SECURITY COMPASS WHITEPAPER

Scaling Software Risk Assessments

Security Compass

Why conduct risk assessments?

You can't defend your systems against risks you don't know about, so the first step in any security program should be to document the risk-facing systems, projects, or processes. Simply enumerating risks is not enough, however. Since it is impossible to eliminate all risk – and likely not desirable given the cost vs. benefit of attempting to do so – organizations need to evaluate and prioritize which risks to address.

A well-run risk assessment accomplishes this by examining the impact each risk poses on organizational goals, the prevalence of threats, and the probability of a successful attack. This allows organizations to make informed decisions and to prioritize issues, thus maximizing the impact on their risk profile with available time, money, and security resources. Without a thorough risk assessment, a security program's priorities are based only on guesswork.

This is the reason why all regulatory standards require organizations to understand the risks in their systems. For example, HIPAA requires "an accurate and thorough assessment of the potential risks and vulnerabilities to sensitive information." Likewise, ISO 27001, PCI-DSS, and Canada's PHIPA and OSFI all require organizations to conduct regularly-scheduled risk assessments, while FDIC 12 CFR 364 requires financial institutions to assess risk to "Identify reasonably foreseeable internal and external threats that could result in unauthorized disclosure, misuse, alteration, or destruction of customer information or customer information systems."

Risk assessment workflow

Risk assessments typically require input from multiple stakeholders. First, risk teams need to identify all in-scope assets and evaluate their sensitivity and criticality to the business. The asset classification and evaluation process can include software, hardware, network devices, shadow projects, communications, data stored by a system, services offered by the assets, and other items. Next, teams catalog threats associated with the in-scope systems, including those that affect individual assets, and determine the likelihood and impact of those threats. This requires an understanding of inherent risks (e.g., account compromise resulting in unauthorized access to the application), residual risks remaining after controls are applied, risk is accepted, or risk is transferred, and, in some cases, specific threats such as tactics and techniques used by likely threat actors against similar organizations.

Based on the organization's risk appetite and applicable regulations, risks are prioritized and required risk-reduction activities are planned. In some cases, teams will require remediation of vulnerabilities. In others, they will recommend technical controls to reduce or transfer risk. Finally, the teams must be able to track each issue to ensure required activities were completed and continue to monitor the environment for changes to the existing risk profile or new risks. Risk assessments can be time-consuming and difficult to manage. To capture the required information and accommodate each functional area, many organizations create spreadsheets with detailed surveys including hundreds of questions. For example, a risk assessment for new software would include questions for engineering about the programming language, software frameworks used, features and functions, and QA tools. Compliance will determine which, if any, regulatory standards or internal policies require compliance. Senior management must define the application's criticality to business goals and their appetite for risk. Security teams provide information on active threats, security testing, and incident response plans. IT organizations answer questions about the deployment environment, logging requirements, and network defenses. Weeks later, when all stakeholders complete their respective surveys, risk assessment teams map risks, threats, and required controls to each answer.

Challenges with manual risk assessments

Scalability

Organizations face many challenges conducting risk assessments manually, and scaling assessments with heavy manual components is not a reasonable option for most teams.

Even small risk assessments can consume 6 to 8 weeks. Cataloging threats and identifying appropriate controls can take weeks. Also, due to other business priorities facing participating stakeholders, predicting assessment schedules can be difficult; compliance may be able to easily determine that a project is subject to the PCI-DSS in some cases, but may need more information on the project to understand if it is in-scope for a different project. Likewise, engineering may have urgent deliverables and be unable to interrupt a sprint to complete the questionnaire.

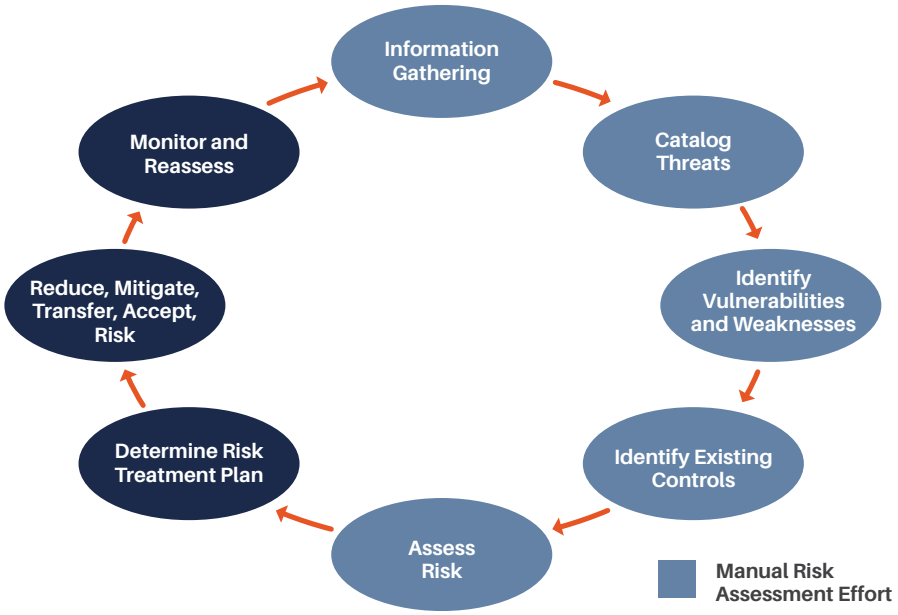

Figure 1: Risk Management Process

Consistency

Ensuring consistency is critical in risk assessments. Given a set of characteristics, all team members should evaluate a project identically. Unfortunately, this does not always happen. Evaluations can be inconsistent across team members and between projects. This makes it difficult to understand and report on an organization's true security profile.

Consistency is difficult when tracking projects using spreadsheets. Answers to questions may not be clear or may require narrative answers, complicating the assessment process. Uniform controls across similar scenarios are simpler to manage and track, and manual processes can also result in inconsistency assigning and applying controls.

Completeness

Because manual risk assessments are time-consuming, organizations may seek short-cuts that result in inconsistencies between projects. For example, organizations often attempt to accelerate the risk assessment process by limiting the information they collect, potentially missing critical input. In other cases, assessors may not recognize the need for information from some stakeholders. Finally, some teams may be delayed in fully responding to questionnaires, forcing assessors to forego their answers.

Audit and Reporting

Spreadsheets may seem to be a simple way to track risks and controls, but, from a regulatory compliance standpoint, they have one key weakness: auditability. Without a central, controlled repository for risk assessment data, with an auditable record of changes, it is difficult to prove compliance to an auditor or corporate Board. For example, when the risk team creates controls, how does one easily determine the following:

- Was the control recorded?
- Was the control enforced?
- Were manual processes tracked and completed?
- Were any new threats identified post-deployment?

Accelerate software risk assessments with SD Elements

SD Elements, a leading Balanced Development Automation platform, accelerates software security risk assessments at scale, while also simplifying the implementation of security and privacy controls. It now has the built-in capability to automate key portions of risk assessments for software assets.

Let's learn how you can reduce risk by using SD Elements.

Automated security and privacy control identification accelerates assessments

You can speed-up the software risk assessment process with SD Elements through automated classification of projects by inherent risk. Our platform provides a dynamic survey that gathers information about your projects to map controls to standards, such as ISO 27001, NIST 800-82, HIPAA, PCI-DSS, GDPR, etc.

Standardization of assessment efforts brings consistency

You can improve visibility into current software risks by assessing security control gaps on a continuous basis. SD Elements also simplifies the identification of control changes or gaps when there are changes in an existing project that may impact its security and privacy posture.

Reduced assessment time enables scalability

By automatically classifying software assets by inherent risk, and rapidly identifying controls, organizations free up resources to expand their risk assessment programs. To further reduce demands on risk, security, and DevOps teams, SD Elements automatically generates tickets and validates compliance through integrations with security testing tools like static analysis or vulnerability and configuration assessment solutions. Controls that require manual tasks, like changing default credentials, can be synchronized with ticketing systems, including Jira and ServiceNow, for completion by IT and DevOps teams. When tasks are marked as "completed" in those systems, SD Elements is automatically updated.

Centralization simplifies compliance and reporting

By using a centralized and auditable workflow, SD Elements simplifies management reporting and compliance audits. Controls are simple to identify and map to a policy or requirement and every change or task completion is logged. SD Elements provides overview reports to communicate risk levels to non-technical staff and includes over 150 customizable reports to track risk for internal compliance and against standards such as GDPR, PCI-DSS, GLBA, and others.

Automate software risk assessments with SD Elements to achieve scale and speed

SD Elements aligns with software risk management frameworks such as the NIST Risk Management Framework for Information Systems & Organizations/NIST Special Publication 800-37 Revision 2

Fast, consistent, and auditable risk assessments

Manual risk assessments require extensive effort from security experts and are difficult to scale across an enterprise. SD Elements can automate many of the manual tasks in a risk assessment, reducing demands on risk, security, and DevOps teams, while allowing greater enterprise coverage. Through a central data repository, standardization of controls to match internal or external requirements, and integration with testing and tracking tools, SD Elements helps organizations reduce risk and simplify compliance.

SecurityCompass

Security Compass, a leading provider of cybersecurity solutions, enables organizations to shift left and build secure applications by design, integrated directly with existing DevSecOps tools and workflows. Its flagship product, SD Elements, allows organizations to balance the need to accelerate software time-to-market while managing risk by automating significant portions of proactive manual processes for security and compliance. SD Elements is the world's first Balanced Development Automation platform. Security Compass is the trusted solution provider to leading financial and technology organizations, the U.S. Department of Defence, government agencies, and renowned global brands across multiple industries. The company is headquartered in Toronto, with offices in the U.S. and India.

1.888.777.2211
info@securitycompass.com
www.securitycompass.com

@SECURITYCOMPASS
SECURITY COMPASS

OFFICES

GLOBAL HEADQUARTERS
1 Yonge Street
Suite 1801
Toronto, Ontario
Canada M5E 1W7

TORONTO
390 Queens Quay W
2nd Floor
Toronto, Ontario
Canada M5V 3A6

NEW JERSEY
621 Shrewsbury Avenue
Suite 215
Shrewsbury, New Jersey
USA 07702

CALIFORNIA
600 California Street
San Francisco, California
94108, USA

INDIA
#4.07
4th Floor, Statesman House
Barakhamba Road, New Delhi
India 110001