Building a Software Security Program

Software Security Maturity Assessment Services
Building a Software Security Program

• Foundstone’s Software Security Maturity Assessment Services
• Case Study
• Summary
• Questions
Contributing authors to all editions of Hacking Exposed

Thought Leadership
You're doing it wrong

Herd

Building a Software Security Program

Common Challenges
Common Challenges

Building a Software Security Program

Cost-effectiveness
Building a Software Security Program
Software Assurance Maturity Model

Operations

Verification

Architecture

Governance

https://www.openassurance.org
<table>
<thead>
<tr>
<th>Strategy &amp; Metrics</th>
<th>Activities</th>
<th>Results</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Estimate business risk profile related to software applications handling or storing credit card information</strong></td>
<td>Establish data and software applications handling credit card information based on business risk</td>
<td>A concrete list of the most critical business-level risks caused by software within PCI scope</td>
</tr>
<tr>
<td><strong>Classify data and software applications handling credit card information based on business risk</strong></td>
<td>Establish and measure per classification security goals relevant to data security and software applications handling or storing credit card information</td>
<td>A tailored roadmap that addresses the security needs for your organization with minimal overhead</td>
</tr>
</tbody>
</table>
| **Conduct periodic industry wide cost comparisons of compliance efforts related to secure software development** | Collect metrics for historic security spending | **Objective**
| **Establish a PCI centric software security program roadmap** | Build and maintain a PCI centric software security program roadmap from secure development and compliance goals | **Activities**
| **Per project consideration of compliance efforts and security expenses** | Establish security within the organization that the organization needs for your organization with the assurance program will grow over time | **Results**

**Objective**

- Establish unified strategic roadmap for software security within the organization
- Evaluate security needs for your organization with the assurance program that addresses the scope relevant based on software handling with PCI

**Activities**

- Per project consideration of compliance efforts and risk acceptance
- Establish data and software applications handling or storing credit card information based on business risk
- Establish security within the organization that the organization needs for your organization with the assurance program that addresses the scope relevant based on software handling with PCI

**Results**

- Organization wide understanding of how the assurance program will grow over time
- Better informed stakeholders with respect to relative value of data and software applications handling or storing credit card information
-比较好理解的组织内关于保证计划将如何成长的了解
- 具有更好知情的持票方对于数据和软件应用程序处理或存储信用卡信息的相对价值
- 能够更好地理解保证计划将如何成长的组织内
Key Benefits

- Offers a head start to improve an organization's software security posture
- Maps current security practices against recommendations by the maturity model
- Highlights gaps in SDLC maturity model
- Gathers supporting evidence through risk-based testing approach

Building a Software Security Program

SSMA - Phase 1 (Assessment)
Building a Software Security Program

SSMA – Key Findings

People Gaps

- Secure software development training program
- Security strategy aligned with external compliance driver

Process Gaps

- Tools for automation of processes
- Development tools integrating with security tools
- Technology Gaps
- Security & change control
- Standardize Web server and DB server build processes
- VMware Security Management Practice
- Security Testing Practice
- Code Review Practice
- Design Review Practice
- Security Architecture Practice
- Guidance implementing a SDL such as:

Security & change control
Building a Software Security Program

SSMA – Sample Score Card & Check Point

Current State – Check Point

Future State – Check Point

Strategy & Metrics

Vulnerability Management

Security Testing

Code Review

Design Review

Security Architecture

Security Requirements

Threat Assessment

Education & Guidance

Policy & Compliance

Environment Hardening
Building a Software Security Program

Software Security Maturity Assessment Services

- Role based training
- Security Testing Practice
- Remediation Guidance
- Role based infrastructure
- Security Testing
- Security Architecture
- Secure architecture remediation
- Review policies and compliance
- Change management
- Operations & Security Governance
- Infrastructure & Architecture
- Testing & Training
- Awareness & Planning
- Reporting
- Portfolio
- Application
- Business Risk
- App Risk Assessment
- Threat Assessment
- Change management control, DevOps
- Build project plan
- Build maturity roadmap
- Remediation practices
- Secure development lifecycle (SDLC)
- Review strategy
- Review policies
- Policies & Governance
- Business Risk
- Project Management
- Change Control
- DevOps
- Software Engineering
- Architecture
- Infrastructure
- Security Testing
- Training
- Awareness
- Planning
Building a Software Security Program

SSMA – Sample Score Card & Check Point
Phase 2 – Awareness & Planning

Establish Project Audit Practice

Build Standards, policies (Secure Development Policy)

Build SharePoint-like knowledge base or repository to support security

Sample topics:
- Application Security Risks 101
- PCI & The OWASP Top 10
- PCI & SANS Top 25
- Application Security Risks 101

Delivered by groups (Builder, Breakers, Defenders)

Deliver 15 minute Security Brown Bags

Establish and share strategic software security roadmap

Policy & Compliance

Education & Guidance

Strategy & Metrics
Building a Software Security Program

Phase 2 – Awareness & Planning
Phase 3 - Training & Testing

Building a Software Security Program

- Establish point of contact and informal response team
- Conduct security tests of applications portfolio
- Conduct security code reviews of applications with high risk
- Testing Checklist (CR, WAPT, HCR)
- Guidelines (WSC.NET Cheat Sheets, Hardening Guides)
- Conduct security code reviews of applications with high risk
- Enhance remediation guidance
- Conclude role base “hands on” technical training
- Continue security brown bags
Taking a Strategic Approach to Enterprise Security

Playbook
Building a Software Security Program

Phase 4 - Infrastructure & Architecture

- Build Threat Assessment practice
- Conduct Threat Assessment practice per project code base
- Expand and continue Code Review and WAPT practice
- Build Design Review Practice per project code base
- Document and align security requirements per project code
- Provide secure architecture design guidance and support
### What does maturity look like?

**Taking a Strategic Approach to Enterprise Security**

<table>
<thead>
<tr>
<th>Objective</th>
<th>Activities</th>
</tr>
</thead>
<tbody>
<tr>
<td>A. Identify and understand high-level threats to the organization and individual projects</td>
<td>A. Develop a threat profile for specific threat models.</td>
</tr>
<tr>
<td>B. Increase awareness of and threat assessment and improvement of mitigation of per-case models per project.</td>
<td>B. Incorporate threat intelligence into the third-party components.</td>
</tr>
<tr>
<td>C. Explicitly evaluate risk from third-party components and third-party software and third-party components.</td>
<td>C. Develop a weighting system for measurement of threats.</td>
</tr>
</tbody>
</table>

**TA 3**

- Incorporate threat intelligence into the third-party components.
- Increase awareness of and threat assessment and improvement of mitigation of per-case models per project.
- Develop a weighting system for measurement of threats.

**TA 2**

- Develop a threat profile for specific threat models.
- Incorporate threat intelligence into the third-party components.
- Increase awareness of and threat assessment and improvement of mitigation of per-case models per project.

**TA 1**

- Incorporate threat intelligence into the third-party components.
- Increase awareness of and threat assessment and improvement of mitigation of per-case models per project.
- Develop a weighting system for measurement of threats.
Taking a Strategic Approach to Enterprise Security

Threat Assessment Practice
Taking a Strategic Approach to Enterprise Security
Building a Software Security Program

Phase 5 - Governance & Security Operations

- Maintain formal operational security guides
- Manage procedures
- Coordinate and enhance code release and relevant change
- Conduct industry wide cost comparisons
- Document metrics for security expenditure
Some Success Metrics

Building a Software Security Program

- 80% CR code coverage for Top 10 software applications per project code
- 85% of projects updated with security requirements and design analysis
- 80% of stakeholders aware of threats per project code base
- 80% Vendors briefed on security requirements and standards
- 80% of staff knowledgeable about policies and standards
- 80% of applications in compliance with policies and standards
- 80% of requirements updated with security requirements
Building a Software Security Program

Some Success Metrics

Security Bug Status Distribution

Cumulative Security Bugs - Open vs. Closed

Security Bug Latency

McAfee Confidential
Some Success Metrics

Building a Software Security Program
Building a Software Security Program

SSMA Methodology

- Governance & Operational Security
- Infrastructure & Architecture
- Training & Testing
- Awareness & Planning

SSMA Key Benefits

- Cost effective guided approach supported by check points to ensure positive direction
- Comparison of current SDL activities vs. best practices
- A flexible plan to apply

Case Study (SSM Execution)

- SDL Gap Analysis followed by in depth audit
- 3 maturity levels
- Governance, Construction, Verification and Deployment