Governance

Description of Security Practices

Intro

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 information 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 internal 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 lifecycle 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 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 organization, 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.

Governance

Activities overview

Summary,
redundant

Strategy & Metrics

...more on page 24

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

Policy & Compliance

...more on page 28

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

Education & Guidance

...more on page 32

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

Governance

Assessment worksheet

Strategy & Metrics

	Score 0.0	0.2	0.5	1.0	
✦Is there a software security assurance program in place?	No	<1 yr	>1 yr	Mature	
✦Are development staff aware of future plans for the assurance program?	No	Some	Half	Most	
✦Do the business stakeholders understand your organization's risk profile?	No	Some	Half	Most	SM 1
✦Are many of your applications and resources categorized by risk?	No	Some	Half	Most	
✦Are risk ratings used to tailor the required assurance activities?	No	Some	Half	Most	
✦Does the organization know about what's required based on risk ratings?	No	Some	Half	Most	SM 2
✦Is per-project data for the cost of assurance activities collected?	No	Some	Half	Most	
✦Does your organization regularly compare your security spend with that of other organizations?	No	Once	Every 2-3 yrs	Annually	SM 3

additional guidance, like in Assessment Excel?

Policy & Compliance

	Score 0.0	0.2	0.5	1.0	
✦Do project stakeholders know their project's compliance status?	No	Some	Half	Most	
✦Are compliance requirements specifically considered by project teams?	No	Not Apply	Ad-hoc	Yes	PC 1
✦Does the organization utilize a set of policies and standards to control software development?	No	Per Team	Org Wide	Integrated Process	
✦Are project teams able to request an audit for compliance with policies and standards?	No	Some	Half	Most	PC 2
✦Are projects periodically audited to ensure a baseline of compliance with policies and standards?	No	Some	Half	Most	
✦Does the organization systematically use audits to collect and control compliance evidence?	No	Bus Area	Org Wide	Org Wide & Required	PC 3

Education & Guidance

	Score 0.0	0.2	0.5	1.0	
✦Have developers been given high-level security awareness training?	No	Once	2-3 yrs	Annually	
✦Does each project team understand where to find secure development best-practices and guidance?	No	Some	Half	Most	EG 1
✦Are those involved in the development process given role-specific security training and guidance?	No	Some	Half	Most	
✦Are stakeholders able to pull in security coaches for use on projects?	No	Some	Half	Most	EG 2
✦Is security-related guidance centrally controlled and consistently distributed throughout the organization?	No	Per Team	Org Wide	Integrated Process	
✦Are developers tested to ensure a baseline skill-set for secure development practices?	No	Once	Every 2-3 yrs	Annually	EG 3

Strategy & Metrics

	SM 1	SM 2	SM 3
Objective	**Establish unified strategic roadmap for software security within the organization.**	**Measure relative value of data and software assets and choose risk tolerance.**	**Align security expenditure with relevant business indicators and asset value.**
Activities	A. Estimate overall business risk profile B. Build and maintain assurance program roadmap	A. Classify data and applications based on business risk B. Establish and measure per-classification security goals	A. Conduct periodic industry-wide cost comparisons B. Collect metrics for historic security spend
Assessment	✦ Is there a software security assurance program in place? ✦ Are development staff aware of future plans for the assurance program? ✦ Do the business stakeholders understand your organization's risk profile?	✦ Are many of your applications and resources categorized by risk? ✦ Are risk ratings used to tailor the required assurance activities? ✦ Does the organization know about what's required based on risk ratings?	✦ Is per-project data for the cost of assurance activities collected? ✦ Does your organization regularly compare your security spend with that of other organizations?
Results	✦ Concrete list of the most critical business-level risks caused by software ✦ Tailored roadmap that addresses the security needs for your organization with minimal overhead ✦ Organization-wide understanding of how the assurance program will grow over time	✦ Customized assurance plans per project based on core value to the business ✦ Organization-wide understanding of security-relevance of data and application assets ✦ Better informed stakeholders with respect to understanding and accepting risks	✦ Information to make informed case-by-case decisions on security expenditures ✦ Estimates of past loss due to security issues ✦ Per-project consideration of security expense versus loss potential ✦ Industry-wide due diligence with regard to security

Strategy & Metrics

SM 1

Establish unified strategic roadmap for software security within the organization

Activities

A. Estimate overall business risk profile

Interview business owners and stakeholders and create a list of worst-case scenarios across the organization's various application and data assets. Based on the way in which your organization builds, uses, or sells software, the list of worst-case scenarios can vary widely, but common issues include data theft or corruption, service outages, monetary loss, reverse engineering, account compromise, etc.

After broadly capturing worst-case scenario ideas, collate and select the most important based on collected information and knowledge about the core business. Any number can be selected, but aim for at least three and no more than seven to make efficient use of time and keep the exercise focused.

Elaborate a description of each of the selected items and document details of contributing worst-case scenarios, potential contributing factors, and potential mitigating factors for the organization.

The final business risk profile should be reviewed with business owners and other stakeholders for understanding.

B. Build and maintain assurance program roadmap

Understanding the main business risks to the organization, evaluate the current performance of the organization against each the twelve practices. Calculate a score for each practice based on the answers to the multiple choice questions using the toolbox spreadsheet or SAMM survey application.

Once a good understanding of current status is obtained, the next goal is to identify the practices that will be improved in the next iteration. Select them based on business risk profile, other business drivers, compliance requirements, budget tolerance, etc. Once practices are selected, the goals of the iteration are to achieve the next objective under each.

Iterations of improvement on the assurance program should be approximately 3-6 months, but an assurance strategy session should take place at least every three months to review progress on activities, performance against success metrics and other business drivers that may require program changes.

Assessment

- Is there a software security assurance program in place?
- Are development staff aware of future plans for the assurance program?
- Do the business stakeholders understand your organization's risk profile?

Results

- Concrete list of the most critical business-level risks caused by software
- Tailored roadmap that addresses the security needs for your organization with minimal overhead
- Organization-wide understanding of how the assurance program will grow over time

Success Metrics

- >80% of stakeholders briefed on business risk profile in the past six months
- >80% of staff briefed on assurance program roadmap in the past three months
- >1 assurance program strategy session in the past three months

Costs

- Buildout and maintenance of business risk profile
- Quarterly evaluation of assurance program

Personnel

- Developers
- Architects
- Managers
- Business Owners
- QA Testers
- Security Auditor

Related Levels

- Policy & Compliance - 1
- Threat Assessment - 1
- Security Requirements - 2

SM 2

Strategy & Metrics

Measure relative value of data and software assets and choose risk tolerance

Assessment

- Are many of your applications and resources categorized by risk?
- Are risk ratings used to tailor the required assurance activities?
- Does the organization know about what's required based on risk ratings?

Results

- Customized assurance plans per project based on core value to the business
- Organization-wide understanding of security-relevance of data and application assets
- Better informed stakeholders with respect to understanding and accepting risks

Success Metrics

- >90% applications and data assets evaluated for risk classification in the past 12 months
- >80% of staff briefed on relevant application and data risk ratings in the past six months
- >80% of staff briefed on relevant assurance program roadmap in the past three months

Costs

- Buildout or license of application and data risk categorization scheme
- Program overhead from more granular roadmap planning

Personnel

- Architects
- Managers
- Business Owners
- Security Auditor

Related Levels

- Policy & Compliance - 2
- Threat Assessment - 2
- Design Review - 2

Activities

A. Classify data and applications based on business risk

Establish a simple classification system to represent risk-tiers for applications. In its simplest form, this can be a High/Medium/Low categorization. More sophisticated classifications can be used, but there should be no more than seven categories and they should roughly represent a gradient from high to low impact against business risks.

Working from the organization's business risk profile, create project evaluation criteria that maps each project to one of the risk categories. A similar but separate classification scheme should be created for data assets and each item should be weighted and categorized based on potential impact to business risks.

Evaluate collected information about each application and assign each a risk category based upon overall evaluation criteria and the risk categories of data assets in use. This can be done centrally by a security group or by individual project teams through a customized questionnaire to gather the requisite information.

An ongoing process for application and data asset risk categorization should be established to assign categories to new assets and keep the existing information updated at least biannually.

B. Establish and measure per-classification security goals

With a classification scheme for the organization's application portfolio in place, direct security goals and assurance program roadmap choices can be made more granular.

The assurance program's roadmap should be modified to account for each application risk category by specifying emphasis on particular practices for each category. For each iteration of the assurance program, this would typically take the form of prioritizing more higher-level objectives on the highest risk application tier and progressively less stringent objectives for lower/other categories.

This process establishes the organization's risk tolerance since active decisions must be made as to what specific objectives are expected of applications in each risk category. By choosing to keep lower risk applications at lower levels of performance with respect to the security practices, resources are saved in exchange for acceptance of a weighted risk. However, it is not necessary to arbitrarily build a separate roadmap for each risk category since that can leads to inefficiency in management of the assurance program itself.

Strategy & Metrics

SM 3

Align security expenditure with relevant business indicators and asset value

Activities

A. Conduct periodic industry-wide cost comparisons

Research and gather information about security costs from intra-industry communication forums, business analyst and consulting firms, or other external sources. In particular, there are a few key factors that need to be identified.

First, use collected information to identify the average amount of security effort being applied by similar types of organizations in your industry. This can be done either top-down from estimates of total percentage of budget, revenue, etc. or it can be done bottom-up by identifying security-related activities that are considered normal for your type of organization. Overall, this can be hard to gauge for certain industries, so collect information from as many relevant sources as are accessible.

The next goal of researching security costs is to determine if there are potential cost savings on third-party security products and services that your organization currently uses. When weighing the decision of switching vendors, account for hidden costs such as retraining staff or other program overhead.

Overall, these cost-comparison exercises should be conducted at least annually prior to the subsequent assurance program strategy session. Comparison information should be presented to stakeholders in order to better align the assurance program with the business.

B. Collect metrics for historic security spend

Collect project-specific information on the cost of past security incidents. For instance, time and money spent in cleaning up a breach, monetary loss from system outages, fines and fees to regulatory agencies, project-specific one-off security expenditures for tools or services, etc.

Using the application risk categories and the respective prescribed assurance program roadmaps for each, a baseline security cost for each application can be initially estimated from the costs associated with the corresponding risk category.

Combine the application-specific cost information with the general cost model based on risk category, and then evaluate projects for outliers, i.e. sums disproportionate to the risk rating. These indicate either an error in risk evaluation/classification or the necessity to tune the organization's assurance program to address root causes for security cost more effectively.

The tracking of security spend per project should be done quarterly at the assurance program strategy session, and the information should be reviewed and evaluated by stakeholders at least annually. Outliers and other unforeseen costs should be discussed for potential affect on assurance program roadmap.

Assessment

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

Results

- Information to make informed case-by-case decisions on security expenditures
- Estimates of past loss due to security issues
- Per-project consideration of security expense versus loss potential
- Industry-wide due diligence with regard to security

Success Metrics

- >80% of projects reporting security costs in the past three months
- >1 industry-wide cost comparison in the past year
- >1 historic security spend evaluation in the past year

Costs

- Buildout or license industry intelligence on security programs
- Program overhead from cost estimation, tracking, and evaluation

Personnel

- Architects
- Managers
- Business Owners
- Security Auditor

Related Levels

- Issue Management - 1