# OWASP SAMM

## and other Software Security Assurance Frameworks

August Johnson

# Who the hell am I?

Security Architect at Netsmart Technologies

# Software Security Assurance

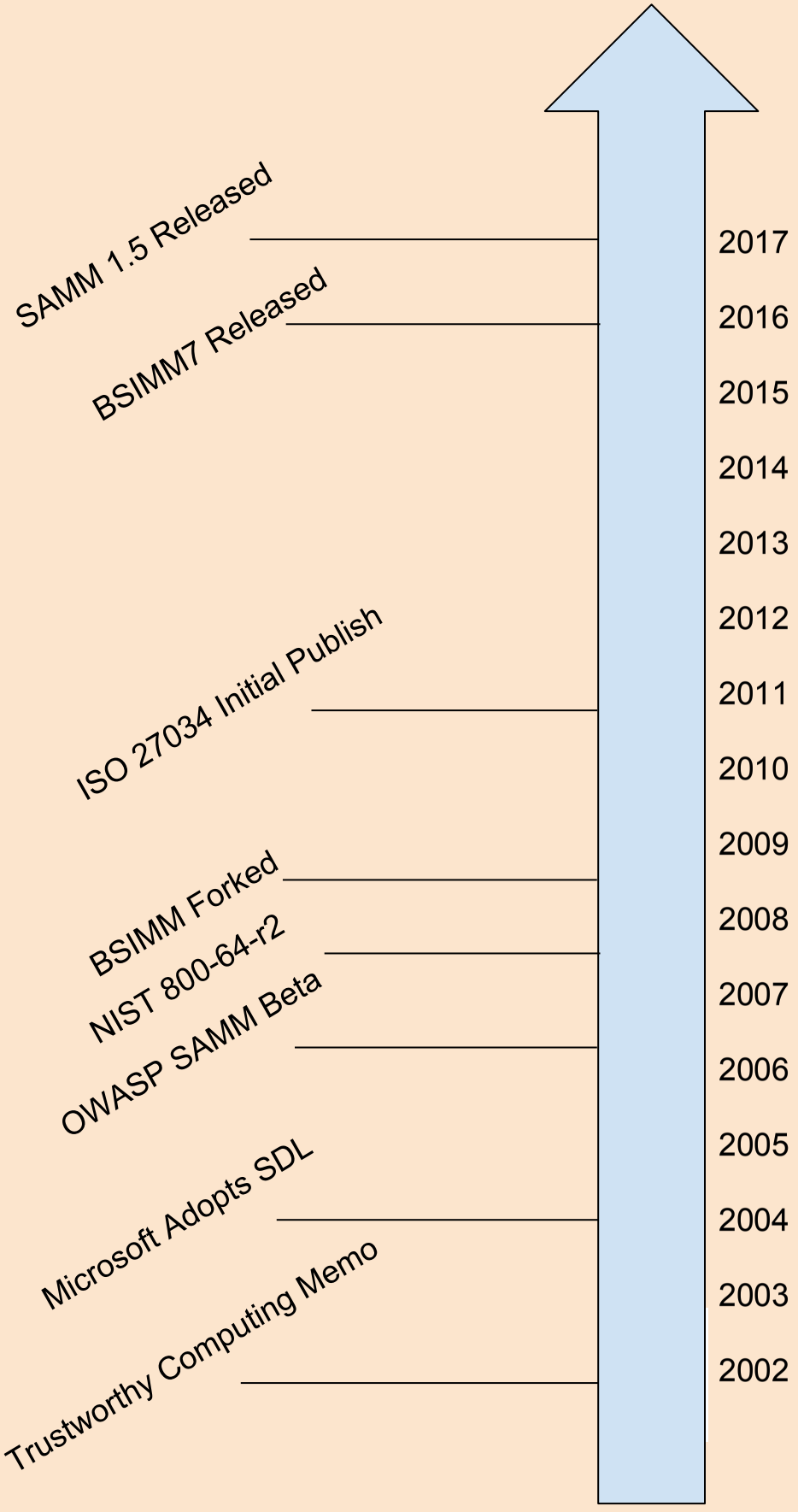
Process that **helps design and implement** software that **protects the data and resources** contained in and controlled by the software.

# Software Security Assurance - Who is it for?

If you have involvement or influence in the creation or maintenance of software, there are items in here that can apply to you.

# Common Models

- ISO 27034
- NIST SP-800-64
- Microsoft SDL (Security Development Lifecycle)
- BSIMM (Building Security In Maturity Model)
- OWASP SAMM (Software Assurance Maturity Model)


SAMM 1.5 Released
BSIMM7 Released
ISO 27034 Initial Publish
BSIMM Forked
NIST 800-64-r2
OWASP SAMM Beta
Microsoft Adopts SDL
Trustworthy Computing Memo
2017
2016
2015
2014
2013
2012
2011
2010
2009
2008
2007
2006
2005
2004
2003
2002

# ISO 27034

Heavy, wordy, not user-friendly.

Only part of the standard is officially published, missing some key pieces.

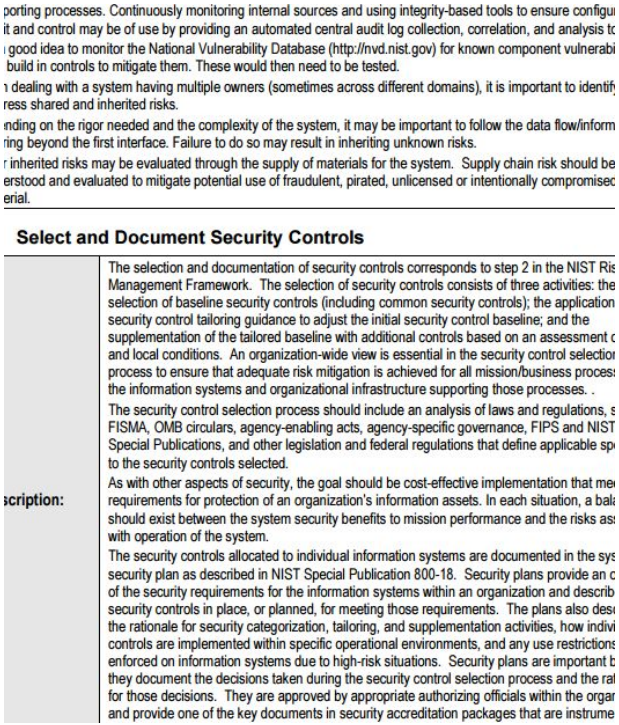
# NIST SP-800-64

Gov’t only.

Giant, headache inducing wall of text.

Free!

Actually lays things out pretty decently once you get into it, if a bit dated.



porting processes. Continuously monitoring internal sources and using integrity-based tools to ensure configu
it and control may be of use by providing an automated central audit log collection, correlation, and analysis to
good idea to monitor the National Vulnerability Database (http://nvd.nist.gov) for known component vulnerabi
build in controls to mitigate them. These would then need to be tested.

dealing with a system having multiple owners (sometimes across different domains), it is important to identify
ress shared and inherited risks.

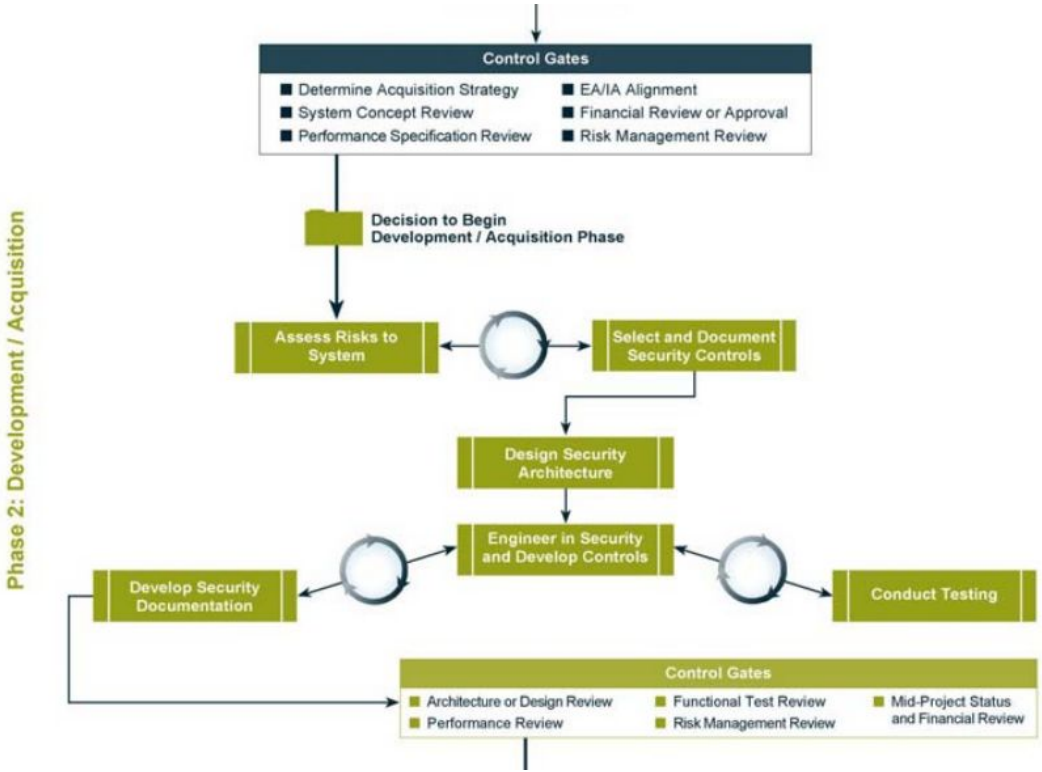
nding on the rigor needed and the complexity of the system, it may be important to follow the data flow/inform
ring beyond the first interface. Failure to do so may result in inheriting unknown risks.

inherited risks may be evaluated through the supply of materials for the system. Supply chain risk should be
erstood and evaluated to mitigate potential use of fraudulent, pirated, unlicensed or intentionally compromised
erial.

**Select and Document Security Controls**

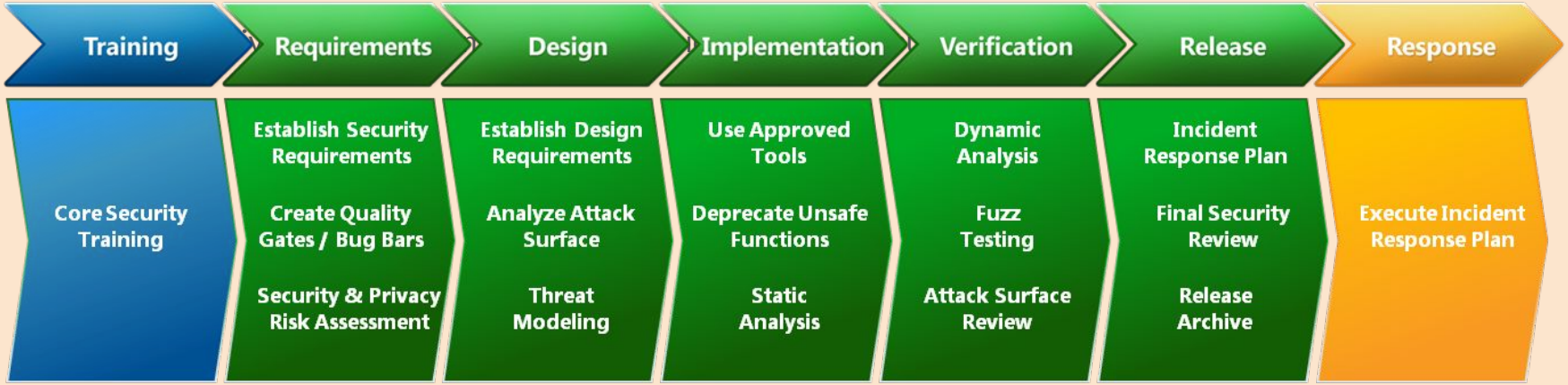
| | |
|---|---|
| scription: | The selection and documentation of security controls corresponds to step 2 in the NIST Ris Management Framework. The selection of security controls consists of three activities: the selection of baseline security controls (including common security controls); the application security control tailoring guidance to adjust the initial security control baseline; and the supplementation of the tailored baseline with additional controls based on an assessment and local conditions. An organization-wide view is essential in the security control selection process to ensure that adequate risk mitigation is achieved for all mission/business process the information systems and organizational infrastructure supporting those processes. .<br>The security control selection process should include an analysis of laws and regulations, s FISMA, OMB circulars, agency-enabling acts, agency-specific governance, FIPS and NIST Special Publications, and other legislation and federal regulations that define applicable sp to the security controls selected.<br>As with other aspects of security, the goal should be cost-effective implementation that me requirements for protection of an organization's information assets. In each situation, a bala should exist between the system security benefits to mission performance and the risks ass with operation of the system.<br>The security controls allocated to individual information systems are documented in the sys security plan as described in NIST Special Publication 800-18. Security plans provide an o of the security requirements for the information systems within an organization and describ security controls in place, or planned, for meeting those requirements. The plans also desc the rationale for security categorization, tailoring, and supplementation activities, how indivi controls are implemented within specific operational environments, and any use restrictions enforced on information systems due to high-risk situations. Security plans are important b they document the decisions taken during the security control selection process and the ra for those decisions. They are approved by appropriate authorizing officials within the organ and provide one of the key documents in security accreditation packages that are instrume |

# NIST SP-800-64



# Microsoft Security Development Lifecycle

Scope is different than most of the rest.



# BSIMM

Basically a big set of survey results.

Descriptive, not Prescriptive

BSIMM8

# Measuring Real-world Practices

“Just the facts.”

In-person interview with the organizations.

BSIMM professional completing the interviews.


Strategy & Metrics
Compliance & Policy
Training
Attack Models
Security Features & Design
Standards & Requirements
Architecture Analysis
Code Review
Security Testing
Penetration Testing
Software Environment
Configuration Mgmt. & Vulnerability Mgmt.
3.0
2.5
2.0
1.5
1.0
0.5
0.0
Cloud (16 of 109)
Healthcare (17 of 109)

# BSIMM - Helpful Concepts and Conclusions

Software Security Group - Internal group charged with carrying out and facilitating software security.

Everyone struggles.

Trend is definitely towards increased maturity.

# Fun Stats from the BSIMM

Of Organizations surveyed:

67% Provide awareness training.

40% Have an operations inventory of applications.

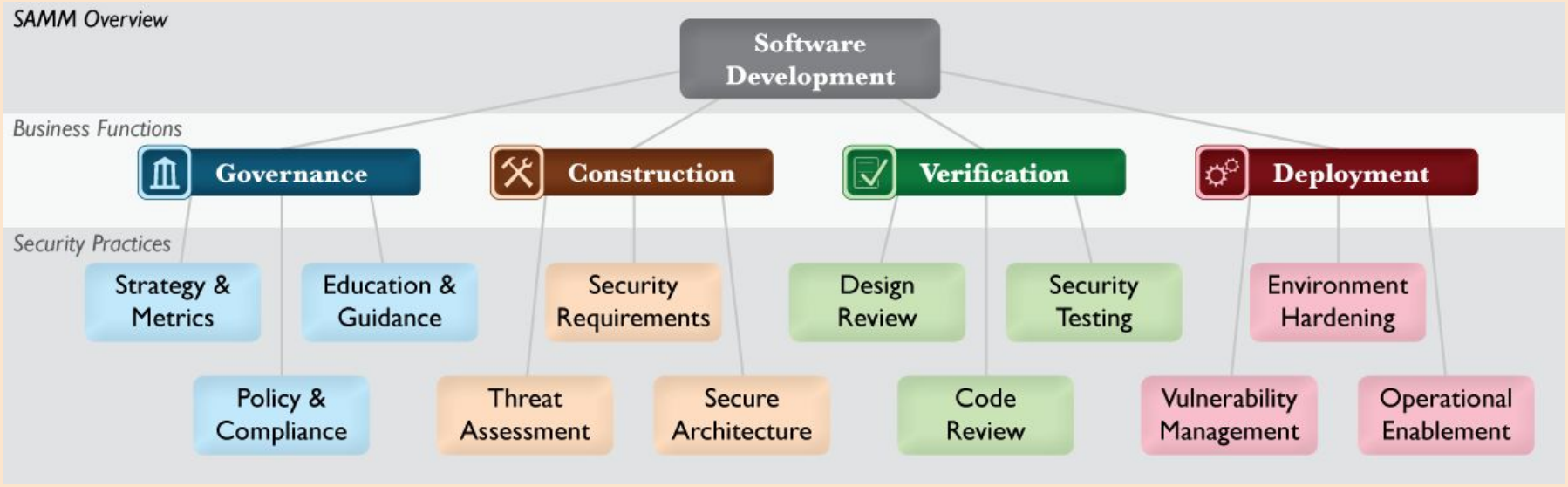
25% Identify PII data inventory.

21% Provide penetration testers with all available information.

11% Have a bug bounty program.

# OWASP SAMM

“...to help organizations formulate and implement a strategy for software security that is tailored for the specific risks facing the organization.”


SAMM Overview
Software Development
Business Functions
Governance
Construction
Verification
Deployment
Security Practices
Strategy & Metrics
Education & Guidance
Security Requirements
Design Review
Security Testing
Environment Hardening
Policy & Compliance
Threat Assessment
Secure Architecture
Code Review
Vulnerability Management
Operational Enablement

# Governance

- Strategy and Metrics
  - Establishing the framework
  - Risk classification
- Policy and Compliance
  - Regulations and Standards
  - Audits
- Education and Guidance
  - Pretty much exactly what it sounds like.

# Construction

- Threat Assessment
  - Identifying explicit threats at a project level.
  - Weighting those threats.
- Security Requirements
  - Proactively specifying expected behavior
  - More mature: pushing requirements to suppliers.
- Secure Architecture
  - “Build secure software by default.”
  - Reusable service and components, approved frameworks, centralized services.

# Verification

- Design Review
  - Detect architecture-level issues.
  - Evolves towards formal inspection, and baselines for design assessments.
- Implementation Review
  - More eyes on code means less bugs and vulnerabilities.
  - Automation (SASTs)
- Security Testing
  - Runtime Inspection, human, robot, and otherwise.

# Operations

- Issue Management
  - Have an incident response process, to start with.
  - Go from there.
- Environment Hardening
  - Patching.
  - Monitoring.
- Operational Enablement
  - Kind of like the user manual for the operators of the software.
  - “Formal operational security guidelines.”

# Deep dive: Education and Guidance 1 - 3

EG1 Objective:
“Offer development staff access to resources around topics of secure programming and deployment.”

EG2 Activities:
* Conduct role specific application security training.
* Utilize security coaches to enhance project teams

EG3 Results: Efficient remediation of vulnerabilities in both ongoing and legacy code bases.

# Deep Dive: Implementation Review 1 - 3

AKA Code Review

Starts with checklists and point-reviews.

Proceeds to automation, and significant integration of that tool.

Ends with enforced, objective goals for judging code-level security.

# Deep Dive: Environment Hardening 1 - 3

Understand baseline operational environment for applications and software.

Establish reliable patching and monitoring systems.

Deploy protection tools, and expand audit program.

# Tools available for the SAMM

- Great big PDF
- Wiki, with about 85% of the content of the PDF.
- SAMM_Assessment_Toolbox_v1.5_FINAL.xlsx

# Self-Assessment

- One of the first steps.
- How bad is it?
- Probably not as bad as you fear, but definitely not great.

# Self-Assessment - Lightweight

## (AUDIENCE PARTICIPATION)

| | Education & Guidance | Answer | Interview Notes | Rating |
|---|---|---|---|---|
| EG1 | **Have developers been given high-level security awareness training?**<br>*Guidance:* Application security awareness training is provided to all developers.<br>*Guidance:* Training covers topics such as common vulnerabilities and best practice recommendations for eliminating vulnerabilities.<br>*Guidance:* Training is conducted at least annually as well as on demand based on need. | **Yes, we did it once** | 2017 Roadmap item. | **0.30** |
| | **Does each project team understand where to find secure development best-practices and guidance?**<br>*Guidance:* Resources regarding secure development practices have been assembled and made available to developers.<br>*Guidance:* Management informs development groups that they are expected to utilize secure development resources.<br>*Guidance:* A checklist based on the secure development resources has been created to ensure guidelines are met during | **Yes, a small percentage are/do** | 2017 Roadmap item. The resources are | |

# Assessment Results

| Current Maturity Score | | | | |
|---|---|---|---|---|
| | | Maturity | | |
| Security Practices | Current | 1 | 2 | 3 |
| Strategy & Metrics | 0.00 | 0.00 | 0.00 | 0.00 |
| Policy & Compliance | 1.60 | 0.75 | 0.35 | 0.50 |
| Education & Guidance | 0.30 | 0.20 | 0.10 | 0.00 |
| Threat Assessment | 0.10 | 0.10 | 0.00 | 0.00 |
| Security Requirements | 1.20 | 0.50 | 0.60 | 0.10 |
| Secure Architecture | 0.10 | 0.10 | 0.00 | 0.00 |
| Design Analysis | 0.00 | 0.00 | 0.00 | 0.00 |
| Implementation Review | 0.60 | 0.50 | 0.10 | 0.00 |
| Security Testing | 0.23 | 0.13 | 0.10 | 0.00 |
| Issue Management | 1.32 | 0.47 | 0.25 | 0.60 |
| Environment Hardening | 1.00 | 0.50 | 0.50 | 0.00 |
| Operational Enablement | 1.10 | 0.60 | 0.50 | 0.00 |

# Self-Assessment - Detailed

Prove it!

This is what happens at the end of every  phase.

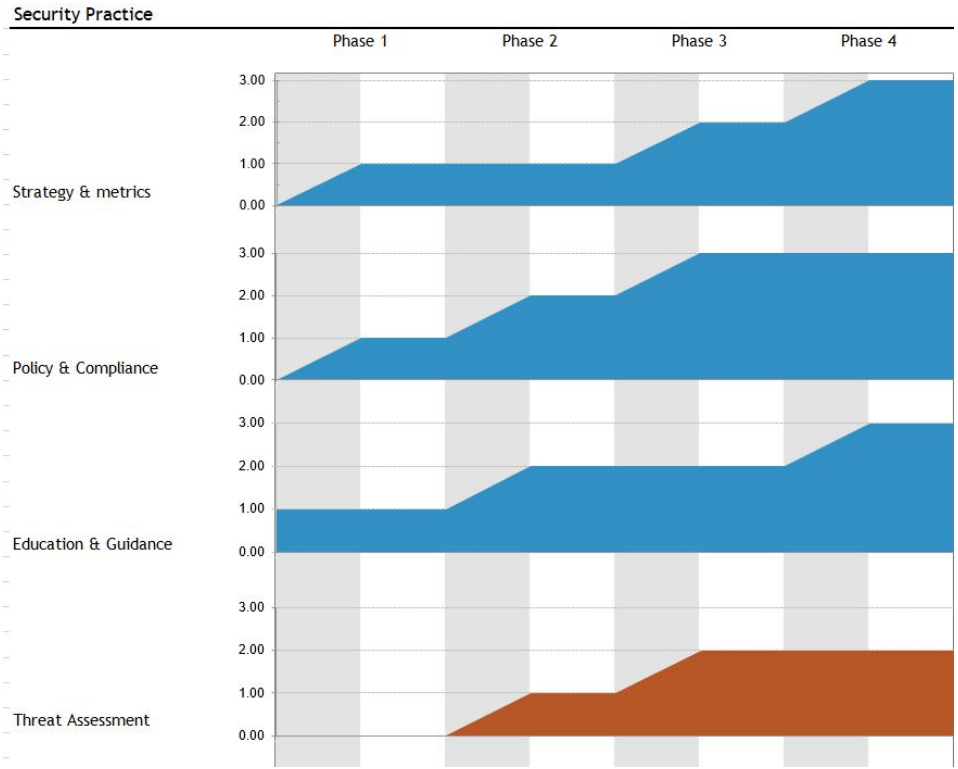
Forever...

# Building a Roadmap

Start where you can.

Align to stuff that's in-flight already.

Use the tools.



# Building a Roadmap - Examples

Small, agile organization with key pieces in place.

Monolithic, resistant to change organization.

Heavily remote organization with diverse technology stacks and siloed teams.

# Setting Metrics

Defining groups/people is harder than you think.

You don’t have to use the ones they pick!

Make them testable and gatherable.

Pick your percentages.  Plan to crank them up.

# Executing your Roadmap

Based on organization size and agility, pick your phase length.

Pick your end goals.

Calculate the difference, and lay it out in the phases.

Tweak it.

Tweak it some more.

# I did it!  What now?

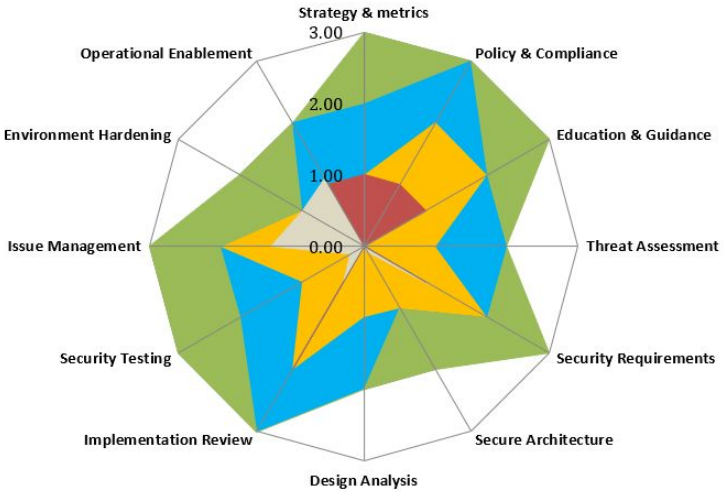
Eh, it never really ends.

The end of the last phase means you have ongoing activities and audits.

Keep upping your metrics.  “100% of devs get 1 on 1 training from drunk Steve Ballmer himself, daily.”

# In Practice - Observations So Far

| Current Maturity Score | | | | |
|---|---|---|---|---|
| | | Maturity | | |
| Security Practices | Current | 1 | 2 | 3 |
| Strategy & Metrics | 0.00 | 0.00 | 0.00 | 0.00 |
| Policy & Compliance | 1.60 | 0.75 | 0.35 | 0.50 |
| Education & Guidance | 0.30 | 0.20 | 0.10 | 0.00 |
| Threat Assessment | 0.10 | 0.10 | 0.00 | 0.00 |
| Security Requirements | 1.20 | 0.50 | 0.60 | 0.10 |
| Secure Architecture | 0.10 | 0.10 | 0.00 | 0.00 |
| Design Analysis | 0.00 | 0.00 | 0.00 | 0.00 |
| Implementation Review | 0.60 | 0.50 | 0.10 | 0.00 |
| Security Testing | 0.23 | 0.13 | 0.10 | 0.00 |
| Issue Management | 1.32 | 0.47 | 0.25 | 0.60 |
| Environment Hardening | 1.00 | 0.50 | 0.50 | 0.00 |
| Operational Enablement | 1.10 | 0.60 | 0.50 | 0.00 |




**Policy & Compliance** — **Level 1**

**Objective**

Understand relevant governance and compliance drivers for the organization.

**Activities**

*A. Identify and monitor external compliance drivers* | *B. Build and maintain compliance guidelines*

**Description**

**People:** The work is primarily completed by the Risk Management Team, with some consultation work and communication to be done by the Security Team.
**Process:** The creation of an ongoing compliance checklist and formalized repository is the primary process defined by this practice. This process can be an extension of our current attestation and compliance processes.
**Tools:** We will likely use ServiceNow for management of this repository and checklist. Many different GRC tools could accomplish this goal.

**Results**

- Increased assurance for handling third-party audit with positive outcome
- Alignment of internal resources based on priority of compliance requirements
- Timely discovery of evolving regulatory requirements that affect your organization

Netsmart Success Metrics

__ >1 Compliance discovery event in the last year.

__ Compliance discovery process documentation updated/reviewed in last year.

__ Compliance guidelines/standards communicated to Technical Leads and Owners in the last year.

# Getting Started

Maybe start with the BSIMM even?

Pick one area that you have some influence over, and measure yourself.

Push for change!

# Questions?


august.johnson@gmail.com

@august on seckc.slack.com

keybase.io/augustjohnson

github.com/augustjohnson