

1.1

SOFTWARE ASSURANCE MATURITY MODEL

HOW TO



This is an OWASP Project

The Open Web Application Security Project (OWASP) is a worldwide free and open community focused on improving the security of application software. Our mission is to make application security “visible,” so that people and organizations can make informed decisions about application security risks. Everyone is free to participate in OWASP and all of our materials are available under a free and open software license. The OWASP Foundation is a 501(c)3 not-for-profit charitable organization that ensures the ongoing availability and support for our work. Visit OWASP online at <http://www.owasp.org>.

License

This work is licensed under the Creative Commons Attribution-Share Alike 3.0 License. To view a copy of this license, visit <http://creativecommons.org/licenses/by-sa/3.0/> or send a letter to Creative Commons, 171 Second Street, Suite 300, San Francisco, California, 94105, USA.



Project leaders: Pravir Chandra

Creative Commons (CC) Attribution
Free Version at: <https://www.owasp.org>

/ CONTENTS

03	Executive Summary	13	SecurityTesting	23	Additional Considerations	33	Training Resource Requirements	44	Maturity Scorecard
05	Applying the Model	14	Operations	23	Outsourced Developmen	33	Outsourced Resources	45	Acknowledgements
06	Using the Maturity Levels	14	Issue Management	23	Web Services Platforms	34	phase 2 (months 3 - 6)	45	Contributors & Reviewers
06	Objective	14	Environment Hardening	23	Organizations Grown by Acquisition		Education & Testing		
06	Activities	15	Operational Enablement	24	Government Organization	34	Target Objectives		
06	Results	16	Creating Scorecards	24	Rationale	35	Implementation Costs		
06	Success Metrics	17	Building Assurance Programs	24	Additional Considerations	35	Internal Resource Requirements		
06	Costs	19	Independent Software Vendor	24	Outsourced Development	36	Training Resource Requirements		
06	Personnel	19	Rationale	24	Web Services Platforms	36	Outsourced Resources		
07	Related Levels	19	Additional Considerations	24	Regulatory Compliance	37	Phase 3 (months 6 - 9)		
07	Conducting Assessments	19	Outsourced Development	27	Case Studies		Architecture & Infrastructure		
08	Governance	19	Internet-Connected Applications	28	VirtualWare	37	Target Objectives		
08	Strategy & Metrics	19	Organizations Grown by Acquisition	28	Business Profile	39	Implementation Costs		
09	Policy & Compliance	21	Online Service Provider	28	Organization	39	Internal Resource Requirements		
09	Education & Guidance	21	Rationale	28	Environment	39	Outsourced Resources		
10	Construction	21	Additional Considerations	28	Key Challenges	40	Phase 4 (months 9 - 12)		
10	Threat Assessment	21	Outsourced Development	28	Implementation Strategy		Governance & Operational Security		
10	Security Requirements	21	Online Payment Processing	31	Phase 1 (months 0 - 3)	40	Target Objectives		
11	Secure Architecture	21	Web Services Platforms		Awareness & Planning	42	Implementation Costs		
12	Verification	21	Organizations Grown by Acquisition	31	Target Objectives	42	Internal Resource Requirements		
12	Design Review	23	Financial Services Organization	31	Implementation Costs	42	Outsourced Resources		
12	Implementation Review	23	Rationale	31	Internal Resource Requirements	43	Ongoing (months 12+)		

EXECUTIVE SUMMARY

The Software Assurance Maturity Model (SAMM) is an open framework to help organizations formulate and implement a strategy for software security that is tailored to the specific risks facing the organization. The resources provided by SAMM will aid in:

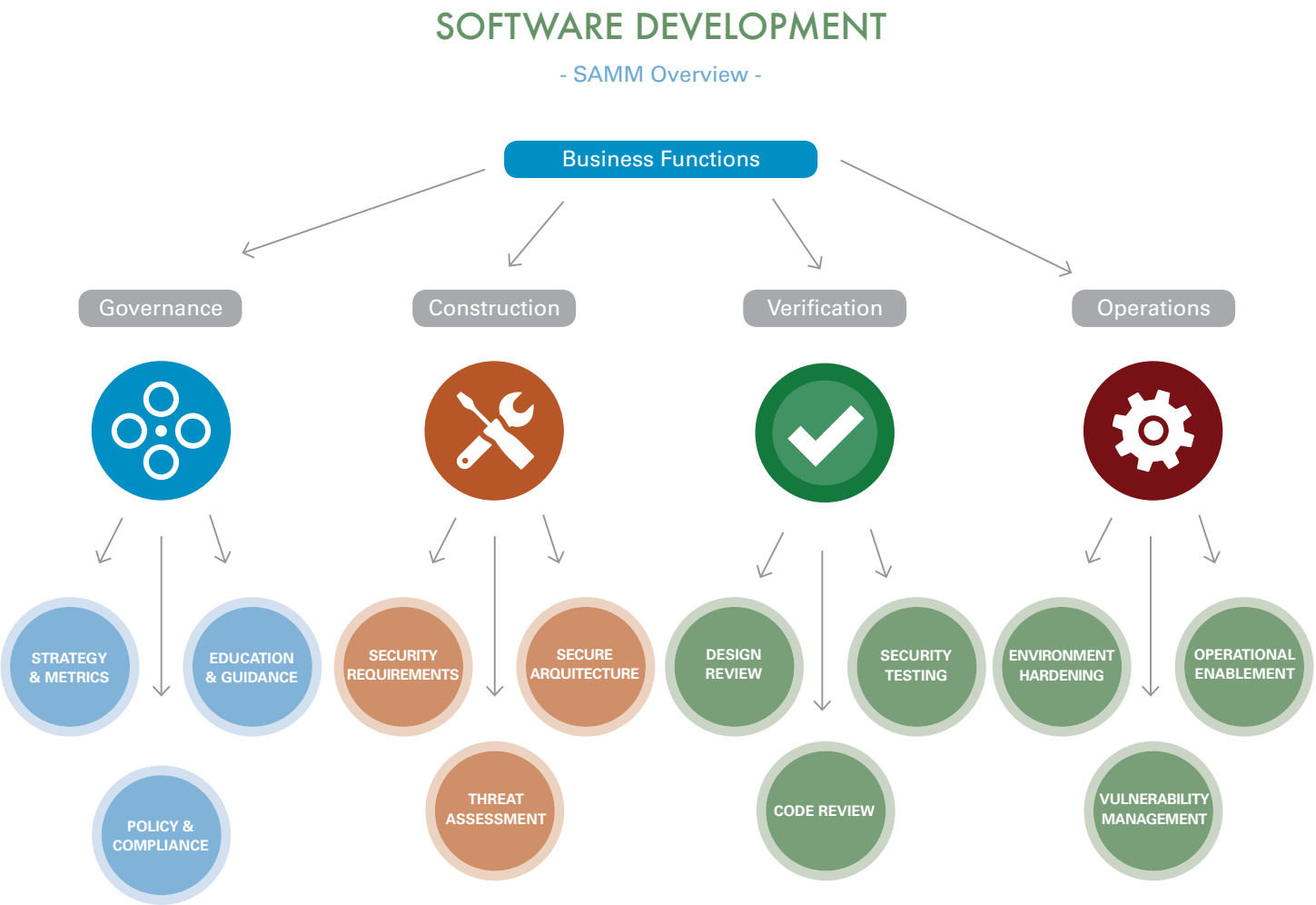
- Evaluating an organization’s existing software security practices
- Building a balanced software security assurance program in well-defined iterations
- Demonstrating concrete improvements to a security assurance program
- Defining and measuring security-related activities throughout an organization

SAMM was defined with flexibility in mind such that it can be utilized by small, medium, and large organizations using any style of development. Additionally, this model can be applied organization-wide, for a single line-of-business, or even for an individual project. Beyond these traits, SAMM was built on the following principles:

- An organization’s behavior changes slowly over time A successful software security program should be specified in small iterations that deliver tangible assurance gains while incrementally working toward long-term goals.
- There is no single recipe that works for all organizations A software security framework must be flexible and allow organizations to tailor their choices based on their risk tolerance and the way in which they build and use software.
- Guidance related to security activities must be prescriptive All the steps in building and assessing an assurance program should be simple, well-defined, and measurable. This model also provides roadmap templates for common types of organizations.

The foundation of the model is built upon the core business functions of software development with security practices tied to each (see diagram below). The building blocks of the model are the three maturity levels defined for each of the twelve security practices. These define a wide variety of activities in which an organization could engage to reduce security risks and increase software assurance. Additional details are included to measure successful activity performance, understand the associated assurance benefits, estimate personnel and other costs.

As an open project, SAMM content shall always remain vendor-neutral and freely available for all to use.





/ APPLYING THE MODEL

Putting it all to work

This section covers several important and useful applications of SAMM. Given the core design of the model itself, an organization can use SAMM as a benchmark to measure its security assurance program and create a scorecard. Using scorecards, an organization can demonstrate improvement through iterations of developing an assurance program. And most importantly, an organization can use SAMM roadmap templates to guide the build-out or improvement of a security assurance initiative.

/ USING THE MATURITY LEVELS

Each of the twelve Security Practices have three Maturity Levels. Each Level has several components that specify the critical factors for understanding and achieving the stated Level. Beyond that, these prescriptive details make it possible to use the definitions of the Security Practices even outside the context of using SAMM to build a software assurance program.

Objective

The Objective is a general statement that captures the assurance goal of attaining the associated Level. As the Levels increase for a given Practice, the Objectives characterize more sophisticated goals in terms of building assurance for software development, deployment and operations.

Activities

The Activities are core requisites for attaining the Level. Some are meant to be performed organization-wide and some correspond to actions for individual project teams. In either case, the Activities capture the core security function and organizations are free to determine how they fulfill the Activities.

Results

The Results characterize capabilities and deliverables obtained by achieving the given Level. In some cases these are specified concretely and in others, a more qualitative statement is made about increased capability.

Success metrics

The Success Metrics specify example measurements that can be used to check if an organization is performing at the given Level. Data collection and management is left to the choice of each organization, but recommended data sources and thresholds are provided..

Costs

The Costs are qualitative statements about the expenses incurred by an organization attaining the given Level. While specific values will vary for each organizations, these are meant to provide an idea of the one-time and ongoing costs associated with operating at a particular Level.

/ PERSONNEL

These properties of a Level indicate the estimated ongoing overhead in terms of human resources for operating at the given Level.

- Developers Individuals performing detailed design and implementation of the software
- Architects Individuals performing high-level design work and large scale system engineering
- Managers Individuals performing day-today management of development staff
- QA Testers Individuals performing quality assurance testing and prerelease verification of software
- Security Auditors Individuals with technical security knowledge related to software being produced
- Business Owners Individuals performing key decision making on software and its business requirements
- Support Operations Individuals performing customer support or direct technical operations support

RELATED LEVELS

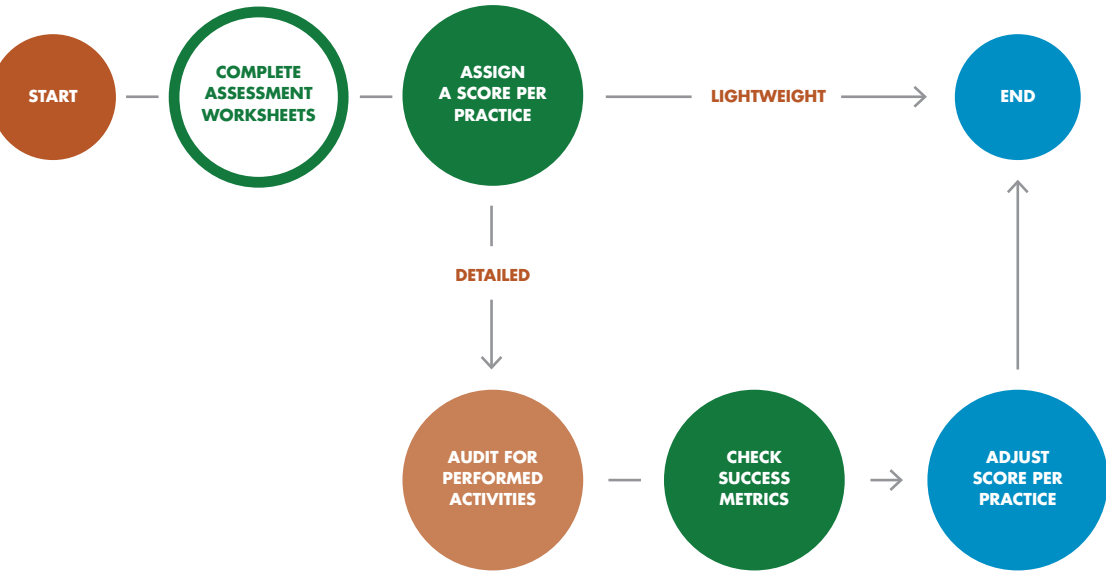
The Related Levels are references to Levels within other Practices that have some potential overlaps depending upon the organization’s structure and progress in building an assurance program. Functionally, these indicate synergies or optimizations in Activity implementation if the Related Level is also a goal or already in place.

CONDUCTING ASSESSMENTS

By measuring an organization against the defined Security Practices, an overall picture of built-in security assurance activities is created. This type of assessment is useful for understanding the breadth of security activities currently in place at an organization. Further, it enables that organization to then utilize SAMM to create a future roadmap for iterative improvement.

The process of conducting an assessment is simply evaluating an organization to determine the Maturity Level at which it is performing, The extent to which an organization’s performance is checked will usually vary according to the drivers behind the assessment, but in general, there are two recommended styles:

- **Lightweight** The assessment worksheets for each Practice are evaluated and scores are assigned based on answers. This type of assessment is usually sufficient for an organization that is trying to map their existing assurance program into SAMM and just wants to get a quick picture of where they stand.
- **Detailed** After completion of the assessment worksheets, additional audit work is performed to check the organization to ensure the Activities prescribed by each Practice are in place. Additionally since each Practice also specifies Success Metrics, that data should be collected to ensure that the organization is performing as expected.



Scoring an organization using the assessment worksheets is straightforward. After answering the questions, evaluate the answer column to determine the Level. It is indicated by affirmative answers on all questions above the markers to the right of the answer column.

Existing assurance programs might not always consist of activities that neatly fall on a boundary between Maturity Levels, e.g. an organization that assesses to a Level 1 for a given Practice might also have additional activities in place but not such that Level 2 is completed. For such cases, the organization’s score should be annotated with a “+” symbol to indicate there’s additional assurances in place beyond those indicated by the Level obtained. For example, an organization that is performing all Level 1 Activities for Operational Enablement as well as one Level 2 or 3 Activity would be assigned a “1+” score. Likewise, an organization performing all Activities for a Security Practice, including some beyond the scope of SAMM, would be given a “3+” score.



GOVERNANCE

Assessment worksheet



	YES	NO	
<ul style="list-style-type: none">• Is there a software security assurance program already in place?• Do most of the business stakeholders understand your organization's risk profile?• Is most of your development staff aware of future plans for the assurance program?			SM 1
<ul style="list-style-type: none">• Are most of your applications and resources categorized by risk?• Are risk ratings used to tailor the required assurance activities?• Does most of the organization know about what's required based on risk ratings?			SM 2
<ul style="list-style-type: none">• Is per-project data for cost of assurance activities collected?• Does your organization regularly compare your security spend with other organizations?			SM 3



	YES	NO	
<ul style="list-style-type: none">Do most project stakeholders know their project's compliance status?Are compliance requirements specifically considered by project teams?			PC 1
<ul style="list-style-type: none">Does the organization utilize a set of policies and standards to control software development?Are project teams able to request an audit for compliance with policies and standards?			PC 2
<ul style="list-style-type: none">Are projects periodically audited to ensure a baseline of compliance with policies and standards?Does the organization systematically use audits to collect and control compliance evidence?			PC 3



	YES	NO	
<ul style="list-style-type: none">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
<ul style="list-style-type: none">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
<ul style="list-style-type: none">Is security-related guidance centrally controlled and consistently distributed throughout the organization?Are most people tested to ensure a baseline skillset for secure development practices?			EG 3



CONSTRUCTION
Assessment worksheet



	YES	NO	
<ul style="list-style-type: none">Do most projects in your organization consider and document likely threats?Does your organization understand and document the types of attackers it faces?Do project teams regularly analyze functional requirements for likely abuses?Are stakeholders aware of relevant threats and ratings?			TA 1
<ul style="list-style-type: none">Do project teams use a method of rating threats for relative comparison?Do project teams specifically consider risk from external software?			TA 2
<ul style="list-style-type: none">Are all protection mechanisms and controls captured and mapped back to threats?			TA 3



	YES	NO	
<ul style="list-style-type: none">Do most project teams specify some security requirements during development?Do project teams pull requirements from best practices and compliance guidance?Are most stakeholders reviewing access control matrices for relevant projects?			SR 1
<ul style="list-style-type: none">Are project teams specifying requirements based on feedback from other security activities?			SR 2
<ul style="list-style-type: none">Are most stakeholders reviewing vendor agreements for security requirements?Are the security requirements specified by project teams being audited?			SR 3



	YES	NO	
• Are project teams provided with a list of recommended third-party components? • Are most project teams aware of secure design principles and applying them? • Do you advertise shared security services with guidance for project teams?			SA 1
• Are project teams provided with prescriptive design patterns based on their application architecture?			SA 2
• Are project teams building software from centrally controlled platforms and frameworks? • Are project teams being audited for usage of secure architecture components?			SA 3



VERIFICATION
Assessment worksheet



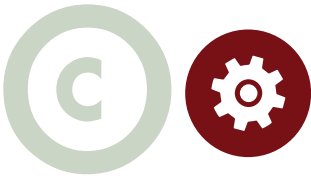
	YES	NO	
• Do project teams document the attack perimeter of software designs? • Do project teams check software designs against known security risks? • Do most project teams specifically analyze design elements for security mechanisms? • Does the design review process incorporate detailed data-level analysis?			DR 1
• Are most project stakeholders aware of how to obtain a formal design review?			DR 2
• Does routine project audit require a baseline for design review results?			DR 3



	YES	NO	
• Do most project teams have review checklists based on common problems? • Are project teams generally performing review of selected high-risk code? • Can most project teams access automated code analysis tools to find security problems? • Do project teams utilize automation to check code against application-specific coding standards?			IR 1
• Do most stakeholders consistently require and review results from implementation reviews?			IR 2
• Does routine project audit require a baseline for implementation review results prior to release?			IR 3

SECURITY TESTING

	YES	NO	
• Are projects specifying some security tests based on requirements? • Do most projects perform penetration tests prior to release? • Are most stakeholders aware of the security test status prior to release?			ST 1
• Are projects using automation to evaluate security test cases? • Do most projects follow a consistent process to evaluate and report on security tests to stakeholders?			ST 2
• Are security test cases comprehensively generated for application-specific logic? • Do routine project audits demand minimum standard results from security testing?			ST 3



OPERATIONS
Assessment worksheet

ISSUE MANAGEMENT

	YES	NO	
• Do most projects have a point of contact for security issues? • Does your organization have an assigned security response team? • Are most project teams aware of their security point(s) of contact and response team(s)?			IM 1
• Does the organization utilize a consistent process for incident reporting and handling? • Are most project stakeholders aware of relevant security disclosures related to their software projects?			IM 2
• Are most incidents inspected for root causes to generate further recommendations? • Do most projects consistently collect and report data and metrics related to incidents?			IM 3

ENVIRONMENT HARDENING

	YES	NO	
• Do the majority of projects document some requirements for the operational environment? • Do most projects check for security updates to third-party software components? • Is a consistent process used to apply upgrades and patches to critical dependencies?			EH 1
• Do most project leverage automation to check application and environment health?			EH 2
• Are stakeholders aware of options for additional tools to protect software while running in operations? • Does routine audit check most projects for baseline environment health?			EH 3



	YES	NO	
• Do you deliver security notes with the majority of software releases? • Are security-related alerts and error conditions documented for most projects? • Are most project utilizing a change management process that's well understood?			OE 1
• Do project teams deliver an operational security guide with each product release?			OE 2
• Are most projects being audited to check each release for appropriate operational security information? • Is code signing routinely performed on software components using a consistent process?			OE 3

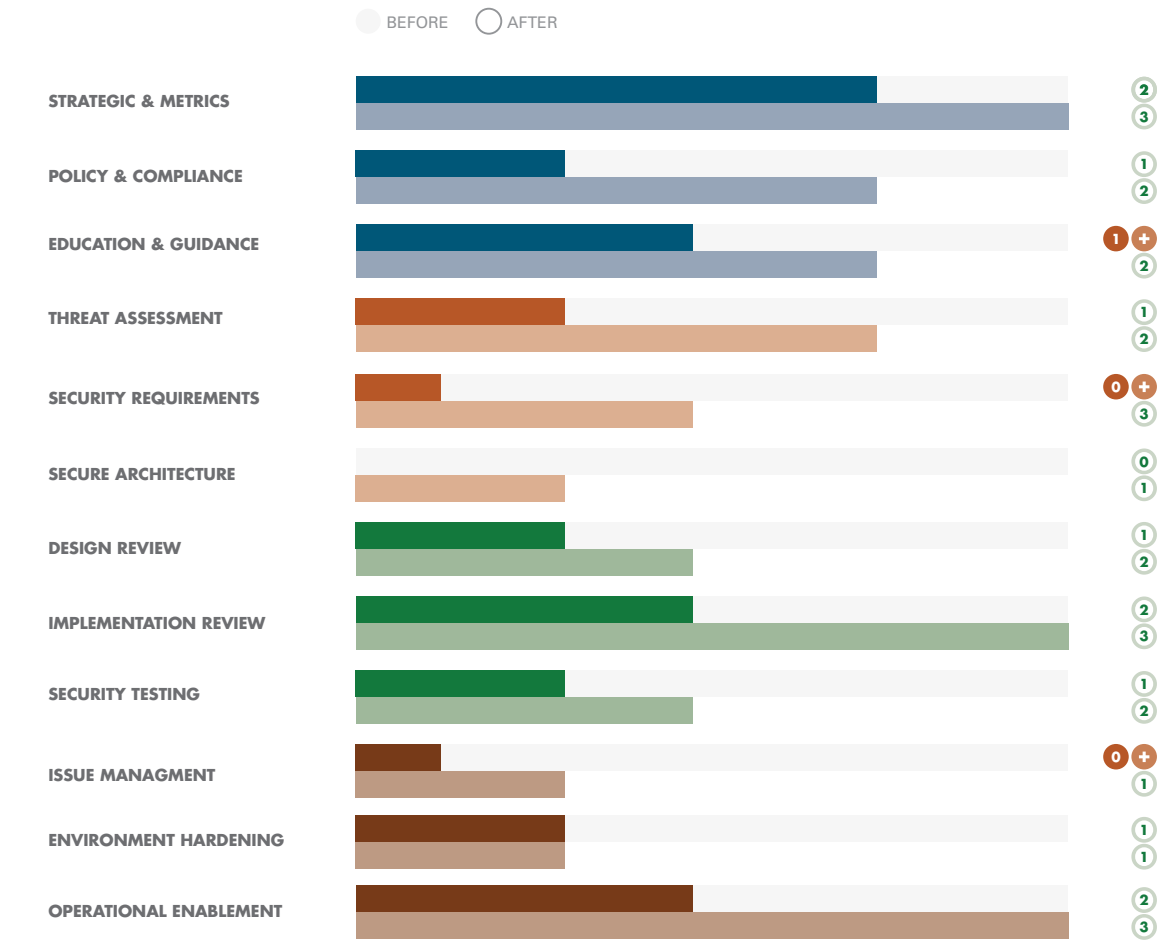
CREATING SCORECARD

Based on the scores assigned to each Security Practice, an organization can create a scorecard to capture those values. Functionally, a scorecard can be the simple set of 12 scores for a particular time. However, selecting a time interval over which to generate a scorecard facilitates understanding of overall changes in the assurance program during the time frame.

Using interval scorecards is encouraged for several situations:

- 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

The figure on the right shows an example scorecard for how an organization’s assurance program changed over the course of one year. If that organization had also saved the data about where they were planning on being at the end of the year, that would be another interesting data set to plot since it would help show the extent to which the plans had to change over the year.



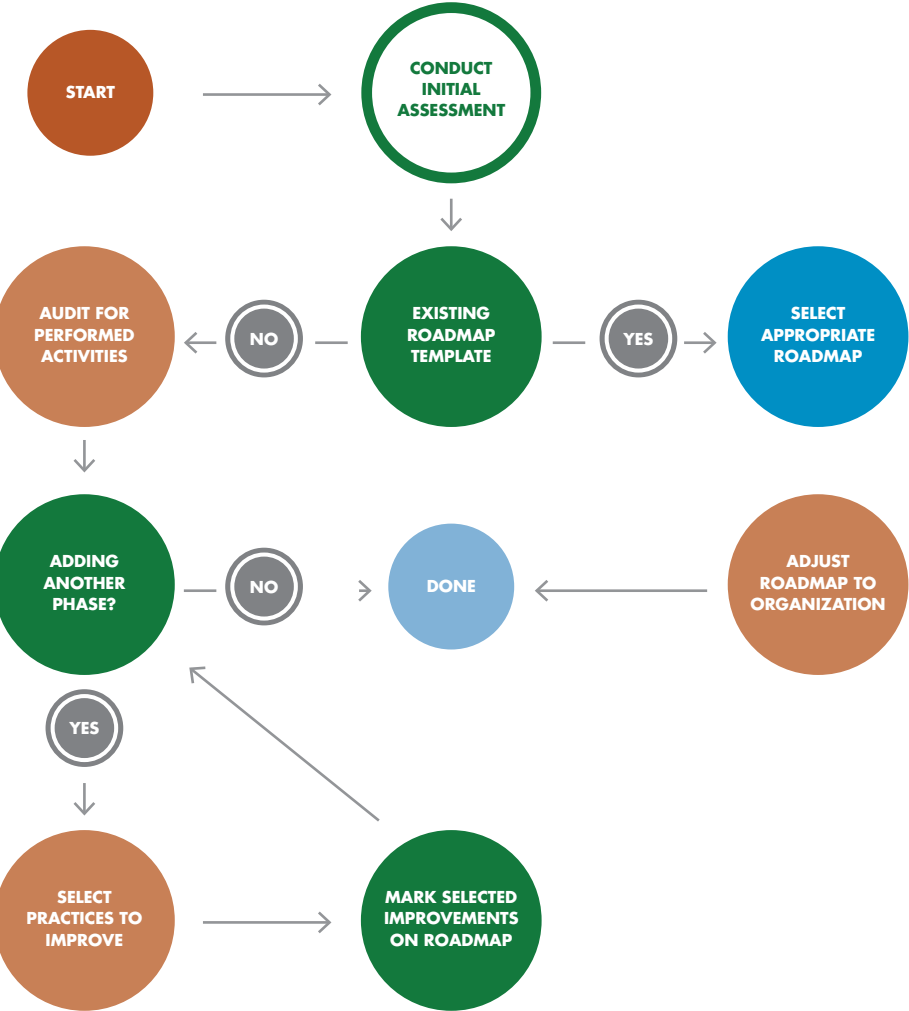
BUILDING ASSURANCE PROGRAMS

One of the main uses of SAMM is to help organizations build software security assurance programs. That process is straightforward, and generally begins with an assessment if the organization is already performing some security assurance activities.

Several roadmap templates for common types of organizations are provided. Thus, many organizations can choose an appropriate match and then tailor the roadmap template to their needs. For other types of organizations, it may be necessary to build a custom roadmap.

Roadmaps (pictured to the right) consist of phases (the vertical bars) in which several Practices are each improved by one Level. Therefore, building a roadmap entails selection of which Practices to improve in each planned phase. Organizations are free to plan into the future as far as they wish, but are encouraged to iterate based on business drivers and organization-specific information to ensure the assurance goals are commensurate with their business goals and risk tolerance.

After a roadmap is established, the build-out of an assurance program is simple. An organization begins an improvement phases and works to achieve the stated Levels by performing the prescribed Activities. At the end of the phase, the roadmap should be adjusted based on what was actually accomplished, and then the next phase can begin.



INDEPENDENT SOFTWARE VENDOR

ROADMAP TEMPLATE

Rationale

An Independent Software Vendor involves the core business function of building and selling software components and applications.

Initial drivers to limit common vulnerabilities affecting customers and users leads to early concentration on Implementation Review and Security Testing activities.

Shifting toward more proactive prevention of security errors in product specification, an organization adds activities for Security Requirements over time.

Also, to minimize the impact from any discovered security issues, the organization ramps up Issue management activities over time.

As the organization matures, knowledge transfer activities from Operational Enablement are added to better inform customers and users about secure operation of the software.

Additional Considerations

Outsourced Development

For organizations using external development resources, restrictions on code access typically leads to prioritization of Security Requirements activities instead of Implementation Review activities. Additionally, advancing Threat Assessment in earlier phases would allow the organization to better clarify security needs to the outsourced developers. Since expertise on software configuration will generally be strongest within the outsourced group, contracts should be constructed to account for the activities related to Operational Enablement.

Internet-Connected Applications

Organizations building applications that use online resources have additional risks from the core Internet-facing infrastructure that hosts the Internet-facing systems. To account for this risk, organizations should add activities from Environment Hardening to their roadmaps.

Drivers and Embedded Development

For organizations building low-level drivers or software for embedded systems, security vulnerabilities in software design can be more damaging and costly to repair. Therefore, roadmaps should be modified to emphasize Secure Architecture and Design Review activities in earlier phases.

Organizations Grown by Acquisition

In an organization grown by acquisition, there can often be several project teams following different development models with varying degrees of security-related activities incorporated. An organization such as this may require a separate roadmap for each division or project team to account for varying starting points as well as project-specific concerns if a variety of software types are being developed.



ONLINE SERVICE PROVIDER

ROADMAP TEMPLATE

Rationale

An Online Services Provider involves the core business function of building web applications and other network-accessible interfaces.

Initial drivers to validate the overall soundness of design without stifling innovation lead to early concentration on Design Review and Security Testing activities.

Since critical systems will be network-facing, Environment Hardening activities are also added early and ramped over time to account for risks from the hosted environment.

Though it can vary based on the core business of the organizations, Policy & Compliance activities should be started early and then advanced according to the criticality of external compliance drivers.

As the organization matures, activities from Threat Assessment, Security Requirements, and Secure Architecture are slowly added to help bolster proactive security after some baseline expectations for security have been established.

Additional Considerations
Outsourced Development

For organizations using external development resources, restrictions on code access typically leads to prioritization of Security Requirements activities instead of Implementation Review activities. Additionally, advancing Threat Assessment in earlier phases would allow the organization to better clarify security needs to the outsourced developers. Since expertise on software configuration will generally be strongest within the outsourced group, contracts should be constructed to account for the activities related to Operational Enablement.

Online Payment Processing

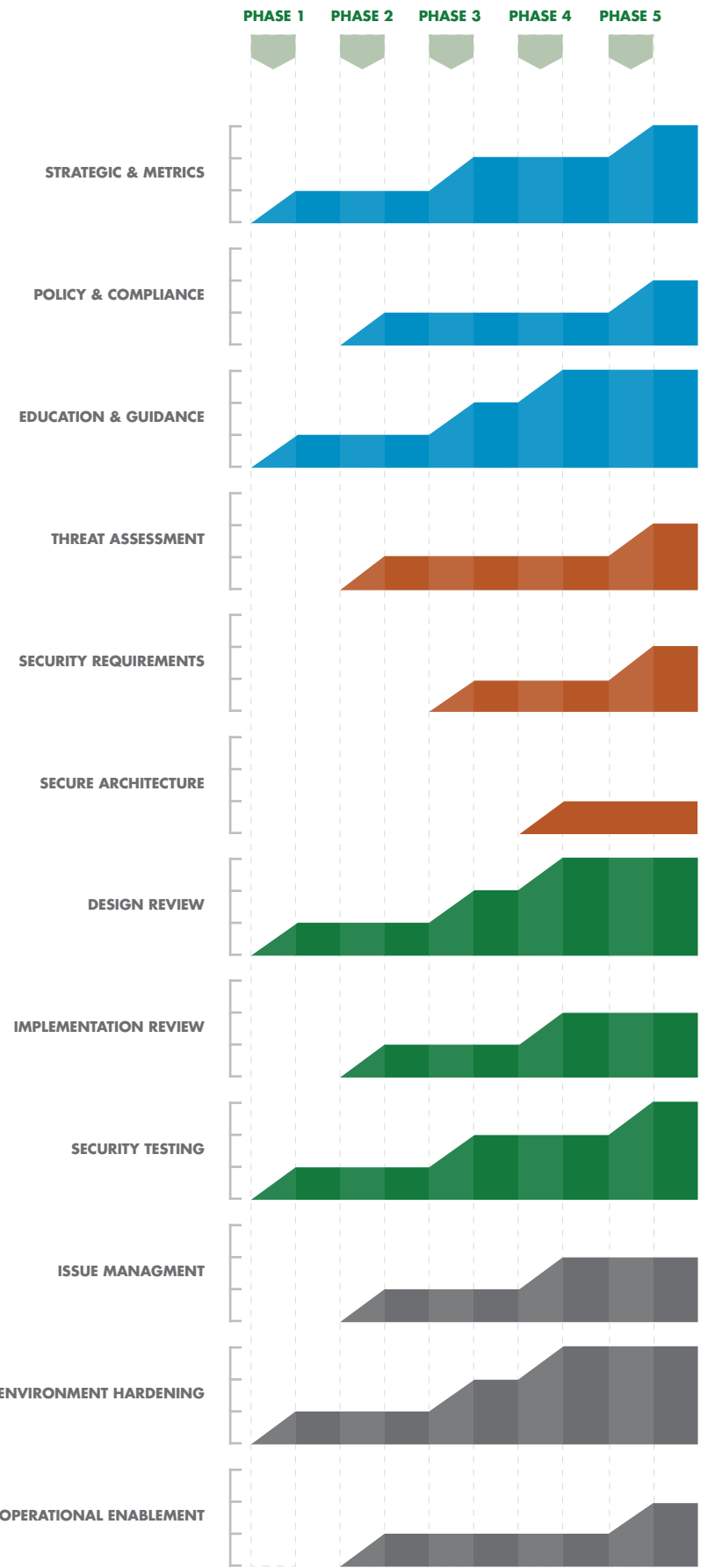
Organizations required to be in compliance with the Payment Card Industry Data Security Standard (PCI-DSS) or other online payment standards should place activities from Policy & Compliance in earlier phases of the roadmap. This allows the organization to opportunistically establish activities that ensure compliance and enable the future roadmap to be tailored accordingly.

Web Services Platforms

For organizations building web services platforms, design errors can carry additional risks and be more costly to mitigate. Therefore, activities from Threat Assessment, Security Requirements, and Secure Architecture should be placed in earlier phases of the roadmap.

Organizations Grown by Acquisition

In an organization grown by acquisition, there can often be several project teams following different development models with varying degrees of security-related activities incorporated. An organization such as this may require a separate roadmap for each division or project team to account for varying starting points as well as project-specific concerns if a variety of software types are being developed.



FINANCIAL SERVICES ORGANIZATION

ROADMAP TEMPLATE

Rationale

A Financial Services Organization involves the core business function of building systems to support financial transactions and processing. In general, this implies a greater concentration of internal and back-end systems that interface with disparate external data providers.

Initially, effort is focused on improving the Practices related to Governance since these are critical services that set the baseline for the assurance program and help meet compliance requirements for the organization.

Since building secure and reliable software proactively is an overall goal, Practices within Construction are started early on and ramped up sharply as the program matures.

Verification activities are also ramped up smoothly over the course of the roadmap to handle legacy systems without creating unrealistic expectations. Additionally, this helps ensure enough cycles are spent building out more proactive Practices.

Since a financial services organization often operates the software they build, focus is given to the Practices within Operations during the middle of the roadmap after some initial Governance is in place but before heavy focus is given to the proactive Construction Practices.

Additional Considerations

Outsourced Development

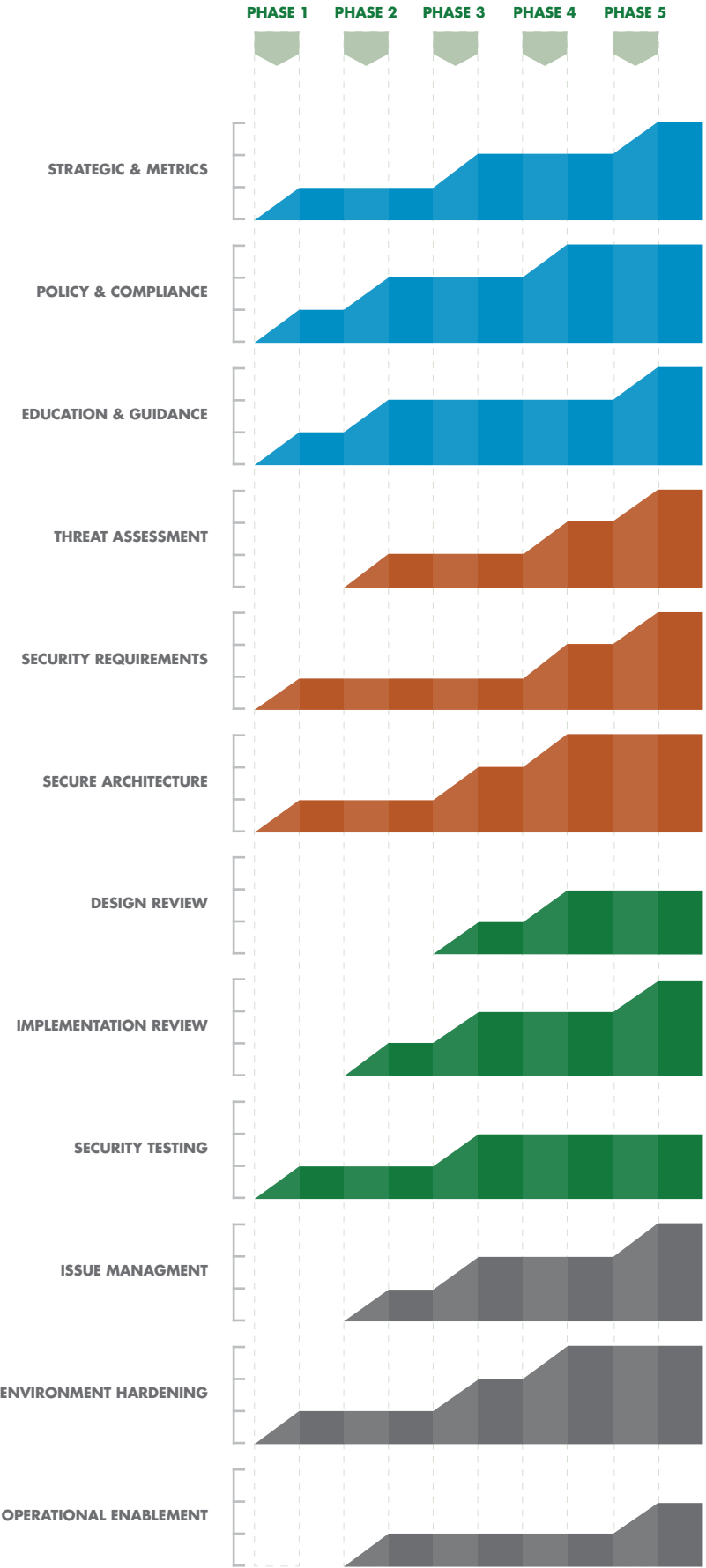
For organizations using external development resources, restrictions on code access typically leads to prioritization of Security Requirements activities instead of Implementation Review activities. Additionally, advancing Threat Assessment in earlier phases would allow the organization to better clarify security needs to the outsourced developers. Since expertise on software configuration will generally be strongest within the outsourced group, contracts should be constructed to account for the activities related to Operational Enablement.

Web Services Platforms

For organizations building web services platforms, design errors can carry additional risks and be more costly to mitigate. Therefore, activities from Threat Assessment, Security Requirements, and Secure Architecture should be placed in earlier phases of the roadmap.

Organizations Grown by Acquisition

In an organization grown by acquisition, there can often be several project teams following different development models with varying degrees of security-related activities incorporated. An organization such as this may require a separate roadmap for each division or project team to account for varying starting points as well as project-specific concerns if a variety of software types are being developed.



GOVERNMENT ORGANIZATION

ROADMAP TEMPLATE

Rationale

A Government Organization involves the core business function of being a state-affiliated organization that builds software to support public sector projects.

Initially, Governance Practices are established, generally to get an idea of the overall compliance burden for the organization in context of the concrete roadmap for improvement.

Because of risks of public exposure and the quantity of legacy code generally in place, early emphasis is given to Security Testing within the Verification Practices and later the more involved Implementation Review or Design Review Practices are developed.

Similar emphasis is placed on the Construction and Operations Practices. This helps establish the organization’s management of vulnerabilities and moves toward bolstering the security posture of the operating environment. At the same time, proactive security activities under Construction are built up to help prevent new issues in software under development.

Additional Considerations
Outsourced Development

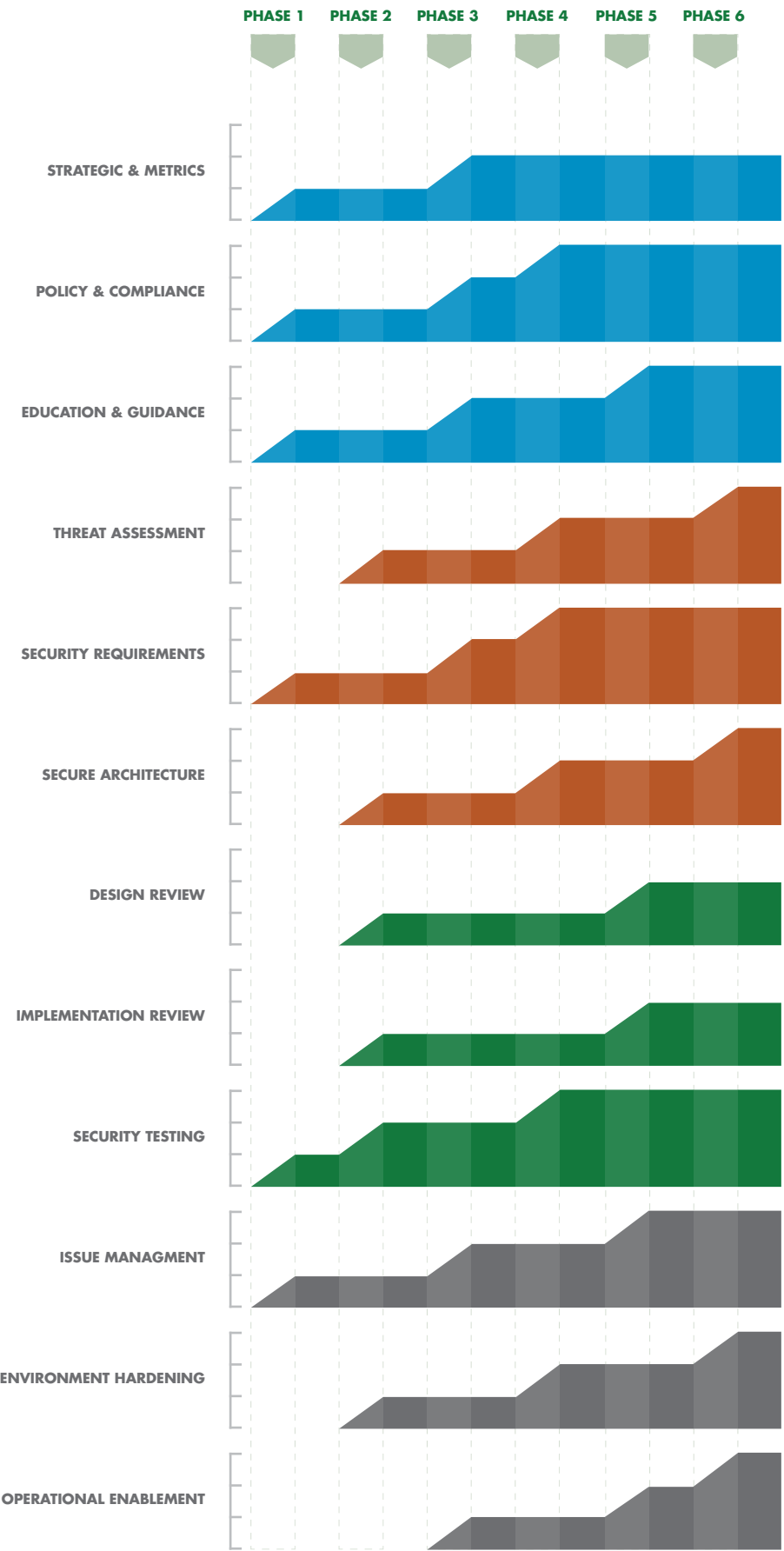
For organizations using external development resources, restrictions on code access typically leads to prioritization of Security Requirements activities instead of Implementation Review activities. Additionally, advancing Threat Assessment in earlier phases would allow the organization to better clarify security needs to the outsourced developers. Since expertise on software configuration will generally be strongest within the outsourced group, contracts should be constructed to account for the activities related to Operational Enablement.

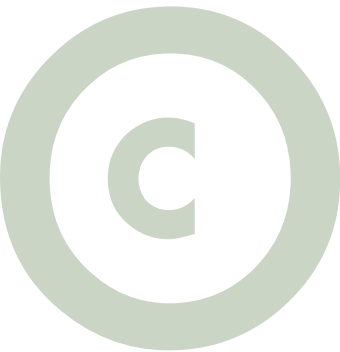
Web Services Platforms

For organizations building web services platforms, design errors can carry additional risks and be more costly to mitigate. Therefore, activities from Threat Assessment, Security Requirements, and Secure Architecture should be placed in earlier phases of the roadmap.

Regulatory Compliance

For organizations under heavy regulations that affect business processes, the build-out of the Policy & Compliance Practice should be adjusted to accommodate external drivers. Likewise, organizations under a lighter compliance load should take the opportunity to push back build-out of that Practice in favor of others.





/ CASE STUDIES

A walkthrough of example scenarios

This section features a selection of scenarios in which the application of SAMM is explained in the context of a specific business case. Using the roadmap templates as a guide, the case studies tell the story of how an organization might adapt best practices and take into account organization-specific risks when building a security assurance program.

/ VIRTUALWARE

CASE STUDY: MEDIUM-SIZED INDEPENDENT SOFTWARE VENDOR

Business Profile

VirtualWare is a leader within their market for providing integrated virtualized application platforms to help organizations consolidate their application interfaces into a single environment. Their technology is provided as a server application and desktop client built for multiple environments including Microsoft, Apple and Linux platforms.

The organization is of medium size (200-1000 employees) and has a global presence around the world with branch offices in most major countries.

Organization

VirtualWare develops their virtualization technology on a mixture of Java, C++ and Microsoft .NET technology. Their core application virtualization technology has been written in C++ and has had a number of reviews for bugs and security, but currently no formal processes exists for identifying and fixing known or unknown security bugs.

VirtualWare has chosen to support their web technology on Java, although the back-end systems are built using Microsoft and C++ technologies. The development team focused on the new web interfaces is primarily composed of Java developers.

VirtualWare employs over 300 developers, with staff broken up into teams based on the projects that they work on. There are 12 teams with around 20–40 developers per team. Within each team there is minimal experience with software security, and although senior developers perform basic assessments of their code, security is not considered a critical goal within the organization.

Each team within VirtualWare adopts a different development model. Currently the two primary methodologies used are Agile SCRUM and iterative Waterfall style approaches. There is minimal to no guidance from the IT department or project architects on software security.

Environment

VirtualWare develops their virtualization technology on a mixture of Java, C++ and Microsoft .NET technology. Their core application virtualization technology has been written in C++ and has had a number of reviews for bugs and security, but currently no formal processes exists for identifying and fixing known or unknown security bugs.

VirtualWare has chosen to support their web technology on Java, although the back-end systems are built using Microsoft and C++ technologies. The development team focused on the new web interfaces is primarily composed of Java developers.

VirtualWare employs over 300 developers, with staff broken up into teams based on the projects that they work on. There are 12 teams with around 20-40 developers per team. Within each team there is minimal experience with software security, and although senior developers perform basic assessments of their code, security is not considered a critical goal within the organization.

Each team within VirtualWare adopts a different development model. Currently the two primary methodologies used are Agile SCRUM and iterative Waterfall style approaches. There is minimal to no guidance from the IT department or project architects on software security.

Key Challenges

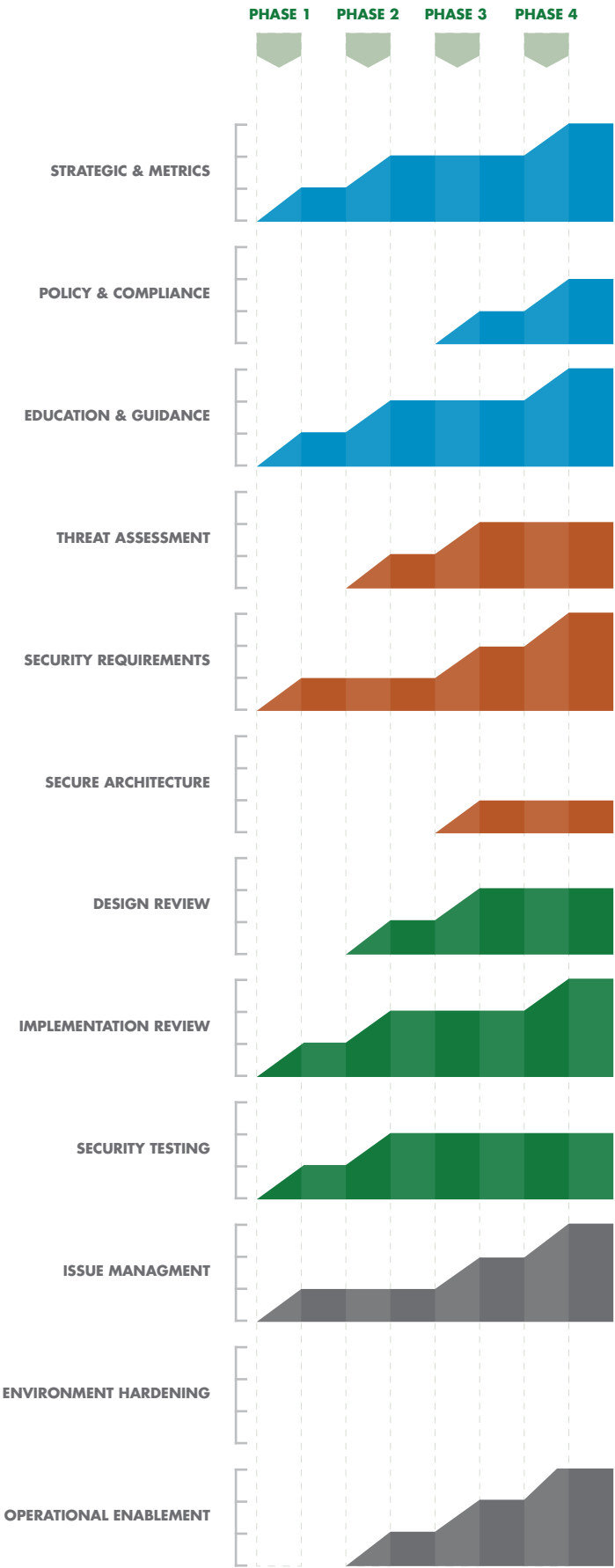
- Rapid release of application features to ensure they maintain their competitive edge over rivals
- Limited experience with software security concepts — currently minimal effort is associated with security related tasks
- Developers leave the organization and are replaced with less experienced developers
- Multiple technologies used within applications, with legacy applications that have not been updated since originally built
- No understanding of existing security posture or risks facing the organization

VirtualWare wanted to focus on ensuring that their new web applications would be delivered securely to their customers. Therefore the initial focus on implementing the security assurance program was on education and awareness for their development teams, as well as providing some base technical guidance on secure coding and testing standards.

The organization previously had received bug requests and security vulnerabilities through their support@virtualware.net address. However as this was a general support address, existing requests were not always filtered down to the appropriate teams within the organization and handled correctly. The need to implement a formal security vulnerability response program was also identified by VirtualWare.

Implementation Strategy

The adoption of a security assurance program within an organization is a long term strategy, and significantly impacts on the culture of developers and the process taken by the business to develop and deliver business applications. The adoption of this strategy is set over a 12 month period, and due to the size of the organization will be relatively easy to implement in that period.



/ PHASE 1 (MONTHS 0 - 3) - AWARENESS & PLANNING

VirtualWare previously identified that they had limited knowledge and awareness of application security threats to their organization and limited secure coding experience. The first phase of the deployment within VirtualWare focused on training developers and implementing guidance and programs to identify current security vulnerabilities.

Development teams within VirtualWare had limited experience in secure coding techniques therefore, an initial training program was developed that can be provided to the developers within the organization on defensive programming techniques.













With over 300 developers and multiple languages supported within the organization one of the key challenges for VirtualWare was to provide an education program that was technical enough to teach developers some of the basics in secure coding concepts. The objective of this initial education course was primarily on coding techniques and testing tools. The course developed and delivered within the organization lasted for 1 day and covered the basics of secure coding.

VirtualWare was aware that they had a number of applications with vulnerabilities and no real strategy in which to identify existing vulnerabilities and address the risks in a reasonable time-frame. A basic risk assessment methodology was adopted and the organization undertook a review of the existing application platforms.

This phase also included implementing a number of concepts for the development team to enhance their security tools. The development teams already had a number of tools available to perform quality type assessments. Additional investigation into code review and security testing tools was performed.

Target Objectives

During this phase of the project, VirtualWare implemented the following SAMM Practices & Activities.

		A. Estimate overall business risk profile B. Build and maintain assurance program roadmap
		A. Conduct technical security awareness training B. Build and maintain technical guidelines
		A. Derive security requirements from business functionality B. Evaluate security and compliance guidance for requirements
		A. Create review checklists from known security requirements B. Perform point-review of high-risk code
		A. Derive test cases from known security requirements B. Conduct penetration testing on software releases
		A. Identify point of contact for security issues B. Create informal security response team(s)

To achieve these maturity levels VirtualWare implemented a number of programs during this phase of the roll-out. The following initiatives were adopted;

- 1 Day Secure Coding Course (High-level) for all developers;
- Build a technical guidance whitepaper for application security on technologies used within the organization;
- Create a risk process and perform high-level business risk assessments for the application platforms and review business risk;
- Prepare initial technical guidelines and standards for developers; ☒Perform short implementation reviews on application platforms that present significant risk to the organization; ☒Develop test and use cases for projects and evaluate the cases against the applications;
- Appointed a role to application security initiatives; ☒Generated a Draft strategic roadmap for the next phase of the assurance program.

Due to the limited amount of expertise in-house within VirtualWare, the company engaged with a third party security consulting group to assist with the creation of the training program, and assist in writing the threat modeling and strategic roadmap for the organization.

One of the key challenges faced during this phase, was to get all 300 developers through a one day training course. To achieve this VirtualWare ran 20 course days, with only a small number of developers from each team attending the course at one time. This reduced the overall impact on staff resources during the training period.

During this phase of the project, VirtualWare invested significant resources effort into the adoption of a risk review process and reviewing the business risk to the organization. Although considerable effort was focused on these tasks, they were critical to ensuring that the next steps implemented by VirtualWare were in line with the business risks faced by the organization.

VirtualWare management received positive feedback from most developers within the organization on the training program. Although not detailed, developers felt that the initial training provided some basic skills that could assist them immediately day to day in writing secure code.

Implementation Costs

A significant amount of internal resources and costs were invested in this phase of the project. There were three different types of costs associated with this phase.

Internal Resource Requirements

Internal resource effort used in the creation of content, workshops and review of application security initiatives within this phase. Effort is shown in total days per role.



Training Resource Requirements (Training per person for period)

Each developer within VirtualWare was required to attend a training course, and therefore every developer had a single day allocated to the application security program.



Outsourced Resources

Due to the lack of knowledge within VirtualWare, external resources were used to assist with the creation of content, and create/ deliver the training program to the developers.



PHASE 2 (MONTHS 3 - 6) - EDUCATION & TESTING

VirtualWare identified in phase 1 that a number of their applications contained vulnerabilities that may be exploited by external threats. Therefore one of the key objectives of this phase was to implement basic testing and review capabilities to identify the vulnerabilities and address them in the code.

The introduction of automated tools to assist with code coverage and findings weaknesses was identified as one of the biggest challenges in this phase of the implementation. Traditionally in the past developers have used automated tools with great difficulty and therefore implementing new tools was seen as a significant challenge.

To ensure a successful rollout of the automation tools within the organization, VirtualWare proceeded with a staged roll-out. The tools would be given to senior team leaders first, with other developers coming online over a period of time. Teams were encouraged to adopt the tools, however, no formal process was put in place for their use.

This phase of the implementation also saw the introduction of a more formal education and awareness program. Developers from the previous training requested more specific training in the areas of web services, and data validation. The new 6 hour specific training course was developed with these two focus areas. VirtualWare also implemented additional training programs for Architects and Managers, and adopted an awareness campaign within the organization.

Target Objectives

During this phase of the project, VirtualWare implemented the following SAMM Practices & Activities.

	<div>SM2</div>	A. Classify data and applications based on business risk B. Establish and measure per-classification security goals
	<div>EG2</div>	A. Conduct role-specific application security training B. Utilize security coaches to enhance project teams
	<div>TA1</div>	A. Build and maintain application-specific threat models B. Develop attacker profile from software architecture
	<div>DR1</div>	A. Identify software attack surface B. Analyze design against known security requirements
	<div>IR2</div>	A. Utilize automated code analysis tools B. Integrate code analysis into development process
	<div>ST2</div>	A. Utilize automated security testing tools B. Integrate security testing into development process
	<div>OE1</div>	A. Capture critical security informaion for operations B. Document procedures for typical application alerts

To achieve these maturity levels VirtualWare implemented a number of programs during this phase of the roll-out. The following initiatives were adopted;

- Additional Education & Training courses for QA Testers, Managers & Architects;
- Conduct data asset classification and set security goals;
- Develop the risk assessment methodology into a threat modeling approach with attack tress nd profiles;
- Review and identify security requirements per application platform;
- Introduction of automated tools to assist with code coverage and security analysis of existing ap- plications and new code bases;
- Review and enhance existing penetration testing programs;
- Enhance the existing software development life-cycle to support security testing as a part of the development process.

VirtualWare adapted the existing application security training program, to provider a smaller less technical version as a Business Application Security awareness program. This was a shorter 4 hour course, and was extended to Managers, Business Owners of the organization.

A high-level review of the existing implementation review and penetration testing programs iden- tified that the process was inadequate and needed to be enhanced to provide better testing and results on application security vulnerabilities. The team set out to implement a new program of performing penetration testing and implementation review. As a part of this program, each senior developer in a program team was allocated approximately 4 days to perform a high-level source implementation review of their application.

VirtualWare management understood that the infrastructure and applications are tightly integrat- ed, and during this phase the operational side of the application platforms (infrastructure) was reviewed. This phase looked at the infrastructure requirements and application integration features between the recommended deployed hardware and the application interfaces.

During this phase the strategic roadmap and methodology for application security was reviewed by the project team. The objective of this review and update was to formally classify data assets and set the appropriate level of business risk associated with the data assets and applications. From this the project team was able to set security goals for these applications.

Implementation Costs

A significant amount of internal resources and costs were invested in this phase of the project. There were three different types of costs associated with this phase.

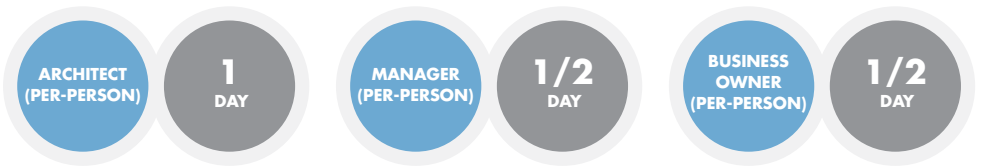
Internal Resource Requirements

Internal resource effort used in the creation of content, workshops and review of application securi- ty initiatives within this phase. Effort is shown in total days per role.



Training Resource Requirements (Training per person for period)

Additional personnel within VirtualWare was required to attend a training course, and therefore several roles had time allocated to training on application security.



Outsourced Resources

Due to the lack of knowledge within VirtualWare, external resources were used to assist with the creation of content, and create/ deliver the training program to the developers.



/ PHASE 3 (MONTHS 6 - 9) - ARCHITECTURE & INFRASTRUCTURE

The third phase of the assurance program implementation within VirtualWare builds on from the previous implementation phases and focuses on risk modeling, architecture, infrastructure and operational enablement capabilities.

The key challenge in this phase was establishing a tighter integration between the application platforms and operational side of the organization. In the previous phase VirtualWare teams were introduced to issue management and the operational side of application security. During this phase VirtualWare has adopted the next phase of these areas and introduced clear incident response processed and detailed change control procedures.

VirtualWare has chosen to start two new areas for this implementation. Although VirtualWare is not impacted by regulatory compliance, a number of their customers have started to ask about whether the platforms can assist in passing regulatory compliance. A small team has been setup within VirtualWare to identify the relevant compliance drivers and create a checklist of drivers.

In the previous phase VirtualWare introduced a number of new automated tools to assist with the review and identification of vulnerabilities. Although not focused on in this phase, the development teams have adopted the new tools and have reported that they are starting to gain a benefit from using these tools within their groups.

Target Objectives

During this phase of the project, VirtualWare implemented the following SAMM Practices & Activities.

		A. Identify and monitor external compliance drivers B. Build and maintain compliance guidelines
		A. Build and maintain abuse-case models per project B. Adopt a weighting system for measurement of threats
		A. Build an access control matrix for resources and capabilities B. Specify security requirements based on known risks
		A. Maintain list of recommended software frameworks B. Explicitly apply security principles to design
		A. Inspect for complete provision of security mechanisms B. Deploy design review service for project teams
		A. Establish consistent incident response process B. Adopt a security issue disclosure process
		A. Create per-release change management procedures B. Maintain formal operational security guides

To achieve these maturity levels VirtualWare implemented a number of programs during this phase of the roll-out. The following initiatives were adopted;

- Define and publish technical guidance on security requirements and secure architecture for projects within the organization;
- Identify and document compliance and regulatory requirements;
- Identify and create guidelines for security of application infrastructure;
- Create a defined list of approved development frameworks;
- Enhance the existing threat modeling process used within VirtualWare;
- Adopt an incident response plan and prepare a security disclosure process;
- Introduce Change Management procedures and formal guidelines for all projects.

To coincide with the introduction of automated tools for developers (from the previous phase), formal technical guidance on secure coding techniques was introduced into the organization. These were specific technical documents relating to languages and technology and provided guidance on secure coding techniques in each relevant language/application.

With a combined approach from the education and awareness programs, technical guidance and then the introduction of automation tools to help the developers, VirtualWare started to see a visible difference in the code being delivered into production versions of their applications. Developers provided positive feedback on the tools and education made available to them under the program.

For the first time in VirtualWare project teams became responsible for their security and design of their application platforms. During this phase a formal review process and validation against best practices were performed by each team. Some teams identified gaps relating to both security and business design that needed to be reviewed. A formal plan was put in place to ensure these gaps were addressed.

A formal incident response plan and change management procedures were introduced during this phase of the project. This was a difficult process to implement, and VirtualWare teams initially struggled with the process as the impact on culture and the operational side of the business was significant. However over time each team member identified the value in the new process and the changes were accepted by the team over the implementation period.

Implementation Costs

A significant amount of internal resources and costs were invested in this phase of the project. There were two different types of costs associated with this phase.

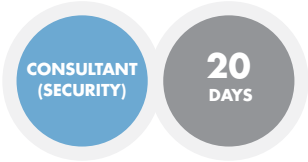
Internal Resource Requirements

Internal resource effort used in the creation of content, workshops and review of application security initiatives within this phase. Effort is shown in total days per role.



Outsourced Resources

Due to the lack of knowledge within VirtualWare, external resources were used to assist with the creation of content, and create/ deliver the processes, guidelines and assist teams.



PHASE 4 (MONTHS 9 - 12) - GOVERNANCE & OPERATIONAL SECURITY

The fourth phase of the assurance program implementation within VirtualWare continues on from the previous phases, by enhancing existing security functions within the organization. By now VirtualWare has implemented a number of critical application security processes and mechanisms to ensure that applications are developed and maintained securely.

A core focus in this phase is bolstering the Alignment & Governance Discipline. These three functions play a critical role in the foundation of an effective long term application security strategy. A completed education program is implemented, whilst at the same time a long term strategic roadmap is put in place for VirtualWare.

The other key focus within this phase is on the operational side of the implementation. VirtualWare management identified previously that the need for incident response plans and dedicated change management processes are critical to the long term strategy.







VirtualWare saw this phase as the stepping stones to their long term future. This phase saw the organization implement a number of final measures to cement the existing building blocks that have been laid down in the previous phases. In the long term this will ensure that the processes, concepts and controls put in place will continue to work within the organization to ensure the most secure outcome for their application platforms.

VirtualWare chose this phase to introduce their customers to their new application security initiatives, provide details of a series of programs to VirtualWare customers about application security, deploying applications securely and reporting of vulnerabilities in VirtualWare applications. The key goal from these programs is to instill confidence in their customer base that VirtualWare applications are built with security in-mind, and VirtualWare can assist customers in ensuring their application environments using their technology are secure.

Target Objectives

During this phase of the project, VirtualWare implemented the following SAMM Practices & Activities.

	<div>SM3</div>	<div>A. Conduct periodic industry-wide cost comparisons</div> <div>B. CCollect metrics for historic security spend</div>
	<div>PC2</div>	<div>A. Build policies and standards for security and compliance</div> <div>B. Establish project audit practice</div>
	<div>EG3</div>	<div>A. Create formal application security support portal</div> <div>B. Establish role-based examination/certification</div>
	<div>SR3</div>	<div>A. Build security requirements into supplier agreements</div> <div>B. Expand audit program for security requirements</div>

		A. Customize code analysis for application-specific concerns B. Establish release gates for implementation review
		A. Conduct root cause analysis for incidents B. Collect per-incident metrics
		A. Expand audit program for operational information B. Perform code signing for application components

To achieve these maturity levels VirtualWare implemented a number of programs during this phase of the roll-out. The following initiatives were adopted;

- Create well defined security requirements and testing program for all projects;
- Create and implement a incident response plan;
- Reviewed existing alerts procedure for applications and document a process for capturing events;
- Create a customer security white-paper on deploying applications security;
- Review existing security spend within projects and determine if appropriate budget has been allocated to each project for security;
- Implement the final education and awareness programs for application roles;
- Complete a long term application security strategy roadmap for the organization.

In previous phases VirtualWare had released a formal incident response plan for customers to submit vulnerabilities found with their code. During this phase, VirtualWare took the results of the submitted vulnerabilities and conducted assessments of why the problem occurred, how and attempted a series of reporting to determine any common theme identified amongst the reported vulnerabilities.

As a part of the ongoing effort to ensure applications are deployed internally securely as well as on customer networks, VirtualWare created a series of white-papers, provided to customers based on industry standards for recommended environment hardening. The purpose of these guidelines is to provide assistance to customers on the best approach to deploying their applications.

During this phase, VirtualWare implemented a short computer based training module so that existing and new developers could maintain their skills in application security. It was also mandated that all “application” associated roles undertake a mandatory 1 day course per year. This was completed to ensure that the skills given to developers were not lost and new developers would be up skilled during their time with the company.

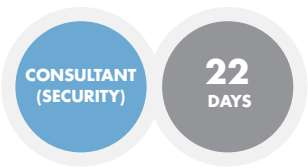
One of the final functions implemented within VirtualWare was to complete a “AS IS” gap assessment and review, and determine how effective the past 12 months had been. During this short program questionnaires were sent to all team members involved as well as a baseline review against SAMM. The weaknesses and strengths identified during this review were documented into the final strategic roadmap for the organization and the next twelve months strategy was set for VirtualWare.

Implementation Costs
A significant amount of internal resources and costs were invested in this phase of the project. There were two different types of costs associated with this phase

Internal Resource Requirements
Internal resource effort used in the creation of content, workshops and review of application security initiatives within this phase. Effort is shown in total days per role.



Outsourced Resources
Due to the lack of knowledge within VirtualWare, external resources were used to assist with the implementation of this phase, including documentation, processes and workshops.



/ ONGOING (MONTHS 12+)

Over the past twelve months VirtualWare has started by implementing a number of training and education programs, to developing internal guidelines and policies. In the final phase of the assurance program implementation, VirtualWare began to publish externally and work with their customers to enhance the security of their customer application platforms.

VirtualWare Management set an original mandate to ensure that software developed within the company was secure, and to ensure that the market was aware of the security initiatives taken and to assist customers in securing their application platforms.

To achieve these management goals the first twelve months set the path for an effective strategy within VirtualWare, and finally by starting to assist customers in securing their application environments. Moving forward VirtualWare has set a number of initiatives within the organization to ensure that the company doesn’t fall into their old habits. Some of these programs include:

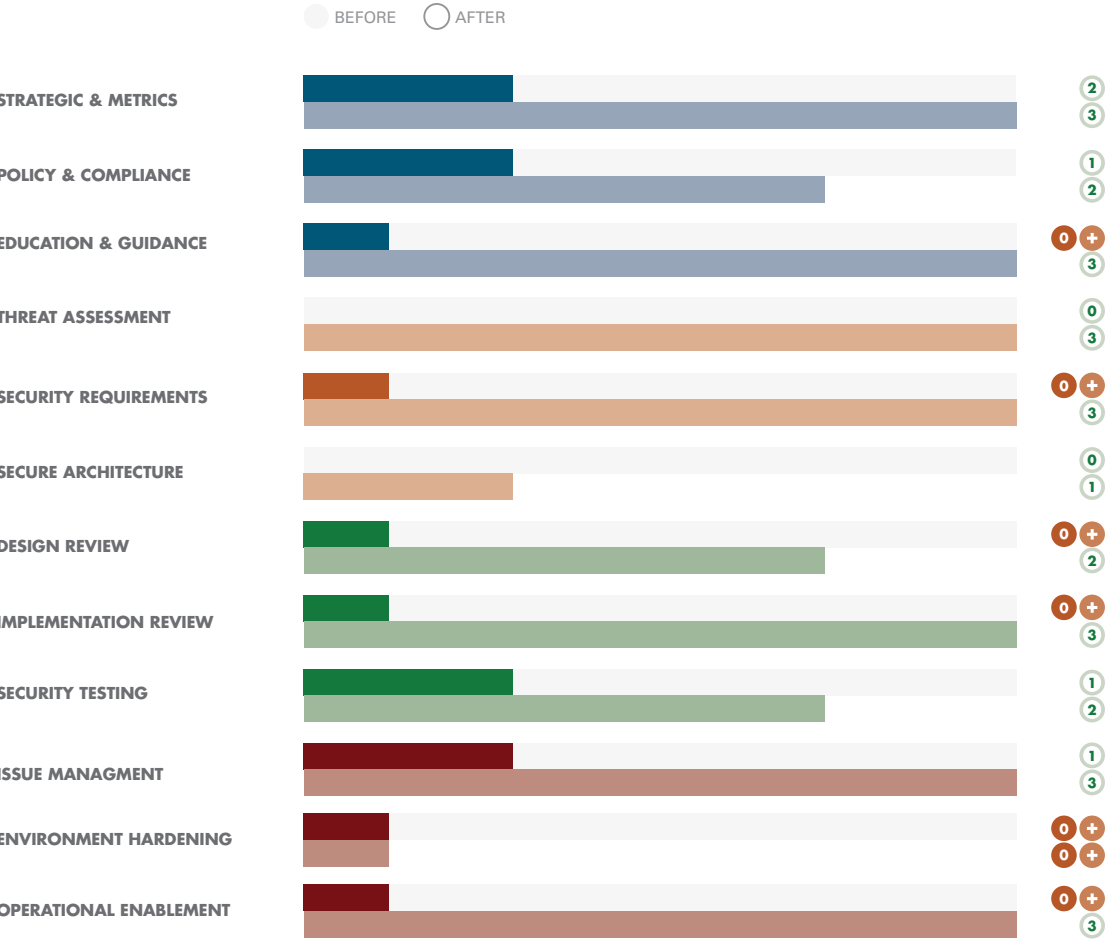
- Business Owners and Team Leaders are aware of the risk associated with their applications and are required to sign-off on applications before release;
- Team Leaders now require all applications to formally go through the security process, and implementation reviews are performed weekly by developers;
- Ongoing yearly training and education programs (including CBT) are provided to all project staff and developers are required to attend a course at least once a year;
- A dedicated Team Leader for Application Security has been created, and is now responsible for customer communications, and customer technical papers and guidelines.

Going forward VirtualWare now has a culture of security being a part of their SDL, thus ensuring that applications developed and provided to customers are secure and robust. An effective process has been put in place where vulnerabilities can be reported on and handled by the organization when required.

During the final implementation phase a project gap assessment was performed to identify any weaknesses that appeared during the implementation. In particular due to the high-turnover of staff, VirtualWare needed to constantly train new developers as they started with the organization. A key objective set to address this problem was an induction program to be introduced specifically for developers so that they receive formal security training when they start with the organization. This will also help to create the mindset that security is important within the organization and its development team.

Maturity Scorecard

The maturity scorecard was completed as a self assessment during the implementation of the software assurance program by VirtualWare. The final scorecard (shown to the right) represents the status of VirtualWare at the time it began and the time it finished its four-phase improvement project.



/ ACKNOWLEDGEMENTS

The Software Assurance Maturity Model (SAMM) was originally developed, designed, and written by Pravir Chandra (chandra@owasp.org), an independent software security consultant. Creation of the first draft was made possible through funding from Fortify Software, Inc. This document is currently maintained and updated through the OpenSAMM Project led by Pravir Chandra. Since the initial release of SAMM, this project has become part of the Open Web Application Security Project (OWASP). Thanks also go to many supporting organizations that are listed on back cover.

/ CONTRIBUTORS & REVIEWERS

This work would not be possible without the support of many individual reviewers and experts that offered contributions and critical feedback. They are (in alphabetical order):

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