# Implementing and Maturing the Security Development Lifecycle (SDL)

Don McKeown

# Agenda

- Review Security Development Lifecycle (SDL)
- OWASP Software Assurance Maturity Model (SAMM)
- Relate SDL to SAMM

# I speak for myself

# About me

I DON'T USUALLY TALK ABOUT MYSELF
BUT WHEN I DO, I'M CAPTIVATED
imgflip.com

# SDL and S-SDLC are synonymous

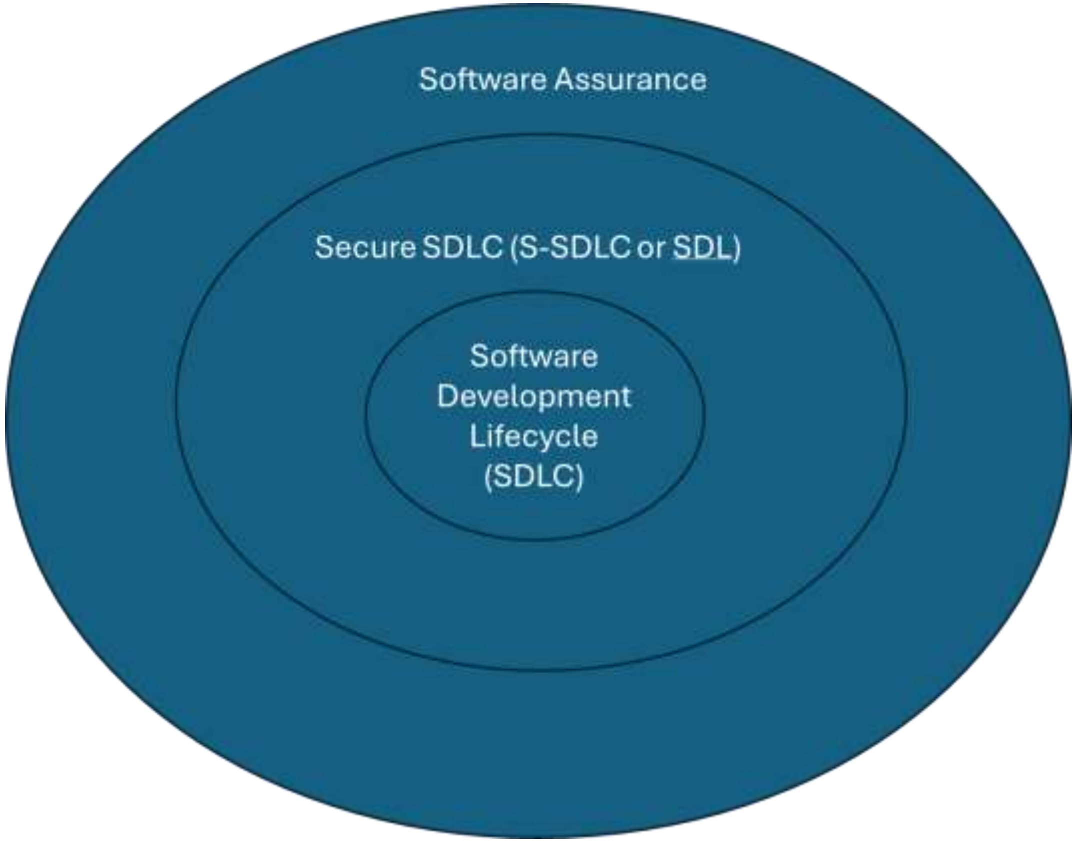
You wanna tomato?

Would you like a
to-MAH-to?

But SDLC can get confusing

# SDL should be a continuous, automated process

- SDLC typically injects security check at a few points
- S-SDLC or DevSecOps, security is continuous, and much of it is automated



Software Assurance

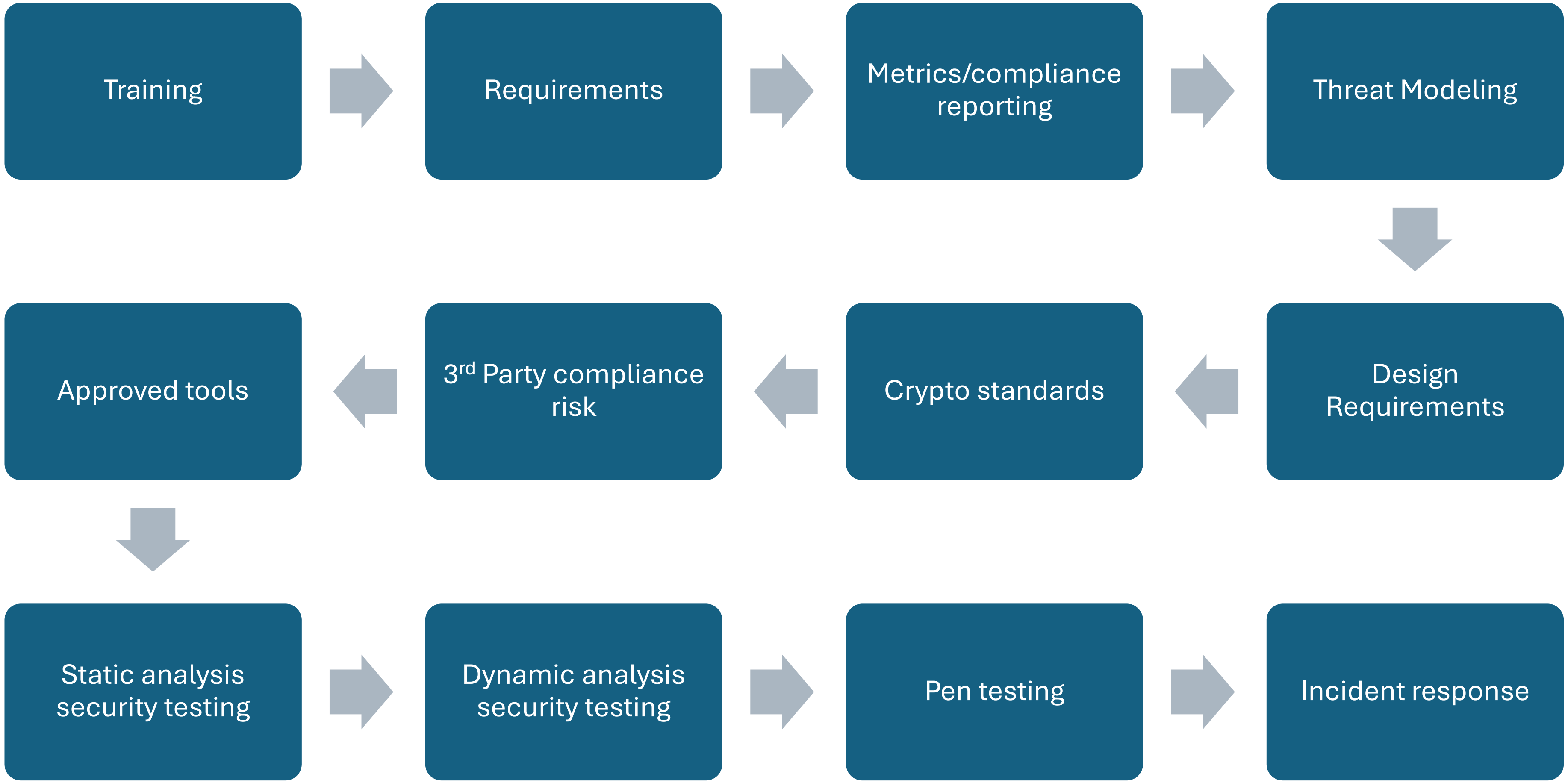
Secure SDLC (S-SDLC or SDL)

Software Development Lifecycle (SDLC)

# SDL is foundational to good products and customer trust

- Reduce odds of incidents and breach
  - Detect/Respond/Recover better when they do happen
- Compliance/Legal
- Create a better product
  - Security is element of quality
  - AI example
  - IAM – passwordless, federation, RBAC, automation
- Build customer trust
  - More customers are directly asking about security practices
  - Security is foundational to privacy

# Twelve MS SDL Practices



Training

Requirements

Metrics/compliance reporting

Threat Modeling

Design Requirements

Crypto standards

3rd Party compliance risk

Approved tools

Static analysis security testing

Dynamic analysis security testing

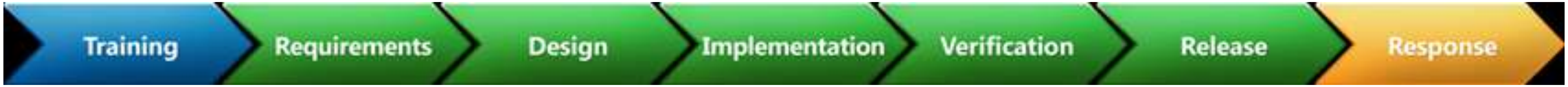
Pen testing

Incident response

# Be proactive rather than reactive – shift left!

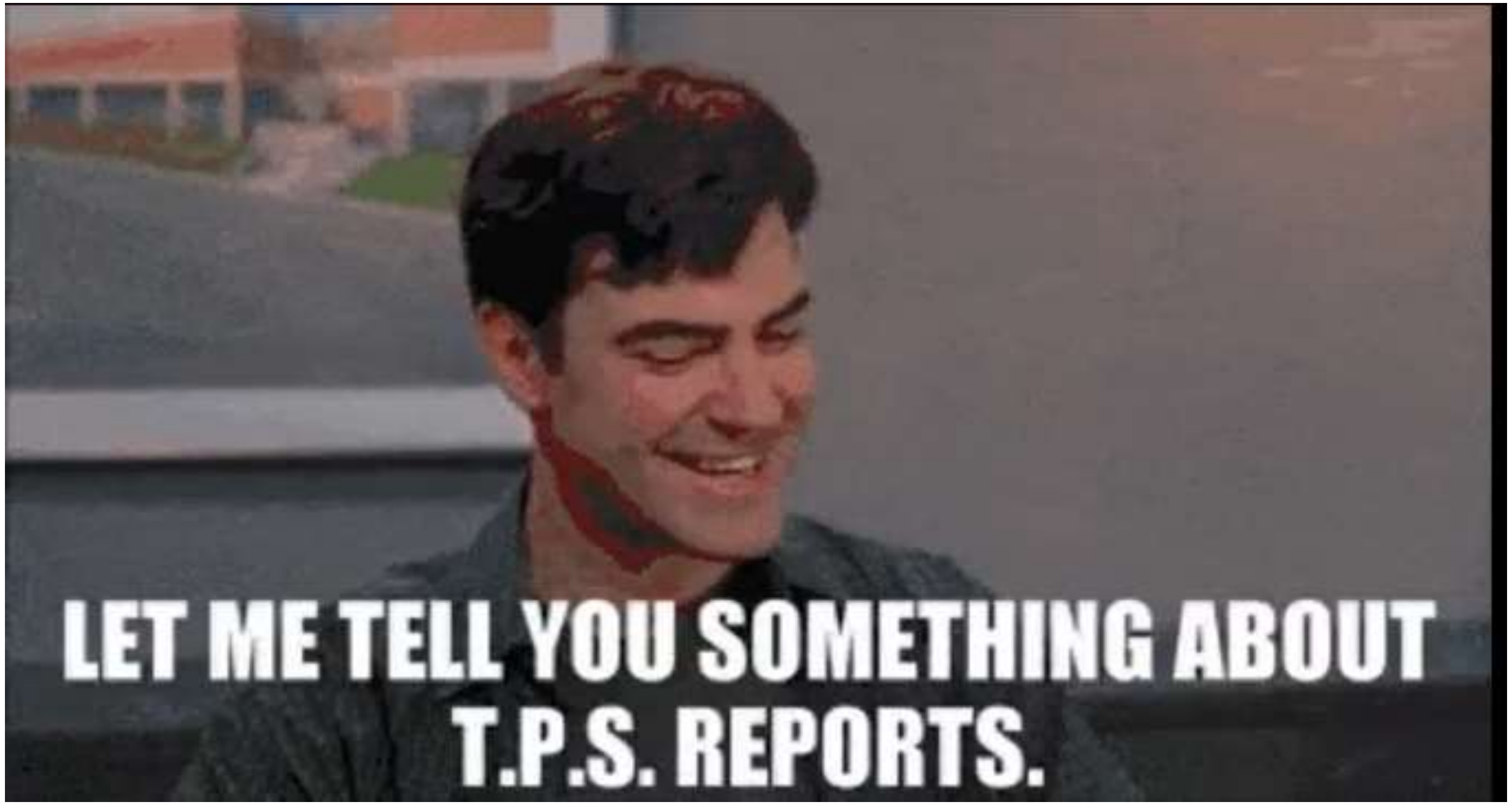
Proactive, less expensive

Reactive, more expensive



# Provide Training

# Training should not check a box



# Training should be metrics driven

- Completion metrics
- Target coding deficiencies
- Score ability to code securely

# Training options

- NOT vanilla online courses
- OWASP projects
  - Juice Shop
  - Top 10
  - Security Shepherd
  - Secure Coding Dojo
- Commercial secure code training options

# Security Champions are critical to training

- Security points of contact w/in dev teams
- Scale security
- Build security culture
- Management support is key

# Security Champions selection should be by criteria

# Define Security Requirements

- Business
- Customer
- Legal and regulatory
- Internal standards
- Review of previous Incidents
- Known threats

# Threat modeling (TM)

# How much threat modeling is needed?

- Systems for Top Secret government information?
- Products that leverage individual's personal health data?
- Website for storing recipes?

- <u>Context is critical</u>
  - Organizational objectives
  - Data sensitivity
  - Risk tolerance/capacity

# The term threat modeling is unintuitive

# Consider not using the term threat modeling

01

Terminology can be a barrier

02

Make TM more business friendly

03

Integrate with Design Requirements stage

04

Call it Security Requirements

# Establish Design Requirements

- Security design requirements aka “Threat modeling”
- Secure design patterns
- Security platform team
- Netflix Wall-E

# Define and Use Cryptography Standards

Don’t roll your own

Easily replaceable

# Manage the Security Risk of Using Third-Party Components

**Pretty much all software is composed of 3rd party components**

Commercial and open source

**Consider how to address license risk**

# Remaining SDL practices

1. Use Approved Tools
2. Perform Static Analysis Security Testing (SAST)
3. Perform Dynamic Analysis Security Testing (DAST)
4. Perform Penetration Testing
5. Establish a Standard Incident Response Process

# Maturing software development

# Frameworks to mature software development

- Bigger picture than SDL
  - Culture
  - Business focus
  - Governance
- Building Software Assurance Maturity Model (SAMM) versus Security In Maturity Model (BSIMM)

| SAMM | BSIMM |
|---|---|
| Open model | Proprietary |
| Prescriptive | Descriptive |
| Traditional Maturity model | Frequency of activities compared w/ other orgs |

# Value of SAMM

✓ **Measure and evaluate current application security posture**

**Define a target maturity level**

**Develop a roadmap to achieve maturity**

SAMM offer prescriptive guidance

**Demonstrate security improvements**

# Tools

SPREADSHEET

OTHERS: SAMMWISE, SAMMY

# SAMM  process is six phases

Prepare

Assess

Set Target

Define Plan

Implement

Roll out

# Prepare

Scope

Stakeholders

Communication plan

# Assess

**Evaluate current practices**

**Determine maturity level**

**Best practices**

Consistency

Format?  Interview or workshop

Determine activities that are n/a

# Set Target

## Define target

## Estimate impact ($)

## Best practices

Consider risk profile

Assurance 5% - 10% of total development cost

# Define the plan

**Determine change schedule**

**Develop/update the roadmap plan**

**Best practices**

Quick wins

Start with awareness/training

Work with program manager, if possible

# Implement

**SAMM offers prescriptive advice**

**Consider impact on processes, people, knowledge, and tools**

**Best practices**

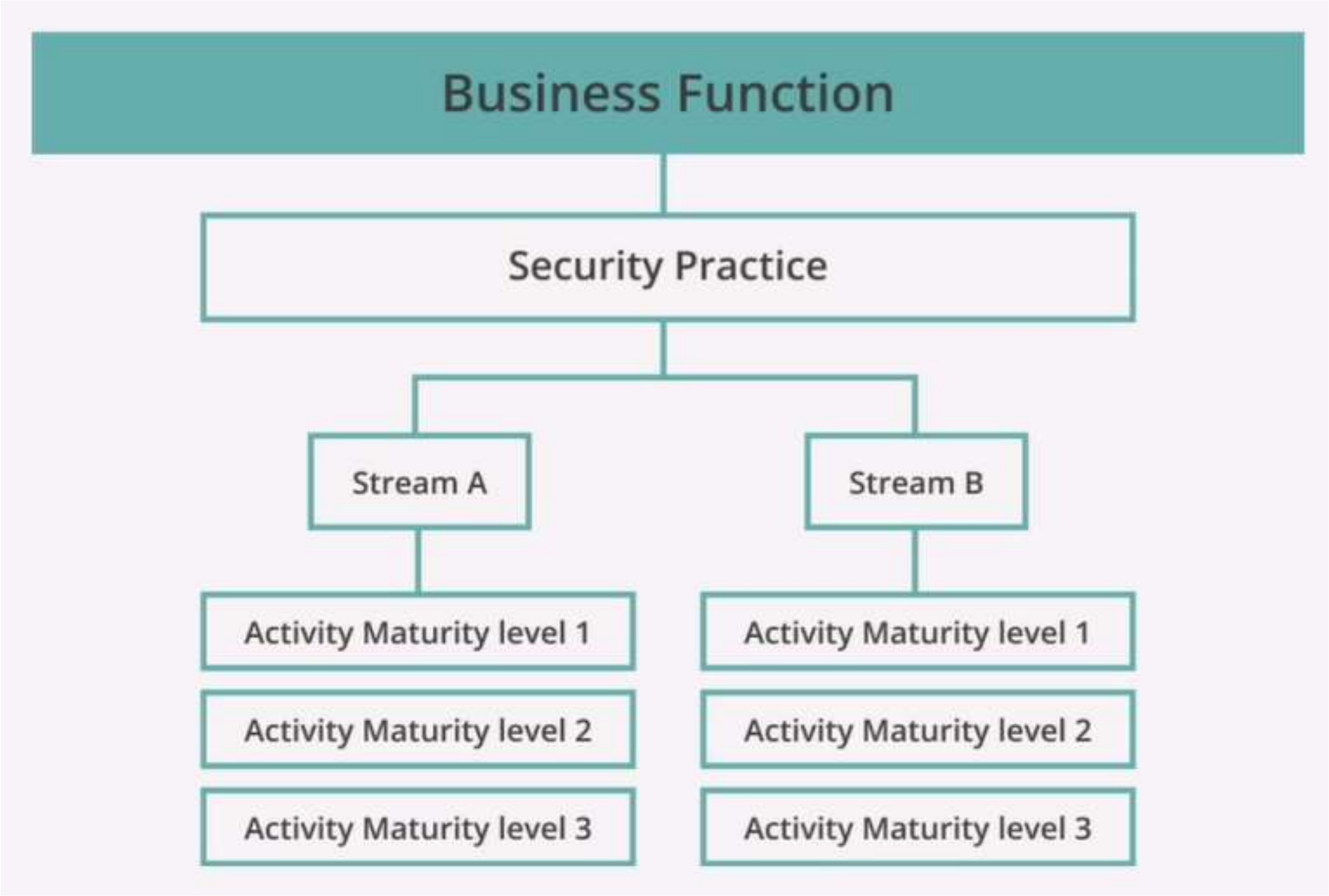
Treat legacy software separately

Avoid operational bottlenecks

# Roll out

- Evangelize improvements
- Measure effectiveness
- Best practices
  - Focus of high impact applications
  - Use team champions to communicate

# SAMM structure

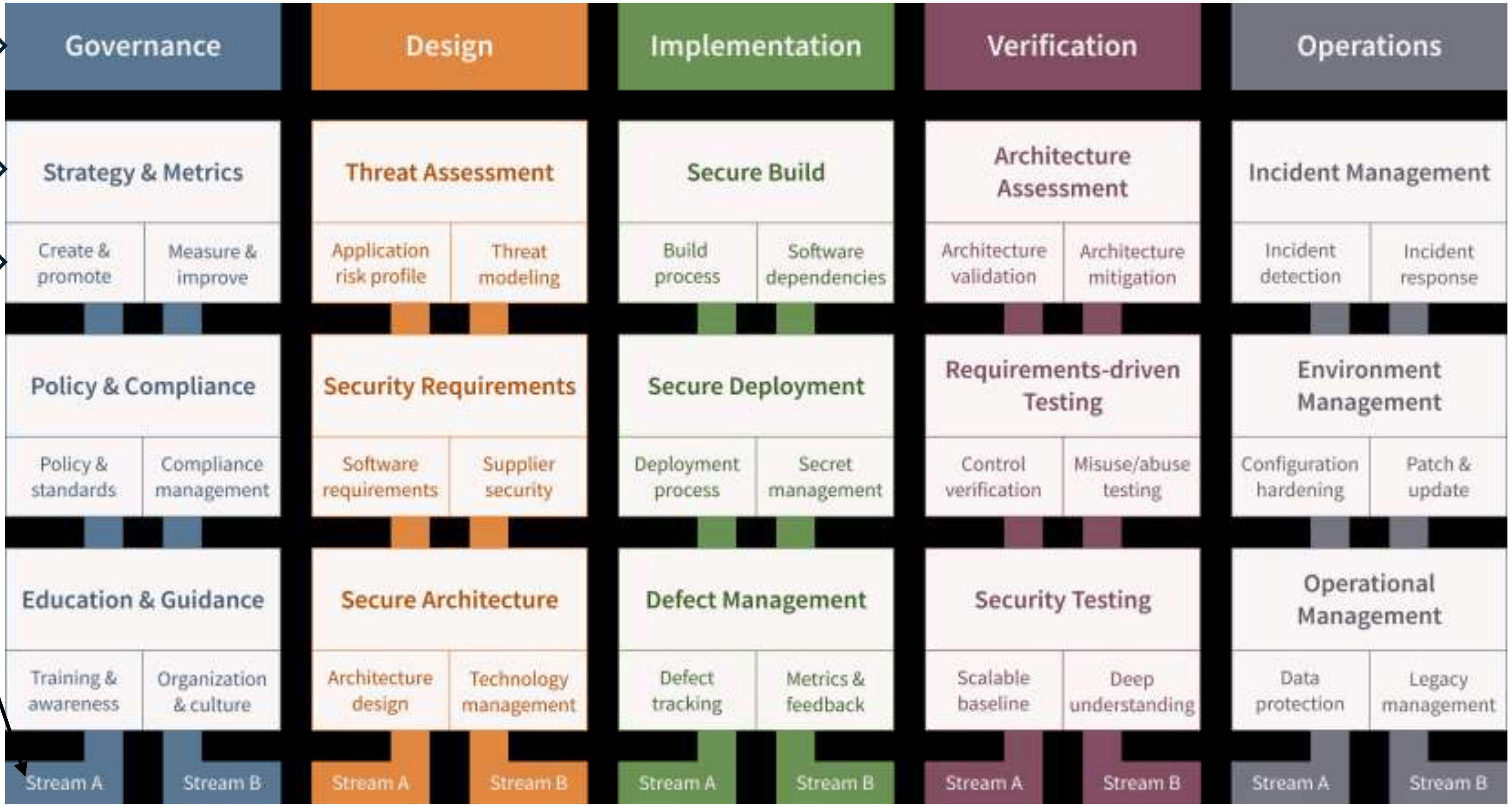

Business Function
Security Practice
Stream A
Stream B
Activity Maturity level 1
Activity Maturity level 2
Activity Maturity level 3
Activity Maturity level 1
Activity Maturity level 2
Activity Maturity level 3

# SAMM structure

Business Functions

Security Practices

Activities



| Governance | | Design | | Implementation | | Verification | | Operations | |
|---|---|---|---|---|---|---|---|---|---|
| Strategy & Metrics | | Threat Assessment | | Secure Build | | Architecture Assessment | | Incident Management | |
| Create & promote | Measure & improve | Application risk profile | Threat modeling | Build process | Software dependencies | Architecture validation | Architecture mitigation | Incident detection | Incident response |
| Policy & Compliance | | Security Requirements | | Secure Deployment | | Requirements-driven Testing | | Environment Management | |
| Policy & standards | Compliance management | Software requirements | Supplier security | Deployment process | Secret management | Control verification | Misuse/abuse testing | Configuration hardening | Patch & update |
| Education & Guidance | | Secure Architecture | | Defect Management | | Security Testing | | Operational Management | |
| Training & awareness | Organization & culture | Architecture design | Technology management | Defect tracking | Metrics & feedback | Scalable baseline | Deep understanding | Data protection | Legacy management |
| Stream A | Stream B | Stream A | Stream B | Stream A | Stream B | Stream A | Stream B | Stream A | Stream B |

# SAMM assesses maturity level and coverage

Maturity Level

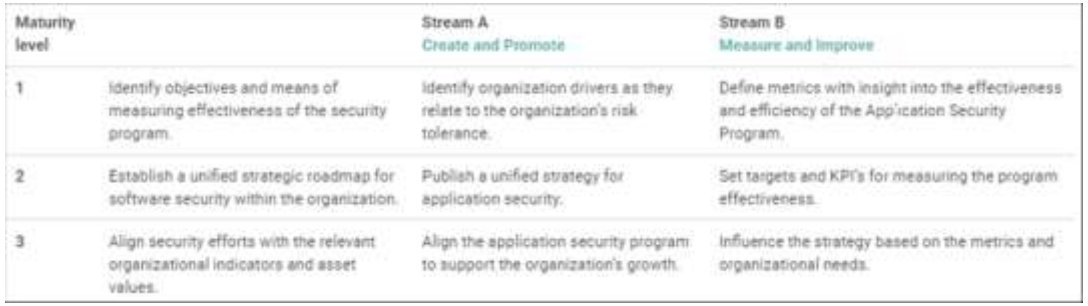
0 – Practice not occurring
1 – Ad hoc
2 – Consistent, repeatable
3 – Continuous improvement

Coverage

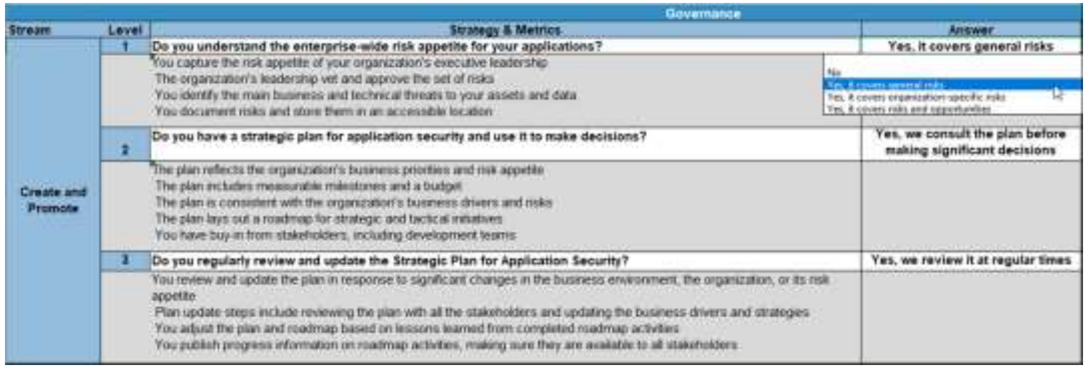
0 – None
.25 – Some / a few
.5 – At least half
1 – Most or all

The goal does not have to be maturity level 3 across your org

# SAMM is questionnaire based



| Maturity level | | Stream A<br>Create and Promote | Stream B<br>Measure and Improve |
|---|---|---|---|
| 1 | Identify objectives and means of measuring effectiveness of the security program. | Identify organization drivers as they relate to the organization's risk tolerance. | Define metrics with insight into the effectiveness and efficiency of the App ication Security Program. |
| 2 | Establish a unified strategic roadmap for software security within the organization. | Publish a unified strategy for application security. | Set targets and KPI's for measuring the program effectiveness. |
| 3 | Align security efforts with the relevant organizational indicators and asset values. | Align the application security program to support the organization's growth. | Influence the strategy based on the metrics and organizational needs. |

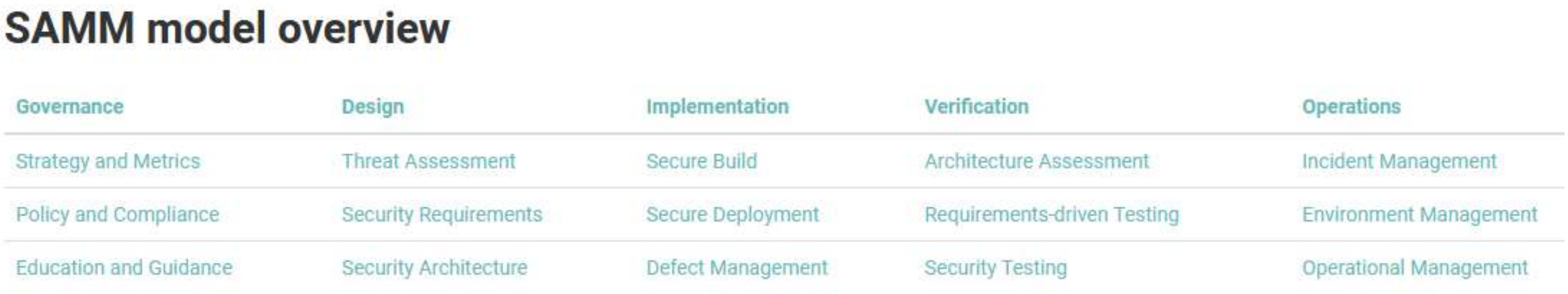


| | | Governance | |
|---|---|---|---|
| Stream | Level | Strategy & Metrics | Answer |
| Create and Promote | 1 | **Do you understand the enterprise-wide risk appetite for your applications?** | **Yes, it covers general risks** |
| | | You capture the risk appetite of your organization's executive leadership<br>The organization's leadership vet and approve the set of risks<br>You identify the main business and technical threats to your assets and data<br>You document risks and store them in an accessible location | |
| | 2 | **Do you have a strategic plan for application security and use it to make decisions?** | **Yes, we consult the plan before making significant decisions** |
| | | The plan reflects the organization's business priorities and risk appetite<br>The plan includes measurable milestones and a budget<br>The plan is consistent with the organization's business drivers and risks<br>The plan lays out a roadmap for strategic and tactical initiatives<br>You have buy-in from stakeholders, including development teams | |
| | 3 | **Do you regularly review and update the Strategic Plan for Application Security?** | **Yes, we review it at regular times** |
| | | You review and update the plan in response to significant changes in the business environment, the organization, or its risk appetite<br>Plan update steps include reviewing the plan with all the stakeholders and updating the business drivers and strategies<br>You adjust the plan and roadmap based on lessons learned from completed roadmap activities<br>You publish progress information on roadmap activities, making sure they are available to all stakeholders | |

No
Yes, it covers general risks
Yes, it covers organization-specific risks
Yes, it covers risks and opportunities

# Need to understand the background of questions

Go to https://owaspsamm.org/model/ :

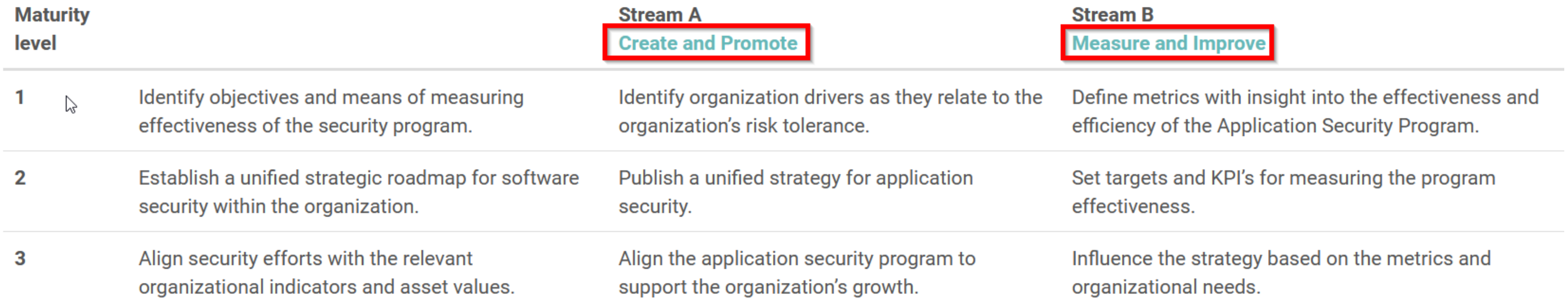


## SAMM model overview

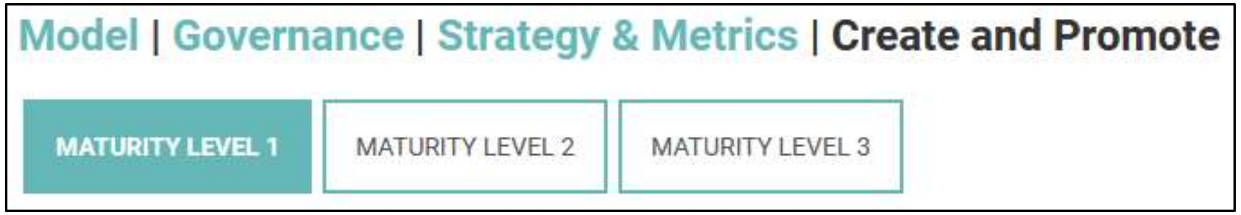
| Governance | Design | Implementation | Verification | Operations |
|---|---|---|---|---|
| Strategy and Metrics | Threat Assessment | Secure Build | Architecture Assessment | Incident Management |
| Policy and Compliance | Security Requirements | Secure Deployment | Requirements-driven Testing | Environment Management |
| Education and Guidance | Security Architecture | Defect Management | Security Testing | Operational Management |

Or check out the little 303 page PDF!
https://owaspsamm.org/resources/pdf/

# But understanding the background of questions is a rabbit hole

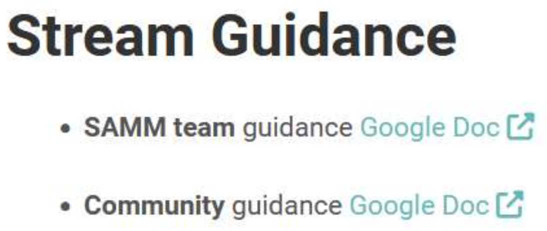


| Maturity level | | Stream A<br>Create and Promote | Stream B<br>Measure and Improve |
|---|---|---|---|
| 1 | Identify objectives and means of measuring effectiveness of the security program. | Identify organization drivers as they relate to the organization's risk tolerance. | Define metrics with insight into the effectiveness and efficiency of the Application Security Program. |
| 2 | Establish a unified strategic roadmap for software security within the organization. | Publish a unified strategy for application security. | Set targets and KPI's for measuring the program effectiveness. |
| 3 | Align security efforts with the relevant organizational indicators and asset values. | Align the application security program to support the organization's growth. | Influence the strategy based on the metrics and organizational needs. |



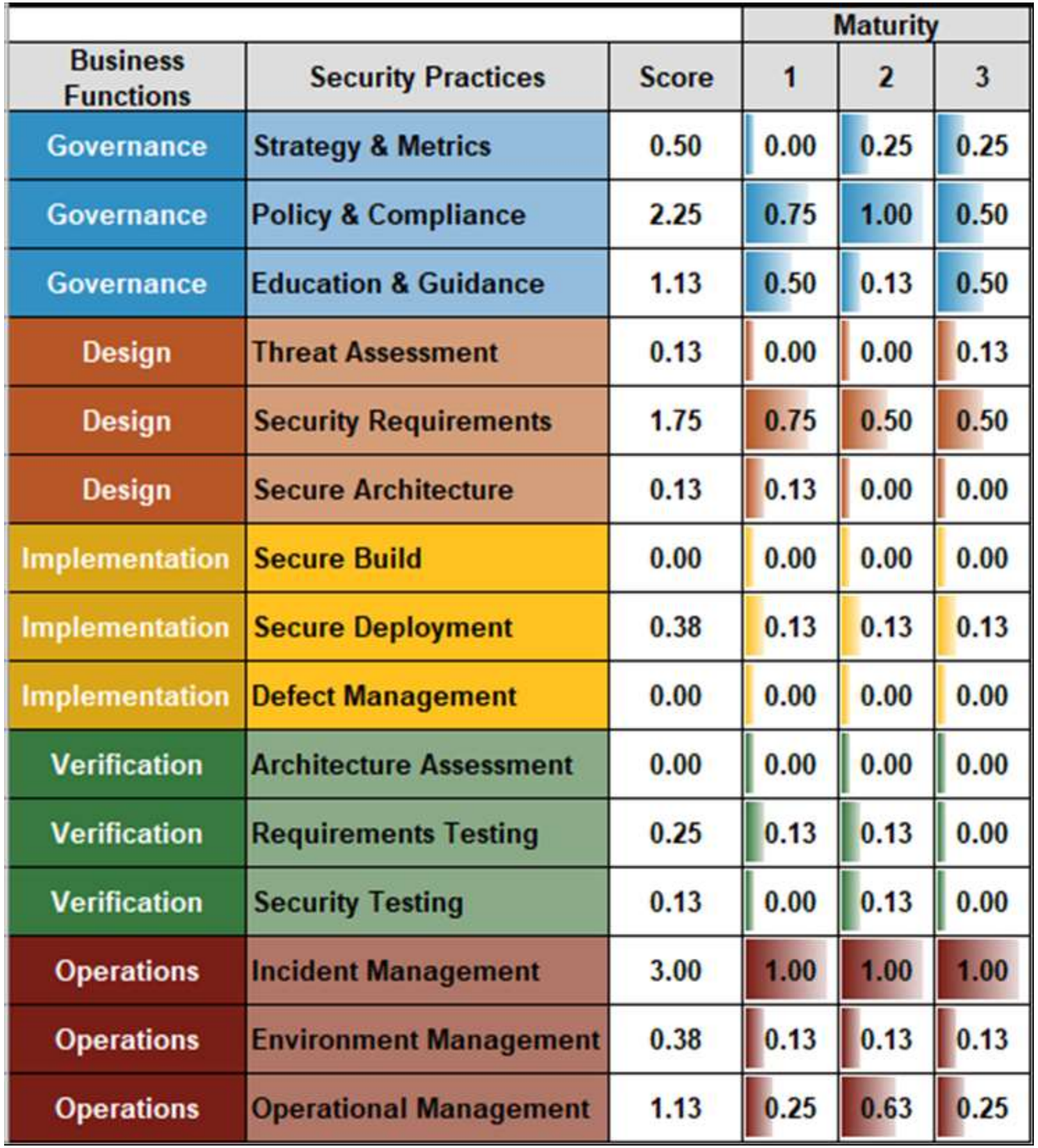
Model | Governance | Strategy & Metrics | Create and Promote

Benefit
Activity
Question
Quality criteria
Answers



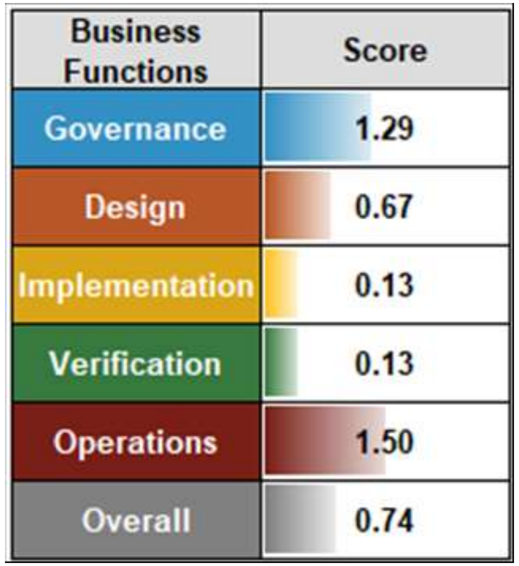
## Stream Guidance

- **SAMM team** guidance Google Doc
- **Community** guidance Google Doc



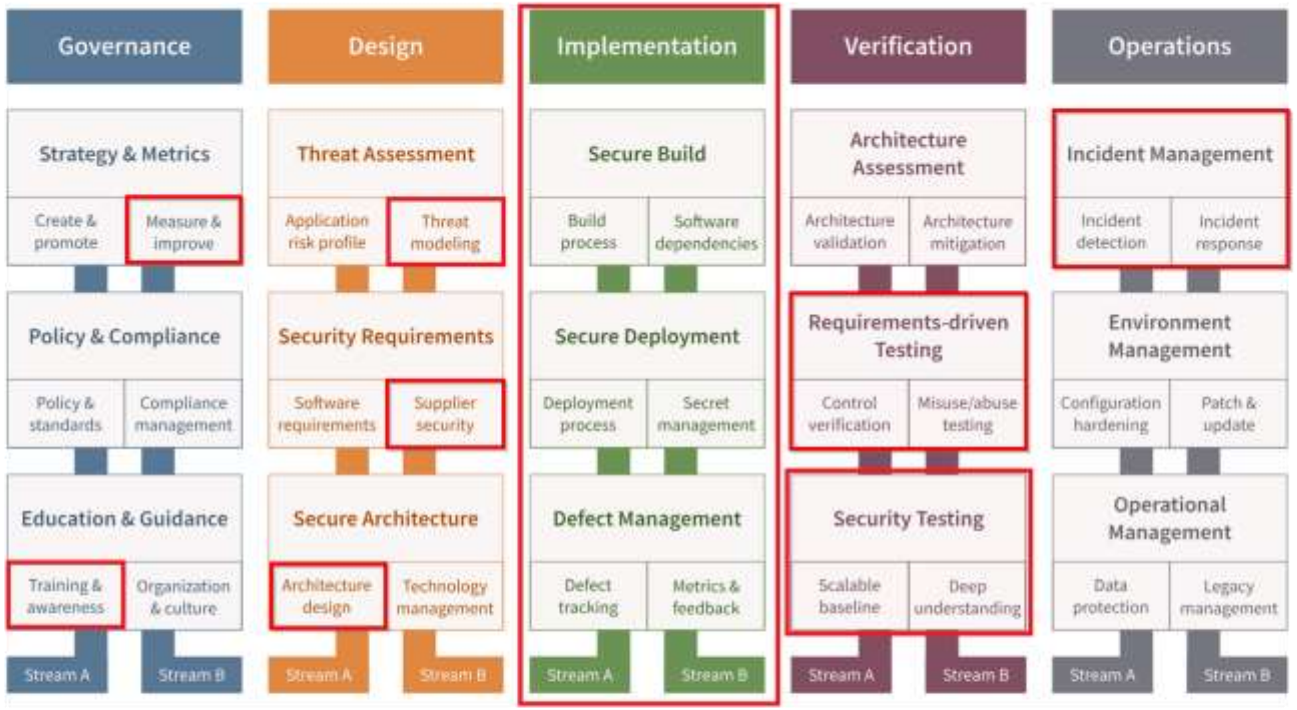
| | | | Maturity | | |
|---|---|---|---|---|---|
| Business Functions | Security Practices | Score | 1 | 2 | 3 |
| Governance | Strategy & Metrics | 0.50 | 0.00 | 0.25 | 0.25 |
| Governance | Policy & Compliance | 2.25 | 0.75 | 1.00 | 0.50 |
| Governance | Education & Guidance | 1.13 | 0.50 | 0.13 | 0.50 |
| Design | Threat Assessment | 0.13 | 0.00 | 0.00 | 0.13 |
| Design | Security Requirements | 1.75 | 0.75 | 0.50 | 0.50 |
| Design | Secure Architecture | 0.13 | 0.13 | 0.00 | 0.00 |
| Implementation | Secure Build | 0.00 | 0.00 | 0.00 | 0.00 |
| Implementation | Secure Deployment | 0.38 | 0.13 | 0.13 | 0.13 |
| Implementation | Defect Management | 0.00 | 0.00 | 0.00 | 0.00 |
| Verification | Architecture Assessment | 0.00 | 0.00 | 0.00 | 0.00 |
| Verification | Requirements Testing | 0.25 | 0.13 | 0.13 | 0.00 |
| Verification | Security Testing | 0.13 | 0.00 | 0.13 | 0.00 |
| Operations | Incident Management | 3.00 | 1.00 | 1.00 | 1.00 |
| Operations | Environment Management | 0.38 | 0.13 | 0.13 | 0.13 |
| Operations | Operational Management | 1.13 | 0.25 | 0.63 | 0.25 |

# Scoring based on responses to questions



| Business Functions | Score |
|---|---|
| Governance | 1.29 |
| Design | 0.67 |
| Implementation | 0.13 |
| Verification | 0.13 |
| Operations | 1.50 |
| Overall | 0.74 |

# SAMM relates to SDL



| Business function | Practice | Stream A | Stream B |
|---|---|---|---|
| Governance | Strategy & Metrics | Create & promote | Measure & improve |
| | Policy & Compliance | Policy & standards | Compliance management |
| | Education & Guidance | Training & awareness | Organization & culture |
| Design | Threat Assessment | Application risk profile | Threat modeling |
| | Security Requirements | Software requirements | Supplier security |
| | Secure Architecture | Architecture design | Technology management |
| Implementation | Secure Build | Build process | Software dependencies |
| | Secure Deployment | Deployment process | Secret management |
| | Defect Management | Defect tracking | Metrics & feedback |
| Verification | Architecture Assessment | Architecture validation | Architecture mitigation |
| | Requirements-driven Testing | Control verification | Misuse/abuse testing |
| | Security Testing | Scalable baseline | Deep understanding |
| Operations | Incident Management | Incident detection | Incident response |
| | Environment Management | Configuration hardening | Patch & update |
| | Operational Management | Data protection | Legacy management |

# Summary

- Implementing SDL well will improve your product
- Automate so that it’s continuous
- Invest in proactive practices such as training and “threat modeling”
- Consider not using the term threat modeling
- Use SAMM to measure current state and roadmap improvements
- Invest time in better understanding SAMM before starting
- Evangelize!

ASK ME A QUESTION
ANY QUESTION
imgflip.com

Thank you  for your time!