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 orga- nizations 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.

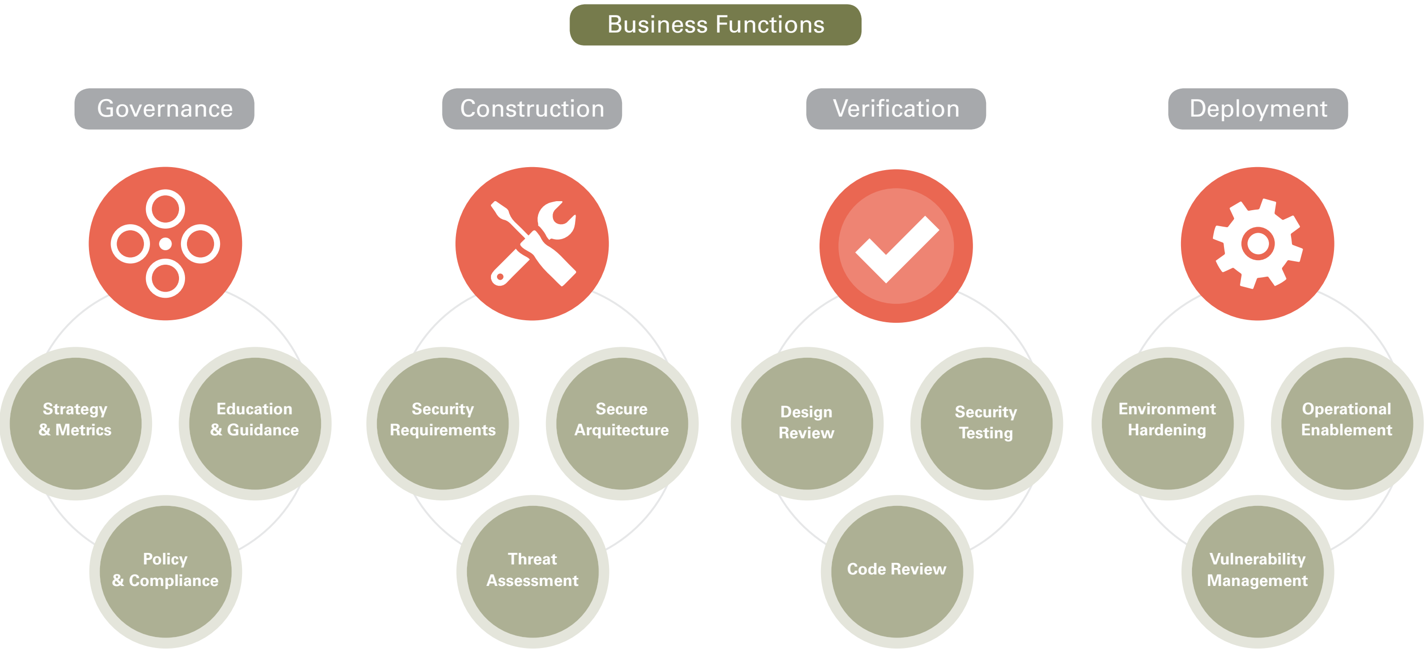
- Guidance related to security activities must be prescriptive - All the steps in building and assessing an assurance program should be simple, well-defined, and measurable. This model also provides roadmap templates for common types of organizations.

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 ma- turity 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.

SOFTWARE DEVELOPMENT

- SAMM Overview -



UNDERSTANDING THE MODEL

A view of the big picture

SAMM is built upon a collection of Security Practices that are tied back into the core Business Functions involved in software development. This section introduces those Business Functions and the corresponding Security Practices for each. After covering the high-level framework, the Maturity Levels for each Security Practice are also discussed briefly in order to paint a picture of how each can be iteratively improved over time.

BUSINESS FUNCTIONS

At the highest level, SAMM defines four critical Business Functions.

Each Business Function (list- ed below) is a category of activities related to the nuts-and-bolts of software development, or stated another way, any organization involved with software development must fulfill each of these Business Functions to some degree.

For each Business Function, SAMM defines three Security Practices.

Each Security Practice (list- ed opposite) is an area of security-related activities that build assurance for the related Business Function. So overall, there are twelve Security Practices that are the independent silos for improvement that map underneath the Business Functions of software development.

For each Security Practice, SAMM defines three Maturity Levels as Objectives.

Each Level within a Security Practice is characterized by a successively more sophisticated Objective defined by specific activities and more stringent success metrics than the previous level. Additionally, each Security Practice can be improved independently, though related activities can lead to optimizations.

GOVERNANCE

Governance is centered on the processes and activities related to how an organization manages overall software development activities. More specifically, this includes concerns that cross-cut groups involved in development as well as business processes that are established at the organization level.

STRATEGY & METRICS

Involves the overall strategic direction of the software assurance program and instrumentation of processes and activities to collect metrics about an organization's security posture.

POLICY & COMPLIANCE

Involves setting up a security and compliance control and audit framework throughout an organization to achieve increased assurance in software under construction and in operation.

EDUCATION & GUIDANCE

Involves increasing security knowledge amongst personnel in software development through training and guidance on security topics relevant to individual job functions.

CONSTRUCTION

Construction concerns the processes and activities related to how an organization defines goals and creates software within development projects. In general, this will include product management, requirements gathering, high-level architecture specification, detailed design, and implementation.

THREAT ASSESSMENT

Involves accurately identifying and characterizing potential attacks upon an organization's software in order to better understand the risks and facilitate risk management.

SECURITY REQUIREMENTS

Involves promoting the inclusion of security-related requirements during the software development process in order to specify correct functionality from inception.

SECURE ARCHITECTURE

Involves bolstering the design process with activities to promote secure-by-default designs and control over technologies and frameworks upon which software is built.

VERIFICATION

Verification is focused on the processes and activities related to how an organization checks and tests artifacts produced throughout software development. This typically includes quality assurance work such as testing, but it can also include other review and evaluation activities.

DESIGN REVIEW

Involves inspection of the artifacts created from the design process to ensure provision of adequate security mechanisms and adherence to an organization's expectations for security.

CODE REVIEW

Involves assessment of an organization's source code to aid vulnerability discovery and related mitigation activities as well as establish a baseline for secure coding expectations.

SECURITY TESTING

Involves testing the organization's software in its runtime environment in order to both discover vulnerabilities and establish a minimum standard for software releases.

DEPLOYMENT

Deployment entails the processes and activities related to how an organization manages release of software that has been created. This can involve shipping products to end users, deploying products to internal or external hosts, and normal operations of software in the runtime environment.

VULNERABILITY MANAGEMENT

Involves establishing consistent processes for managing internal and external vulnerability reports to limit exposure and gather data to enhance the security assurance program.

ENVIRONMENT HARDENING

Implementing controls for the operating environment surrounding an organization's software to bolster the security posture of applications that have been deployed.

OPERATIONAL ENABLEMENT

Identifying and capturing security-relevant information needed by an operator to properly configure, deploy, and run an organization's software.

MATURITY LEVELS

Each of the twelve Security Practices has three defined Maturity Levels and an implicit starting point at zero. The details for each level differs between the Practices, but they generally represent:

0 Implicit starting point representing the activities in the Practice being unfulfilled

1 Initial understanding and ad hoc provision of Security Practice

2 Increase efficiency and/or effectiveness of the Security Practice

3 Comprehensive mastery of the Security Practice at scale

NOTATION

Throughout this document, the following capitalized terms will be reserved words that refer to the SAMM components defined in this section. If these terms appear without capitalization, they should be interpreted based on the their context:

- Business Function also as Function
- Security Practice also as Practice
- Maturity Level also as Level, Objective

GOVERNANCE

Description of Security Practices

Governance is centered on the processes and activities related to how an organization manages overall software development activities. More specifically, this includes concerns that cross-cut groups involved in development as well as business processes that are established at the organization level.

STRATEGY & METRICS

The Strategy & Metrics (SM) Practice is focused on establishing the framework within an organization for a software security assurance program. This is the most fundamental step in defining security goals in a way that's both measurable and aligned with the organization's real business risk. By starting with lightweight risk profiles, an organization grows into more advanced risk classification schemes for application and data assets over time. With additional insight on relative risk measures, an organization can tune its project-level security goals and develop granular roadmaps to make the security program more efficient.

At the more advanced levels within this Practice, an organization draws upon many data sources, both internal and external, to collect metrics and qualitative feedback on the security program. This allows fine tuning of cost outlay versus the realized benefit at the program level.

POLICY & COMPLIANCE

The Policy & Compliance (PC) Practice is focused on understanding and meeting external legal and regulatory requirements while also driving internal security standards to ensure compliance in a way that's aligned with the business purpose of the organization.

A driving theme for improvement within this Practice is focus on project-level audits that gather in- formation about the organization's behavior in order to check that expectations are being met. By introducing routine audits that start out lightweight and grow in depth over time, organizational change is achieved iteratively.

In a sophisticated form, provision of this Practice entails organization-wide understanding of both in- ternal standards and external compliance drivers while also maintaining low-latency checkpoints with project teams to ensure no project is operating outside expectations without visibility.

EDUCATION & GUIDANCE

The Education & Guidance (EG) Practice is focused on arming personnel involved in the software life- cycle with knowledge and resources to design, develop, and deploy secure software. With improved access to information, project teams will be better able to proactively identify and mitigate the specific security risks that apply to their organization.

One major theme for improvement across the Objectives is providing training for employees, either through instructor-led sessions or computer-based modules. As an organization progresses, a broad base of training is built by starting with developers and moving to other roles throughout the organiza- tion, culminating with the addition of role-based certification to ensure comprehension of the material.

In addition to training, this Practice also requires pulling security-relevant information into guidelines that serve as reference information to staff. This builds a foundation for establishing a baseline expectation for security practices in your organization, and later allows for incremental improvement once usage of the guidelines has been adopted.

ACTIVITIES OVERVIEW

STRATEGY & METRICS

	OBJECTIVE	ACTIVITIES
SM 1	Establish unified strategic roadmap for software security within the organization	A. Estimate overall business risk profile B. Build and maintain assurance program roadmap
SM 2	Measure relative value of data and software assets and choose risk tolerance	A. Classify data and applications based on business risk B. Build and maintain assurance program roadmap
SM 3	Align security expenditure with relevant business indicators and asset value	A. Conduct periodic industry- wide cost comparisons B. Collect metrics for historic security spend

POLICY & COMPLIANCE

	OBJECTIVE	ACTIVITIES
PC 1	Understand relevant governance and compliance drivers to the organization	A. Identify and monitor external compliance drivers B. Build and maintain compliance guidelines
PC 2	Establish security and compliance baseline and understand per-project risks	A. Build policies and standards for security and compliance B. Establish project audit practice
PC 3	Require compliance and measure projects against organization-wide policies and standards	A. Create compliance gates for projects B. Adopt solution for audit data collection

EDUCATION & GUIDANCE

	OBJECTIVE	ACTIVITIES
EG 1	Understand relevant governance and compliance drivers to the organization	A. Identify and monitor external compliance drivers B. Build and maintain compliance guidelines
EG 2	Establish security and compliance baseline and understand per-project risks	A. Build policies and standards for security and compliance B. Establish project audit practice
EG 3	Require compliance and measure projects against organization-wide policies and standards	A. Create compliance gates for projects B. Adopt solution for audit data collection

/ CONSTRUCTION

Description of Security Practices

Governance is centered on the processes and activities related to how an organization manages overall software development activities. More specifically, this includes concerns that cross-cut groups involved in development as well as business processes that are established at the organization level.

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 as- surance 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.

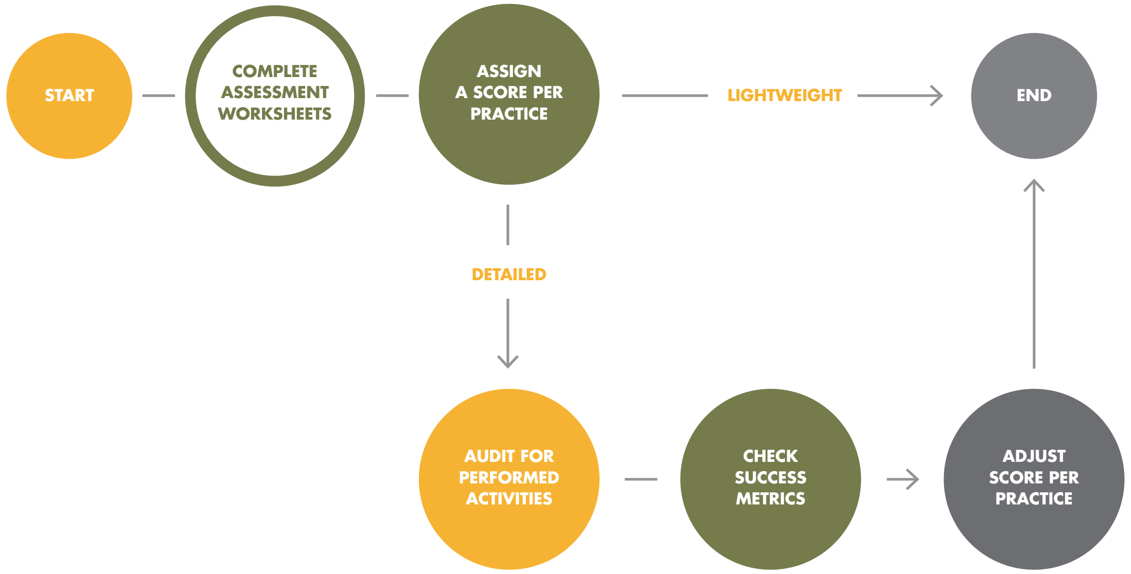
USING THE MATURITY LEVELS

By measuring an organization against the defined Security Practices, an overall picture of built-in se- curity 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 usu- ally vary according to the drivers behind the assessment, but in general, there are two recommended styles:

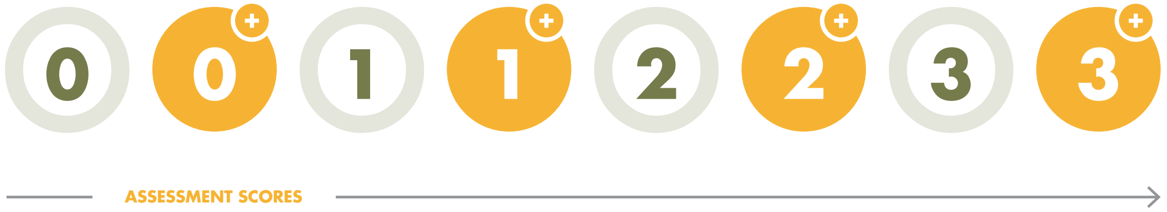
Lightweight
The assessment worksheets for each Practice are evaluated and scores are assigned based on answers. This type of assessment is usually sufficient for an organization that is trying to map their existing assurance program into SAMM and just wants to get a quick picture of where they stand.

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.


START
COMPLETE ASSESSMENT WORKSHEETS
ASSIGN A SCORE PER PRACTICE
LIGHTWEIGHT
END
DETAILED
AUDIT FOR PERFORMED ACTIVITIES
CHECK SUCCESS METRICS
ADJUST SCORE PER PRACTICE

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 be- tween 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 Activi- ties 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

STRATEGY & METRICS

YES NO

- 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

- 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

- Is per-project data for cost of assurance activities collected?
- Does your organization regularly compare your security spend with other organizations?

SM 3

POLICY & COMPLIANCE

YES NO

- Do most project stakeholders know their project's compliance status?
- Are compliance requirements specifically considered by project teams?

PC 1

- 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

- 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

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?

PC 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?

PC 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?

PC 3