OpenSAMM

The Anatomy of Real-World Security Programs

http://www.opensamm.org

Pravir Chandra
OpenSAMM Project Lead
chandra@owasp.org

What are we talking about?

- Lessons from real programs
- A mild intro to the OpenSAMM model
- The project and it's future

Lessons From Walking the Path

We do __ for security.

We're all snowflakes.

It’ll help, I promise...

It's not technical, you geek.

Control your future.

Real ROI is possible.

Specifically, get specific.

Multiply thyself.

Measure on a moving scale.

SAMM v. BSIMM v. SDL

The OpenSAMM model

Drivers for a Maturity Model

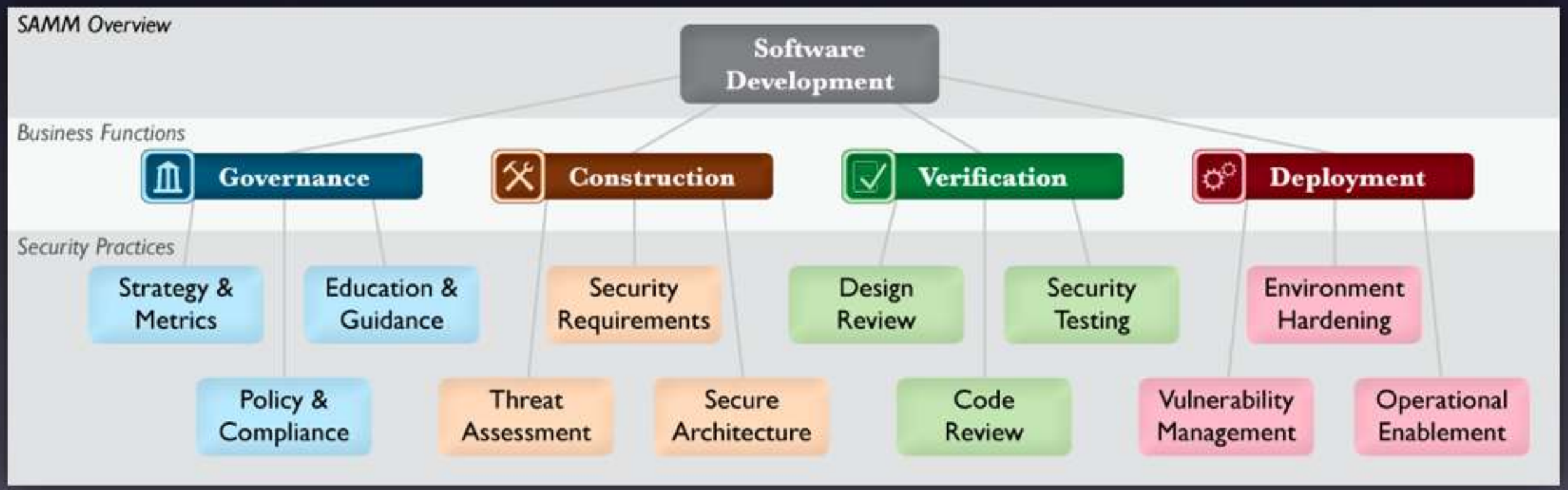
- An organization's behavior changes slowly over time
  - Changes must be iterative while working toward long-term goals
- There is no single recipe that works for all organizations
  - A solution must enable risk-based choices tailor to the organization
- Guidance related to security activities must be prescriptive
  - A solution must provide enough details for non-security-people
- Overall, must be simple, well-defined, and measurable

SAMM Business Functions

- Start with the core activities tied to any organization performing software development
- Named generically, but should resonate with any developer or manager

SAMM Security Practices

- From each of the Business Functions, 3 Security Practices are defined
- The Security Practices cover all areas relevant to software security assurance
- Each one is a 'silo' for improvement



Under each Security Practice

- Three successive Objectives under each Practice define how it can be improved over time
  - This establishes a notion of a Level at which an organization fulfills a given Practice
- The three Levels for a Practice generally correspond to:
  - (0: Implicit starting point with the Practice unfulfilled)
  - 1: Initial understanding and ad hoc provision of the Practice
  - 2: Increase efficiency and/or effectiveness of the Practice
  - 3: Comprehensive mastery of the Practice at scale

Check out this one...

Education & Guidance

...more on page 42

	EG 1	EG 2	EG 3
Objective	**Offer development staff access to resources around the topics of secure programming and deployment**	**Educate all personnel in the software life-cycle with role-specific guidance on secure development**	**Mandate comprehensive security training and certify personnel for baseline knowledge**
Activities	A. Conduct technical security awareness training B. Build and maintain technical guidelines	A. Conduct role-specific application security training B. Utilize security coaches to enhance project teams	A. Create formal application security support portal B. Establish role-based examination/certification

Per Level, SAMM defines...

- Objective
- Activities
- Results
- Success Metrics
- Costs
- Personnel

Education & Guidance

EG 1

Offer development staff access to resources around the topics of secure programming and deployment

Activities

A. Conduct technical security awareness training

Either internally or externally sourced, conduct security training for technical staff that covers the basic tenets of application security. Generally this can be accomplished via instructor-led training in 1-2 days or via computer-based training with modules taking about the same amount of time per developer.

Course content should cover both conceptual and technical information. Appropriate topics include high-level best practices surrounding input validation, output encoding, error handling, logging, authentication, authorization. Additional coverage of commonplace software vulnerabilities is also desirable such as a Top 10 list appropriate to the software being developed (web applications, embedded devices, client-server applications, back-end transaction systems, etc.). Wherever possible, use code samples and lab exercises in the specific programming language(s) that applies.

To rollout such training, it is recommended to mandate annual security training and then hold courses (either instructor-led or computer-based) as often as required based on development headcount.

B. Build and maintain technical guidelines

For development staff, assemble a list of approved documents, web pages, and technical notes that provide technology-specific security advice. These references can be assembled from many publicly available resources on the Internet. In cases where very specialized or proprietary technologies permeate the development environment, utilize senior, security-savvy staff to build security notes over time to create such a knowledge base in an ad hoc fashion.

Ensure management is aware of the resources and briefs oncoming staff about their expected usage. Try to keep the guidelines lightweight and up-to-date to avoid clutter and irrelevance. Once a comfort-level has been established, they can be used as a qualitative checklist to ensure that the guidelines have been read, understood, and followed in the development process.

Results

- Increased developer awareness on the most common problems at the code level
- Maintain software with rudimentary security best-practices in place
- Set baseline for security knowhow among technical staff
- Enable qualitative security checks for baseline security knowledge

Success Metrics

- >50% development staff briefed on security issues within past 1 year
- >75% senior development/architect staff briefed on security issues within past 1 year
- Launch technical guidance within 3 months of first training

Costs

- Training course buildout or license
- Ongoing maintenance of technical guidance

Personnel

- Developers (1-2 days/yr)
- Architects (1-2 days/yr)

Related Levels

- Policy & Compliance - 2
- Security Requirements - 1
- Secure Architecture - 1

Conducting assessments

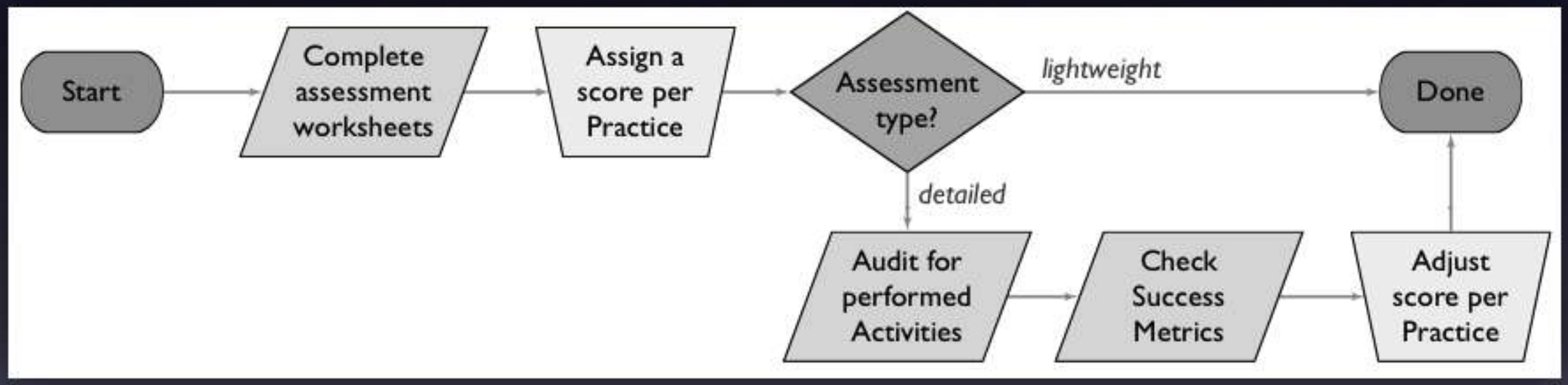
- SAMM includes assessment worksheets for each Security Practice

Education & Guidance

	Yes/No	
✦ Have most developers been given high-level security awareness training?		
✦ Does each project team have access to secure development best practices and guidance?		EG 1
✦ Are most roles in the development process given role-specific training and guidance?		
✦ Are most stakeholders able to pull in security coaches for use on projects?		EG 2
✦ Is security-related guidance centrally controlled and consistently distributed throughout the organization?		
✦ Are most people tested to ensure a baseline skill-set for secure development practices?		EG 3

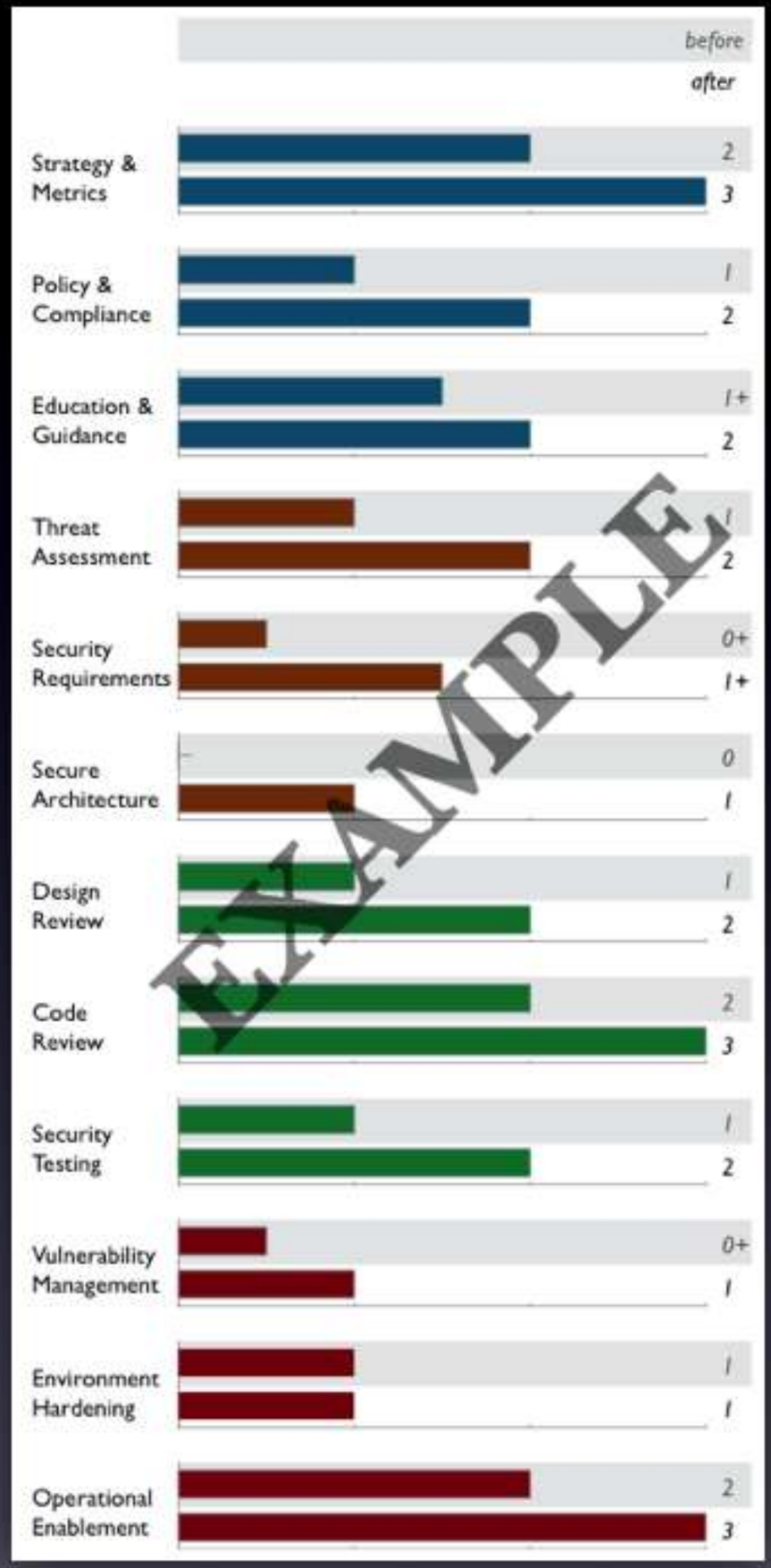
Assessment process

- Supports both lightweight and detailed assessments
- Organizations may fall in between levels (+)



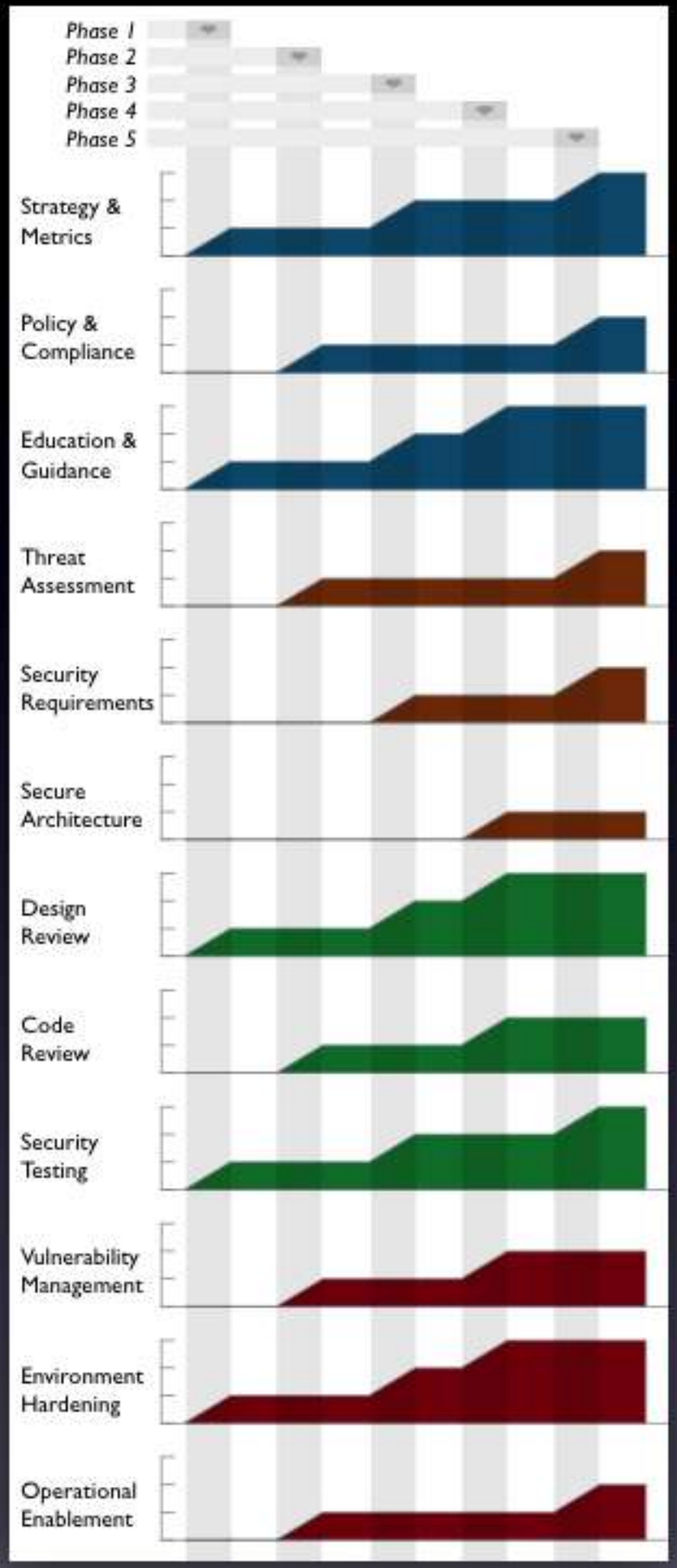
Creating Scorecards

- Gap analysis
  - Capturing scores from detailed assessments versus expected performance levels
- Demonstrating improvement
  - Capturing scores from before and after an iteration of assurance program build-out
- Ongoing measurement
  - Capturing scores over consistent time frames for an assurance program that is already in place

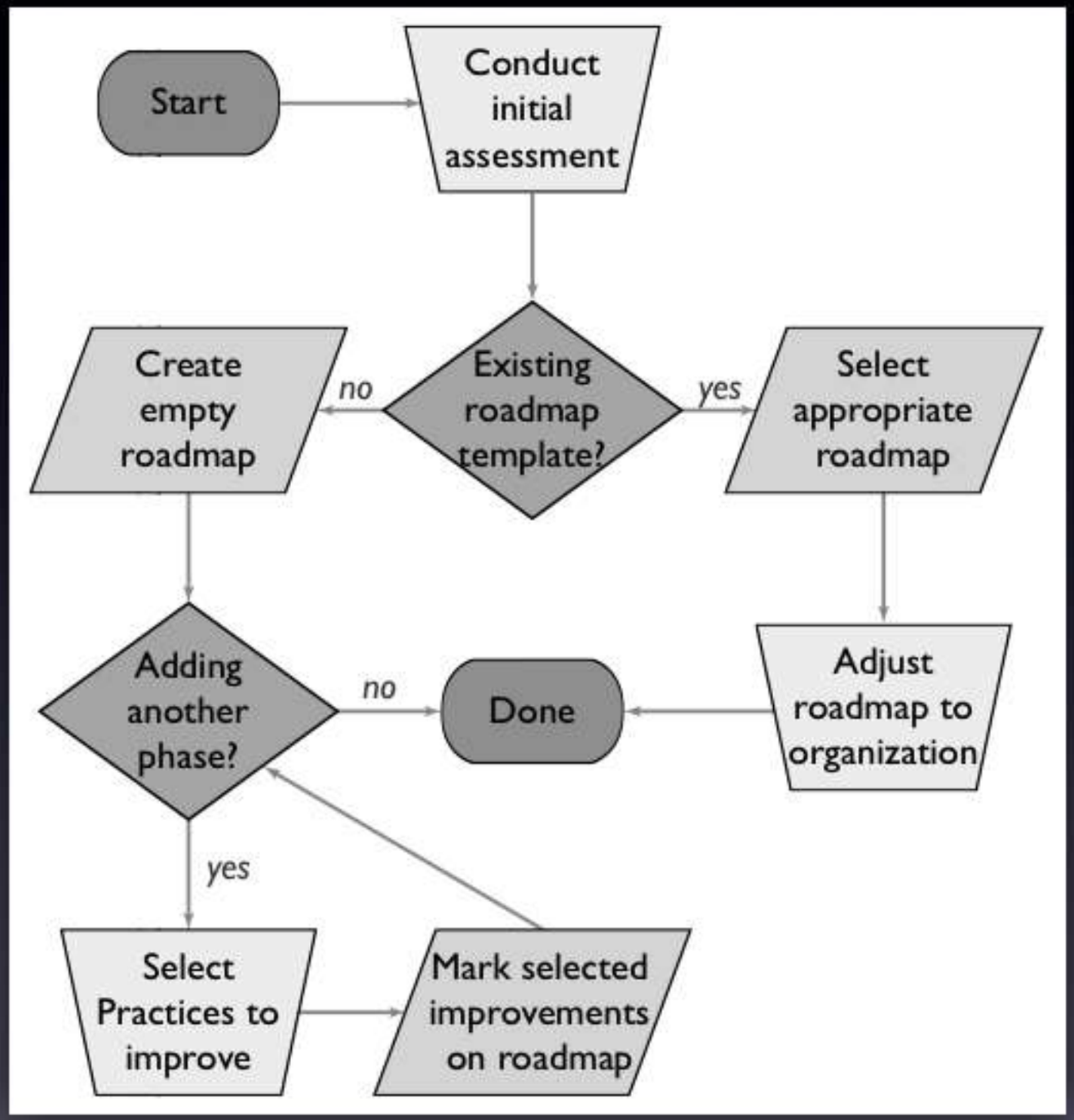


Roadmap templates

- To make the "building blocks" usable, SAMM defines Roadmaps templates for typical kinds of organizations
  - Independent Software Vendors
  - Online Service Providers
  - Financial Services Organizations
  - Government Organizations
- Organization types chosen because
  - They represent common use-cases
  - Each organization has variations in typical software-induced risk
  - Optimal creation of an assurance program is different for each



Building Assurance Programs



The OpenSAMM project

Quick stats

- About 40+ orgs using OpenSAMM for their programs
- 7500 unique hits in the last 12 months
- Dozens of contributed tools/resources

Expert contributions

- Built based on collected experiences with 100's of organizations
  - Including security experts, developers, architects, development managers, IT managers

Author & Project Lead

Pravir Chandra

Contributors/Reviewers

Fabio Arciniegas	Brian Chess	Matteo Meucci	John Steven
Matt Bartoldus	Dinis Cruz	Jeff Payne	Chad Thunberg
Sebastien Deleersnyder	Justin Derry	Gunnar Peterson	Colin Watson
Jonathan Carter	Bart De Win	Jeff Piper	Jeff Williams
Darren Challey	James McGovern	Andy Steingruebl	

Industry support

FORTIFY

OWASP
The Open Web Application Security Project

ASPECT SECURITY

coveros

DENIM GROUP

GOTHAM DIGITAL SCIENCE

leviathan security group

Minded security

Security Compass

WhiteHat SECURITY

The OpenSAMM Project

- http://www.opensamm.org
- Beta released August 2008, 1.0 released March 2009
- Dedicated to defining, improving, and testing the SAMM framework
- Always vendor-neutral, but lots of industry participation
  - Open and community driven
- Targeting new releases every ~18 months
- Change management process

Future plans

- Mappings to existing standards and regulations (many underway currently)
  - PCI, COBIT, ISO-17799/27002, ISM3, etc.
- Additional roadmaps where need is identified
- Additional case studies
- Feedback for refinement of the model
- Translations into other languages

Get involved

- Use SAMM and tell us about it
  - Blog, email, etc.
- Latest news at http://www.opensamm.org
  - Sign up for the mailing list

OpenSAMM

Thanks for your time! Questions?

http://www.opensamm.org

Pravir Chandra
OpenSAMM Project Lead
chandra@owasp.org