Objective Level 1: Measure relative value of data and software assets and choose risk tolerance

Proposed Level1 ActA: Estimate overall business risk profile

To develop risk-based assurance program, interview business owners and stakeholders and create a list of worst-case scenarios across the organization’s various application and data assets including application and data. 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 3 and no more than 7 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.

While creating final business risk profile, explicitly reference evolving threat landscape and recent incidents at other organizations to bring awareness. Make it clear how threats could become real incidents when threats are not addressed proactively.

Proposed Level1 ActB: Classify assets 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.

Objective Level 2: Articulate business case; and establish unified strategic roadmap for software security within the organization

Proposed Level 2 ActA: Build and maintain assurance program roadmap

Understanding the main business risks to the organization, build a business case to justify expenditure. Evaluate the current performance of the organization against each of the twelve Practices. Assign a score for each Practice from 1, 2, or 3 based on the corresponding Objective if the organization passes all the cumulative success metrics. If no success metrics are being met, assign a score of 0 to the Practice. 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 3 months to review progress on activities, performance against success metrics and other business drivers that may require program changes.

Proposed Level 2 ActB: Establish and measure per-classification security goals and align security expenditure with relevant business indicators and asset value

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.

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.

Objective Level 3: Establish and utilize objective measurements to help improve security posture of the organization

Proposed Level 3 ActA: Identify and communicate metrics to measure effectiveness and progress

The intent of metrics is to define and measure progress against security roadmap in quantitative terms. Make sure metrics are well understood by all stakeholders and drive necessary behavior change. It is advisable to stay away from qualitative metrics. Example of metric could be number of detected & fixed vulnerabilities in a given time frame. Metrics and data collection can be manual process at the beginning. And as program advances, Metrics and data collection need be automated to avoid additional overhead. Good metrics are agnostic of development methodology – waterfall, agile, iterative since various parts of the organization might be using different methodology; and at a different stage in their journey to agile.

Proposed Level 3 ActB: Use metrics to advance security goals

With well-defined metrics in place and metrics collection mechanism established, regularly share metrics on security posture with all stakeholders including employees. The intent is to bring awareness of the progress being made and drive improvement and behavior change. Keep metrics to manageable number to retain their effectiveness and usefulness. It’s better to use few meaningful metrics that organization will actually use. The dashboard of security metrics per project should be reviewed at least quarterly to drive improvements.

Objective Level 3+: Continuously manage risk tolerance of data and application assets at acceptable level.

Proposed Level 3+ ActA: Establish proactive continuous Risk Management strategy

With one time overall business risk profile established at the beginning as level 1 activity, establish mechanism to continuously manage level of Risk impact and probability at regular interval – preferably before major release or once every 6 months. The risk can be factored as the probability of the asset being compromised and the business impact caused by the exploit of the vulnerability. Security risk in terms of threats and vulnerabilities needs to be converted to the business risk by taking value of asset into account to quantify risk. In its simplest form, risk can be classified in qualitative measures such as high, medium and low. Risk can be managed either proactive or reactive. Proactive risk management involves addressing threats and vulnerabilities before they’re exploited. Reactive risk management is discussed later as part of issue management practice.

Proposed Level 3+ ActB: Actively manage organizational risk

Once risk is identified, organization needs to decide on action plan for managing the risk. At this level, organization employs continuous risk management. Depending on risk level, risk can be mitigated, accepted, avoided or transferred. Depending on the assessment of the level of risk impact and probability, for example, an organization might decide to accept the risks whose likelihood and impact are low, mitigate or reduce the risks (e.g. by applying security measures) that have high probability and low impact, transfer or share the risks (e.g. to/with a third party such as through contractual agreements) that are of low probability and high impact and avoid the risks (e.g. such as not to implement high risk functions, not to adopt high risk technologies) that have high probability and high impact.

In case organization decides to accept the high risk, an explicit exception management process needs to be followed with clear accountability and commitment to address risk in next iteration. Risk acceptance needs to be explicitly communicated to executive management.