OWASP - SAMM

Matt Bartoldus
Gotham Digital Science

OWASP

12 March 2009

The OWASP Foundation

http://www.owasp.org

Introduction

- Me
- Who Are You?
  - Hacker, Tester
  - Assessment (security auditors)
  - Architect
  - Developer
  - Management
  - Business Owner
  - Consultant (all the above)
  - Other

Agenda

- Overview of Software Security Issues
  - It is all so very young!
- Introducing SAMM
- Uses of SAMM
- SAMM Core Functions / Activities
- Use Case – SAMM to Measure
- Use Case – SAMM to Implement
- Future of SAMM

Overview of Software Security Issues

Software Security Issues

- Relatively Same Drivers Across Industries
  - Compliance
    - PCI-DSS, SOX, DPA, etc
  - Protection
    - Brand/reputation; from criminals (cyber crime)
  - Governance
    - Function of good corporate governance

Ask

Software Security Issues

- What does ‘it’ look like?
- How can we understand and manage ‘this’?
- Do we have enough resources / skills to do ‘this’?
- How does ‘this’ fit in with the Security function, shouldn’t they do ‘it’?
- We are used to security projects that implement tools or systems but now we need to change our processes?
- Isn’t there an established method or model for all ‘this’?

Young Discipline in a Young Industry

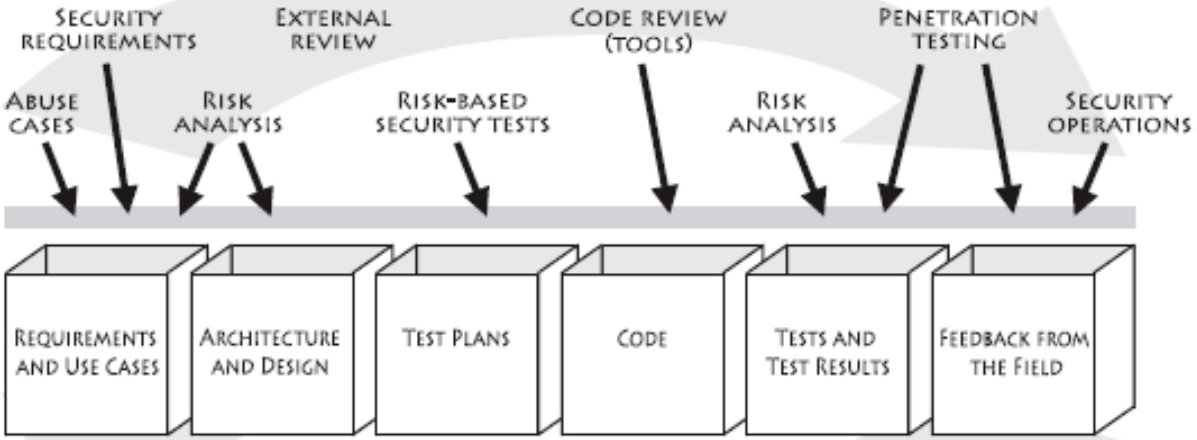
- BS7799 came out mid-90s
- Shifting Focus within Industry
  - PBX to Infrastructure to Database/Application
- PCI-DSS
  - CISP – 2001 – mention of change control as a best practice item
  - PCI-DSS v1.2 – late 2008 – Requirement 6

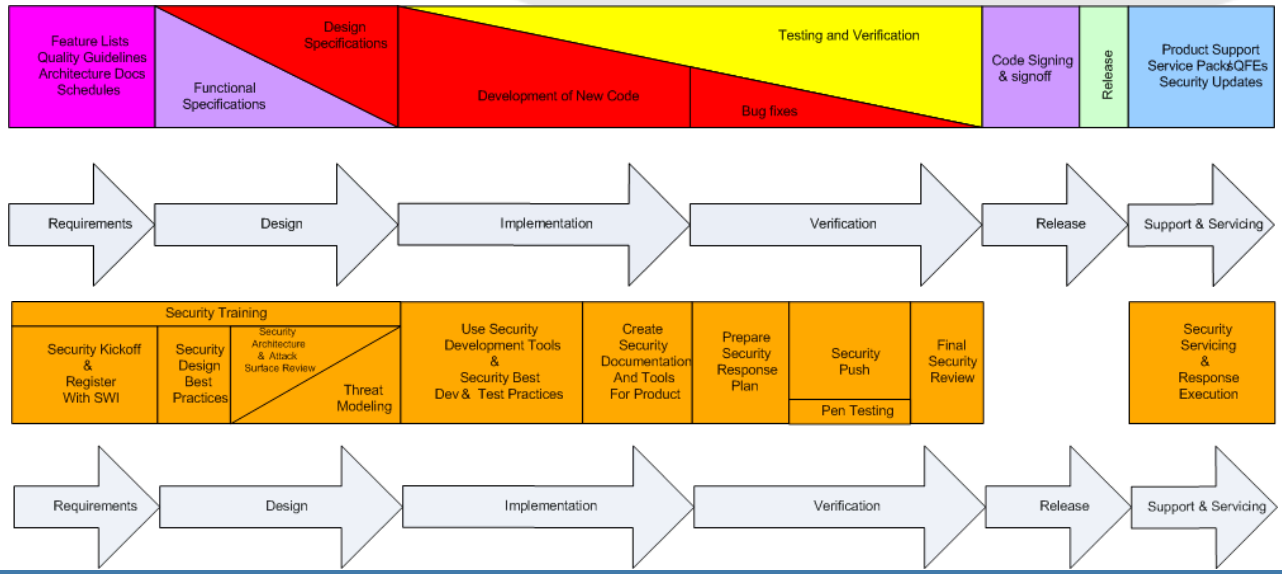
Ask – What is this discipline?

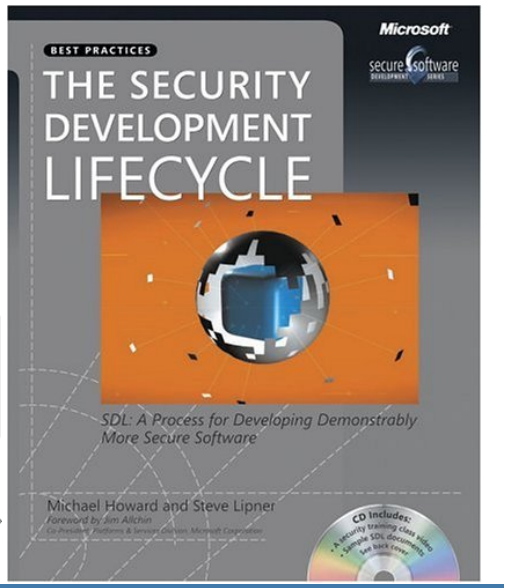
So what is 'this' discipline called?

- Software Assurance
- SSA - Software Security Assurance
- SDL – Security Development Lifecycle
- SDLC – to confuse everyone
- sSDLC – secure Software Development Lifecycle
- SPLC – Secure Project Lifecycle
- CLASP - Comprehensive, Lightweight Application Security Process
- 7 Touchpoints
- SSF – System Security Framework

Other approaches to Security in the SDLC







Motivation for a maturity model approach

- Changing an organisation is hard

  Simple, well-defined, measurable
  always trumps
  complex, nuanced, ethereal

- Software security is a result of many activities
  - Combination of people, process, and automation
- There is no single formula for all organisations
  - Business risk from software depends on what the business does
- An assurance program must be built over time
  - Organisations can't change overnight. Use a phased approach.

The Software Assurance Maturity Model (SAMM)

Why is SAMM relevant?

- **SAMM is to become an OWASP project**
  - Headed by Pravir Chandra in the US
  - Will be setup within a month
  - New release due any day now

- **Security Assurance is more pervasive than a lot of people would expect.**

The Software Assurance Maturity Model

- Collaboratively written by experts within this field with review and feedback.
- Funded by Fortify Software
- Beta released in Aug 2008
- Creative Commons Attribution-Share Alike License (ie: open)

Goals and Purpose

- To define building blocks for an assurance program
  - Delineate all functions within an organisation that *could* be improved over time
- To allow organizations to create customized roadmaps
  - Each organisation can choose the order and extent they improve each function
- To provide sample roadmaps for common types of organisations
  - Each roadmap is a baseline that can be tweaked based on the specific concerns of a given organisation

What SAMM in NOT

- Prescriptive ‘howto’ document
- ‘One size fits all’ methodology
- Audit checklist for secure development

What can you do with SAMM?

Guidance

- What needs to be done
- General idea of skills and resource needs
- Understand what is involved

Measurement - Assurance program scorecards

- By assessing an organisation's practices against SAMM activities, they can be given a score for each activity (against objectives)
  - Demonstrate gaps against best practices
- Using a scorecard, an organisation can demonstrate quantifiable improvement
- Down the road possibility: certification of an organisation's assurance program

Context / Framework for Business

- Communicate outside of Security lab / office
- Substantiate business requirement / risks
- Set out a common understanding (get everyone on the same page)

Build Implementation Roadmap

- Use Guidance
- Measure
- Put into business context (for funding and management support)
- Build phased implementation plan

SAMM Core Functions?

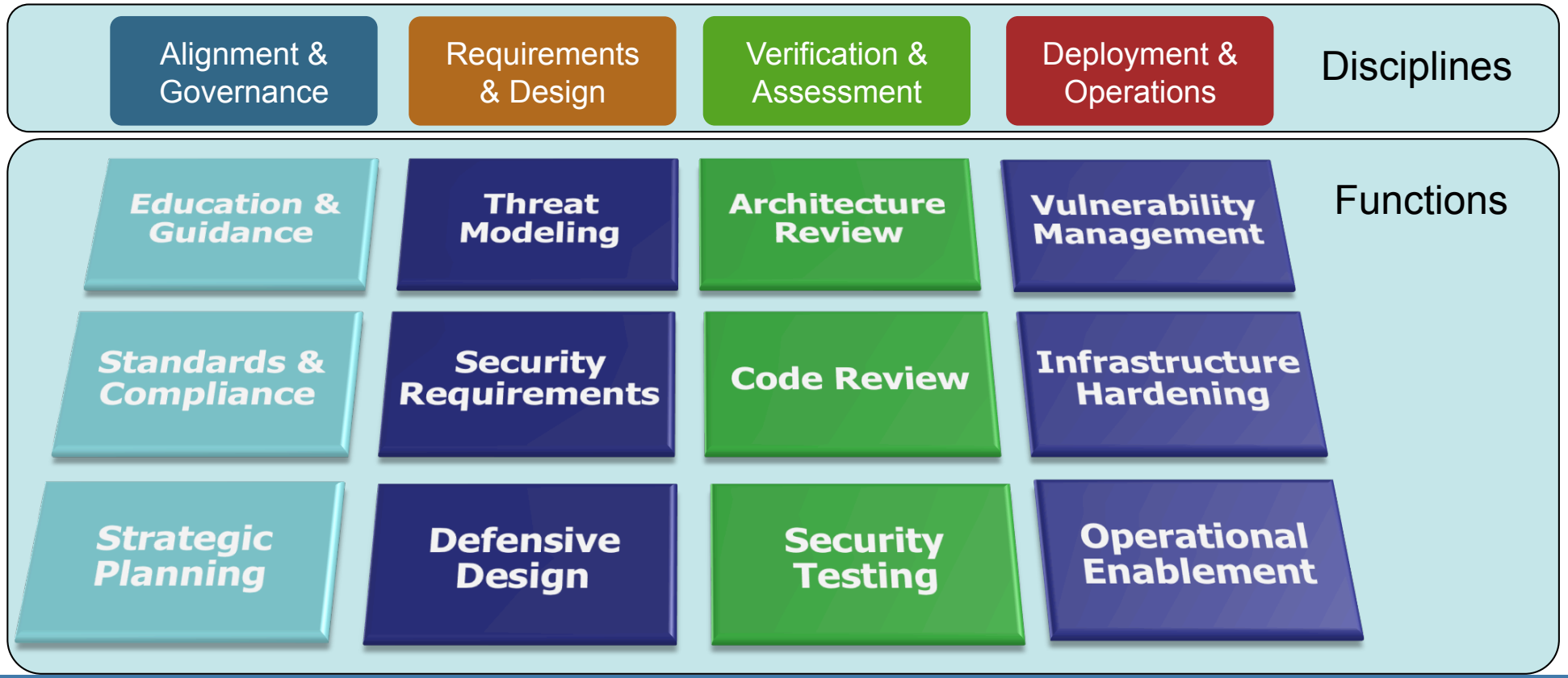
Four high-level Disciplines

- All security-related activities mapped under 4 ***Disciplines***, each representing a group of related business functions

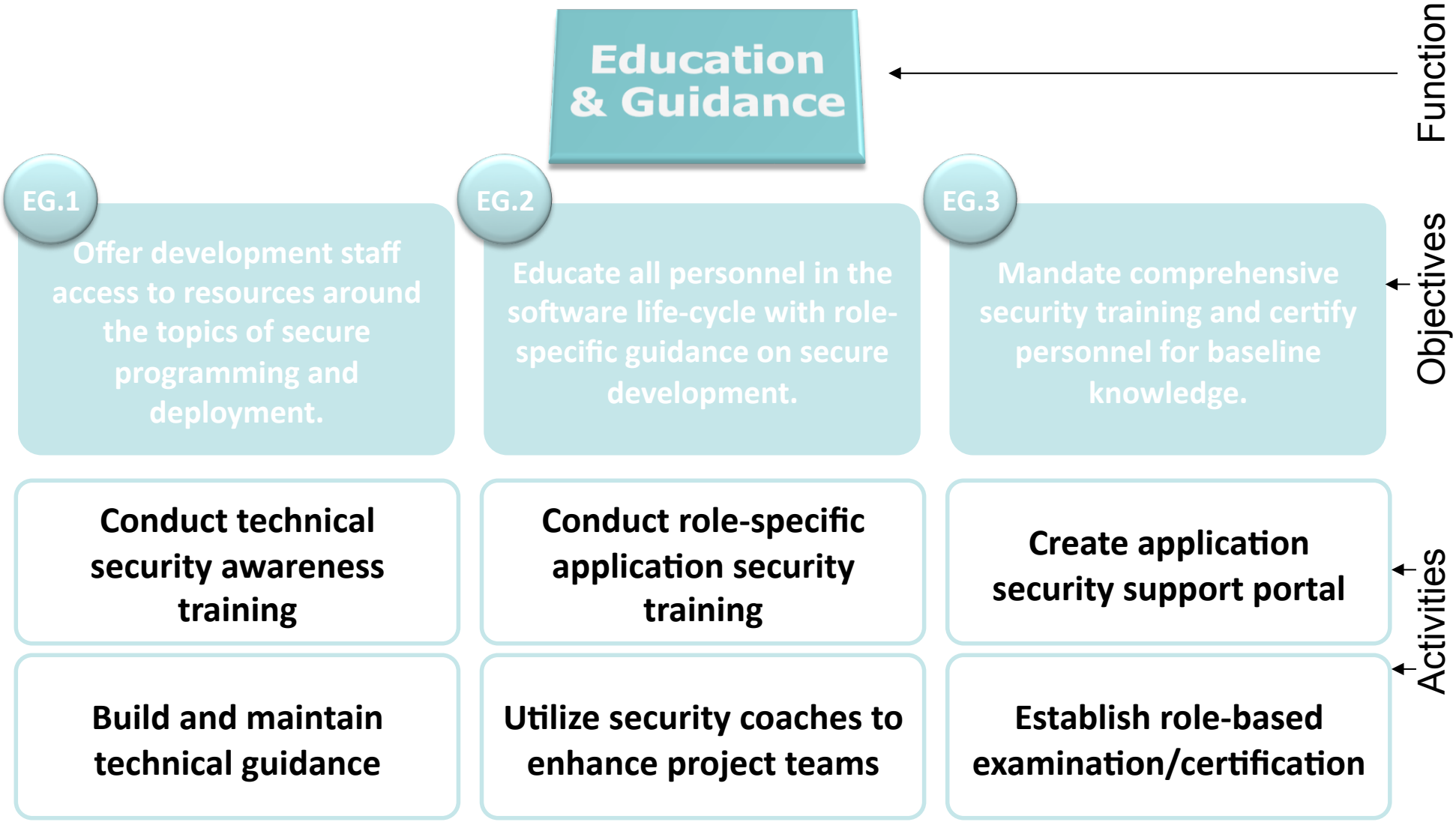
Alignment & Governance	Requirements & Design	Verification & Assessment	Deployment & Operations
Activities related to security program management and cross-cutting organizational concerns	Activities related to the product conception and software design processes	Activities related to reviewing, testing, and validating software	Activities related to knowledge transfer and maintenance of running software

What's under each Discipline?

- The 4 Disciplines are high-level categories for activities
  - Three security Functions under each Discipline are the specific silos for improvement within an organisation



For example, Education & Guidance:



Standards and Compliance - SC

- Understand standards and compliance drivers of the organisation in order to meet their needs.

- Set out compliance gates

Security Requirements - SR

- In order to plan for information security to be built in to software, it has to be detailed as requirements so they can be developed and tested in the same way as functional requirements
- Security requirements need to be tailored based on several risk factors such as the type of software being developed, data that will be processed or who will have access.

Threat Modelling - TM

- Threat Modelling is an activity performed in order to focus on what the threats are to an application and likely attacks it may face once developed and deployed.

- Information security requirements are then matched up against the identified threats in order to determine whether the security requirements have addressed all identified threats appropriately.

Architecture Review - AR

- the review of software designs and architecture models for potential security related deficiencies.

- The security requirements developed for the project as well as either the organisation's security architecture or best practices are used as the basis for the review.

Code Review – CR

- Source code analysis for information security related issues within code.
- Use checklists and sampling
- Automated tools for deeper inspection

Security Testing – ST

- This activity is the one that is most recognisable in the industry as it has been performed for many years.
- Includes traditional penetration testing such as black-box and white box testing.
- SAMM also suggests performing more tailored testing based on test cases derived from the security requirements

Using SAMM to Measure

BSIMM

- Fortify and Cigital Study
  - 9 large organisations who create software
  - Benchmarking and sharing of good practice

Measuring for Implementation – EU Financial Organisation

- Discussed SDLC and related security processes within the organisation
- Mapped to SAMM activities
- Used CMMI type scores for each activity (think COBIT controls measurement)

Using SAMM to Implement

Implementing SAMM – Large EU Organisation

- Used measurement results to frame planning
- Determined goals based on results and chose activities needed to implement initially
- Put all into context to talk with management for support
- Enabled us to see dependencies on other areas of the business


Questions?