Certified Security Solutions, Inc.

Security Kaizen™

Security Performance Management

FAQ

1 What is Security Kaizen?

Security Kaizen is an approach to information security that uses objective, systematic and analytic methods to manage and optimize security performance. Security Kaizen treats security as a dimension of quality, and it is based on mature, proven and well understood quality management principles, tools and techniques.

Security Kaizen incorporates a variety of components that can be used to solve different problems and to achieve different goals, ranging from tactical to strategic, and ranging from small-group to organization-wide activities.

This FAQ addresses tactical process- and project-focused small-group Security Kaizen activities.

2 Why do Security Kaizen?

Demands on information security are increasing due to legislative and contractual compliance requirements, market and competitive pressures, and technology and business volatility. With those demands comes the need to get the most out of information security investments.

Security Kaizen is a response to those demands. Security Kaizen provides the means and methods to effectively manage and optimize security performance. The system can optimize the return from security investments, based on objective and quantifiable performance data.

More traditional efforts that focus on compliance, policy, audit and risk assessment will continue. However, those efforts alone are insufficient for high performance organizations that demand more from their information security investment.

3 What is a performance management system?

A performance management system integrates inputs, metrics, functions and outputs into a feedback system. The proficiency of the performance management system is dependent on an accurate understanding of each of those elements, and the relationships between elements. The ultimate effectiveness of the performance management system is dependent on an accurate understanding of the relationship of those elements to the rest of the

organization. Security Kaizen articulates and validates those elements and their relationships to each other and to the rest of the organization.

4 How do you quantify security performance?

The performance characteristics that are the focus of your Security Kaizen effort will depend on your business objectives. For example, some organizations may want to improve effectiveness with no increase in time or cost; other organizations may want to reduce time or cost while maintaining the same level of effectiveness.

Measurements may be based on security-specific processes, or the impact that security controls have on other business processes. Security Kaizen includes identification and development of metrics and measurements, instrumentation and data collection, and presentation of performance in the form of management scorecards and process dashboards.

5 What is acceptable security performance?

Acceptable performance—how much, at what cost, with which tradeoffs—are business decisions. Security Kaizen does not define "acceptable" performance, but does provide the tools and information needed to optimize performance, and to make informed and objective business decisions.

Eventually we expect performance standards that will allow comparison or benchmarking. However, meaningful "apples-to-apples" comparisons and benchmarking between organizations will require a degree of maturity and standardization that, for information security, is still far in the future.

6 What about risk assessment?

Many information security risk assessment efforts focus on assets and their value. However, most business information assets have little or no value outside the context of a business process that uses that information to add value. Security Kaizen provides that missing context by illuminating the value-add, providing an objective basis for asset valuation and consequent risk assessment.

Security Kaizen also includes tools to analyze potential failure modes—whether due to overt or unintended acts—and improve the robustness of a process in the face of those failures. Whether the cause is hacker, operator error, or bad data, the result is often the same, and all of those failure modes must be considered.

Security Kaizen can also use risk assessment efforts. As a rule, assets and threats that have been identified as significant provide a good basis for selecting processes that are candidates for Security Kaizen efforts.

7 What about policy?

Without objective performance data to inform policy, there is no useful feedback to determine if policies are effective and efficient. The result is an open loop system with results that are too often like "pushing on a string". Security Kaizen helps close the loop.

8 What about compliance?

Compliance is largely a side effect of performance management. Policy is a statement of intent; compliance determines adherence to policy; neither provides a meaningful measure of performance. That is, how effectively and efficiently a system achieves the intended effect as articulated in policy. Security Kaizen fills that gap, and objective performance data and the performance management system documentation provides evidence of due diligence.

Security Kaizen can also use the results of compliance efforts. For example, the documentation created to fulfill compliance requirements can form the basis for selecting appropriate projects. That documentation can often be used to help build the performance management system.

9 What about governance?

By providing a gauge for policy, risk and compliance, Security Kaizen helps align efforts across stakeholders, ensure that stakeholder interests are represented, that those interests are reflected in the performance of the organization, and that there is objective evidence of that performance.

However, any single Security Kaizen deployment project is not intended to achieve organization-wide stakeholder alignment. That will come eventually, if Security Kaizen is applied across the entire organization. When and if an organization decides to pursue that goal, organization-wide or strategic Security Kaizen approaches are used, in addition to project or small-group methods. That also first requires building organizational capability.

10 How does this differ from other "security metrics" efforts?

Many "security metrics" efforts provide little more than a scorecard. While such scorecards are useful, they are not sufficient for performance management and optimization.

Cause-and-effect relationships must be understood and validated if the metrics are to provide useful guidance. That includes validation of the data quality and the requirements of the customers consuming the scorecards or dashboards. That design and validation is part of Security Kaizen, providing metrics that are input to both scorecards and dashboards.

The objective of Security Kaizen is performance management and optimization. Metrics are one of several elements involved in achieving that objective. Out of that context, metrics provide limited value, and in the worst cases can lead to unintended and unpleasant consequences.

11 What's the difference between a scorecard and dashboard?

We divide metrics into scorecards and dashboards:

- A scorecard tells you what has happened. Scorecards are most often used by management to determine if the organization is "on track". A scorecard does not tell you the cause, or indicate what actions are required for improvement. Scorecards are a product of a Security Kaizen deployment project.

- A dashboard that is integrated with a properly designed performance management system provides both an indication of performance (what), and an indication the actions needed to change performance (how), whether that action is to rectify a problem or improve performance. Dashboards are a product of a security Kaizen deployment project, and are essential for ongoing management and optimization.

By analogy, a school report card of a student's grades is a type of scorecard. The report card indicates only that action may be required. The report card does not suggest what action is required to improve the student's grades.

12 What does a Security Kaizen effort look like?

A basic Security Kaizen effort is divided into two major parts:

- Deployment. Deployment is a project with specific and bounded scope, time and effort. Deployment includes defining, designing, developing, installing and operating the performance management system.
- Optimization. Optimization comes after the performance management system is deployed. Optimization projects aim to improve or otherwise optimize performance. Expect that the optimization projects will also revisit deployment, as more information is obtained.

There is also a nominal part-time maintenance effort that is required to ensure the continuing integrity of the performance management system after deployment, regardless of whether any optimization projects are undertaken.

13 Why separate deployment and optimization?

We can reasonably predict or bound the time and effort required for a deployment project. It is impossible to estimate optimization effort in advance—each optimization project will have specific goals, scope and effort. The degree and speed of optimization depends on business objectives and priorities, the complexity and maturity of the process, the frequency, quantity and quality of data available for analysis, and the knowledge and skill of the people involved.

14 How long does a deployment project take?

A good target for a basic Security Kaizen deployment project is 12-14 weeks. While some efforts may demand a longer and more complex project, it is generally preferable to keep the project duration short enough that the team can keep the goal in sight, while providing sufficient time for analysis and reflection.

15 Who is involved in a deployment project?

The Security Kaizen philosophy is that the people who operate a process are the people who know the process best (the "process" or "gemba" members). Those people are the heart of deployment and optimization efforts, facilitated and advised by other subject matter experts as needed.

The core team typically consists of 4-5 process members and 1-2 Security Kaizen experts and facilitators. Those core members are involved in all activities.

Additional team members who participate on an as-needed basis include a management sponsor or champion, process owner, financial or cost-accounting analyst, and data collection/presentation analyst. Continuity, cohesion and efficiency require that both core and as-needed team members be permanent (or as permanent as possible) for the duration of the deployment effort.

Involvement by others in the organization is generally limited to focused interviews of key process customers. Those interviews provide the "voice of the customer" (VoC) and are an essential input to the project. Customers may include down-stream process owners, upper management, and those involved in risk management, compliance and audit.

16 What is the level of effort for a deployment project?

Expect a total of 250-400 effort-hours for a 12-14 week Security Kaizen deployment project. That includes a core team of 5-6 people and 3-4 other members on an as-needed basis. Customer interviews generally consume a very small portion of the overall effort.

A project involves both group and individual work. All core team members participate in weekly team meetings, working as a group. Each week focuses on specific tasks and milestones, and includes just-in-time and hands-on training in the tools and techniques required to perform the tasks. Approximately half of the work is conducted as a group.

17 What is the return on investment?

Return on investment depends on the effort required for deployment of the performance management system, the opportunities for optimization, and the investment required to exploit those opportunities. Except as noted below, those factors cannot be estimated with any accuracy in advance.

Long-term benefits also accrue from increasing organizational capability. In order to build that capability, early projects are typically, and intentionally, limited in scope, with correspondingly modest returns. Eventually teams will leap tall buildings in a single bound, but that will come only after discipline, exercise and experience.

18 Who is Certified Security Solutions, Inc.?

Certified Security Solutions (CSS) specializes in information security consulting. We help our clients maximize the performance of their existing investments in technologies and capabilities. Our services and expertise include enterprise security strategy, authentication and authorization solutions, and application and platform security.

For more information, please contact:

Certified Security Solutions, Inc.
http://www.css-security.com
sales@css-security.com

550 Kirkland Way
Kirkland, WA 98033
425-216-0720