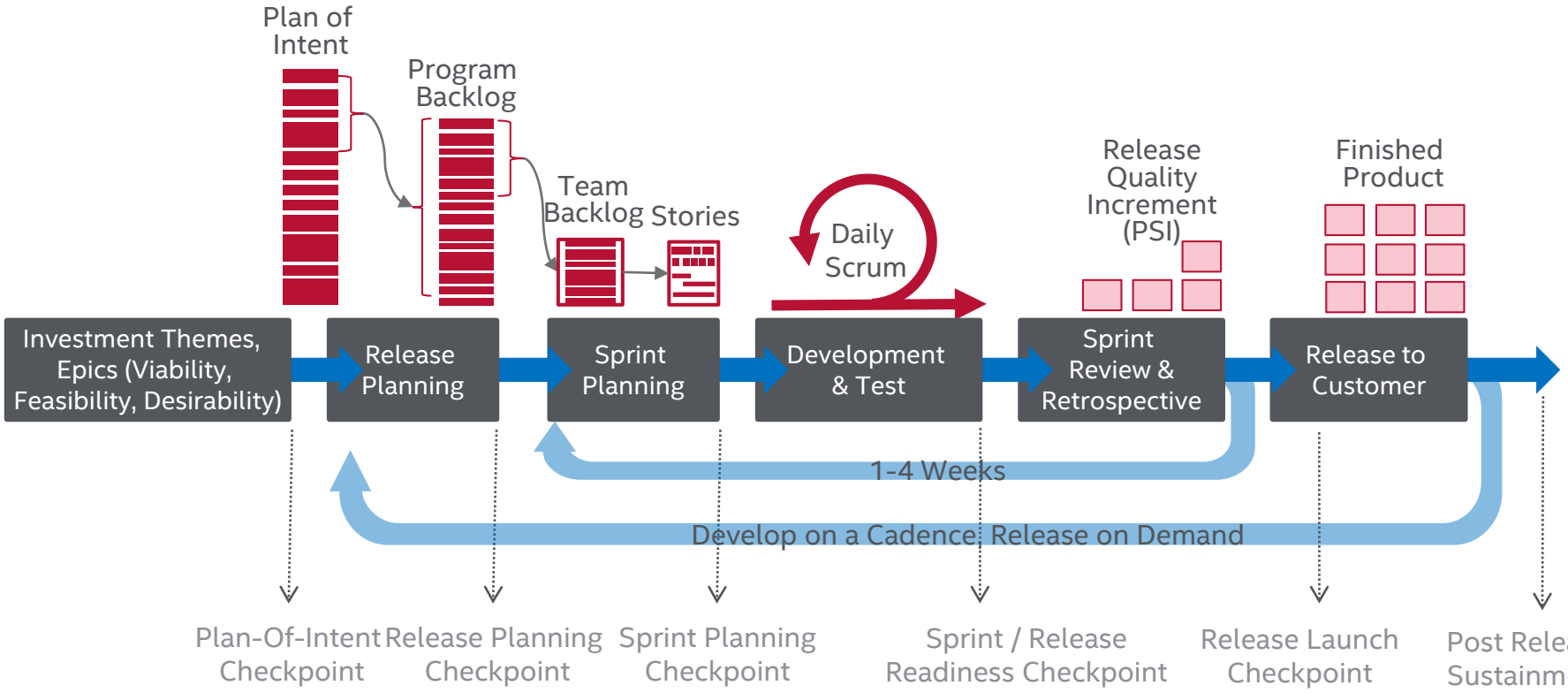
- Fastest growing methodology for Cloud technology



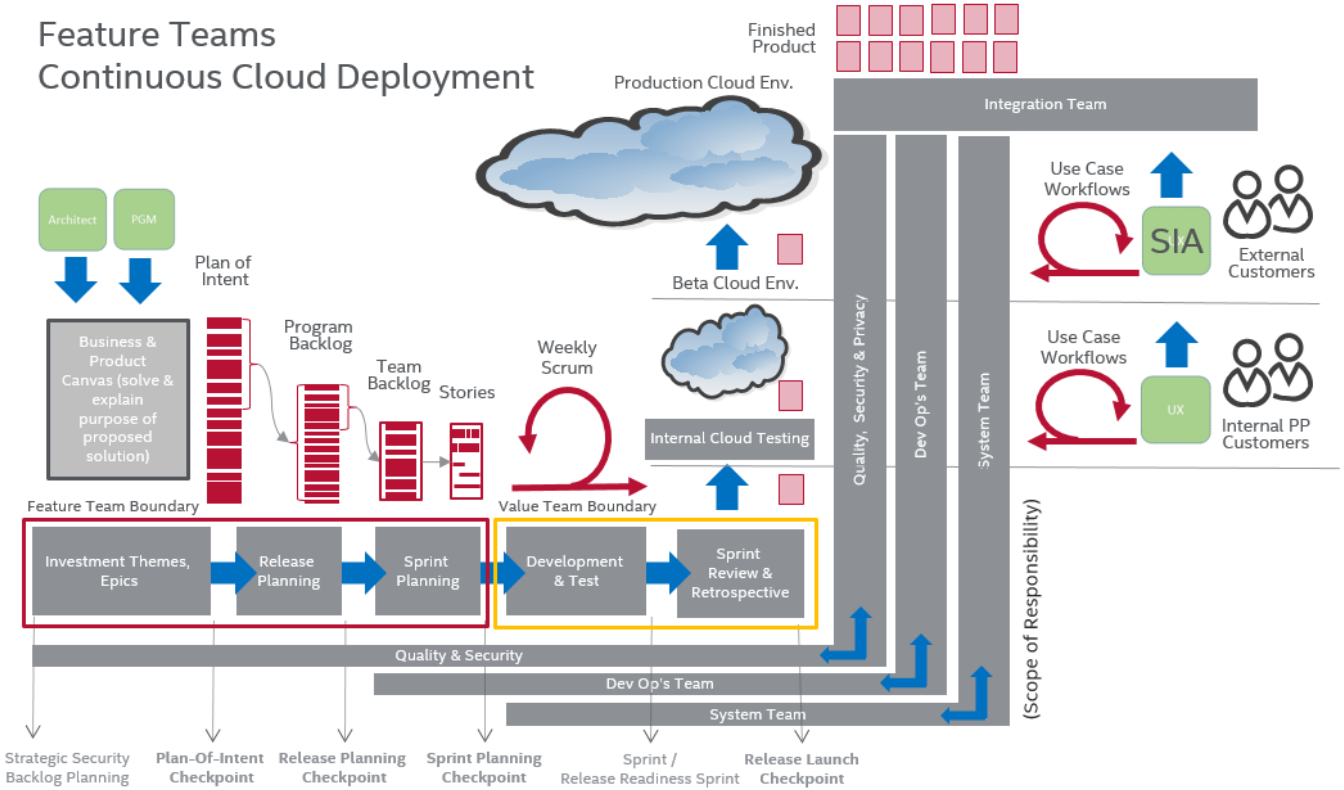
McAfee Waterfall SDL (SDLC)



Intel Security Agile SDLC

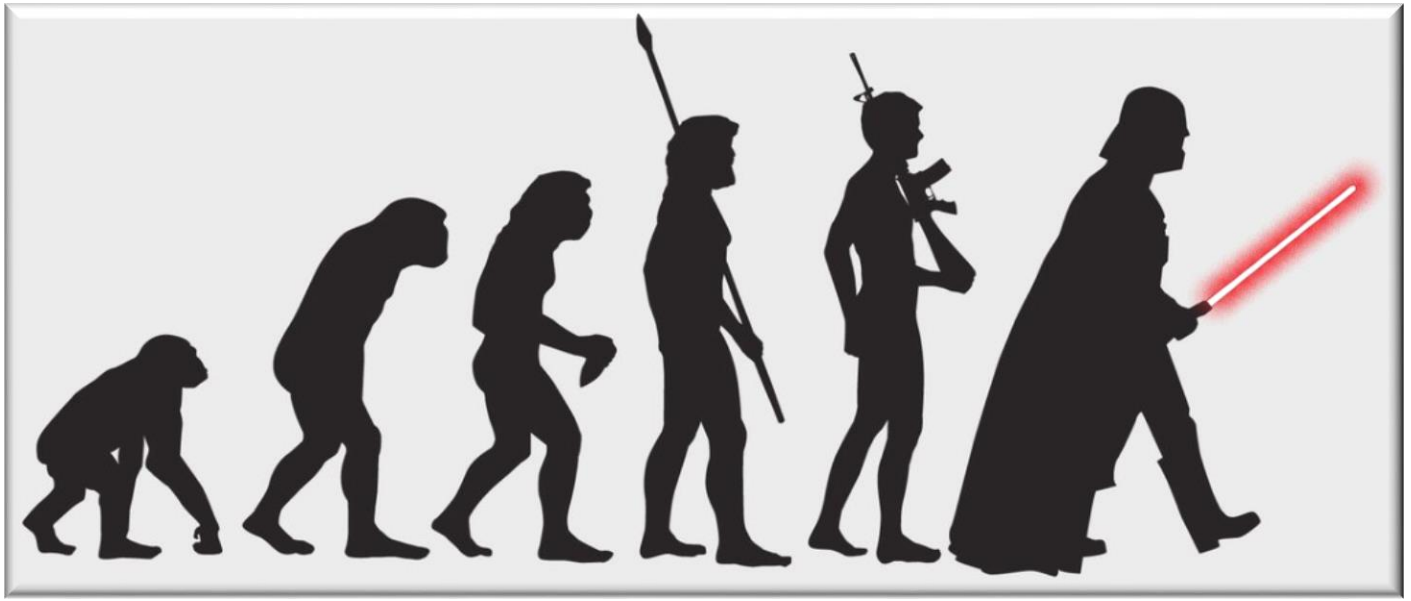


Intel Security Agile SDL Adapted to the Cloud



Problem Statement

Problem: We have an SDL. How well are the product teams following it?



Maturity Models

Common SDL Maturity Models

- **BSIMM**: Build Security In Maturity Model – Cigital
- **SAMM**: Software Assurance Maturity Model – OWASP
- **DFS**: Design For Security – Intel
- **Microsoft SDL**: Optimized Model

Other SDL Frameworks

- **ISO 27034**: Application Security Controls

PSMM Design Constraints

1. No budget for cool applications
   - Use COTS tools
2. No budget for additional auditors
   - Peer review
3. Be simple
   - Automated, not weighted, minimal training and effort
4. Low overhead
   - Minimal burden on engineering teams
5. Produce insightful metrics

PSMM Implementation Requirements

1. Provide a detailed MS Word doc fully listing requirements for each parameter level
2. Provide simple drop-down lists in MS Excel
3. Allow and adjust for “0 – Not Applicable”
4. Map PSMM to other maturity models
5. Allow for phased roll-out, reporting at different org. levels

Solution

Solution: The Intel Product Security Maturity Model (PSMM)

- Measures how well both the **operational** and **technical** aspects of product security are being performed
- Provides a simple, yet powerful, model which has been adopted and is being used company-wide
- Data is collected at multiple levels to improve accuracy

Solution (cont.)

- Five maturity levels
  1. None
  2. Basic
  3. Initial
  4. Acceptable
  5. Mature
- Focus on process, quality of activity execution, and outcomes

20 PSMM Parameters

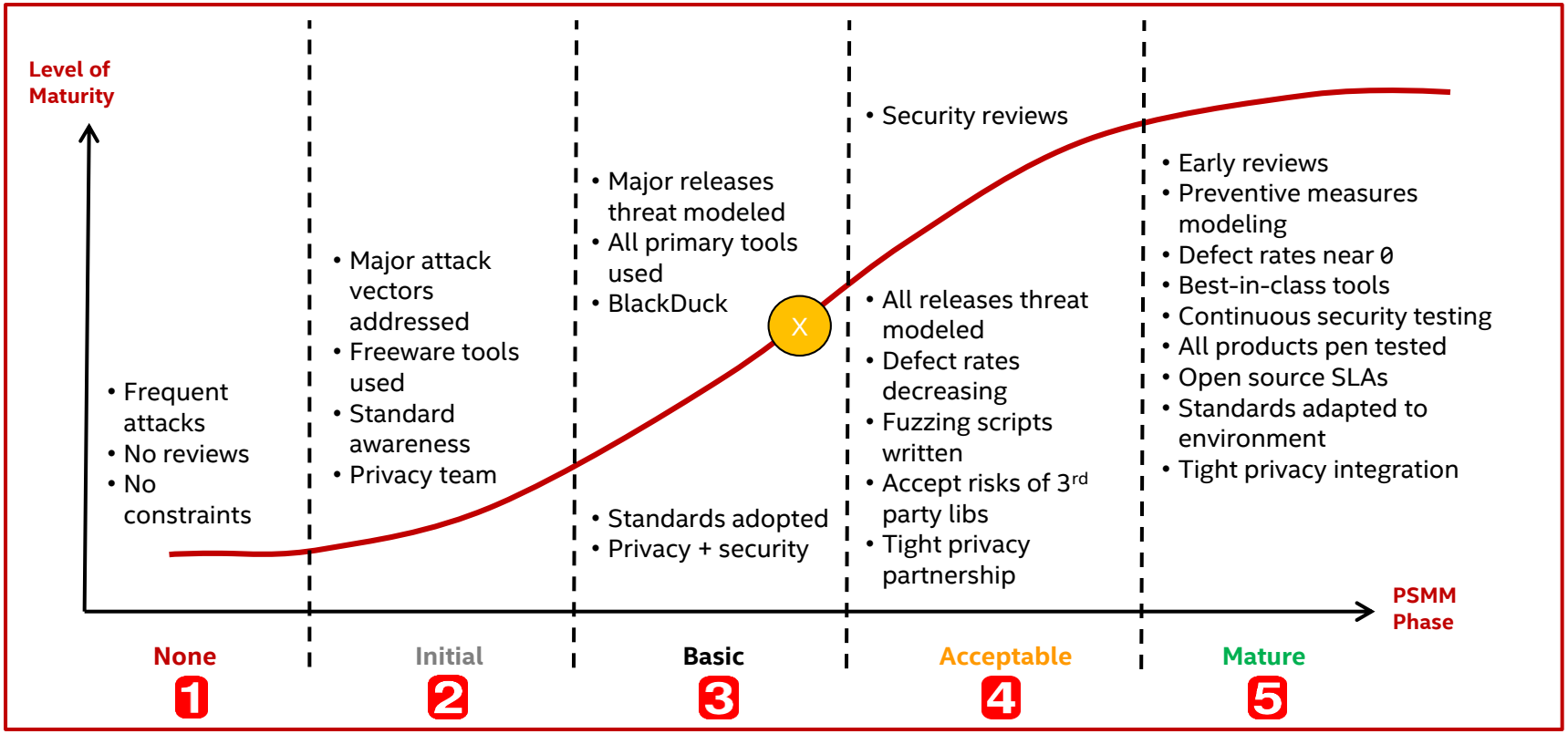
Operational

1. Program
2. Resources
3. SDL
4. PSIRT
5. Policy
6. Process
7. Training
8. Reporting & Tracking Tools

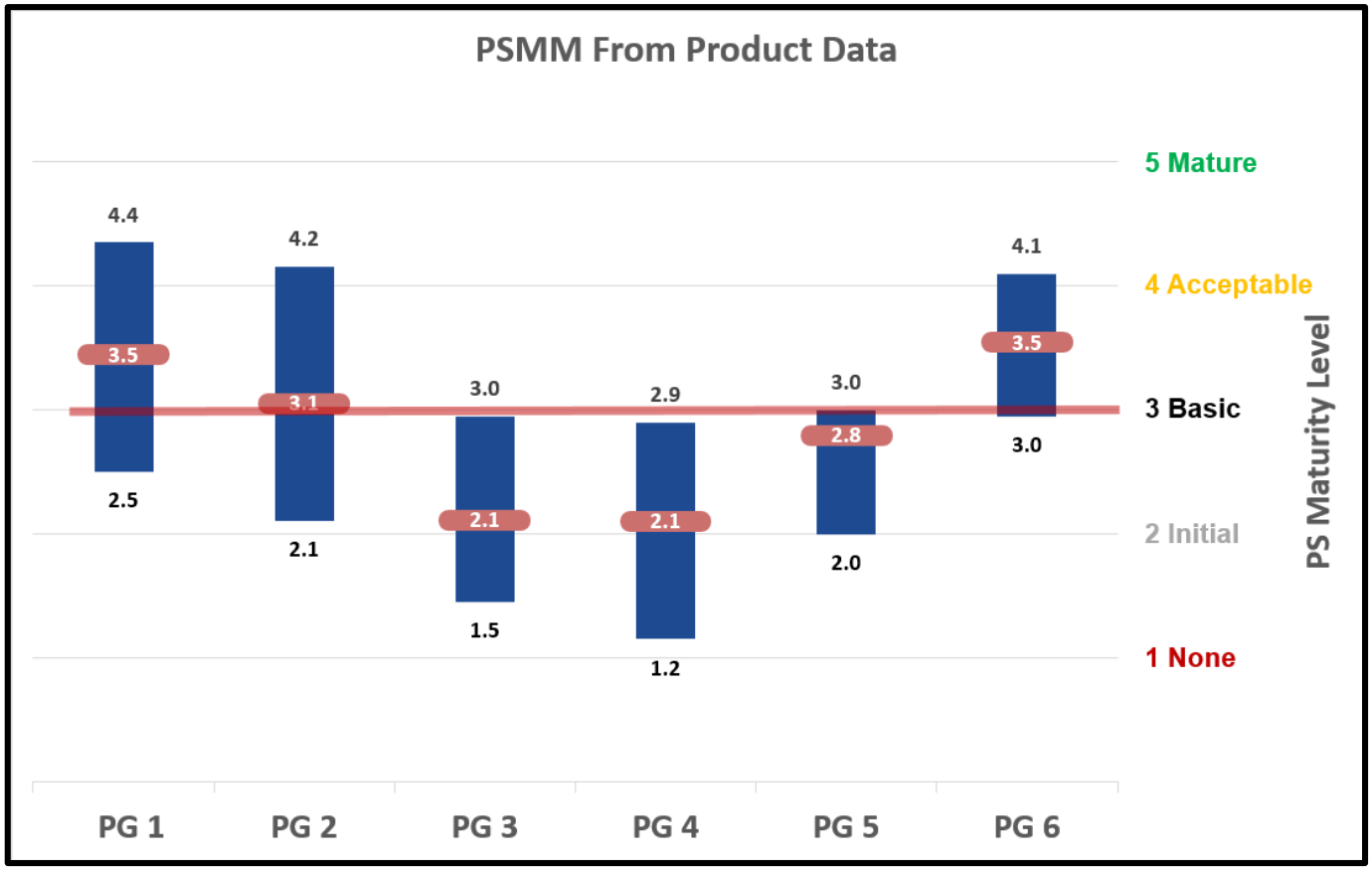
Technical

1. Security Requirements Plan [Waterfall] / Security Definition of Done (DoD) [Agile]
2. Architecture and Design Reviews
3. Threat Modeling
4. Security Testing
5. Static Analysis
6. Dynamic Analysis
7. Fuzz Testing
8. Vulnerability Scans / Penetration Testing
9. Manual Code Reviews
10. Secure Coding Standards
11. Open Source / 3rd Party COTS Libraries
12. Privacy

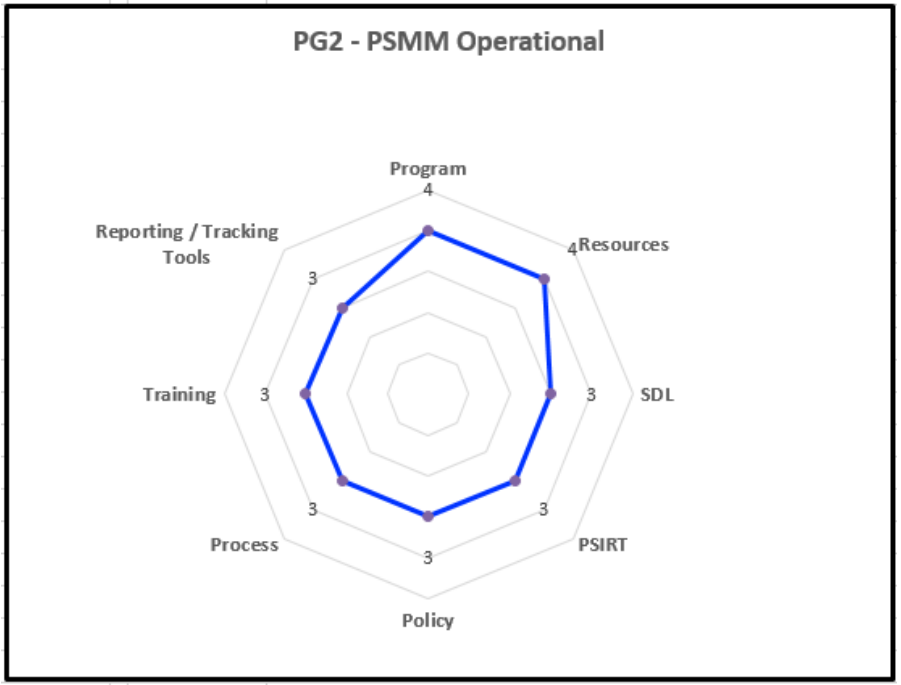
PSMM – Overall State of the Company – Technical

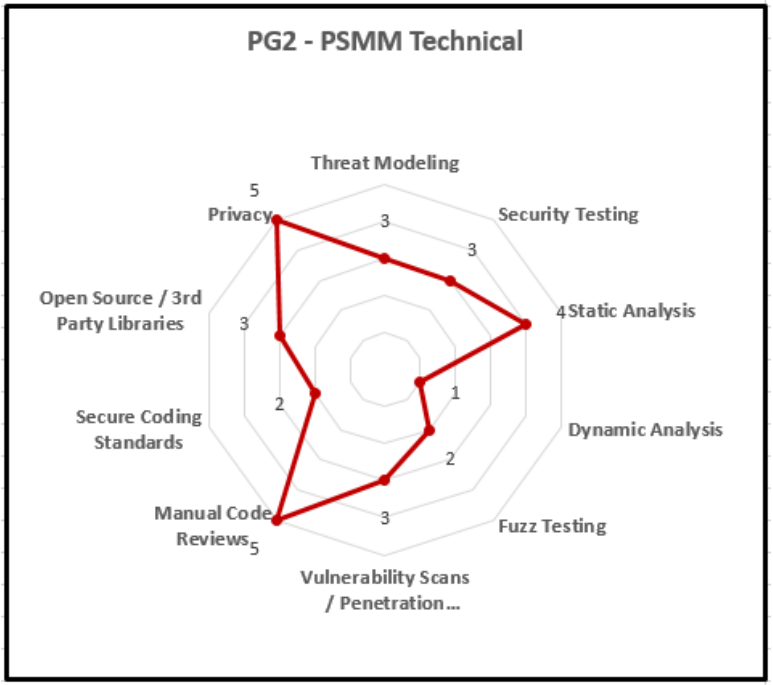


PSMM – State by Product Group / BU



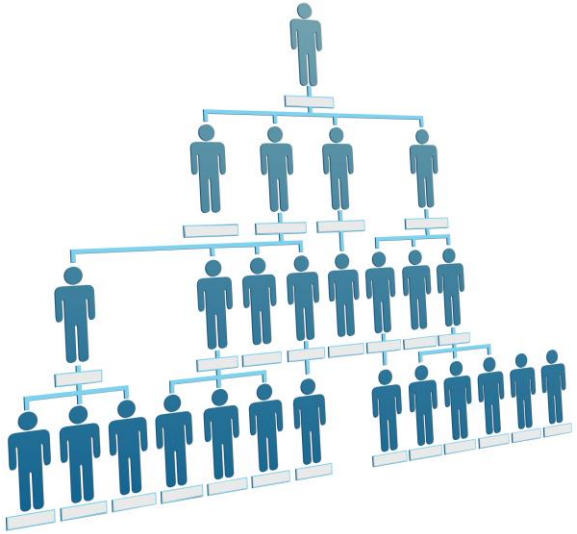
PSMM - Product / Product Group Spider Diagrams



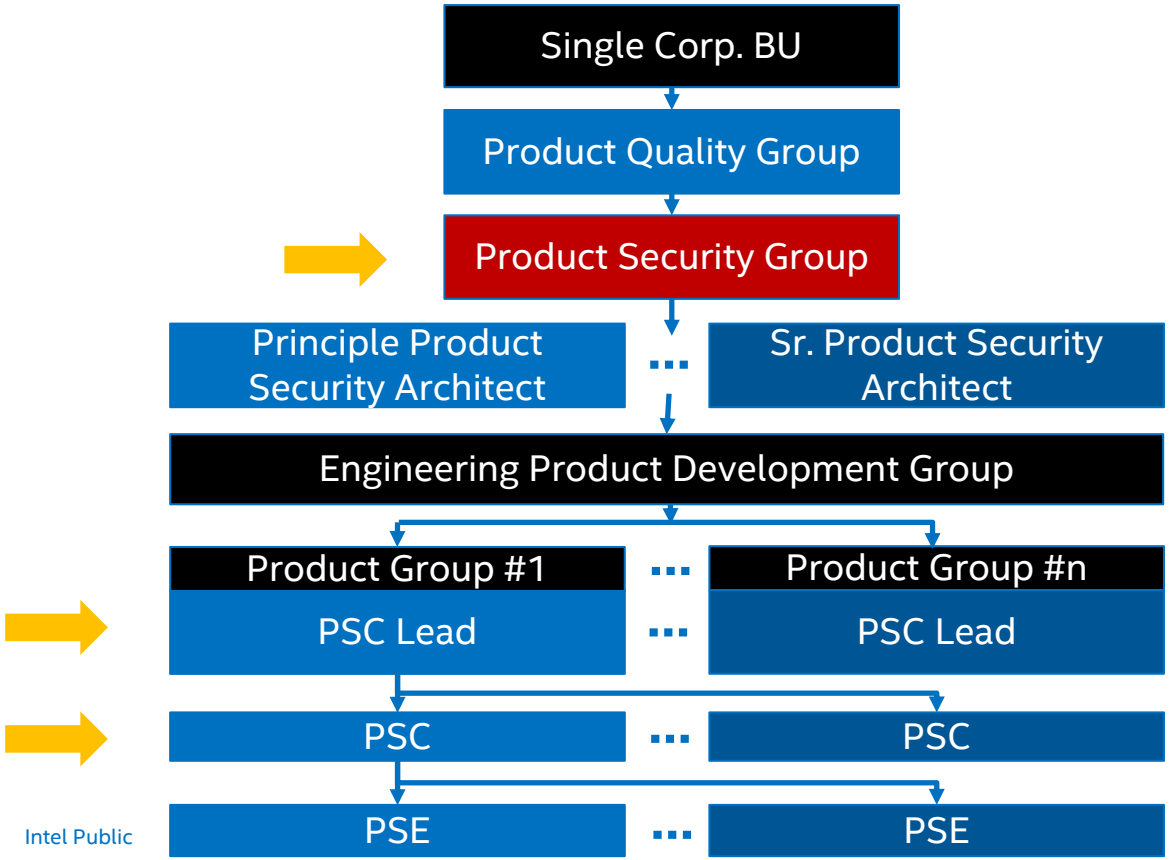


PSMM Data Collection Levels

- PSMM Data Levels
  1. Entire Corp.
  2. All Corp. BUs side-by-side
  3. Single Corp. BU
  4. All Product Groups in a Single Corp. BU
  5. Single Product Group
  6. Single Product Line
  7. Agile Team (optional)
  8. Individual (training only)
- Data can be collected at any and all levels; the lower the better
- Data should be refreshed every 6 months



Organizational Structure – Who Collects the Data



EVP & GM

VP

Sr. Director

Sr. Architect

SVP Engineering

VP Engineering

Architect

Sr. Engineer

QA Engineer

Objectively Measuring PSMM Levels

Validation: How do we keep it honest? Peer Review

- Individual PSCs score their own products
  - If they do not know the answers then they should engage their product teams to get accurate answers
- PSCs from one product group are assigned to review metrics from their peers in a different product group
- PSC Leads score their entire product group from their perspective
- PSC Leads review the scores of their product group's PSCs and other product group leads to identify and correct gross inaccuracies
- The Product Security and Privacy Governance Team (SDLGov) performs rolling audits to ensure compliance, accuracy and consistency

Simple Scoring

PSMM Level	Min. Score	Max. Score	Considered "In" Score
0-NA	0	19	0-19
1-None	20	39	20-29
2-Basic	40	59	30-49
3-Initial	60	79	50-69
4-Acceptable	80	94	70-84
5-Mature	95	100	85-100

- Simple addition to compute scores (20 x 5 = 100)
- Non-weighted
- Operational, Technical, and Combined scores

Detailed MS Word Doc – PSIRT

4.4 PSIRT

This parameter measures how well the company's brand and customers are protected from externally reported product vulnerabilities. PSIRT = Product Security Incident Response Team.

Level 1 None

- No incident response team
- No incident response procedures

Detailed MS Word Doc – PSIRT

4.4 PSIRT

Level 2 Initial

- Setup and establish a partnership with the Computer Security Incident Response Team (CSIRT)
- Security Architects become PSCs and form an early warning system
- **BSIMM-CMVM1.1**: Create or interface with incident response

Detailed MS Word Doc – PSIRT

4.4 PSIRT

Level 3 Basic

- Crisis management procedures defined and used
- PSCs trained on Security Bulletin creation
- Must be able to achieve PSIRT SLA response times
- **BSIMM-CMVM1.2**: Identify software defects found in operations monitoring and feed them back to development

Detailed MS Word Doc – PSIRT (cont.)

4.4 PSIRT

Level 4 Acceptable

- Dedicated PSG-managed team with well-defined procedures
- PSCs create quality Security Bulletins
- Must be able to consistently achieve all PSIRT SLA response times
- **BSIMM-CMVM2.1**: Have emergency codebase response
- **BSIMM-CMVM2.2**: Track software bugs found in operations through the fix process

Detailed MS Word Doc – PSIRT (cont.)

4.4 PSIRT

Level 5 Mature

- 24x7 coverage integrated with entire company
- PSCs are fast, accurate, and follow process
- Consistently achieve all PSIRT SLA response times
- **BSIMM-CMVM3.1**: Fix all occurrences of software bugs found in operations
- **BSIMM-CMVM3.2**: Enhance the SSDL to prevent software bugs found in operations
- **BSIMM-CMVM3.3**: Simulate software crisis
- **BSIMM-CMVM3.4**: Operate a bug bounty program (optional)

Detailed MS Word Doc – Technical

5.4 Security Testing

This parameter measures how well software security requirements are being performed and verified by both engineering and QA.

Level 1 None

- No security plan. No security plan testing or validation performed.

Level 2 Initial

- Security plan created. Security plan testing and validation performed occasionally.

Level 3 Basic

- Security plan testing and validation performed completely at least once before release
- Functional Testing (what you know) performed to verify intended behavior

Level 4 Acceptable

- Security plan testing and validation performed completely several times before release
- Negative Space Testing (what hackers know) performed to identify non-intended behavior

Level 5 Mature

- Security plan testing and validation performed continuously and completely both before and after release

Technical

Intel PSMM Level 4: Acceptable

1. **Security Requirements Plan/DoD**: Product teams conduct and report on required security tasks as defined in their security plan for their project milestones
2. **Architecture and Design Reviews**: Frequent architecture reviews are conducted
3. **Threat Modeling**: Trained security architects oversee frequent reviews accounting for all known attack vectors
4. **Security Testing**: Security testing performed completely several times
5. **Static Analysis**: Majority of products analyzed frequently, defect rate decreasing
6. **Dynamic Analysis**: Applicable products analyzed frequently, high and medium severity issues fixed. Defect rate near zero (0) in finished product.
7. **Fuzz Testing**: Scans run frequently, high and medium severity issues fixed, new custom scripts created
8. **Penetration Testing**: Resident pen testing expert available, defects in Bugzilla
9. **Manual Code Reviews**: Conducted on all potentially risky code using a shared tool
10. **Secure Coding Standards**: Following adopted standards
11. **Open Source/3rd Party COTS Libraries**: Fully maintaining all documented 3rd party libraries and versions shipped across all supported releases
12. **Privacy**: Privacy is integrated with product security

MS Excel Drop Down Lists

	A	B	C	D	E	F	G
1	**Intel Security PSMM Parameter Scoring Drop Down Lists**						
2			**Last Updated: 14 August 2015**				
3							
4			**NOTE**: Do not delete. This worksheet is needed for the dropdown lists in the other worksheets.				
5			See the "Intel Security PSMM" document for a full description of each level for each parameter.				
6			The PSMM templates and documents are not confidential, however the real data collected by Intel is confidential.				
7							
8	**Operational Parameters**				**Technical Parameters**		
9		**Para**	**Short Description**			**Para**	**Short Description**
10	1	**Program**			1	**Security Requirements Plan / Defenition of Done (DoD)**	
11			**0-NA:** Not Applicable				**0-NA:** Not Applicable
29			**4-Acceptable:** Complies with ISO 27034; SDL evidence; proactive, not reactive; exception process				**4-Acceptable:** Trained security architects oversee frequent reviews accounting for all known attack vectors
30			**5-Mature:** Adapted to agile and waterfall, HW/SW, IoT; high maturity level scores				**5-Mature:** Separation of privileges and type enforcement address unknown attack vectors
31	4	**PSIRT**			4	**Security Testing**	
32			**0-NA:** Not Applicable				**0-NA:** Not Applicable
33			**1-None:** No incident response procedures or team				**1-None:** No security plan. No security plan testing or validation performed.
34			**2-Initial:** Setup and establish a partnership with CSIRT; PSCs are early warning system				**2-Initial:** Security plan created. Security plan testing and validation performed occasionally.
35			**3-Basic:** Crisis management procedures defined and used; PSCs trained on SB creation				**3-Basic:** Security plan testing and validation performed completely at least once before release
36			**4-Acceptable:** Dedicated PSG-managed team with well-defined procedures; PSCs create quality SBs				**4-Acceptable:** Security plan testing and validation performed completely several times before release

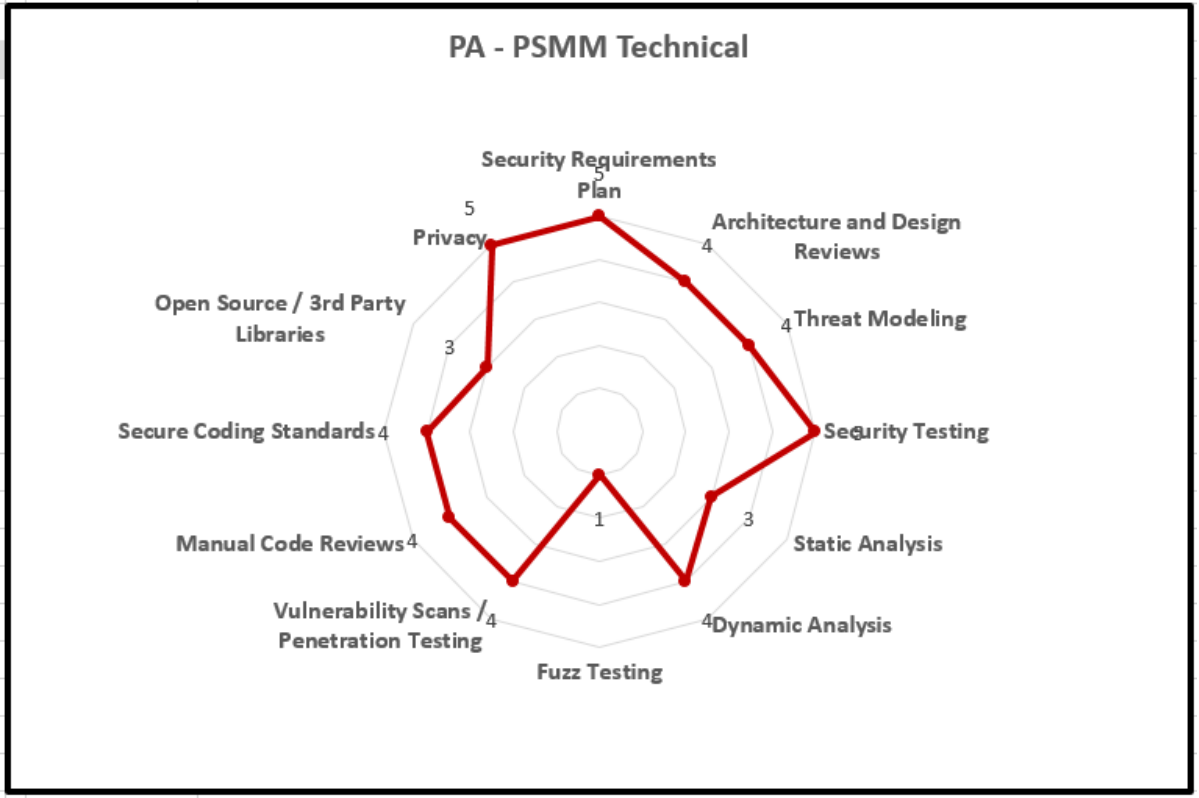
3	**Threat Modeling**	
		0-NA: Not Applicable
		1-None: Lack of modeling exposed by large number of customer reported vulnerabilities and attacks
		2-Initial: Major attack vectors identified and addressed
		3-Basic: Formal threat modeling conducted by product/security architects before all major releases
		4-Acceptable: Trained security architects oversee frequent reviews accounting for all known attack vectors
		5-Mature: Separation of privileges and type enforcement address unknown attack vectors

MS Excel Product Scorecard

	A	B	C	D	E
1		**<Company> PSMM Scorecard - Product**			
2		To be completed by each PSC for each of their product lines.			
3					**<Company> Confidential - For Internal Use Only**
4		**Product Acronym:**		PA	
5		**Product Name:**		Product A	
6		**Date Scored:**		October 1, 2015	
7					
8		**INSTRUCTIONS:**		Go to the "Product PMM Level" column (E) and use the dropdowns to select maturity level 1-5 for each row.	
9				Grey cells contain formulas. Do not overwrite.	
10				See the "Intel Security PSMM" document for a full description of each level for each parameter.	
11					
13		**Technical Parameters**		**Points**	**Product PSMM Level**
15	1	**Security Requirements Plan**		5	5-Mature: Product teams engage their PSCs early
16	2	**Architecture and Design Reviews**		4	4-Acceptable: Frequent architecture reviews are conducted
17	3	**Threat Modeling**		4	4-Acceptable: Trained security architects oversee frequent reviews accounting for all known attack vectors
18	4	**Security Testing**		5	5-Mature: Continuous security testing
19	5	**Static Analysis**		3	3-Basic: Static analysis runs automatically with builds
20	6	**Dyna**			
21	7	**Fuzz**			
22	8	**Vuln**			
23	9	**Man**			
24	10	**Secure Coding Standards**		4	4-Acceptable: Following adopted standards; Product Group's startards really are standards
25	11	**Open Source / 3rd Party Libraries**		3	3-Basic: Run inventory tools (e.g. BlackDuck)
26	12	**Privacy**		5	5-Mature: Product security implies privacy; all new products conduct a privacy review
28		Technical Subtotal:		46	
29		**Technical PSMM Score:**		**3.8**	**4-Acceptable**

0-NA: Not Applicable
1-None: Use no static analysis tools or use compiler flags only
2-Initial: Use one or more static analysis tools
3-Basic: Static analysis runs automatically with builds
4-Acceptable: Majority of product analyzed frequently; defect rate decreasing
5-Mature: Defects fixed quickly; real defect rate near zero (0)

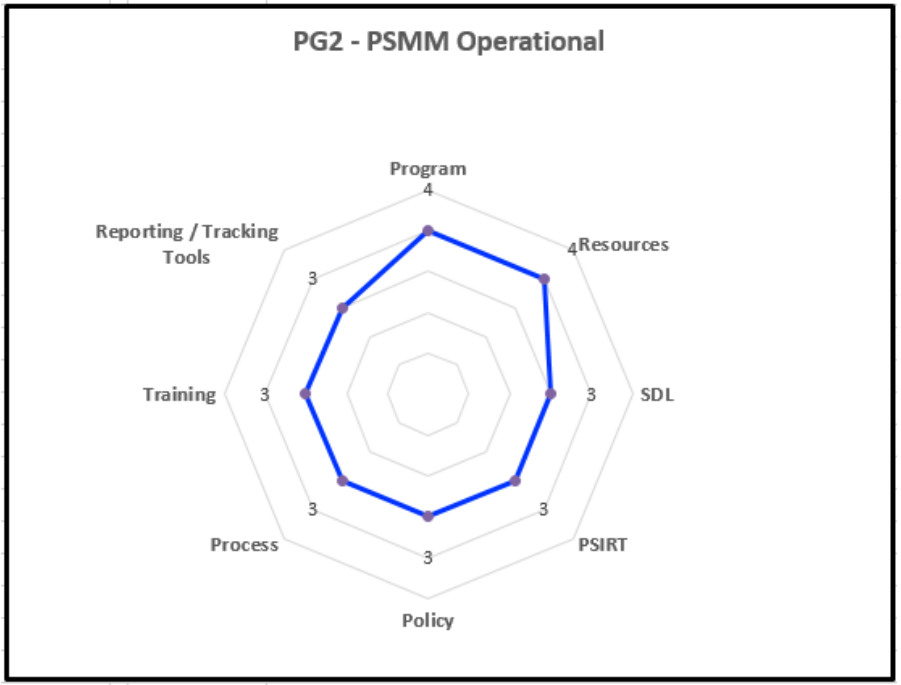
MS Excel Product Spider Diagram

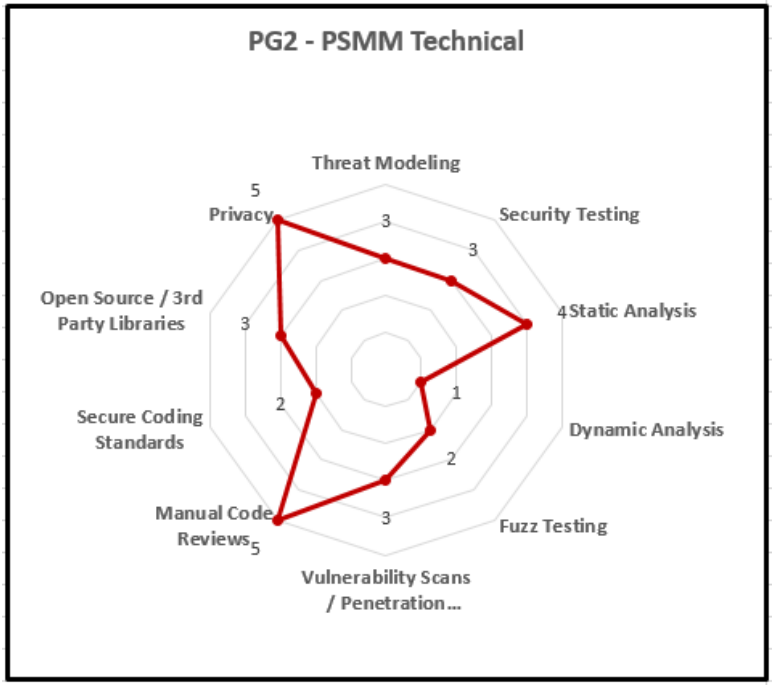


MS Excel Product Group Scorecard

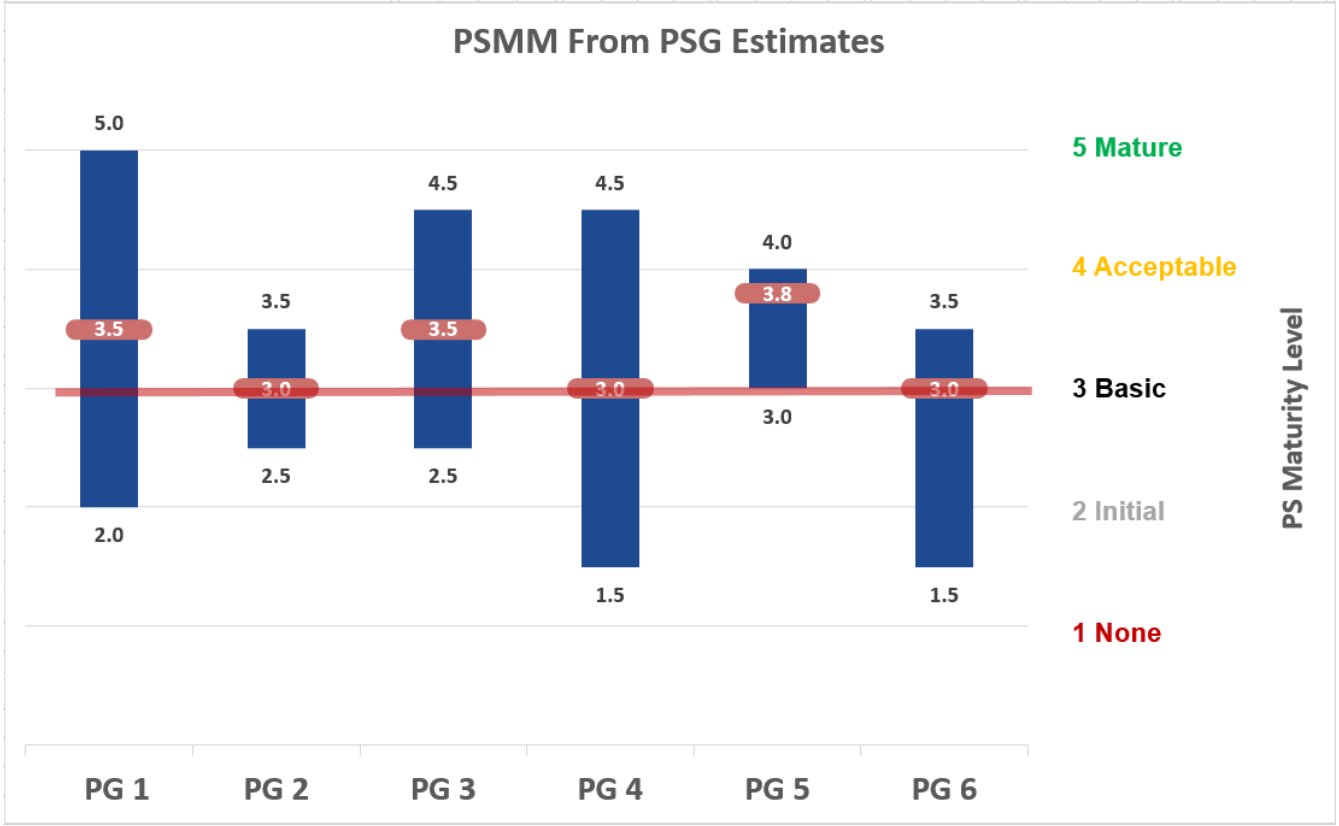
		Operational Parameters	Points	BU PSMM Level
1	Program	4	4-Acceptable: Demonstrates BUs' continued improvement efforts, community contribution, and leadership i
2	Resources	4	4-Acceptable: Have a PSC for each Tier-1 & Tier-2 product
3	SDL	3	3-Basic: SDL defined, published and used, engineering trained
4	PSIRT	3	3-Basic: Crisis management procedures defined and used; PSCs trained on SB creation
5	Policy	3	3-Basic: Policies published, followed, and enforced
6	Process	3	3-Basic: Sustainable security methodologies and best practices adopted
7	Training	3	3-Basic: Mandatory set of defined product security courses; PSCs have completed mandatory courses
8	Reporting / Tracking Tools	3	3-Basic: Issues and reviews tracked in detailed spreadsheets; PSCs reporting PSIRT and Security review data
		Technical Parameters	**Points**	**BU PSMM Level**
1	Security Requirements Plan/DoD	4	4-Acceptable: Product teams conduct and report on required security tasks
2	Architecture and Design Reviews	2	2-Initial: Informal architectural review conducted by engineering
3	Threat Modeling	3	3-Basic: Formal threat modeling conducted by product/security architects before all major releases
4	Security Testing	3	3-Basic: Occasional security testing
5	Static Analysis	4	4-Acceptable: Majority of product analyzed frequently; defect rate decreasing
6	Dynamic Analysis	1	1-None: User feedback only from their tools
7	Fuzz Testing	2	2-Initial: Free/Open Source tools used by SDET (e.g. Peach Fuzzer)
8	Vulnerability Scans / Penetration Testing	3	3-Basic: Vulnerability scans occasionally performed, defects analyzed
9	Manual Code Reviews	5	5-Mature: Conducted regularly using a code sharing collaboration tool (e.g. SmartBear Collaborator)
10	Secure Coding Standards	2	2-Initial: Aware of standards, occasional adherence
11	Open Source / 3rd Party Libraries	3	3-Basic: Run inventory tools (e.g. BlackDuck)
12	Privacy	5	5-Mature: Product security implies privacy; all new products conduct a privacy review
	Operational Subtotal:	26	
	Technical Subtotal:	37	
	Operational PSMM Score:	3.3	3-Basic
	Technical PSMM Score:	3.1	3-Basic
	PSMM Score:	**3.2**	**3-Basic**

MS Excel Product Group Spider Diagrams

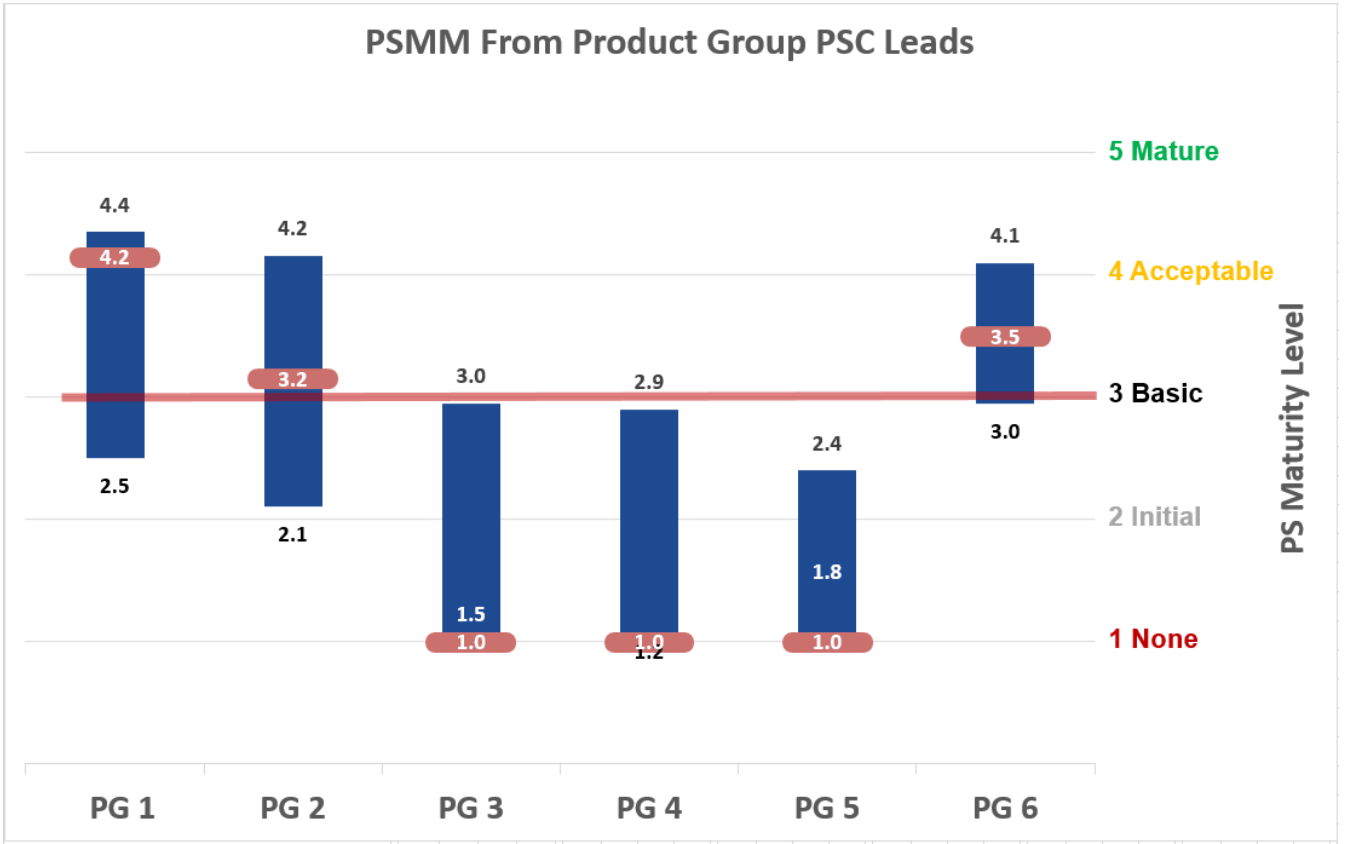




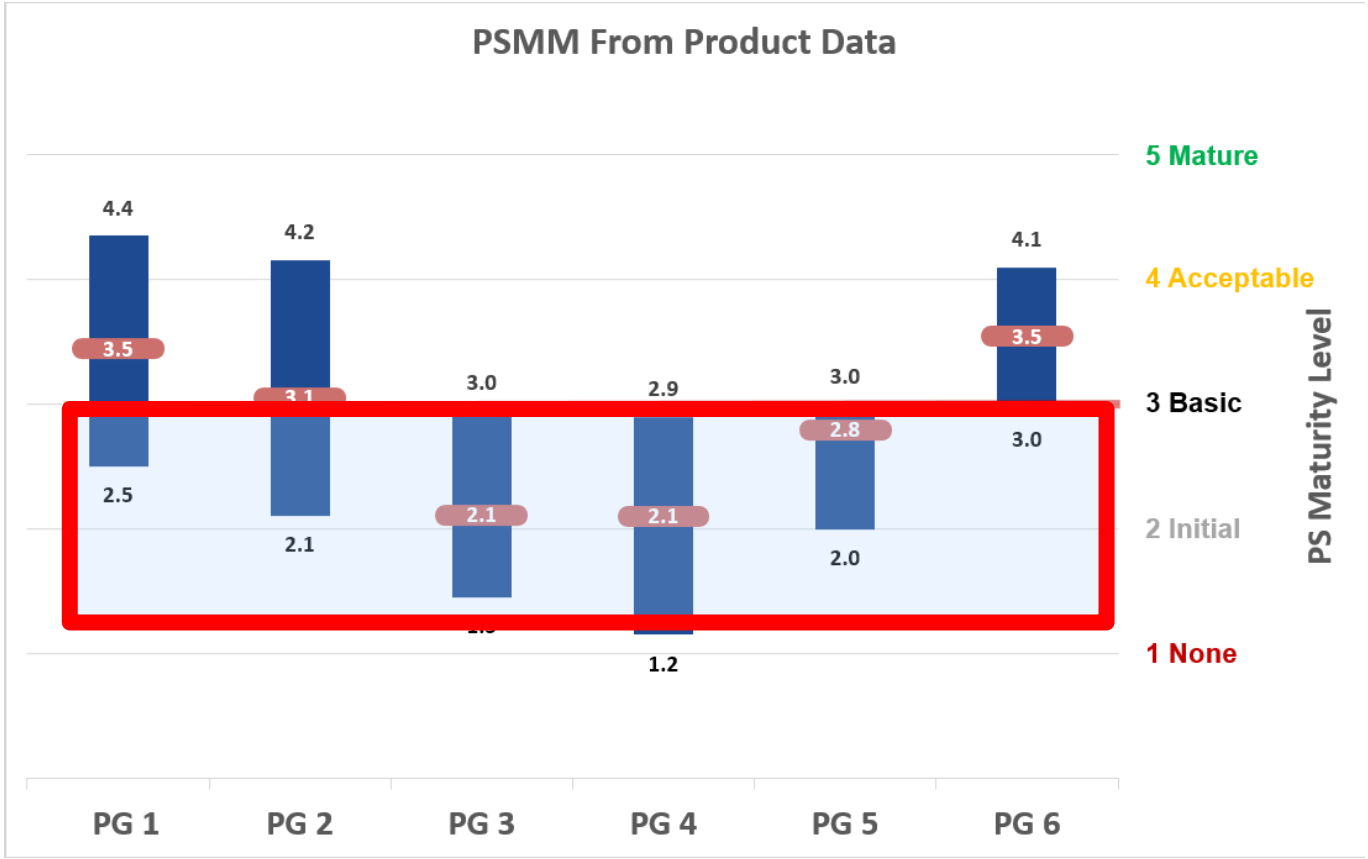
Least Accurate Metric – From PSG Estimates



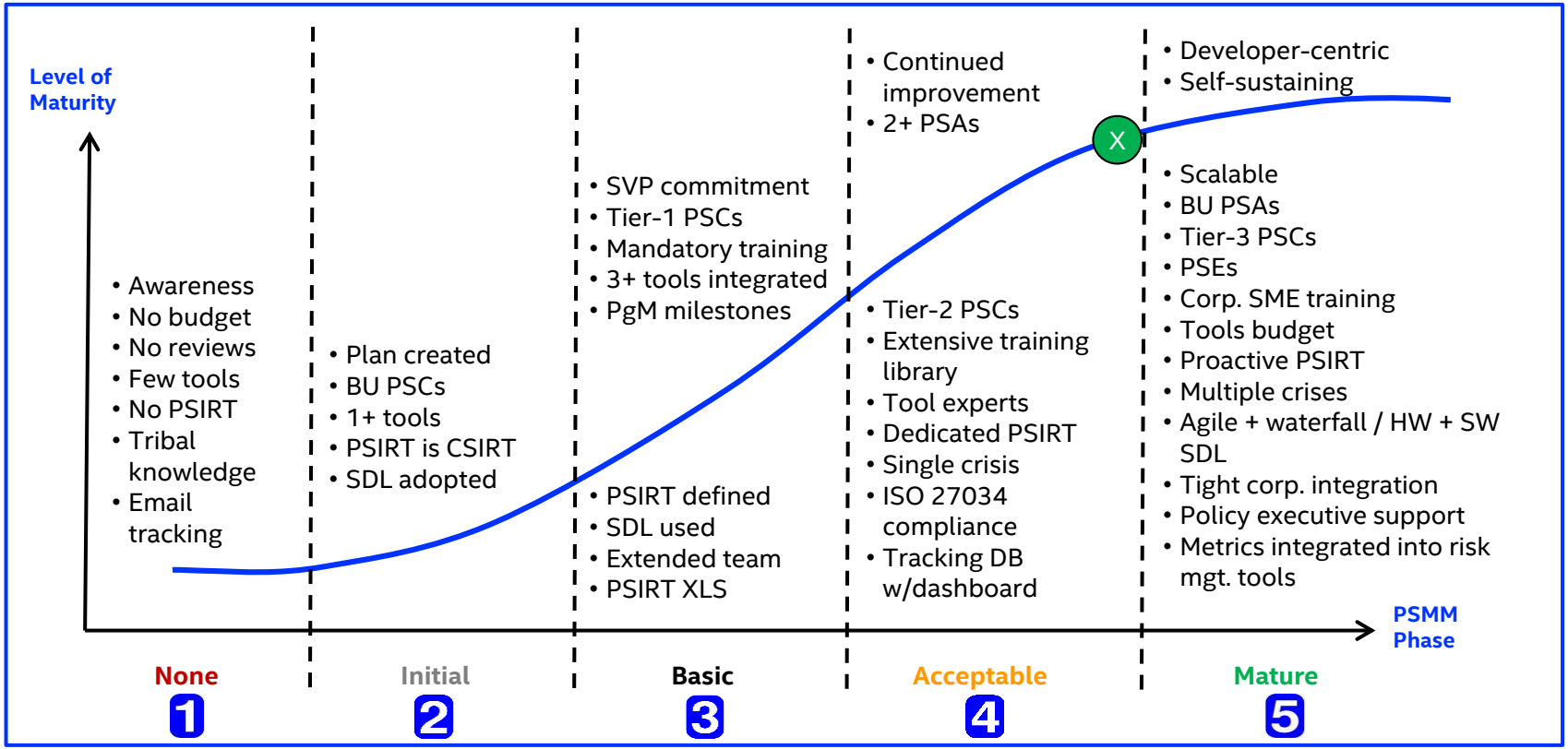
Somewhat Accurate Metric – From PSC Leads



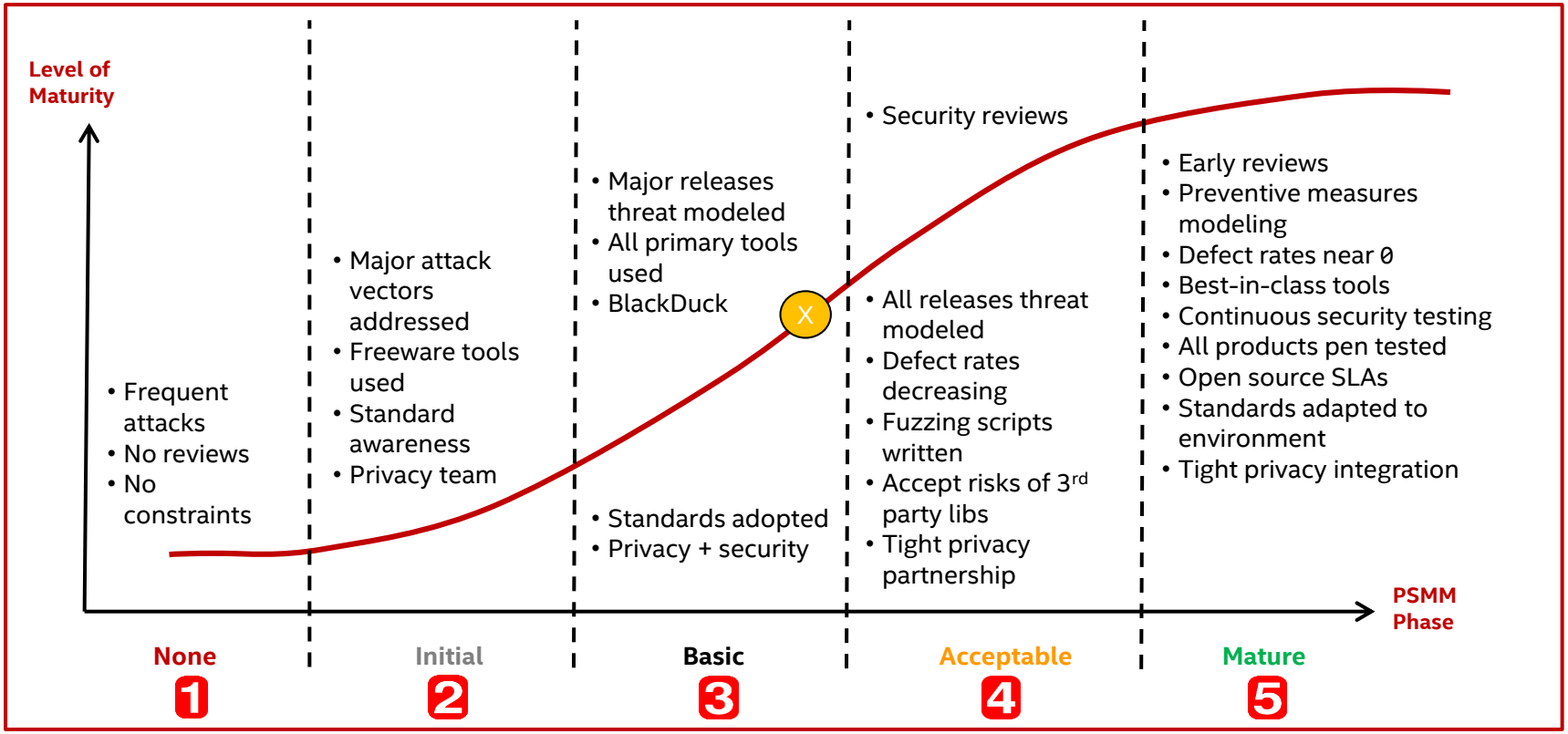
Most Accurate Metric – From Product Data



PSMM – Operational



PSMM – Technical



Key Takeaways

1) **PSMM**: A simple yet powerful way to measure the security maturity of your product security program, deliverables and outcomes

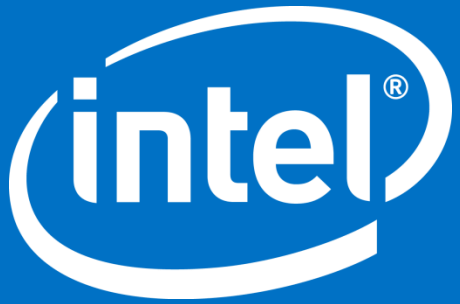
2) **Cost**: Minimal budget, typically no additional resources needed, uses existing tools, minimal engineering overhead

3) **Metrics**: Product security metrics to drive towards 4-Acceptable and 5-Mature PSMM levels; focus on what matters per product line

4) **Effort**: 20% effort to reach 4-Acceptable, +80% to reach 5-Mature

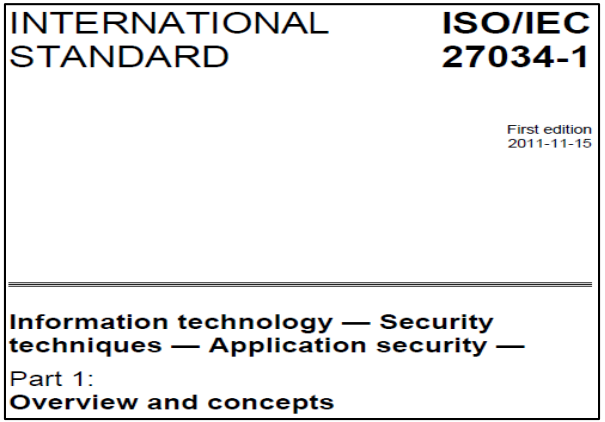
Q&A

Harold Toomey
Sr. Product Security Architect
Product Security Group
Intel Security
Harold.A.Toomey@Intel.com
W: (972) 963-7754
M: (801) 830-9987



Backup Slides

ISO 27034


INTERNATIONAL STANDARD

ISO/IEC 27034-1

First edition 2011-11-15

Information technology — Security techniques — Application security —

Part 1: Overview and concepts

ISO 27001/2: IT Security

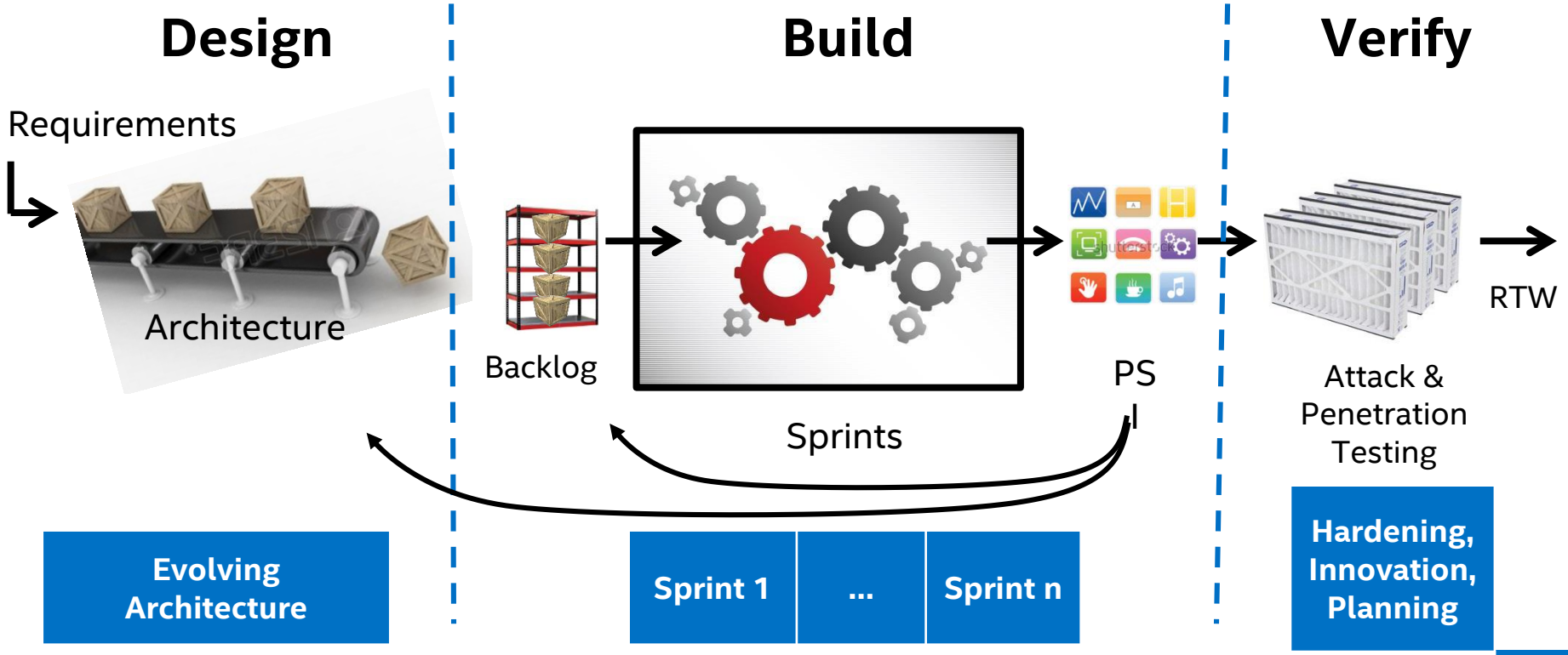
ISO 27034: Application Security

- Part 1: Overview & concepts (Nov. 2011)
- Part 2: Organization normative framework (Aug. 2015)
- Part 3: Application security management process
- Part 4: Application security validation
- Part 5: Protocols and application security controls data structure
- Part 6: Security guidance for specific applications

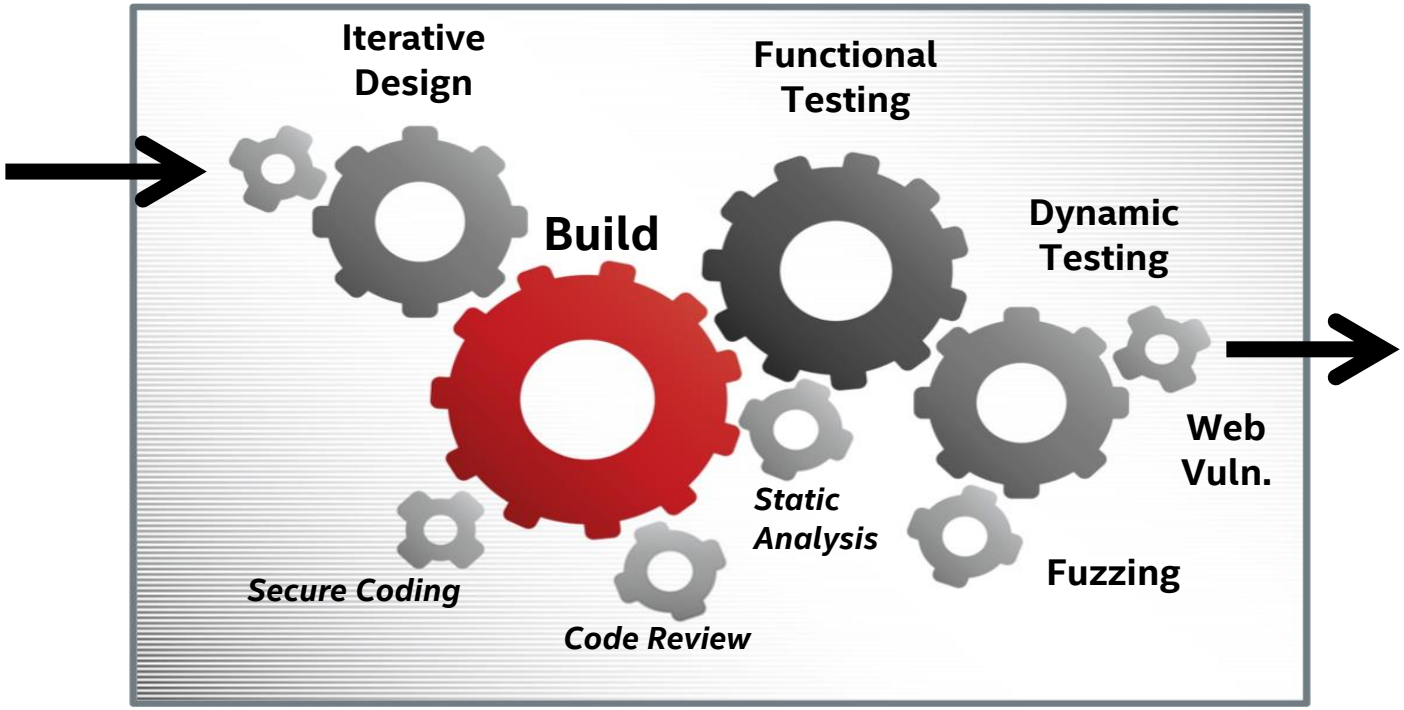
Indicates what needs to be done

Process focused

Agile SDLC


Design
Build
Verify
Requirements
Architecture
Backlog
Sprints
PS
I
Attack &
Penetration
Testing
RTW
Evolving
Architecture
Sprint 1
...
Sprint n
Hardening,
Innovation,
Planning

Agile SDL Sprint



Agile SDL Activities

Plan of Intent:
- Security activity mapping
- Answer 7 key security questions
- Initial privacy review initiated

Release Planning:
- Security plan creation
- Threat modeling
- Security architecture review
- Open source & 3rd party COTS whitelist
- Initial privacy review completed

Post Release Sustainment:
- PSIRT program
- Security metrics

Sprint Planning:
- Security plan execution
- Iterative threat model updates
- All security activities mapped in backlog
- Security backlog prioritization
- Static, dynamic & fuzzing activities
- Security Definition of Done (DoD)
- Black Duck Protex, license compliance

Development & Test:
- Security plan executed
- Security backlog verified
- Static, dynamic & fuzzing executed

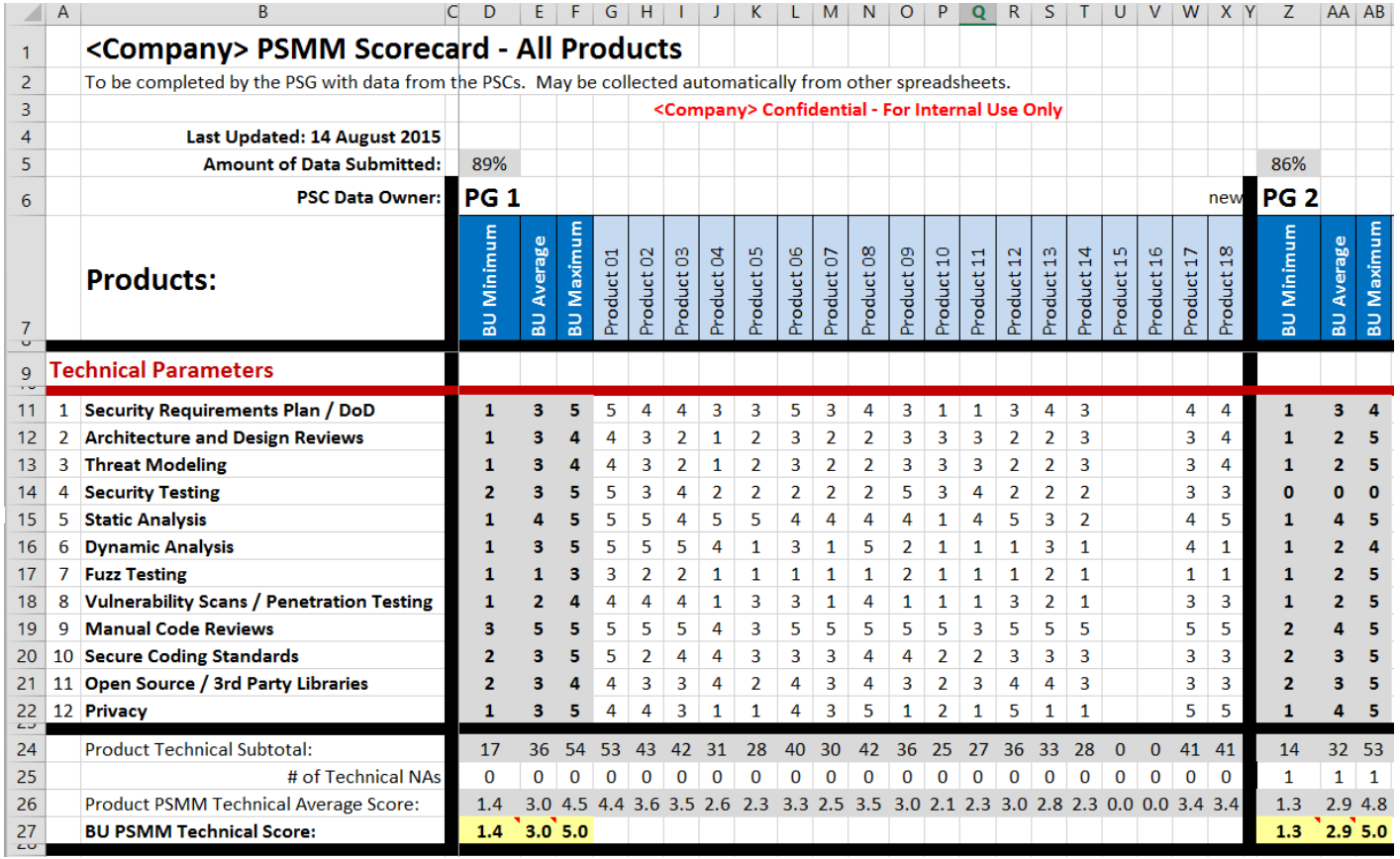
Sprint Review & Retrospective:
- Iterative security plan completed
- Security defects at “zero”
- Security exceptions tracked
- Open source & 3rd party COTS approved
- PSI security metrics achieved
- Security tools (tunes & optimized)

Release Launch Checkpoint:
- Security plan archived
- Security activities completed & reported on
- Security Definition of Done (DoD) achieved
- Threat model fully implemented
- All security exceptions documented
- Open source & 3rd party COTS exceptions
- Final privacy review

Roles & Responsibilities

Role	Responsibilities
Sr. Director Product Security	Owns all product security within BU
Product Security Architect (**PSA**)	Mentor PSCs for threat modeling, security architecture reviews, security reviews, tools, PSIRT, training
PSC Product Group Lead	Over all Product Group PSCs and products w/out PSCs
Product Security Champion (**PSC**)	Collocated security engineer / architect POC for a product
Software / Security Architect	(See PSC)
Product Security Evangelist (**PSE**)	Collocated security QA POC for a product
Support Engineering Operations (**SEO**)	Tech Support champion for a product
Product Privacy Champion **(PPC)**	(See PSC)

MS Excel All Product Groups Products Scorecard



1		**<Company> PSMM Scorecard - All Products**																																				
2		To be completed by the PSG with data from the PSCs. May be collected automatically from other spreadsheets.																																				
3																																						
4		**Last Updated: 14 August 2015**																																				
5		**Amount of Data Submitted:**	89%																																	86%		
6		**PSC Data Owner:**	**PG 1**																																	**PG 2**		
7		**Products:**	**BU Minimum**	**BU Average**	**BU Maximum**	**Product 01**	**Product 02**	**Product 03**	**Product 04**	**Product 05**	**Product 06**	**Product 07**	**Product 08**	**Product 09**	**Product 10**	**Product 11**	**Product 12**	**Product 13**	**Product 14**	**Product 15**	**Product 16**	**Product 17**	**Product 18**														**BU Minimum**	**BU Average**	**BU Maximum**
9		**Technical Parameters**																																				
11	1	**Security Requirements Plan / DoD**	**1**	**3**	**5**	5	4	4	3	3	5	3	4	3	1	1	3	4	3			4	4													**1**	**3**	**4**
12	2	**Architecture and Design Reviews**	**1**	**3**	**4**	4	3	2	1	2	3	2	2	3	3	3	2	2	3			3	4													**1**	**2**	**5**
13	3	**Threat Modeling**	**1**	**3**	**4**	4	3	2	1	2	3	2	2	3	3	3	2	2	3			3	4													**1**	**2**	**5**
14	4	**Security Testing**	**2**	**3**	**5**	5	3	4	2	2	2	2	2	5	3	4	2	2	2			3	3													**0**	**0**	**0**
15	5	**Static Analysis**	**1**	**4**	**5**	5	5	4	5	5	4	4	4	4	1	4	5	3	2			4	5													**1**	**4**	**5**
16	6	**Dynamic Analysis**	**1**	**3**	**5**	5	5	5	4	1	3	1	5	2	1	1	1	3	1			4	1													**1**	**2**	**4**
17	7	**Fuzz Testing**	**1**	**1**	**3**	3	2	2	1	1	1	1	1	2	1	1	1	2	1			1	1													**1**	**2**	**5**
18	8	**Vulnerability Scans / Penetration Testing**	**1**	**2**	**4**	4	4	4	1	3	3	1	4	1	1	1	3	2	1			3	3													**1**	**2**	**5**
19	9	**Manual Code Reviews**	**3**	**5**	**5**	5	5	5	4	3	5	5	5	5	5	3	5	5	5			5	5													**2**	**4**	**5**
20	10	**Secure Coding Standards**	**2**	**3**	**5**	5	2	4	4	3	3	3	4	4	2	2	3	3	3			3	3													**2**	**3**	**5**
21	11	**Open Source / 3rd Party Libraries**	**2**	**3**	**4**	4	3	3	4	2	4	3	4	3	2	3	4	4	3			3	3													**2**	**3**	**5**
22	12	**Privacy**	**1**	**3**	**5**	4	4	3	1	1	4	3	5	1	2	1	5	1	1			5	5													**1**	**4**	**5**
24		Product Technical Subtotal:	17	36	54	53	43	42	31	28	40	30	42	36	25	27	36	33	28	0	0	41	41													14	32	53
25		# of Technical NAs	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0													1	1	1
26		Product PSMM Technical Average Score:	1.4	3.0	4.5	4.4	3.6	3.5	2.6	2.3	3.3	2.5	3.5	3.0	2.1	2.3	3.0	2.8	2.3	0.0	0.0	3.4	3.4													1.3	2.9	4.8
27		**BU PSMM Technical Score:**	**1.4**	**3.0**	**5.0**																															**1.3**	**2.9**	**5.0**

MS Excel All Product Groups

<Company> PSMM Scorecard - All Product Groups (PGs)

To be completed by the PSG with data from the PSCs. May be collected automatically from other spreadsheets.

<Company> Confidential - For Internal Use Only

	PG1				PG2				PG3			
Last Updated: 14 August 2015												
Amount of Data Submitted:		88.9%				86.4%				100.0%		
Product Groups (PGs):	From Product Group PS Leads	Min. From Products	Ave. From Products	Max. From Products	From Product Group PS Leads	Min. From Products	Ave. From Products	Max. From Products	From Product Group PS Leads	Min. From Products	Ave. From Products	Max. From Products
Operational Parameters												
1 Program	4				4				1			
2 Resources	5				4				1			
3 SDL	4				3				1			
4 PSIRT	4				3				1			
5 Policy	4		NA		3		NA		1		NA	
6 Process	3				3				1			
7 Training	4				3				1			
8 Reporting / Tracking Tools	5				3				1			
Technical Parameters												
1 Security Requirements Plan / DoD	4	1	3	5	4	1	3	4	1	1	3	5
2 Architecture and Design Reviews	4	1	3	4	2	1	2	5	1	1	3	4
3 Threat Modeling	4	1	3	4	3	1	2	5	1	2	2	3
4 Security Testing	4	2	3	5	3	0	0	0	1	2	3	5
5 Static Analysis	5	1	4	5	4	1	4	5	1	2	4	5
6 Dynamic Analysis	5	1	3	5	1	1	2	4	1	1	2	4
7 Fuzz Testing	2	1	1	3	2	1	2	5	1	1	2	3
8 Vulnerability Scans / Penetration Testing	5	1	2	4	3	1	2	5	1	2	3	4
9 Manual Code Reviews	5	3	5	5	5	2	4	5	1	4	5	5
10 Secure Coding Standards	4	2	3	5	2	2	3	5	1	1	3	4
11 Open Source / 3rd Party Libraries	4	2	3	4	3	2	3	5	1	3	3	4
12 Privacy	4	1	3	5	5	1	4	5	1	1	4	5
PG Operational Subtotal:	33				26				8			
PG Technical Subtotal:	50	17	36	54	37	14	32	53	12	21	34	51
# of Operational NAs	0				0				0			
# of Technical NAs	0	0	0	0	0	1	1	1	0	0	0	0
PG PSMM Score:	4.2	2.5	3.5	4.4	3.2	2.1	3.1	4.2	1.0	1.5	2.1	3.0

	PG4				PG5				PG6			
Amount of Data Submitted:		100.0%				100.0%				100.0%		
Product Groups (PGs):	From Product Group PS Leads	Min. From Products	Ave. From Products	Max. From Products	From Product Group PS Leads	Min. From Products	Ave. From Products	Max. From Products	From Product Group PS Leads	Min. From Products	Ave. From Products	Max. From Products
Operational Parameters												
1 Program	1				1				4			
2 Resources	1				1				4			
3 SDL	1				1				3			
4 PSIRT	1				1				3			
5 Policy	1		NA		1		NA		3		NA	
6 Process	1				1				4			
7 Training	1				1				4			
8 Reporting / Tracking Tools	1				1				4			
Technical Parameters												
1 Security Requirements Plan / DoD	1	1	3	4	1	3	4	4	4	3	4	5
2 Architecture and Design Reviews	1	1	2	4	1	2	3	4	3	2	3	4
3 Threat Modeling	1	1	2	3	1	2	3	4	3	2	3	4
4 Security Testing	1	1	3	4	1	3	4	4	4	3	4	5
5 Static Analysis	1	1	4	5	1	2	3	5	3	2	4	5
6 Dynamic Analysis	1	1	3	4	1	2	3	4	3	1	3	3
7 Fuzz Testing	1	1	3	4	1	2	2	4	2	1	3	4
8 Vulnerability Scans / Penetration Testing	1	1	2	4	1	3	4	4	4	4	4	4
9 Manual Code Reviews	1	3	4	5	1	2	3	5	3	2	3	5
10 Secure Coding Standards	1	1	3	4	1	3	3	4	4	3	4	4
11 Open Source / 3rd Party Libraries	1	2	4	4	1	2	3	4	3	2	3	5
12 Privacy	1	1	3	5	1	2	4	5	5	5	5	5
PG Operational Subtotal:	8				8				29			
PG Technical Subtotal:	12	15	34	50	12	28	40	51	41	30	42	53
# of Operational NAs	0				0				0			
# of Technical NAs	0	0	0	0	0	0	0	0	0	0	0	0
PG PSMM Score:	1.0	1.2	2.1	2.9	1.0	1.8	2.4	3.0	3.5	3.0	3.5	4.1

	PG1			
Last Updated: 14 August 2015				
Amount of Data Submitted:		88.9%		
Product Groups (PGs):	From Product Group PS Leads	Min. From Products	Ave. From Products	Max. From Products
Operational Parameters				
1 Program	4			
2 Resources	5			
3 SDL	4			
4 PSIRT	4			
5 Policy	4		NA	
6 Process	3			
7 Training	4			
8 Reporting / Tracking Tools	5			

PSMM – % Overhead Costs

NOTE: High overhead % is bad