Key Performance Indicators for Security Governance, Part 1

Having reliable metrics or key performance indicators (KPIs) in the field of information security is a prerequisite to building a successful security program. Measuring operational efficiency, costs and benefits has always been a concern for managers, and information security is no exception. Security officers encounter difficulties in communicating the added value of IS for business, particularly because of the lack of clearly defined standards and measurement objectives.

There are several principles to help chief information security officers (CISOs) develop metrics intended for governance bodies and decision makers. These fairly generic principles can then be adapted by security officers to establish a catalog of metrics within the frameworks of their organizations.

Why It Is Important to Measure Security

Building IS controls to mitigate risk is not enough.[1] Security is seen as a means to achieve business objectives, but ever-increasing investments in security can foster a sense of frustration and misunderstanding among senior executives.[2] Measuring the added value of security is essential for good governance. Senior management, who is ultimately accountable for security, requires relevant KPIs to assess the adequacy of a security program. It needs a pragmatic approach to monitor the effectiveness of security countermeasures, adjust investments, and fine-tune the security program and strategy. Steering efforts toward defined strategy and goals is not possible without relying on agreed-upon means to measure success or progress toward defined objectives. Specific metrics are also requested by different regulatory frameworks.

Questions such as "Is our security adequate?," "To what extent does information security contribute to business objectives?" and "Can we reduce IS spending?" are not just legitimate, they are essential.[3] Assessing the effectiveness of security controls means being able to adjust programs and decide on investments.

Why It Is Difficult to Measure Security

Information security within an organization has no clearly defined dimensions. There are no universally recognized measurement standards either. The risk level or the degree of risk mitigation are often subjective and are not supported by underlying quantitative metrics. Notions such as number of incidents, level of protection, cost and return on protective measures have different meanings for different people or organizations. The adequacy or quality of security in the business context is relative and depends on many factors. For example, there is

Andrej Volchkov
Is an independent consultant in the field of information security governance and program management. He has 30 years of experience as a security program manager and is responsible for new technologies, IT change management and architecture within a major financial institution in Switzerland. He is an invited speaker at Geneva University School of Economics and Management (GSEM) Switzerland, and a speaker at several international conferences. He is a member of multiple international IT and security associations.

Enjoying this article?

- Read *COBIT® Focus Area: Information Security Using COBIT® 2019. www.isaca.org/COBIT-Focus-Area-Information-Security*
- Learn more about, discuss and collaborate on COBIT and Frameworks in ISACA's Online Forums. https://engage.isaca.org/onlineforums

no standard for measuring the adequacy of security for a given sector or enterprise size. Statistics or logs as provided in security tools (e.g., number of incidents, viruses, attempted penetrations, vulnerabilities) are generally of no help to decision makers. These metrics must be correlated with other indicators to identify trends based on defined criteria to assess costs and benefits. The fact that organizations are reluctant to share information on security events, attacks and breaches weakens the overall perception of risk among senior executives.[4]

Categorizing High-Level Information Security Metrics

Before proposing a categorization of metrics for governance, it is important to remember the requirements or questions that managers have regarding information security.[5] These are mainly needed to justify the costs, be able to anticipate the results or benefits, know at any time the level or the capacity to mitigate known or unknown risk, and be able to supervise progress toward defined objectives. Once these concerns have been determined, the following categories of metric classifications can be proposed:

- **Financial metrics**—Concerned with the financial impact of security controls
- **Maturity assessment**—Evaluates the state of security as a whole or in some specific domain such as cybersecurity, continuity, application security or management
- **Modeling**—Intends to simplify analyses in the absence of real data
- **Assumption-based measurement**—Consists of limiting and focusing measurement efforts
- **Progress toward objectives**—Consists of establishing KPIs to measure the degree of progress toward a set of given objectives
- **Operational metrics**—Articulates the effectiveness of security controls and processes
- **Cost analysis**—Provides relevant indicators for security spending governance
- **Benchmarking**—Makes it possible to compare the process in place with those of other organizations or codes of good practices

Financial Metrics

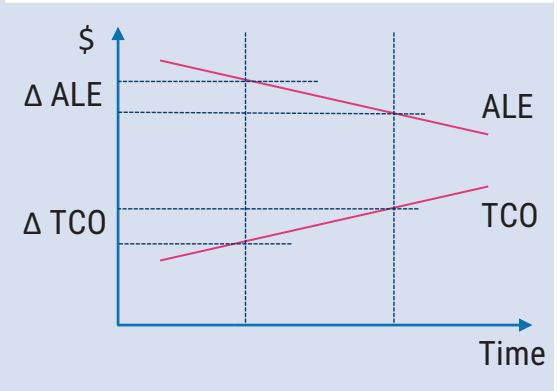
Financial metrics in the field of information security help assess investment opportunities in protection solutions or the return on security investments (ROSI). There are some widely accepted notions that can be used such as annualized loss expectancy (ALE), total cost of ownership (TCO) or economic value added (EVA).

ALE is an evaluation of potential annual losses as a result of risk impact. This assessment may concern all risk or only certain scenarios. The calculation of ALE by itself is meaningless unless it is accompanied by an assessment of the probability of risk occurrence.

The ALE measurement is better understood in relation to the TCO by comparing the trends or evolution of the two values. TCO includes all costs, hardware, software and human resources within an information security program and illustrates how much security costs.

The benefit from security investments alone or the EVA is difficult to calculate, but it can be inferred indirectly by observing variations in ALE and TCO over time. Both trends are presented in **figure 1**.

Figure 1—Example of ALE and TCO Trends



The EVA of security investments could then be expressed as:

EVA = ΔALE/ΔTCO

EVA should always be less than one for security investments to be cost effective. Indeed, if EVA is greater than one according to this formula, then the cost of security and underlying protective measures are not enough to compensate for potential losses. If EVA equals one, then security costs just barely compensate for potential losses. EVA as expressed here can be considered the same as ROSI.

Trying to calculate the global ROSI within an organization is a hazardous and difficult mission. On the other hand, it is relatively easy to calculate for some isolated technical protection solutions (e.g., antivirus protection). Delineating the scope and identifying the purpose of the measurements are key in this process. It is also essential to understand the meaning of "benefit" provided by security controls. For example, the benefit of a car's braking system is obvious. Without a clear measurement of the added value, one cannot design the metrics and calculate the ROSI. Although it may be helpful to calculate the ROSI accurately, it is more important to assess its magnitude based on risk analysis.

The benefit of security is the difference between the inherent risk (without any security control in place) and residual risk (after setting up security controls). If it is considered that countermeasures modify the probability (P) of occurrences (e.g., the probability of the occurrence of an attack decreases because of measures such as antivirus or intrusion detection), risk impacts (or ALE) can then be calculated as:

Impact of the inherent risk = Cost of incident x P(inherent risk)

Impact of the residual risk = Cost of incident x P(residual risk)

The benefit can then be expressed as:

Benefit (EVA) = Impact of inherent risk - Impact of residual risk

The ROSI can be expressed as:

ROSI = Benefit - Cost of countermeasures

If this could be a metric of the benefit of security investments, then it is very important security officers be able to demonstrate how the established (or envisioned) controls shrink the probability and/or impact level of risk occurrence.

Another financial metric that can be used is the protection capacity index (PCI), which can be expressed as:

PCI = (IR – RR) / IR

IR equals the impact of inherent risk (IR) weighted by its probability of occurrence, and RR equals the impact of residual risk (RR) weighted by its probability of occurrence. "IR - RR" represents the risk reduction capacity.

> "THE BENEFIT OF SECURITY IS THE DIFFERENCE BETWEEN THE INHERENT RISK (WITHOUT ANY SECURITY CONTROL IN PLACE) AND RESIDUAL RISK (AFTER SETTING UP SECURITY CONTROLS)."

Security control is most efficient if the PCI tends toward one. This will happen if the impact of the RR tends toward zero or if the difference between the IR and RR is very large. For these kinds of metrics to be useful, only the operational costs directly related to risk mitigation should be taken into consideration. In other words, it is important to look only at controls that reduce the impact of analyzed risk.

> "THE MATURITY ASSESSMENT PROCESS JUSTIFIES AND SUPPORTS INFORMATION SECURITY AND IT INITIATIVES IN A SECURITY PROGRAM."

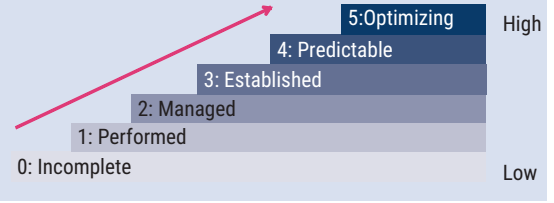
Therefore, the PCI can be used as a metric to prioritize risk mitigation initiatives.

Maturity Assessment

Governance requires simple, standardized ways to visualize the state of security or the capacity to mitigate security risk. Security posture, capacity and maturity are synonyms for means that allow the state of security to be presented in a concise and standardized way. Different standards or codes of good practices can be used under certain conditions to assess the overall security posture.

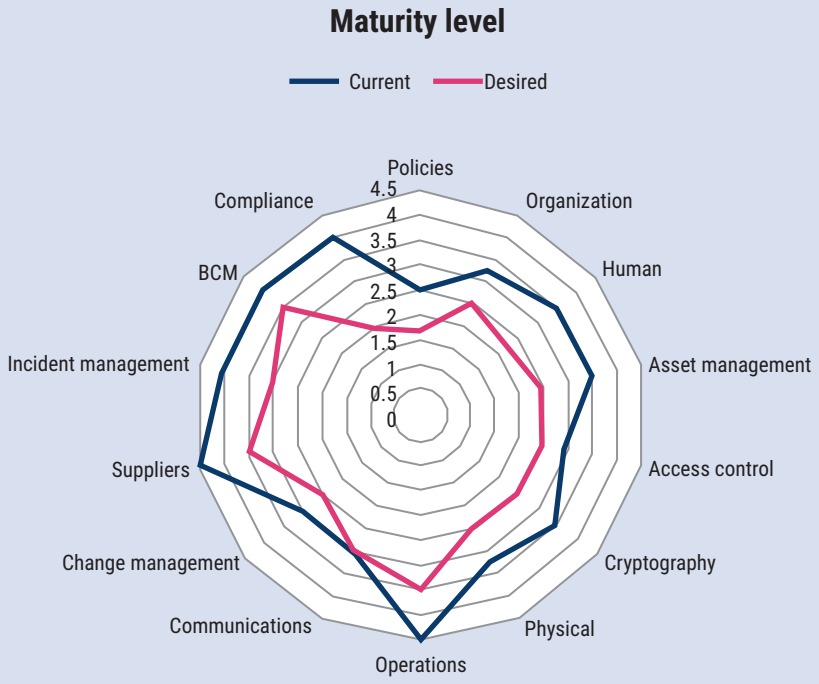
Maturity models can be used to evaluate processes or capacities according to a scale of values. Guidance such as International Organization for Standardization (ISO) Standard ISO 27001 or the US National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 *Security and Privacy Controls for Federal Information Systems and Organizations* or Cybersecurity Framework (CSF) may be used to establish a list of processes or control objectives for which maturity will be assessed. A specific maturity model then proposes evaluation criteria for each process. Many examples of value scales exist, such as ISO/International Electrotechnical Commission (IEC) ISO/IEC 15504 *Information technology—Process assessment* (**figure 2**).

Figure 2—Process Maturity Scale



The maturity model or a tool supporting it can then be used to generate a graph presenting gaps between the actual and desired maturity levels for different processes and control objectives (**figure 3**).

Figure 3—Maturity Assessment Result



Several methods or tools exist to measure the maturity of a security program, such as the Open Information Security Management Maturity Model (O-ISM3) from The Open Group.[6] Large consulting firms also offer their own maturity assessment models.

The maturity assessment process justifies and supports information security and IT initiatives in a security program. Assessing maturity, much like a risk assessment exercise, is an opportunity to discuss and compare views on security issues by involving business leaders, risk managers, auditors and other stakeholders.

Modeling

Many disciplines use models to represent complex realities to simulate and observe the behavior of a system, make "what if?" analyses, or extrapolate trends. To better understand the opportunities of using these techniques in the field of IS, one should consider the example of modeling the return on investment (ROI) in the context of a change management project.

The example in **figure 4** shows the use of modeling to assess the ROI in the context of a technology or solution change. Many change management projects can use similar techniques to evaluate the ROI of, for example, building a security operations center (SOC), installing a new intrusion detection system (IDS), strengthening authentication processes or building a role-based access control system (RBAC). It is helpful to compare the evolution of the operational costs or risk levels inherent in the current solution to the expected operational costs or risk level of the new solution. Even though the new solution may be more efficient in the exploitation or operation phase, implementation costs should not be neglected. The breakeven point is the point of time from which an ROI can be expected.

Indicators resulting from modeling will be viable only if estimated costs and benefits are managed very precisely. Another advantage of a model is the simulation of different scenarios. Changes in the breakeven point and the evolution of ROI by changing parameters such as the cost of the project and the evolution of operational expenses can be observed. This can highlight trends and delineate the confidence interval of the ROI (**figure 5**).

Figure 4—Modeling Operational Costs

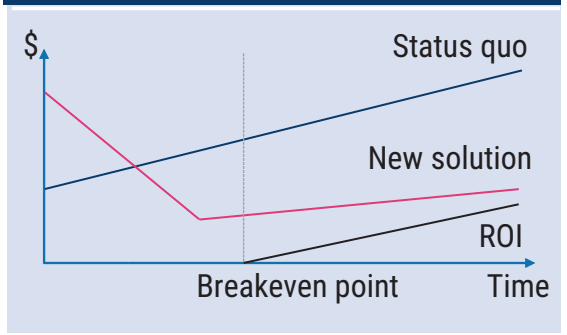
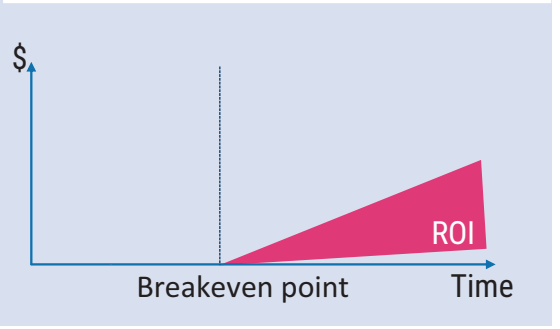


Figure 5—Confidence Interval for ROI



Assumption-Based Metrics

The saying "You cannot improve what you cannot measure" may be complemented by "You cannot measure if you do not know for what you are looking." The more complex the measurement goals, the less useful metrics will be and the harder they will be to find. A measurement goal that is simple and detailed makes it easier to define the associated metrics. For example, if it is suspected that the level of security awareness is not adequate in a business unit, the line manager can ask for specific measures to assess it.

Making assumptions about the state of a security control or process facilitates the choice of metrics that can be used to approve or disapprove them. An assumption can be broken down into several sub-assumptions to define the metrics more precisely. The example shown in **figure 6** contains three metrics that can be used to demonstrate or disprove the initial assumption.

Figure 6—Example of Metrics for Initial Assumption		
Assumption/Objective	**Sub-assumption**	**Metrics**
There is a clear service level agreement (SLA) on the time to recovery for critical processes.	All critical processes are formally identified.	Number of critical processes not formally identified
	There is an SLA for time to recovery for all identified critical processes.	Number of SLAs for time to recovery
	Recovery tests include all critical processes.	Number of critical processes tested during a period

Different assumption-based measuring methods exist such as goal, question, metric (GQM).[7]

Progress Toward Objectives

Each revision of the objectives must be accompanied by metrics expressing the degree of progress. The balanced scorecard (BSC) is a popular tool for tracking performance and progress toward goals that support the business strategy and is well known and appreciated among senior executives.[8] Establishing and monitoring information security objectives in BSC format with associated metrics is an excellent means of communication with senior management.

Financial performance is not the only perspective used to evaluate the contribution of information security toward an organization's strategy. The BSC approach advocates benchmarking according to the objectives set in four perspectives: operations, client relationship, evolution (learning and growth) and finance. The four perspectives must support the organization's strategy and vision (**figure 7**). A core question concerning information security is associated with each perspective in order to guide security officers when choosing the objectives and KPIs that will be applied.

Operational Metrics

Security operations can be assimilated into the controls set up within the framework of a security program. Operational performance or the capacity to mitigate security risk is an important criterion in the overall governance and management process. It should be measured and presented through figures, ratios and trends along with maturity and risk.

Figure 7—Security BSC Perspectives

Source: Based on Kaplan, N.; *The Balanced Scorecard: Translating Strategy Into Action*, Harvard Business Review Press, USA, 1996.

Because there is no standard checklist of processes or controls to be measured, it can be useful to establish a security control catalog. Then security officers can identify the most important controls that directly support business initiatives and measure their performance. **Figure 8** shows an excerpt of operational metrics with trends.

Cost Analysis

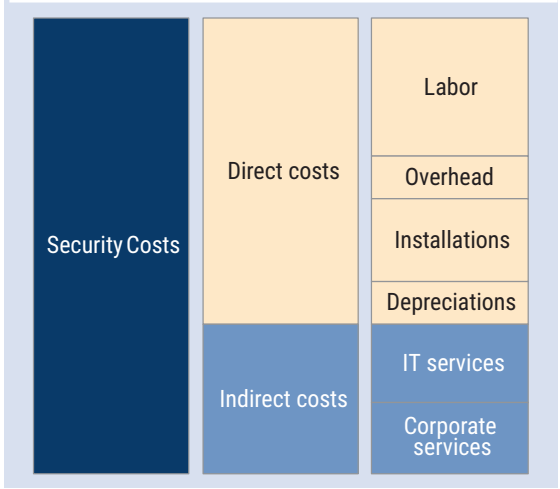
The overall cost of security and the evolution of TCO can be important indicators for governance, especially if they are related to other indicators such as the evolution of the organization's overall expenses, the number of employees, the evolution of risk and business performance. Senior managers are accustomed to analyzing costs. Information security officers should be able to present cost analysis using the same format and

Figure 8—Example of Operational Metrics With Trends		
Measurement Objective	**Metric**	**Trend**
Awareness efficiency	Percentage of employees trained on high risk	↘
Efficiency in resolving audit findings	Average delays in the processing of security audit findings	↗
Configuration management	Number of patched systems/number of systems to be patched	↘
Incident handling	Mean time to resolve incidents	↗
	Average effort for specific analyses and requests over a period of time/number of employees	↘

vocabulary used for other business units, products or services.[9]

One example of cost categories within TCO is presented in **figure 9**.

Figure 9—Example of Security Cost Breakdown



Costs or expenses can be categorized in different ways, taking into account the objectives of the analyses that management needs. For example, to figure out the proportion of the cost of external services (consulting) out of overall costs, a special expense account needs to be used to log that information. Defining cost categories at a higher level of the organization can help greatly to build useful metrics for cost analysis.

Benchmarking

Benchmarking is appreciated by senior executives because it helps to compare the state of security or some of its domains with established standards of best practices and compare the results of different strategies among similar enterprises. However, apart from comparing public financial results, it is difficult to compare IS processes because operational data are not available.

Different techniques can be used to figure out trends with some tangible data that can be used for benchmarking, for example:

- Studies or surveys by consulting or advisory firms
- Results of surveys among similar organizations or during forums
- Studies conducted by business associations within a given sector
- Mandating consultants specialized in conducting benchmarking

> "HAVING CLEAR INSIGHT INTO THE OBJECTIVES OF MEASUREMENT IS ESSENTIAL BEFORE CHOOSING AMONG THE DIFFERENT CATEGORIES OF METRICS."

Conclusion

Having metrics or KPIs is essential for good governance. These indicators help answer the

> "THE MORE COMPLEX THE MEASUREMENT GOALS, THE LESS USEFUL METRICS WILL BE AND THE HARDER THEY WILL BE TO FIND."

questions that managers ask and, thus, facilitate the adjustment of the information security program. However, defining metrics requires effort on the part of executives, security officers and operations professionals. Using technical metrics for communication with senior executives should be avoided. It should be kept in mind that it is essential to answer the questions that managers ask using the language they understand. Having clear insight into the objectives of measurement is essential before choosing among the different categories of metrics presented herein. There are no widely accepted standards, as security metrics must be tailored to the needs of each organization under the responsibility of the security officer. The security metrics presented should be used when reporting to the board and senior management. This article is the first of two that deal with the issue of articulating the value of information security. The second one, "Key Performance Indicators for Security Governance, Part 2," will tackle designing annual security reports.

Endnotes

1 Lingeswara, R.; S. Tammineedi; "Integrating KRIs and KPIs for Effective Technology Risk Management," *ISACA® Journal*, vol. 4, 2018, *www.isaca.org/archives*

2 Brenner, B.; "Companies on IT Security Spending: Where's the ROI?" *CSO Online*, 25 January 2010, *www.csoonline.com/article/2124757/companies-on-it-security-spending—where-s-the-roi-.html*

3 Slater, D.; "Security Metrics: Critical Issues," *CSO Online*, 12 November 2012, *www.csoonline.com/article/2123361/security-metrics—critical-issues.html*

4 Volchkov, A.; "How to Measure Security From a Governance Perspective," *ISACA Journal,* 2013, *www.isaca.org/archives*

5 Bakshi, S.; "Performance Measurement Metrics for IT Governance," *ISACA Journal*, vol. 6, 2016, *www.isaca.org/archives*

6 The Open Group, *Open Information Security Management Maturity Model (O-ISM3)*, Version 2.0, USA, 2017, *https://publications.opengroup.org/c17b*

7 Basili, V. R.; G. Caldiera; H. D. Rombach; *The Goal Question Metric Approach, Institute for Advanced Computer Studies*, University of Maryland, College Park, USA, 1994, *www.cs.umd.edu/users/mvz/handouts/gqm.pdf*

8 Kaplan, N.; *The Balanced Scorecard: Translating Strategy Into Action*, Harvard Business Review Press, USA, 1996

9 Volchkov, A.; *Information Security Governance: Framework and Toolset for CISOs and Decision Makers*, CRC Press, USA, 2018