NORTH TEXAS ISSA #NTXISSA

Beyond ISO 27034 - Intel's Product Security Maturity Model (PSMM)

Harold Toomey
Sr. Product Security Architect & PSIRT Manager
Intel Corp.
2 October 2015

Agenda

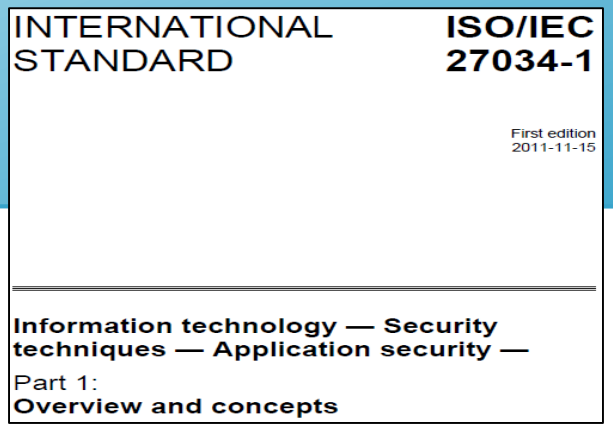
Application / Product / Software Security

- The What
  - ISO 27034
  - SDLC
- The When
  - Agile SDL

  (Security Dev. Lifecycle)
- The How
  - PSMM
  - Org structure
  - 20 Parameters
  - Metrics
  - MS Office

The “What”

ISO 27034


INTERNATIONAL STANDARD

ISO/IEC 27034-1

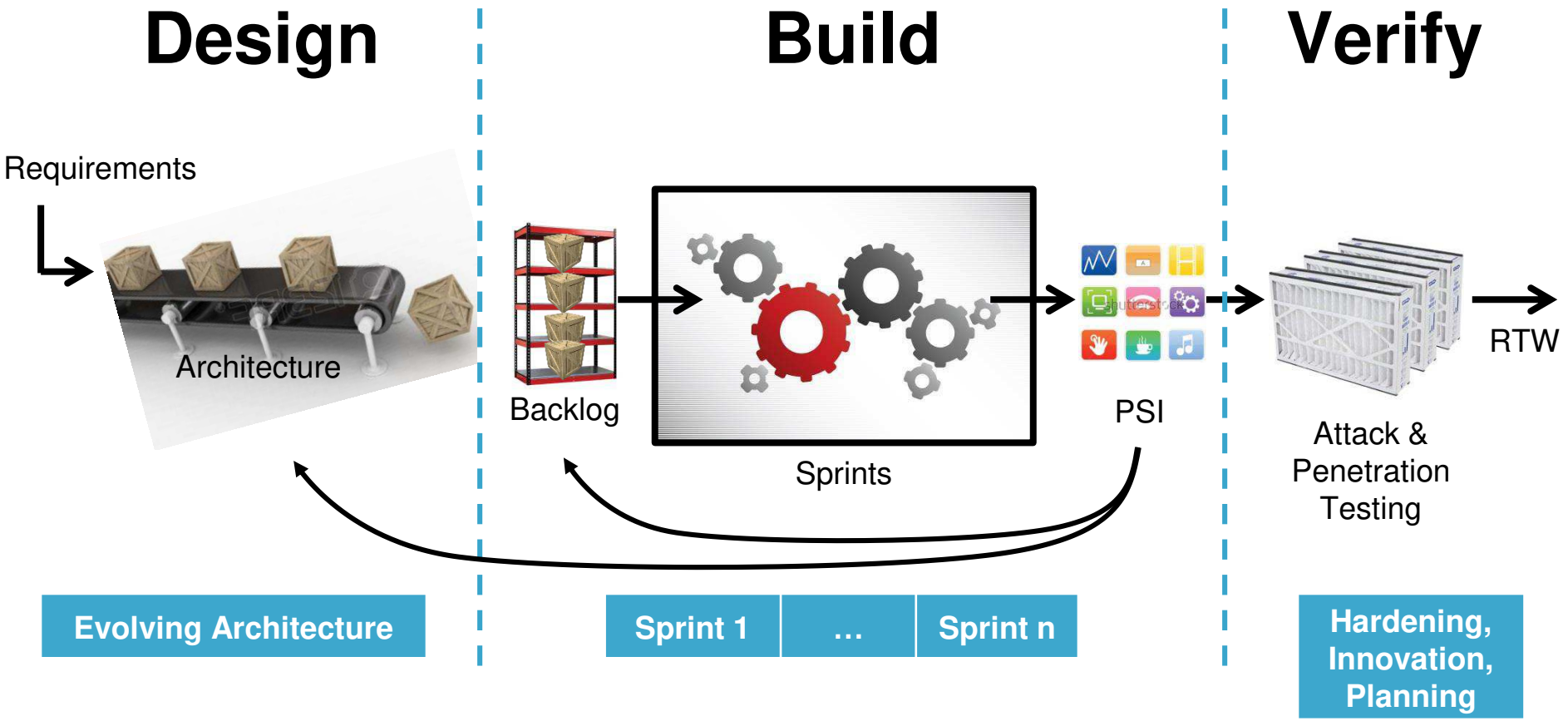
First edition 2011-11-15

Information technology — Security techniques — Application security —

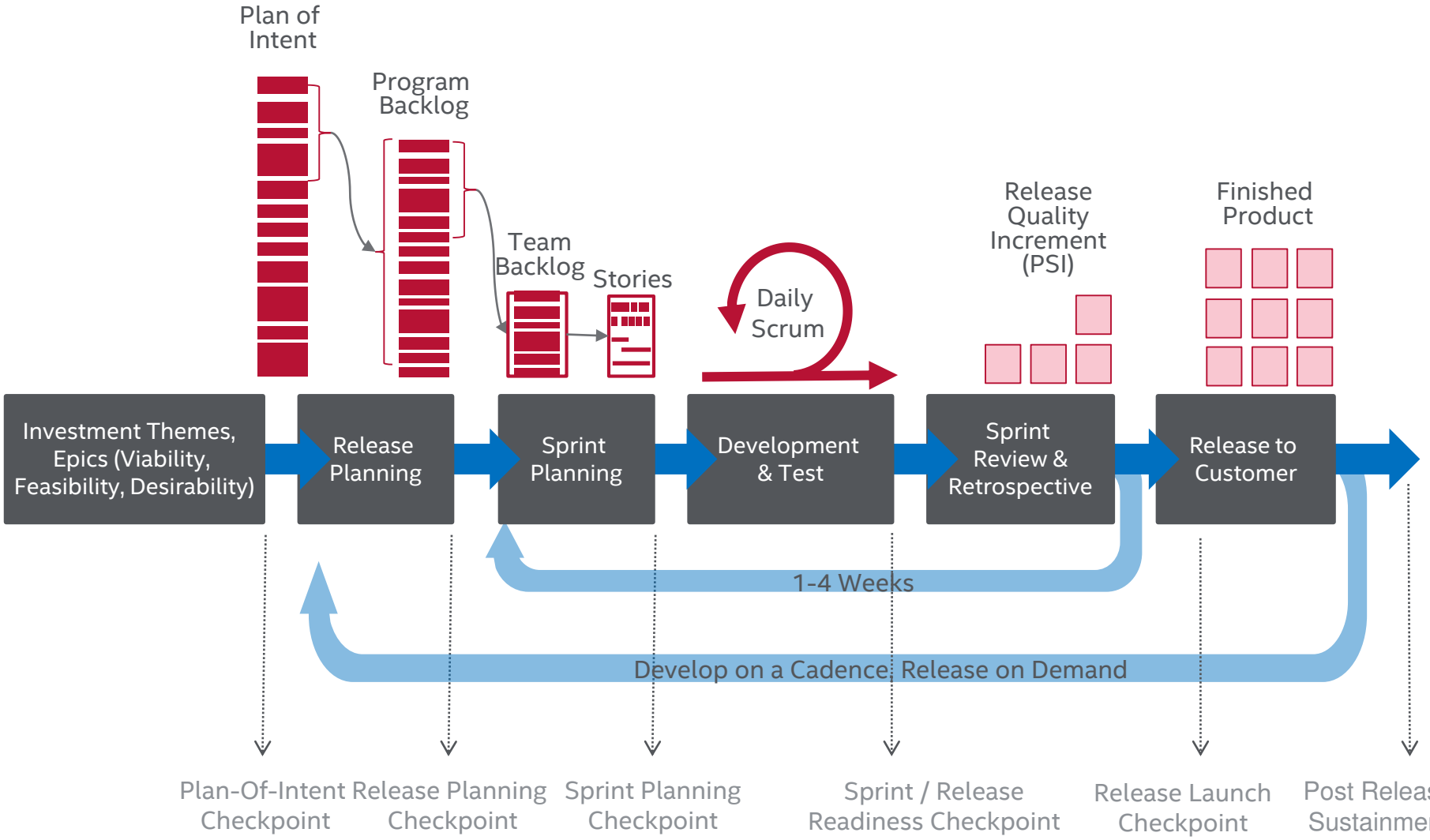
Part 1: Overview and concepts

- 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
PSI
RTW
Attack & Penetration Testing
Evolving Architecture
Sprint 1
…
Sprint n
Hardening, Innovation, Planning

Agile SDLC


Plan of Intent
Program Backlog
Team Backlog
Stories
Daily Scrum
Release Quality Increment (PSI)
Finished Product
Investment Themes, Epics (Viability, Feasibility, Desirability)
Release Planning
Sprint Planning
Development & Test
Sprint Review & Retrospective
Release to Customer
1-4 Weeks
Develop on a Cadence; Release on Demand
Plan-Of-Intent Checkpoint
Release Planning Checkpoint
Sprint Planning Checkpoint
Sprint / Release Readiness Checkpoint
Release Launch Checkpoint
Post Release Sustainment

The “When”

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

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

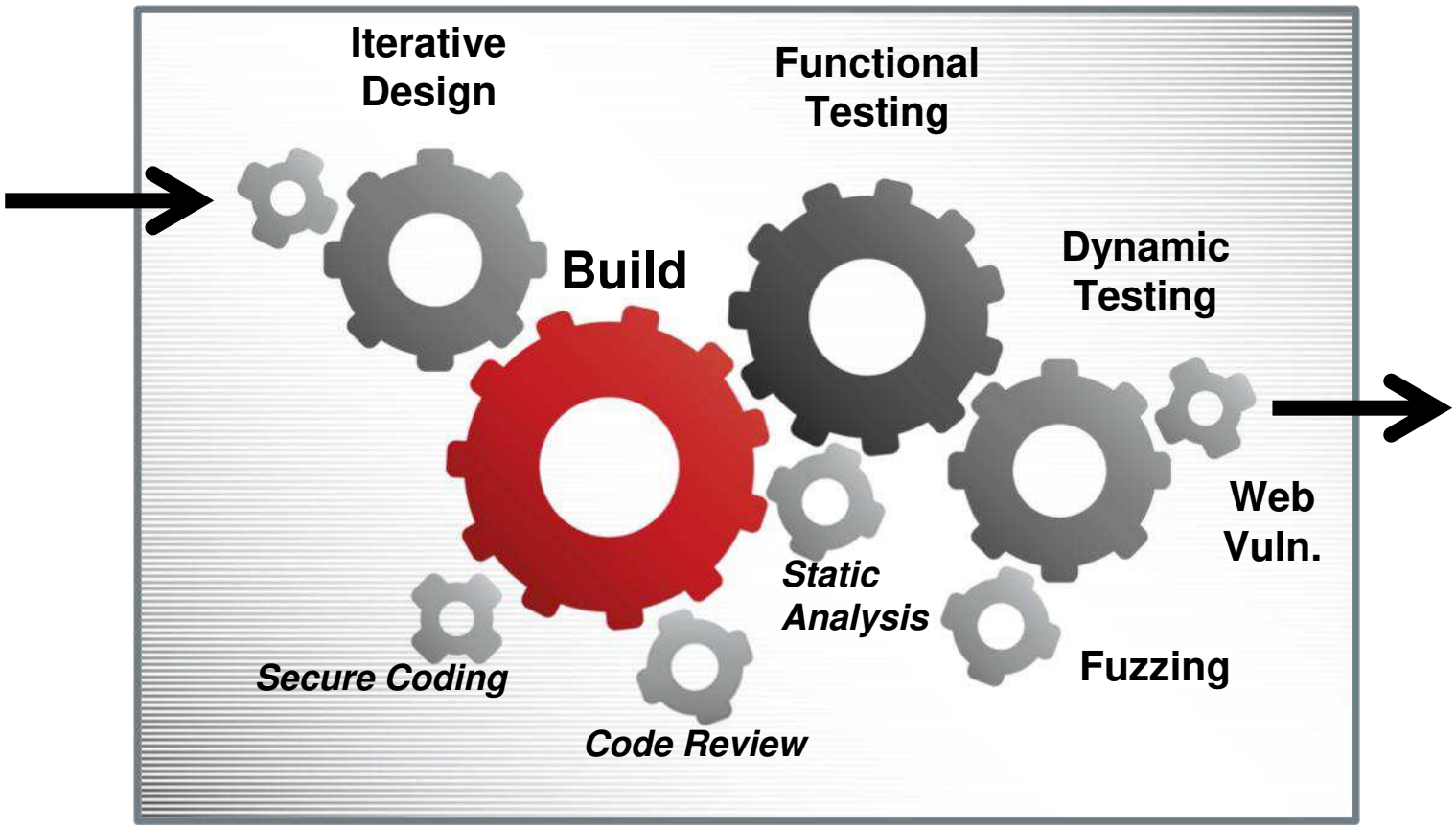
Development & Test:
- Security plan executed
- Security backlog verified
- Static, dynamic & fuzzing executed

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 & sign-off

Post Release Sustainment:
- PSIRT program
- Security metrics

Agile SDL Sprint



Sprint Checkpoint

Sprint$_n$

Product Security Includes:

Operational

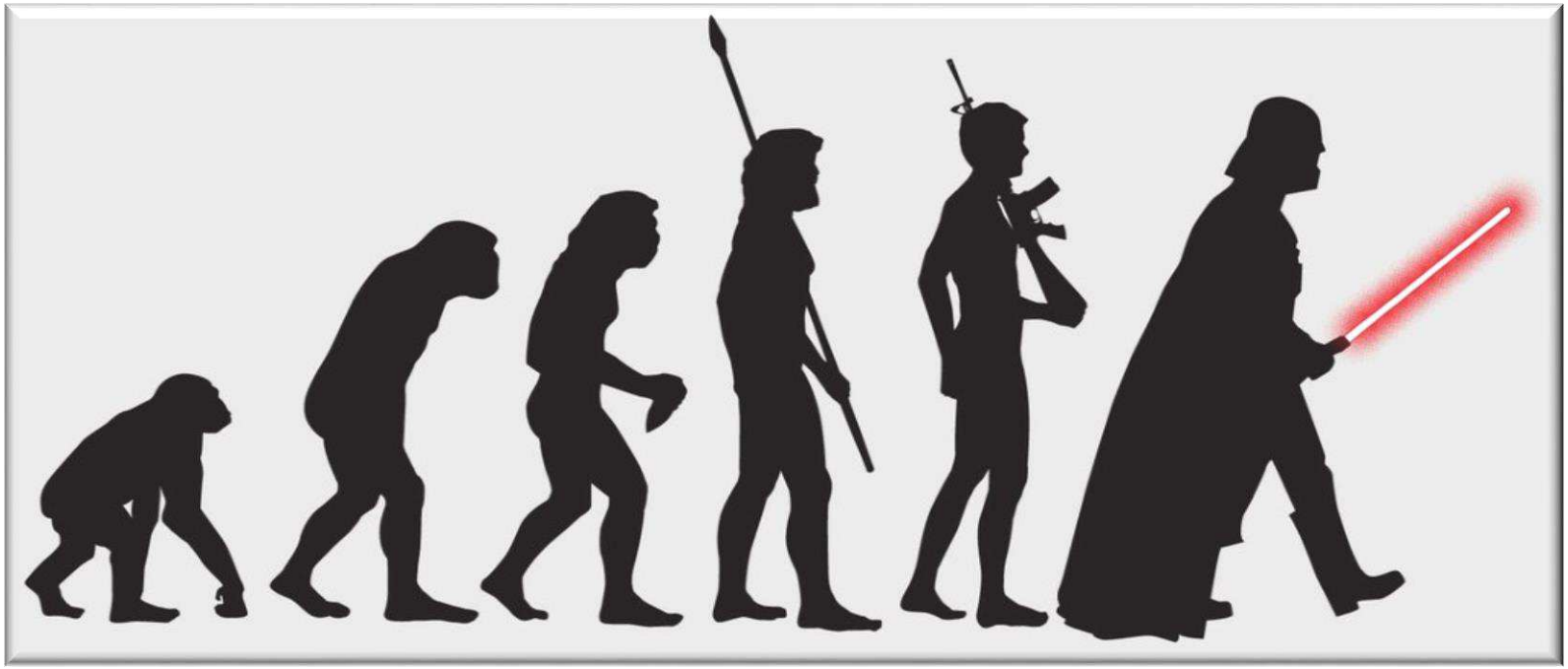
1. Program
2. Resources
3. SDL
4. PSIRT
5. Policy
6. Process
7. Training
8. Reporting & Tracking Tools

Technical

1. Security Requirements Plan [Waterfall] / 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

Problem Statement

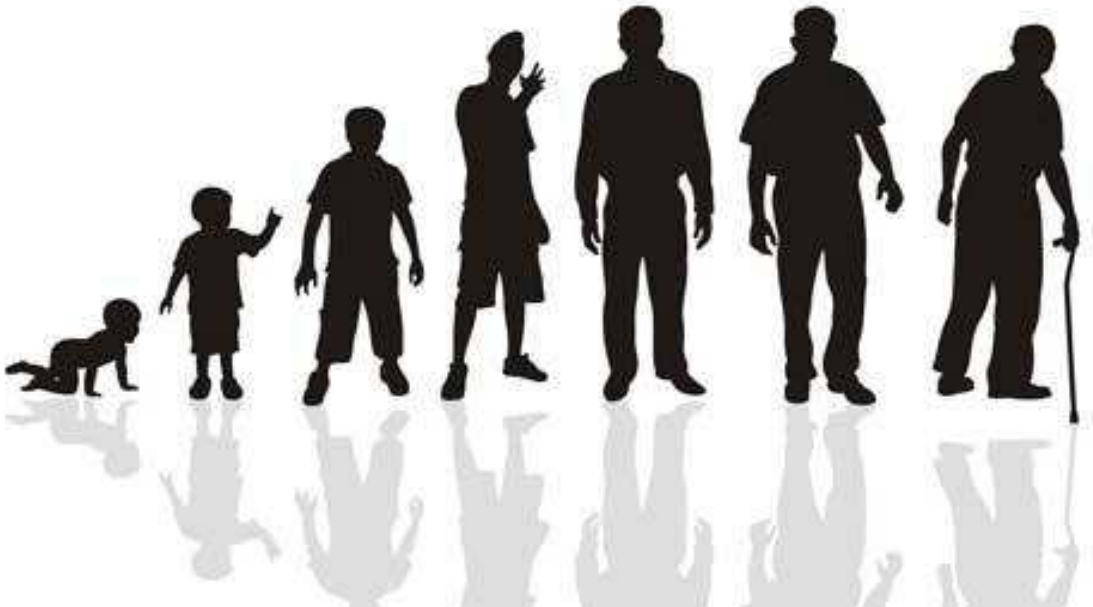
- **Problem:** We have an SDL. How well are the product teams following it?



Maturity Models

Common SDL Maturity Models

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



The “How”

Solution

The Intel Security Product Security Maturity Model (PSMM)

- Measures how well the operational and technical aspects of product security are being done
- Provides a simple, yet powerful, model which has been adopted and used company-wide
- Don't worry about perfect data, you have to start somewhere

PSMM Constraints

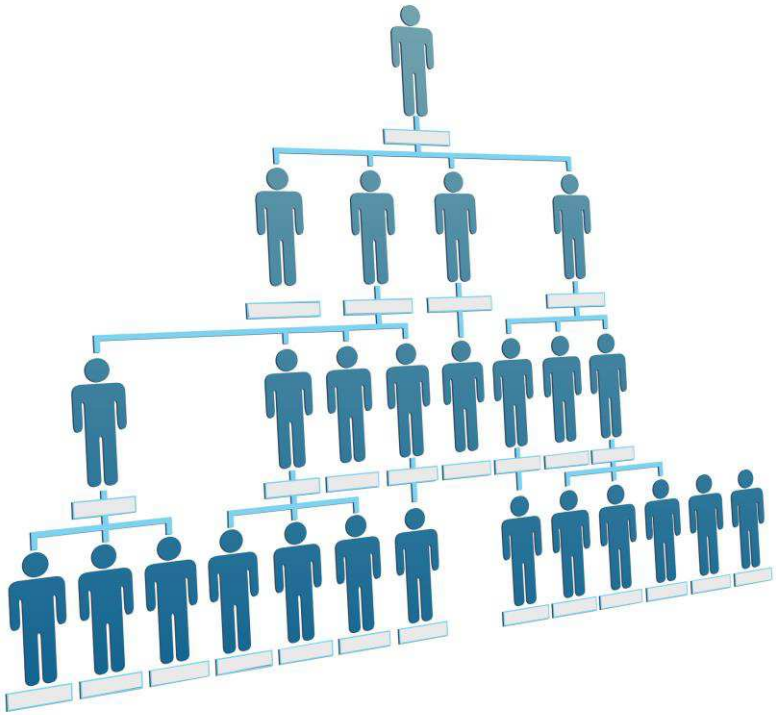
1. No budget for cool applications
   - Use COTS tools
2. No budget for additional auditors
   - Peer review
3. Be simple
   - Automated, not weighted, minimal training
4. Low overhead
   - Not a big burden on engineering teams
5. Produce insightful metrics

Rollout Feedback

1. Provide a detailed Word doc fully listing requirements for each parameter level
   - Include both Process and Quality of Execution
2. Provide simple drop-down lists in XLS
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

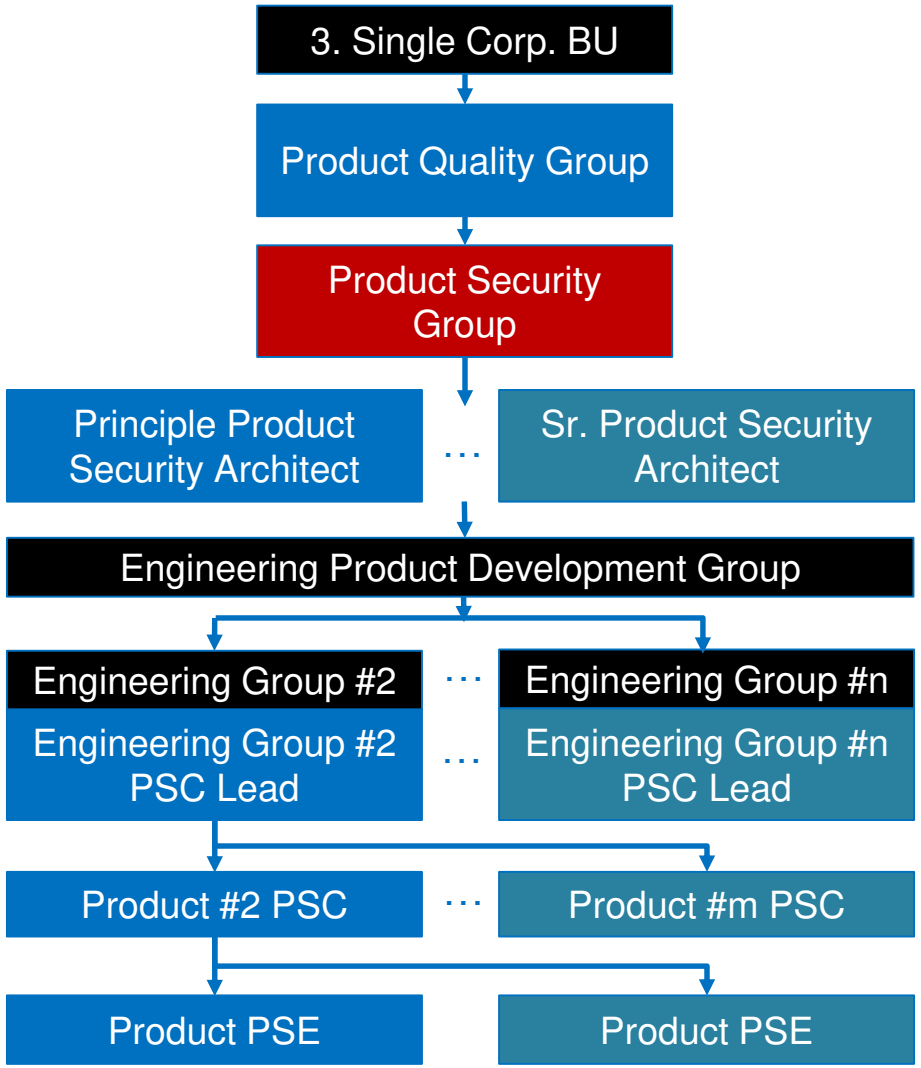
PSMM Data Collection Levels

- PSMM Data Levels
  1. Entire Corp.
  2. All Corp. BUs
  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 level; the lower the better
- Data should be refreshed every 6 months

Organizational Structure



EVP & GM

VP

Sr. Director

Sr. Architect

SVP Engineering

VP Engineering

Architect

Sr. Engineer

QA Engineer

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
TS Subject Matter Expert (**SME**)	Tech Support champion for a product
Privacy Champion	(See PSC)

Objectively Measuring PSMM Levels

How do we keep it honest? (Validation)

- 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 product group from their perspective
- PSC Leads review the scores of other product group leads to identify and correct gross inaccuracies
- The Product Security and Privacy Governance Team performs rolling audits to ensure compliance, accuracy, and consistency

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] / 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

Intel PSMM Level 4: Acceptable

Technical 4

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

Detailed Word Doc

5.4 Security Testing

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

Level

-

Level

-

Level

-

-

Level

-

-

Process vs. Quality of Execution

↑ ↑

Compliant vs. Secure

Level 5 Mature

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

The Spreadsheet

XLS Drop Down Lists

Intel Security PSMM Parameter Scoring Drop Down Lists						
		Last Updated: 14 August 2015				
		NOTE: Do not delete. This worksheet is needed for the dropdown lists in the other worksheets.				
		See the "Intel Security PSMM" document for a full description of each level for each parameter.				
		The PSMM templates and documents are not confidential, however the real data collected by Intel is confidential.				
Operational Parameters				**Technical Parameters**		
Para	**Short Description**			**Para**	**Short Description**	
1	**Program**			1	**Security Requirements Plan / Defenition of Done (DoD)**	
	0-NA: Not Applicable				**0-NA:** Not Applicable	
	1-None: No Product Security Group (PSG) program exists				**1-None:** Ad hoc - local architectural reviews only; No security plans developed at project's start	
	2-Initial: Aware and committed to adoption across the BU				**2-Initial:** Standard security requirement tasks defined	
2						
3						
	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	
	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	
4	**PSIRT**			4	**Security Testing**	
	0-NA: Not Applicable				**0-NA:** Not Applicable	
	1-None: No incident response procedures or team				**1-None:** No security plan. No security plan testing or validation performed.	
	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.	
	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	
	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	

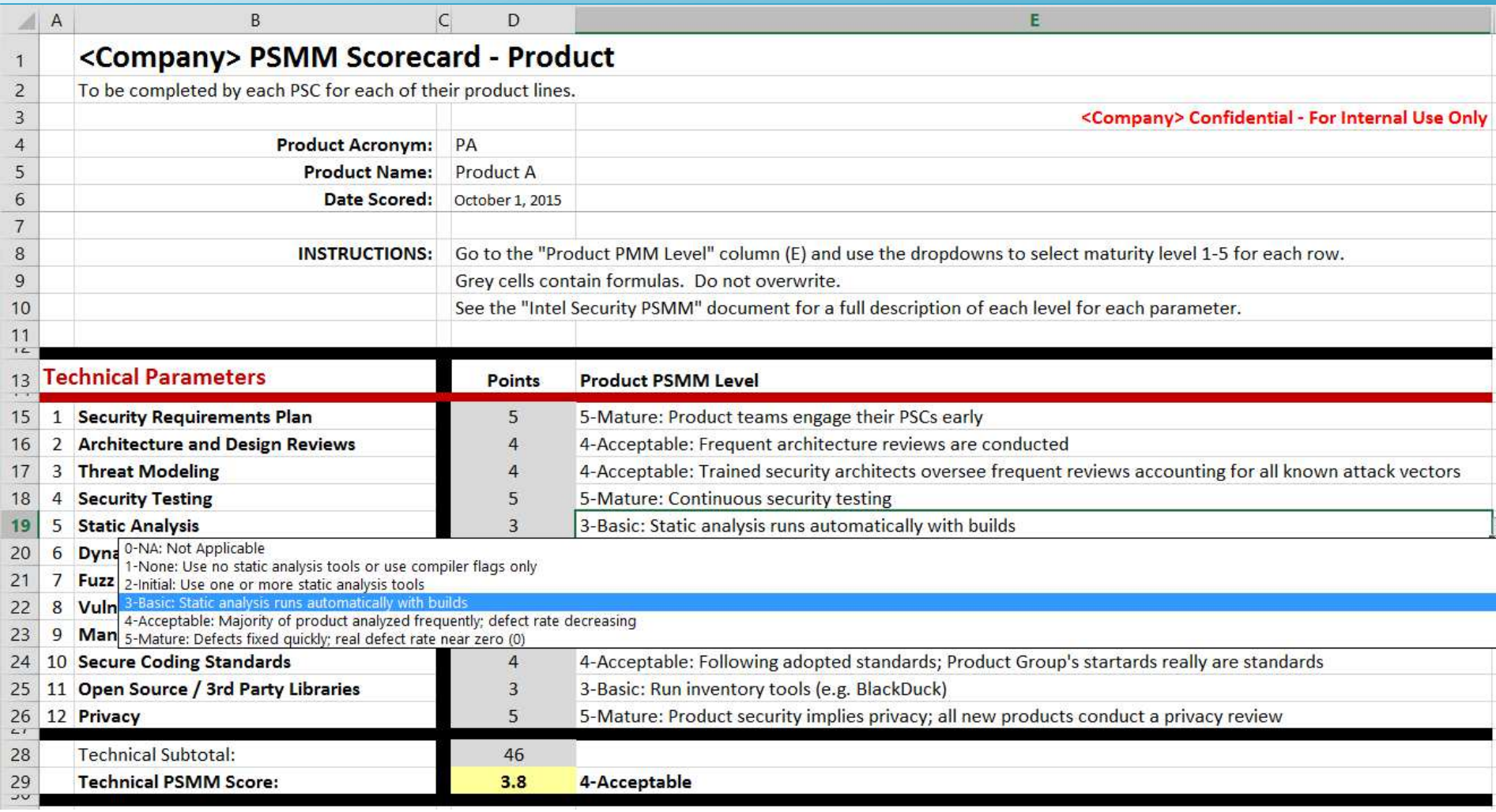
3	**Threat Modeling**	
		0-NA: Not Applicable
		1-None: Lack of modeling exposed by large number of customer reported vulnerabilities and attacks
		2-Initial: Major attack vectors identified and addressed
		3-Basic: Formal threat modeling conducted by product/security architects before all major releases
		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

Simple Scoring

PSMM Level	Min. Score	Max. Score	Considered "In" Score
1-None	20	39	20-29
2-Basic	40	59	30-49
3-Initial	60	79	50-69
4-Acceptable	80	99	70-89
5-Mature	100	100	90-100

- Simple addition to compute scores
- Non-weighted
- Operational, Technical, and Combined scores

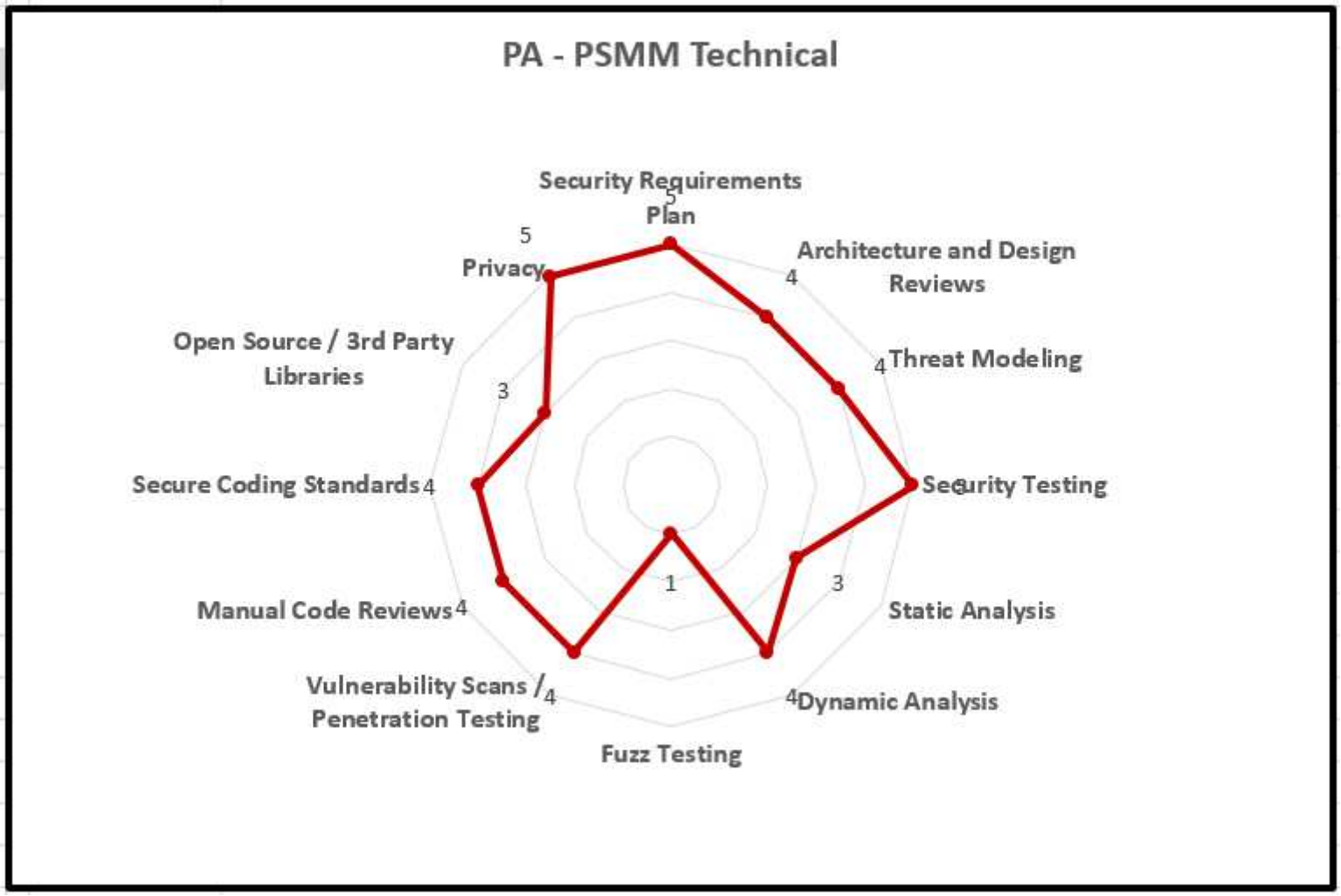
XLS Product Scorecard



	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)

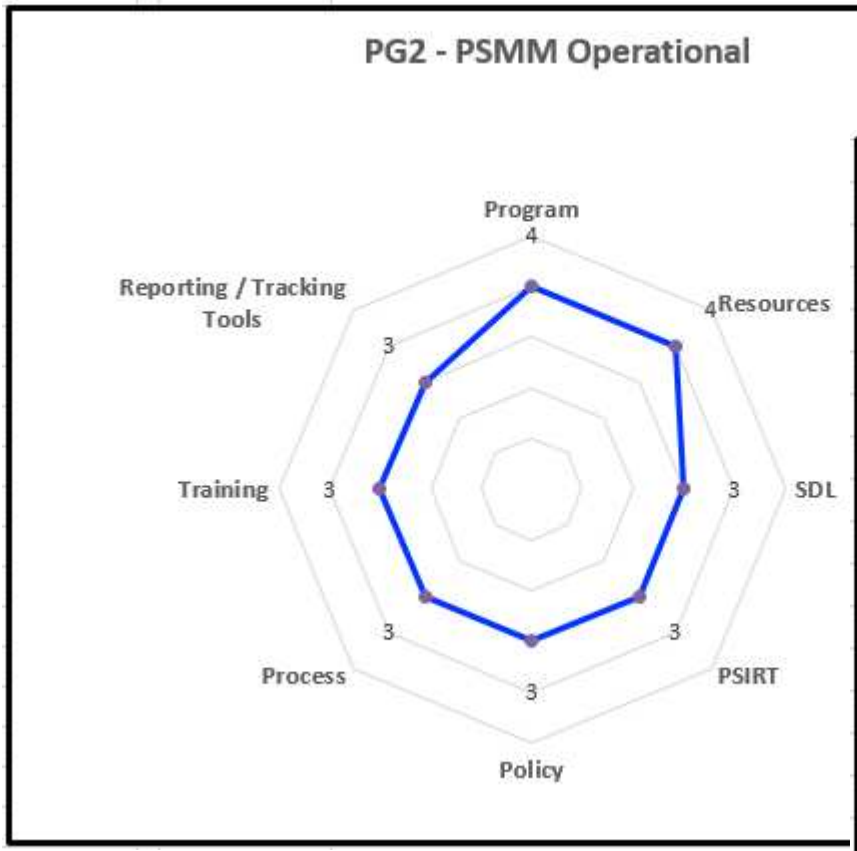
XLS Product Spider Diagram

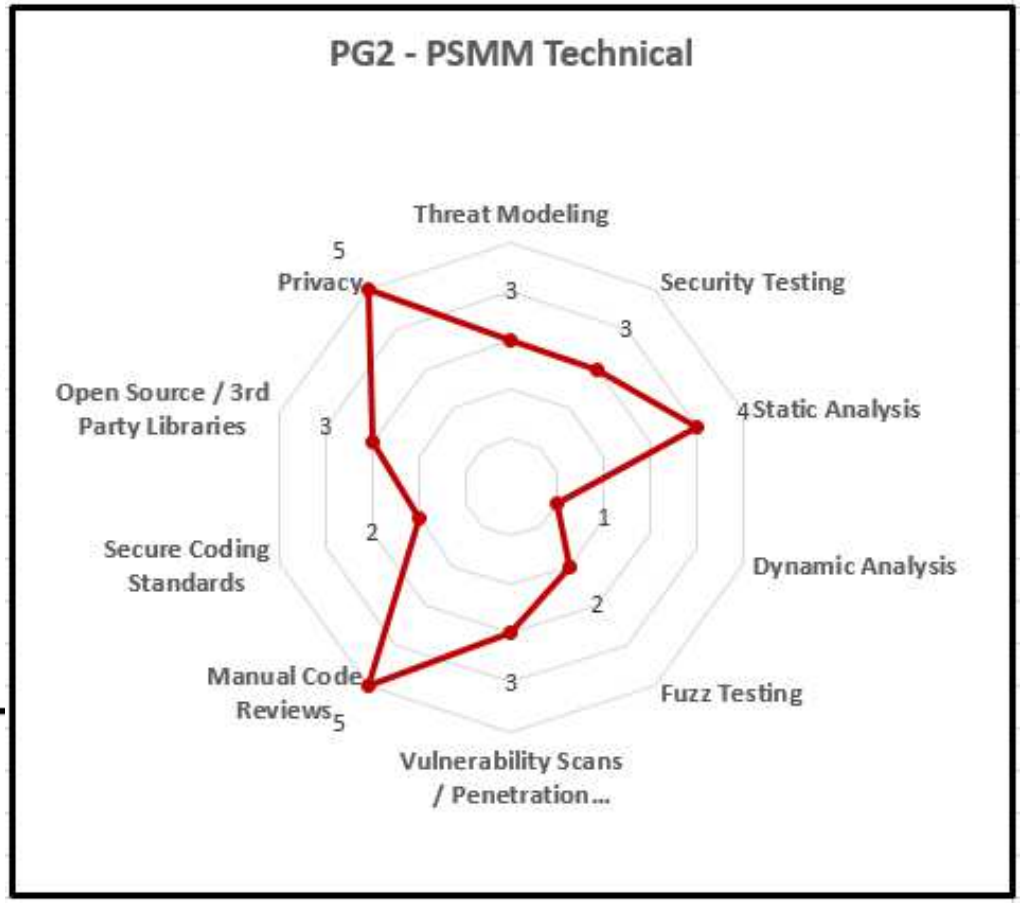


XLS Product Group Scorecard

		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**

XLS Product Group Spider Diagrams





All BU Products Scorecard

<Company> PSMM Scorecard - All Products

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

<Company> Confidential - For Internal Use Only

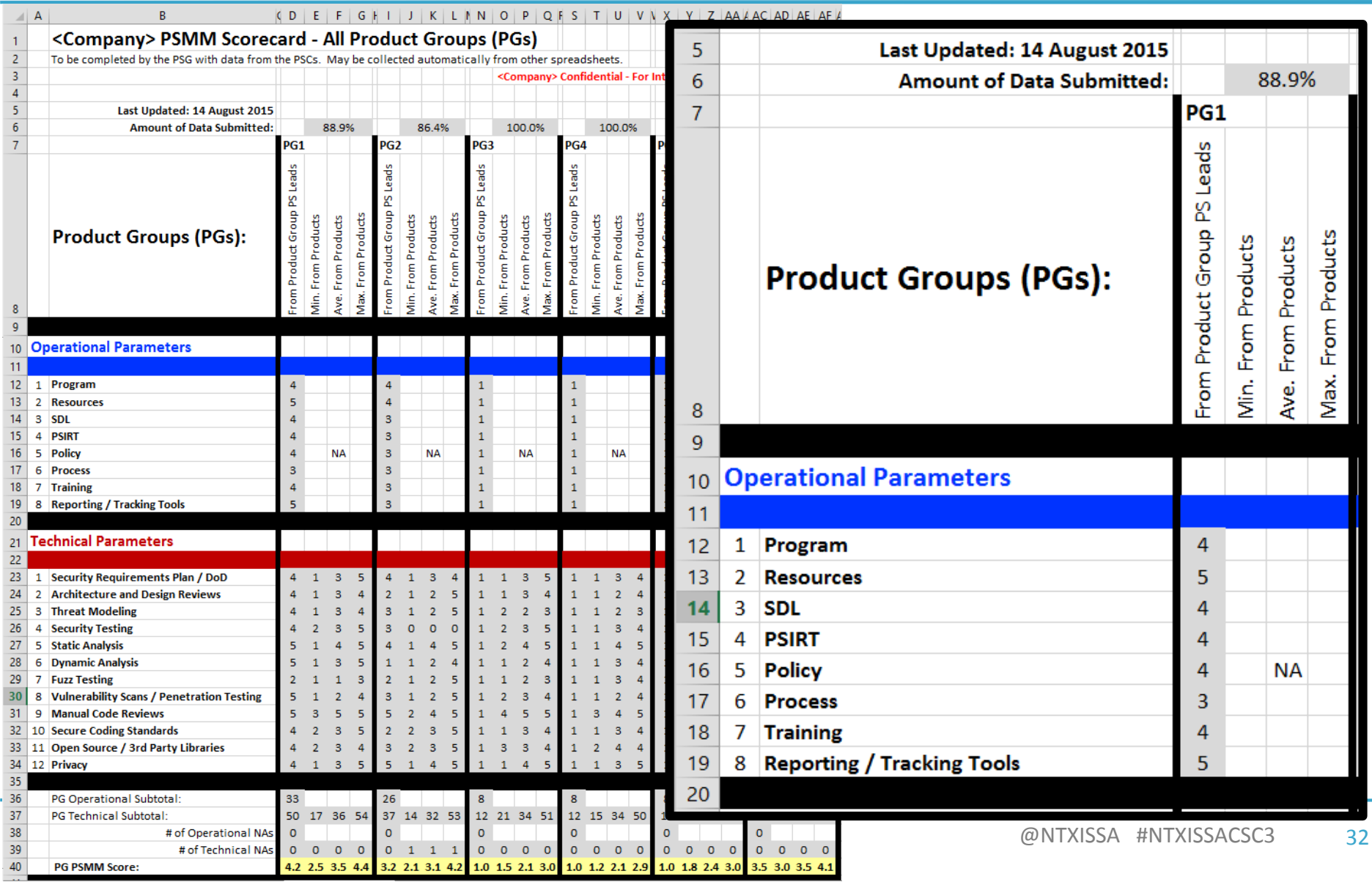
Last Updated: 14 August 2015

Amount of Data Submitted: 89% 86%

PSC Data Owner: PG 1 new PG 2

	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
Technical Parameters																									
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**
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**
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**
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**
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**
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**
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**
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**
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**
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**
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**
12	**Privacy**	**1**	**3**	**5**	4	4	3	1	1	4	3	5	1	2	1	5	1	1			5	5	**1**	**4**	**5**
	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
	# 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
	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
	BU PSMM Technical Score:	**1.4**	**3.0**	**5.0**																			**1.3**	**2.9**	**5.0**

XLS 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 Int

Last Updated: 14 August 2015

Amount of Data Submitted: 88.9% 86.4% 100.0% 100.0%

	Product Groups (PGs):	PG1				PG2				PG3				PG4			
		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	From Product Group PS Leads	Min. From Products	Ave. From Products	Max. From Products
	Operational Parameters																
1	Program	4				4				1				1			
2	Resources	5				4				1				1			
3	SDL	4				3				1				1			
4	PSIRT	4				3				1				1			
5	Policy	4		NA		3		NA		1		NA		1		NA	
6	Process	3				3				1				1			
7	Training	4				3				1				1			
8	Reporting / Tracking Tools	5				3				1				1			
	Technical Parameters																
1	Security Requirements Plan / DoD	4	1	3	5	4	1	3	4	1	1	3	5	1	1	3	4
2	Architecture and Design Reviews	4	1	3	4	2	1	2	5	1	1	3	4	1	1	2	4
3	Threat Modeling	4	1	3	4	3	1	2	5	1	2	2	3	1	1	2	3
4	Security Testing	4	2	3	5	3	0	0	0	1	2	3	5	1	1	3	4
5	Static Analysis	5	1	4	5	4	1	4	5	1	2	4	5	1	1	4	5
6	Dynamic Analysis	5	1	3	5	1	1	2	4	1	1	2	4	1	1	3	4
7	Fuzz Testing	2	1	1	3	2	1	2	5	1	1	2	3	1	1	3	4
8	Vulnerability Scans / Penetration Testing	5	1	2	4	3	1	2	5	1	2	3	4	1	1	2	4
9	Manual Code Reviews	5	3	5	5	5	2	4	5	1	4	5	5	1	3	4	5
10	Secure Coding Standards	4	2	3	5	2	2	3	5	1	1	3	4	1	1	3	4
11	Open Source / 3rd Party Libraries	4	2	3	4	3	2	3	5	1	3	3	4	1	2	4	4
12	Privacy	4	1	3	5	5	1	4	5	1	1	4	5	1	1	3	5
	PG Operational Subtotal:	33				26				8				8			
	PG Technical Subtotal:	50	17	36	54	37	14	32	53	12	21	34	51	12	15	34	50
	# of Operational NAs	0				0				0				0			
	# of Technical NAs	0	0	0	0	0	1	1	1	0	0	0	0	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	1.0	1.2	2.1	2.9

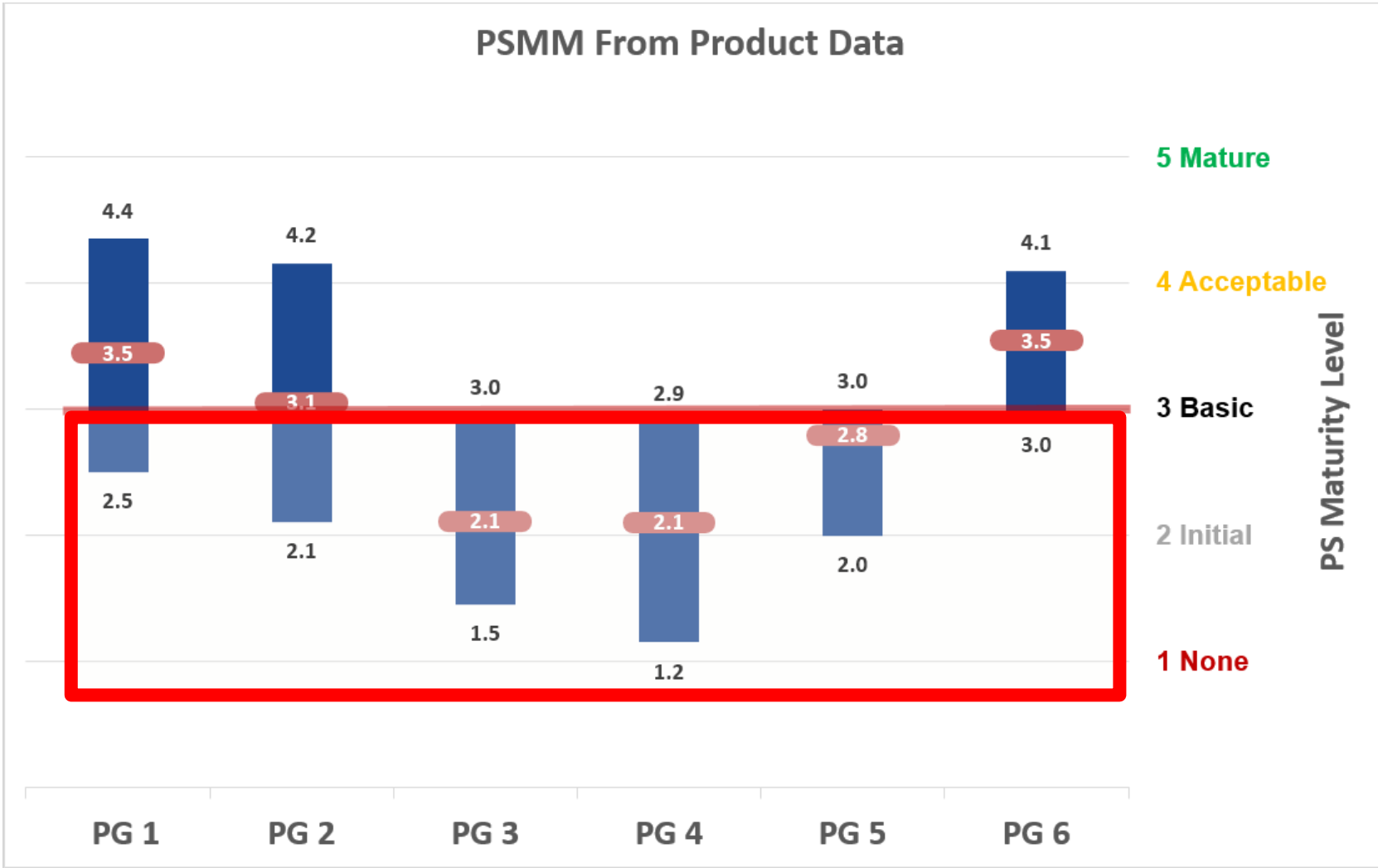
Last Updated: 14 August 2015

Amount of Data Submitted: 88.9%

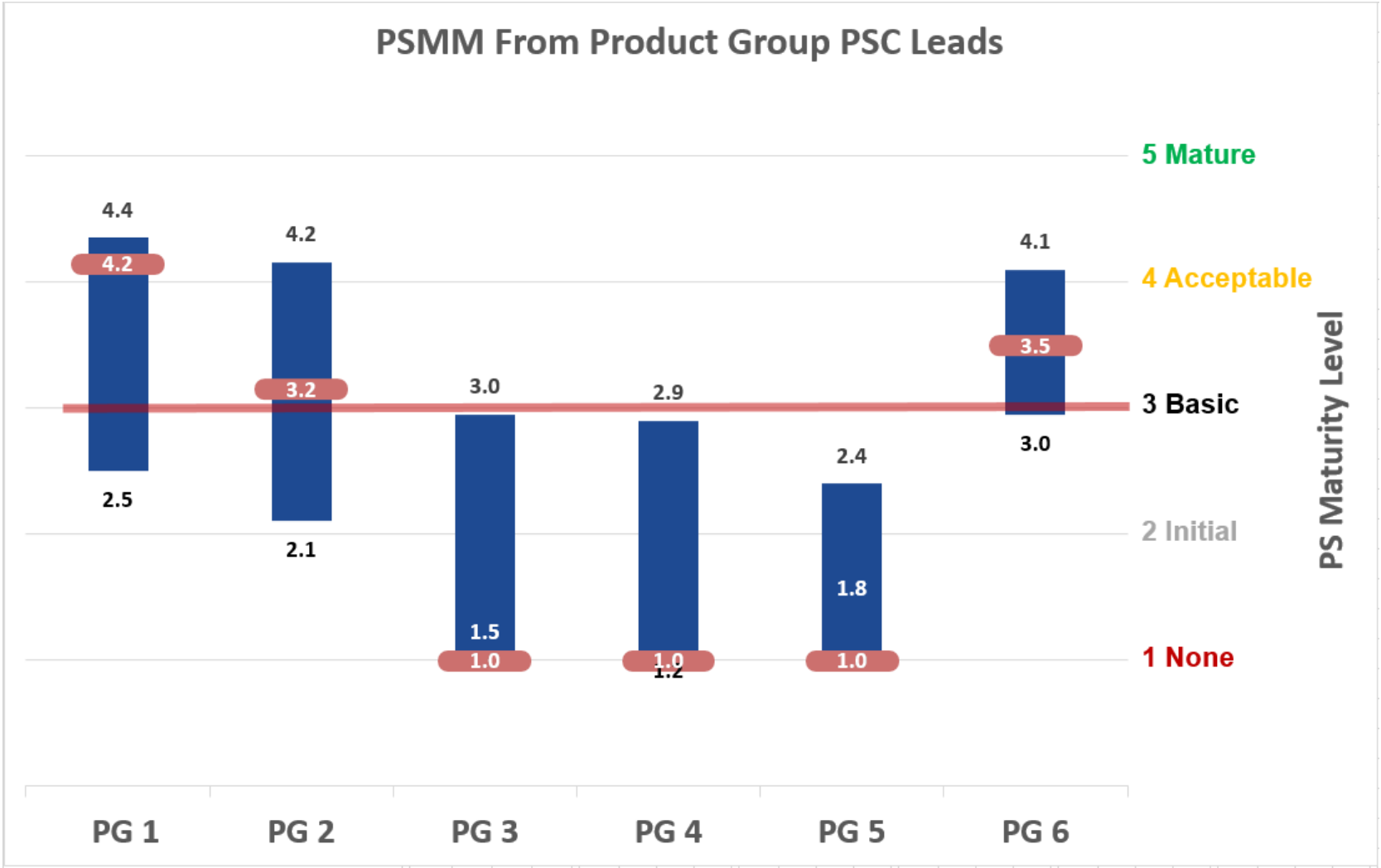
	Product Groups (PGs):	PG1			
		From Product Group PS Leads	Min. From Products	Ave. From Products	Max. From Products
	Operational Parameters				
1	Program	4			
2	Resources	5			
3	SDL	4			
4	PSIRT	4			
5	Policy	4		NA	
6	Process	3			
7	Training	4			
8	Reporting / Tracking Tools	5			

The Metrics

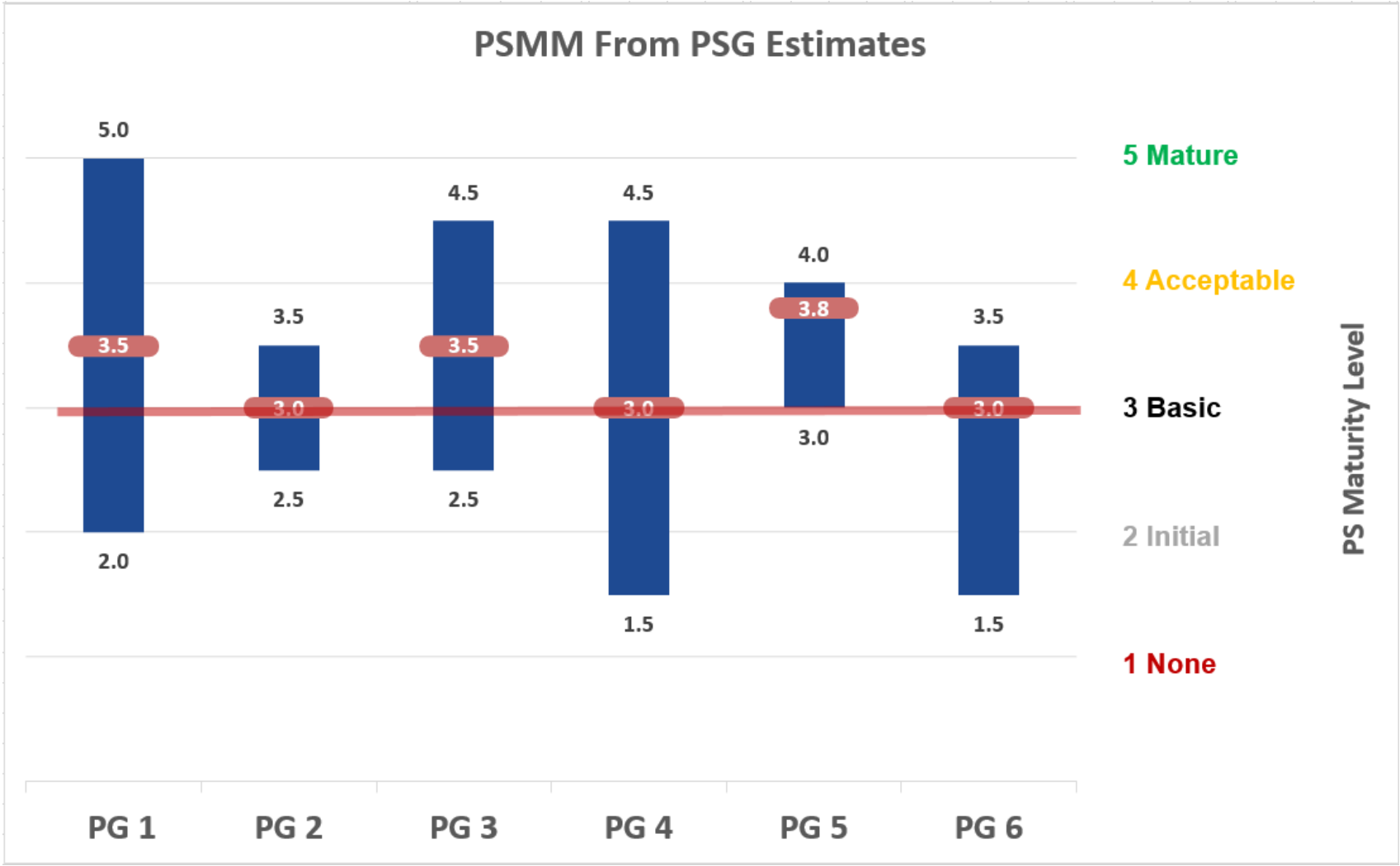
Most Accurate – From Product Data



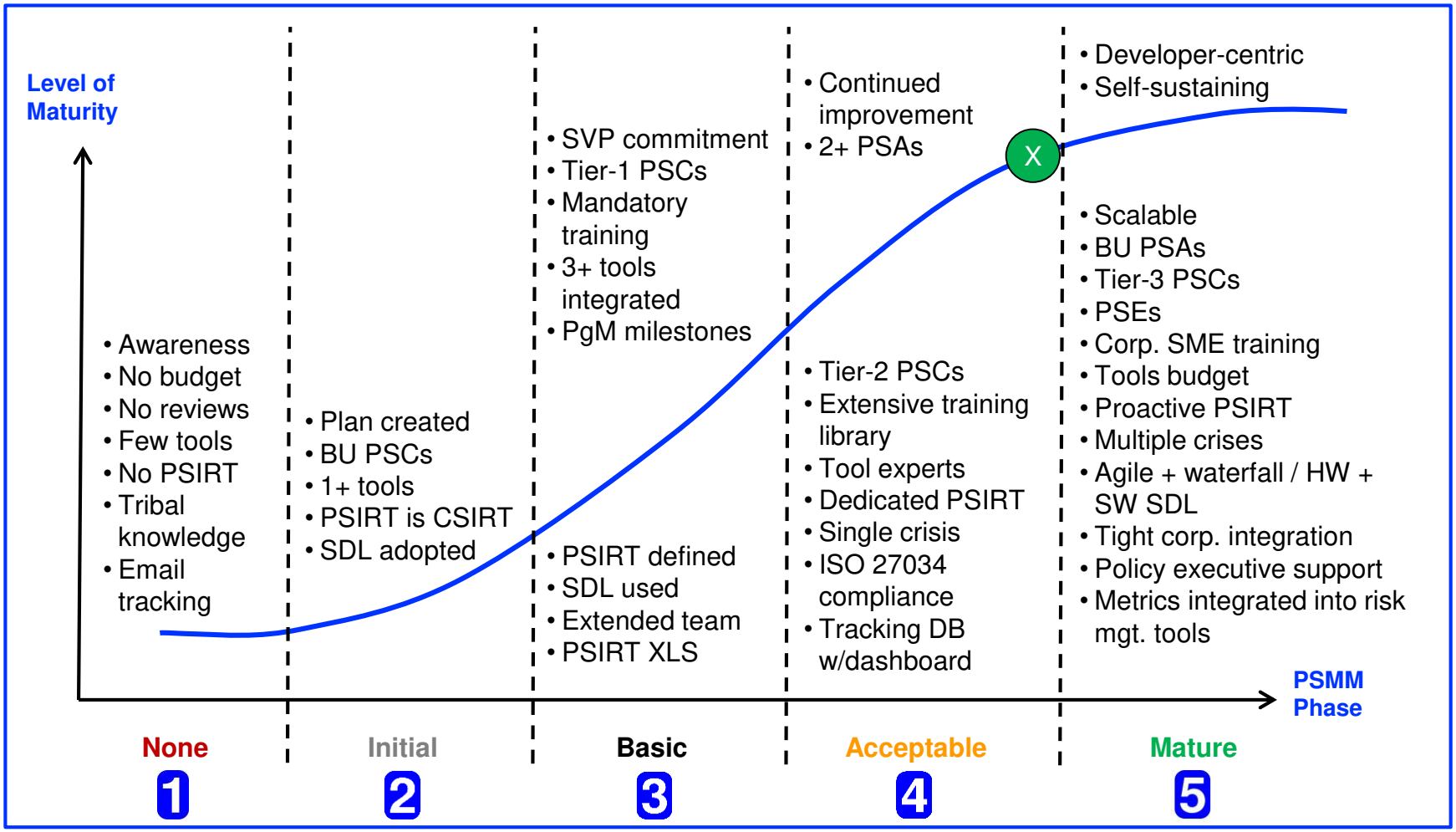
Somewhat Accurate – From PSC Leads



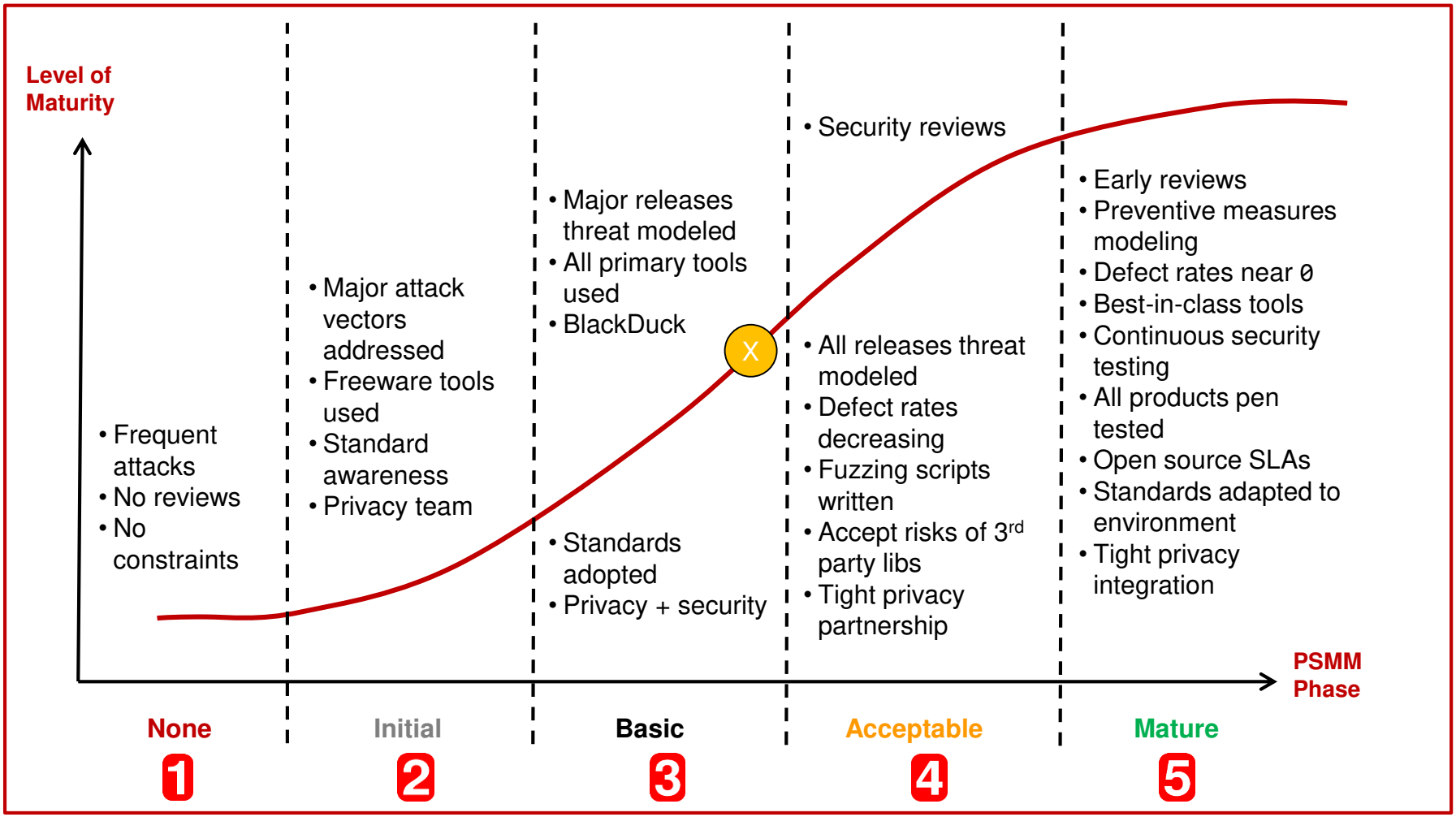
Least Accurate – From PSG Estimates



PSMM – Operational

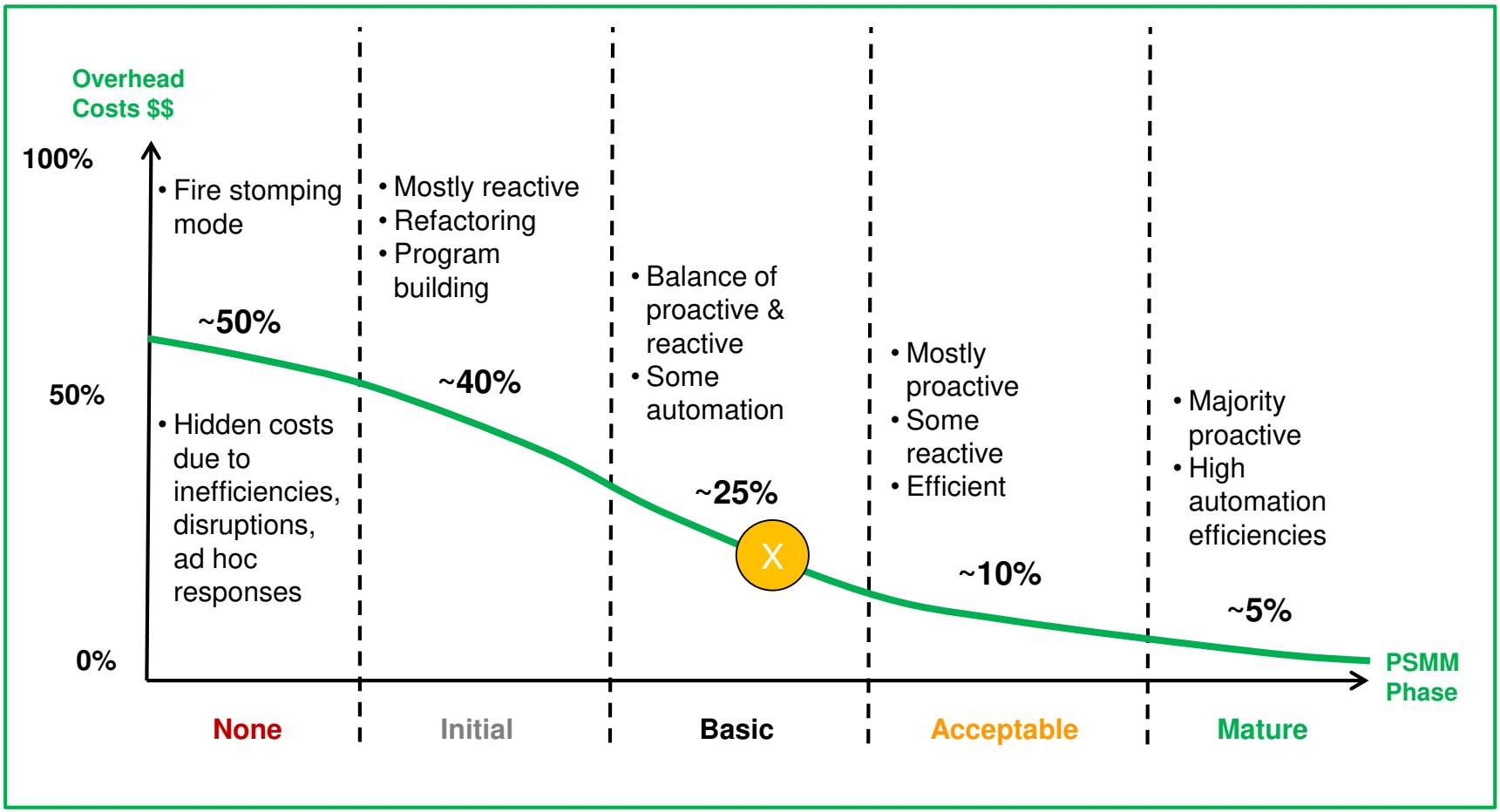


PSMM – Technical



PSMM – % Overhead Costs

NOTE: High overhead % is bad



Three Key Takeaways

1) SDL: Best practices in developing truly secure products / software

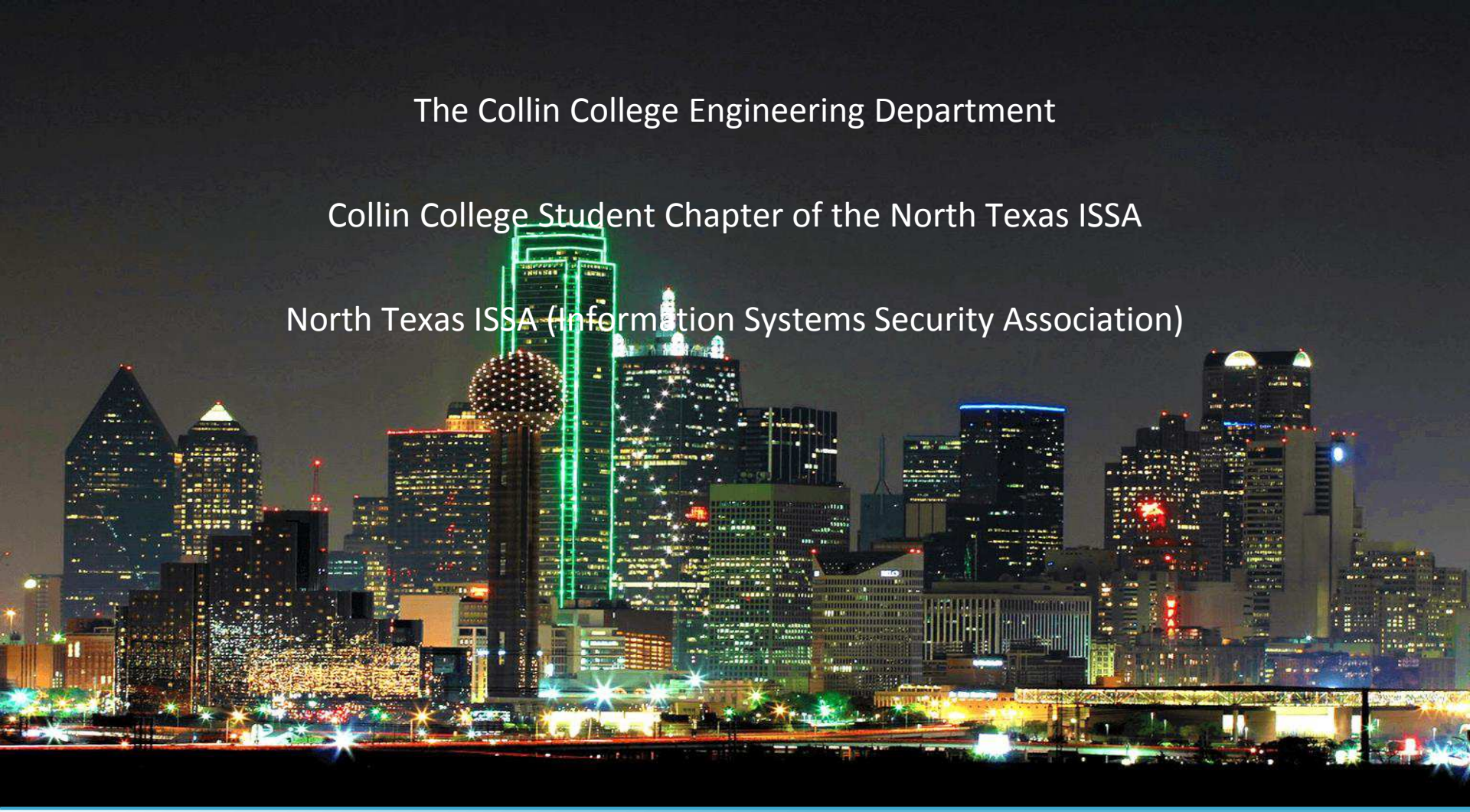
2) PSMM: A simple yet powerful way to measure the security maturity of your product security program and deliverables

3) Metrics: Product security metrics to drive positive change, security and efficiency

Contact Info

Harold Toomey
Sr. Product Security Architect & PSIRT Manager
Product Security Group, ISecG
Intel Corp.

5000 Headquarters Dr., MS 3S407
Plano, TX 75024-5826
Direct: (972) 963-7754
Mobile: (801) 830-9987
Email: Harold.A.Toomey@Intel.com


The Collin College Engineering Department
Collin College Student Chapter of the North Texas ISSA
North Texas ISSA (Information Systems Security Association)

Thank you