Key Performance Indicators for Security Governance, Part 2

Security Reporting for Senior Management

The value of information security may be understood differently within an enterprise. For security specialists, the need for protective measures against known threats is sufficient to justify investments. However, management wants higher level reports presenting results based on figures and understandable ratios to justify the investment in information security. Business unit managers may also not recognize the need to participate fully in the decisions on financing the overall information security infrastructure.

Good governance relies on reports based on key indicators to assess the adequacy of information security, the quality of the security program, return on security investment (ROSI) and progress toward objectives. Security officers are responsible for providing reports that communicate the value of security to work with senior executives to facilitate decisions.

Since security is embedded in many business activities throughout the enterprise, compliance requires a multidisciplinary approach to provide the necessary data to gain support for information security initiatives. Since chief information security officers (CISOs) increasingly report at a higher level in the enterprise and often outside of IT, data are needed to explain the importance of adequately supporting information security financially. These reports should provide near-term costs/benefits for project investments but also articulate the contribution of information security to the enterprise as a whole.

The main goal of these high-level reports is to determine:

- How information security contributes to business development
- Whether information security investments are justified
- What the key information security initiatives are and why they are needed

The elements needed to develop security reports for governing bodies and decision makers that support their decisions are outlined here. The goal is to explain the importance of enterprise-oriented communication and propose a reporting structure based on several strategic key performance indicators (KPIs). This is the second of a two-part series that builds on the metric concepts described in the previous article, "Key Performance Indicators for Security Governance, Part 1."[1]

The Importance of Information Security Reporting for Governance

Good governance relies on reports based on strategic KPIs to assess the information security program. Reporting and oversight provide governing bodies with all the relevant information needed to assess the state of security at a particular point in

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.

time and provide guidance for decision-making. The new position of CISOs as advisors for security and compliance requires proper communication. Security reports are useful only if they use language senior executives understand.

Producing relevant strategic KPIs that are understandable throughout the enterprise enables security officers to strengthen information security's position as a business partner. Strengthening information security's position also helps establish a security culture and the perception of the true value of information security in different business units. Because executives' main concerns are increasing revenues, reducing costs, and improving product quality and services, information security reports are only taken into consideration if they adopt the same business viewpoint using the same language: strategic and functional alignment, achievement of performance objectives, risk mitigation, and adding value for customers.

Security risk areas must be assessed based on outside and inside key risk indicators (KRIs). The rationale for risk assessment should be made accessible to senior management through high-level strategic indicators. Inaccurate information and incomplete financial justification undermine the credibility of information security and weaken the position of security specialists. Therefore, reports should contain KPIs, along with universally accepted units of measurement such as cost, risk, budget, strategy and target.

> "THE RATIONALE FOR RISK ASSESSMENT SHOULD BE MADE ACCESSIBLE TO SENIOR MANAGEMENT THROUGH HIGH-LEVEL STRATEGIC INDICATORS."

Strategic Indicators of a Security Reporting System

Strategic indicators are high-level operational metrics. These indicators are used to present the state of information security from different perspectives.[2] Structuring questions and proposing strategic indicators that answer those questions can help identify the best strategic indicators to be included in the report. The top question concerns the security program itself: Why do we need to invest more in information security? The answer to this question can be found by understanding planned change projects and operational costs of the security program. Projects to change or improve information security capabilities (e.g., improving the intrusion detection system [IDS] or raising the level of awareness of risk among employees) can be triggered only from one of the following sources:

- **Strategy**—Strategic initiatives as defined in the information security strategy
- **Risk**—Mitigating security risk as defined in the action plan
- **Regulatory gaps**—Closing the gaps
- **Maturity**—Improving the level of maturity

The security program will not propose initiatives apart from those coming from one of these sources. In other words, if a security project is not triggered by strategic alignment, the need to mitigate a risk, the need to fill a regulatory gap or the need to improve capacities to protect company assets, then there is no reason for senior executives to approve it.

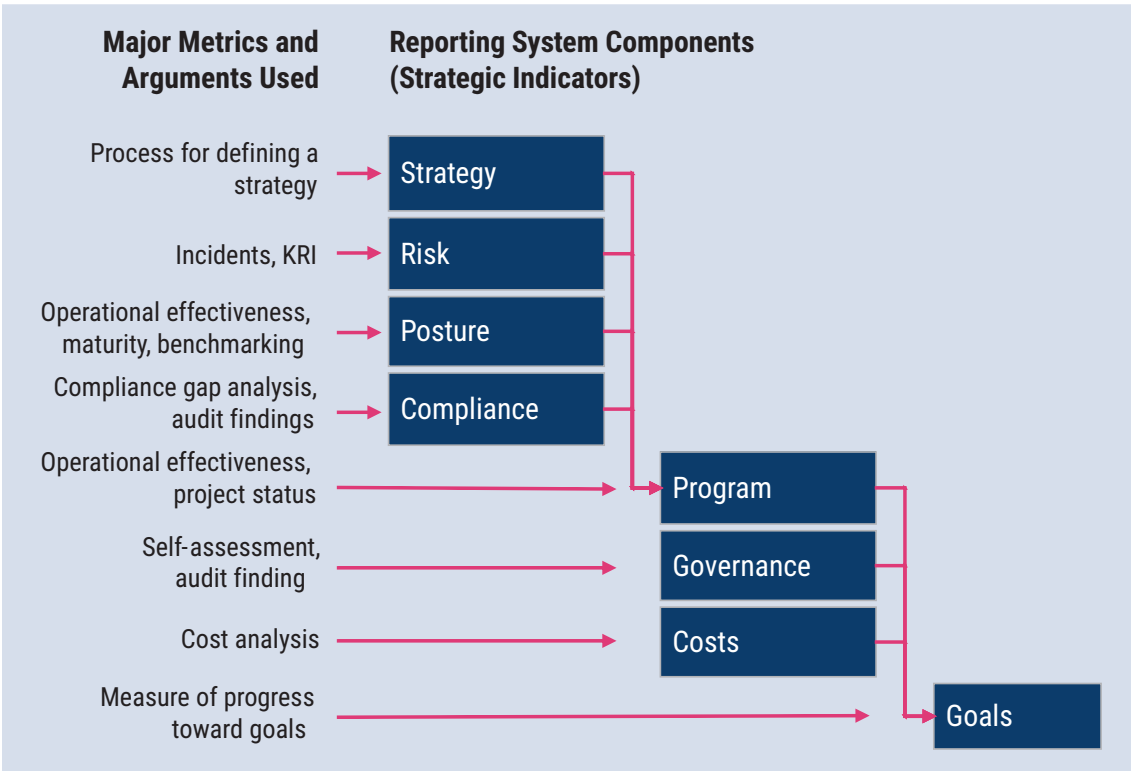
Apart from understanding the imperatives linked to the security program, senior managers are deeply concerned with how information security is managed and the evolution and nature of the associated costs.

It is helpful to break down the strategic or high-level indicators that should be included in annual information security reports (**figure 1**), along with some major metrics used to produce those strategic indicators.[3] The breakout of strategic indicators as proposed here can also be used to structure the composition of the report itself.

The main questions that these indicators must answer are the following:

- **Strategy:**
  - How does information security contribute to achieving the enterprise's strategy?
  - What are information security strategic initiatives?

Figure 1—Strategic Indicators



- **Risk:**
  - What are the enterprise's main security risk areas?
  - What is the action plan to mitigate the security risk?
- **Posture:**
  - What is the enterprise's information security maturity level?
  - Which processes/controls need to be improved and why?
- **Compliance:**
  - What are the enterprise's major information security compliance and audit gaps?
  - What is the status of fixing the compliance and audit gaps?
- **Program:**
  - What does information security do and why is it important to the enterprise?
  - Why does the enterprise need to invest more in information security?
- **Governance:**
  - What improvements could be made in the governance/management process?
- **Costs:**
  - What comprises the enterprise security costs?
  - How do information security costs relate to other enterprise costs?
- **Goals:**
  - To what extent has information security achieved its objectives?
  - What will be next period's goals?

A description of the strategic indicators for each of these perspectives is provided. It is not necessary to strictly follow the suggested template or compile indicators in all of these perspectives. The final information security report will depend on the target audience and their choice of specific strategic indicators. Underlying metrics and technical indicators are covered in part one of this article series.[4]

Strategy

Information security strategy should include the vision (security strategic objectives) and major initiatives that support either the security strategic objectives, business strategic objectives or compliance objectives (**figure 2**). An initiative that

Enjoying this article?

- Read *Supply Chain Resilience and Continuity: Closing Gaps Exposed in a Global Pandemic. http://www.isaca.org/supply-chain-continuity-2020*
- Learn more about, discuss and collaborate on information and cybersecurity in ISACA's Online Forums. *https://engage.isaca.org/onlineforums*

Figure 2—Security Strategy

does not support one of these three objectives would not be understood or supported by the business executive community.

It is important to remember that this is not an exercise to revise the strategy or strategic initiatives. This has already been done by a dedicated committee. What is important is to recall previously accepted strategic objectives and initiatives.

The prerequisite to be able to report on the information security strategy is the existence of the formal process of defining and revising and information security strategy and its alignment with the strategy of the organization. At the time of reporting, it must be well known by the recipients of the report to avoid unnecessary questions.

Risk

The established risk management process in the organization already includes some form of reporting to risk governance bodies or committees. For global information security reporting, there is no need to reproduce the same type of reporting. A simplified variant that includes a list of major or high risk, a reminder of action plans and the state of progress is sufficient. **Figure 3** presents an example of a synthesis of high risk with the action plan and actual status.

The level of risk is determined by its probability and its potential impact and can be classified in categories: low (L), medium (M), high (H) and extremely high (E), according to the risk appetite of the organization.

To provide this kind of reminder of the main risk factors and action plan, a risk management process must be established and be repeatable. The metrics and KRIs used in the risk assessment should not be presented here, but will be made available if additional information is needed.

Figure 3—Reminder of the Main Risk and Action Plan

Risk	Residual Level	Trend	Key Indicators	Actions	Status	Planned Level
External fraud	H	↗	• Number of attempts • Damage suffered • Reaction time	• Awareness • Revision of guidelines • Means of detection • External coordination	According to plan 60 percent	M
Third-party intrusion	H	→	• Penetration test results • External statistics	• Awareness • Elimination of venerabilities • Prevention improvement	According to plan 50 percent	M
Web server attack	H	→	• Result of penetration tests • Level of server updates	• Upgrade configurations	Late 20 percent	M
DDoS (distributed denial of service)	E	↗	• Observations in similar industry	• Migrate to Domain Name System (DNS) provider protection	Urgent	M

Posture

Governance requires simple, standardized ways to visualize the current and desired state of information security. Security posture, capacity and maturity are synonyms for means that allow the state of security to be presented in a concise and standardized way. For each major security process or control objective, security posture or maturity can be presented as a graph containing an evaluation of the current maturity level, the desired maturity level and the perceived gap between the two (**figure 4**).

A maturity assessment process should be established and accepted. It can be conducted using maturity modeling tools, through a benchmarking study, by mandating an external consultancy or by completing an audit. Regardless of the model chosen to present the security posture, it should be accompanied by supporting documents to better explain any differences in current and desired maturity.

Compliance

Compliance gap analyses and audit findings have established priorities among information security initiatives and projects. Reviewing these projects and priorities should not be part of reporting because it is the responsibility of other forums or committees. However, it is very important to report to governing bodies on the overall capacity and issues in the process of remedying these gaps. High-level indicators that could be presented here include the evolution of the number of unfixed gaps or delayed remedies compared with the number of new audit findings.

In the example shown in **figure 5**, the delay in fixing audit findings may indicate a lack of resources, a prioritization conflict or some other issue that governance should address when setting objectives.

The process of compliance gap analysis must be established and well understood by senior management. The aim here is to point out the problems and solutions that may lead to better management of these activities.

Program

A security program is composed of a set of operational controls and an improvement plan with

Figure 4—Example of Current and Desired Maturity Level Presentation

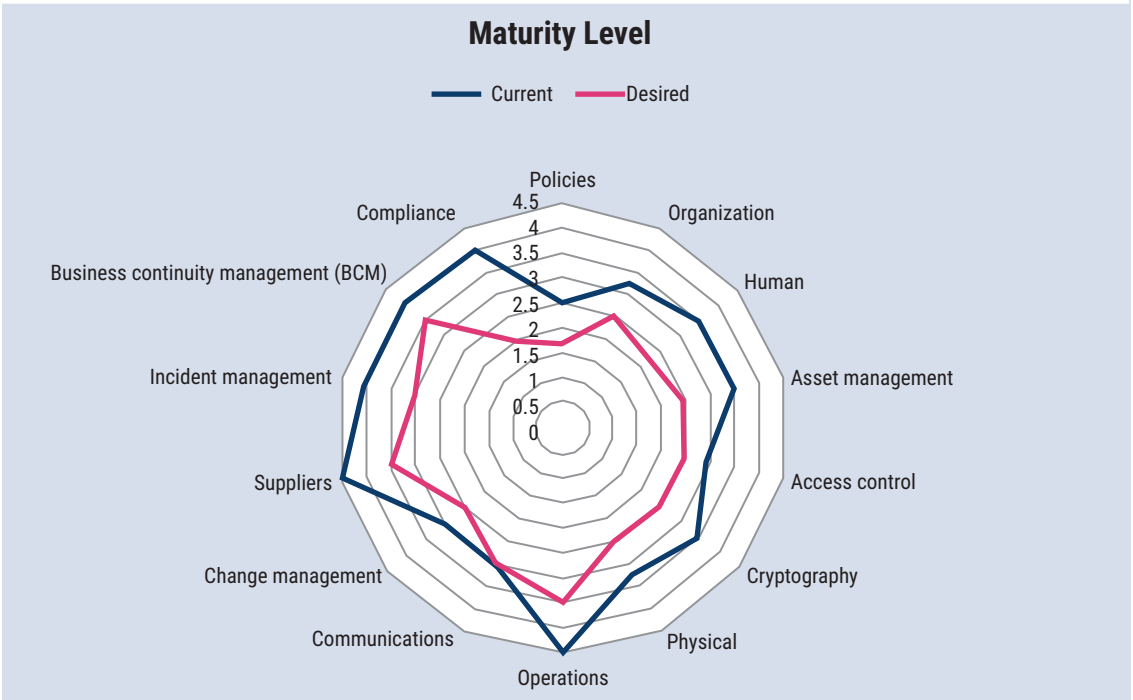
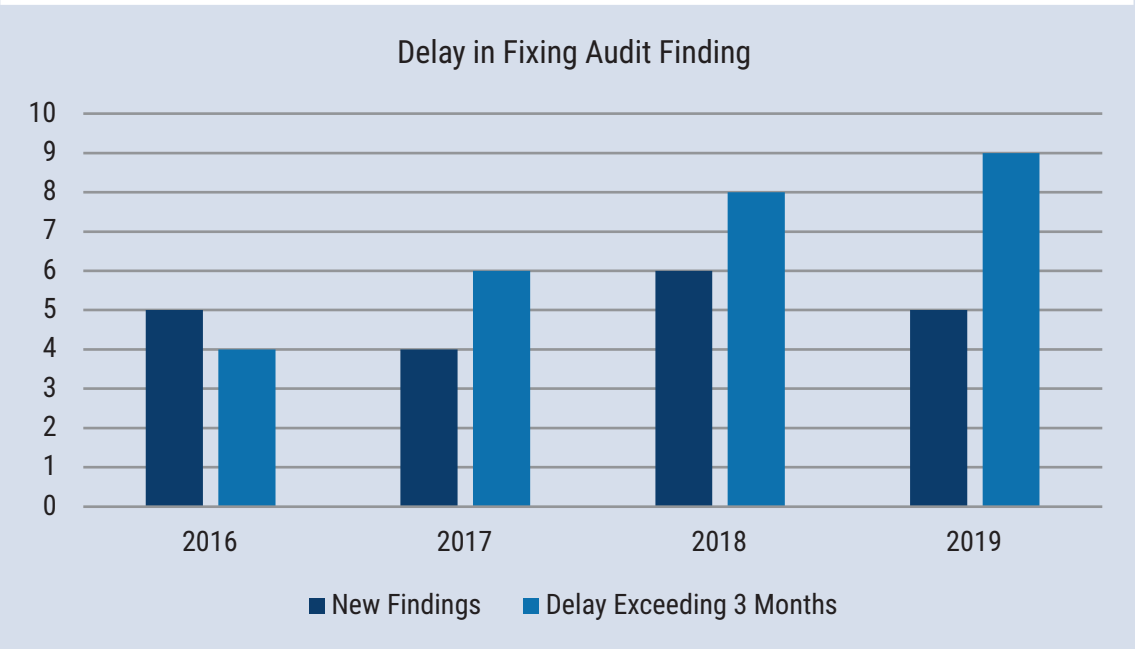


Figure 5—Statistics on the Number of Gaps/Findings and the Capacity to Resolve Them



a road map of projects. The program is sometimes called a business plan or information security road map. Security programs mobilize resources, and their objectives must be justified (explained). The rationale of each project should be presented with origin, dependencies, duration and outcome.

As noted previously, no initiative or investment can exist if it does not support strategy, risk mitigation, capacity improvement and reduction of compliance gaps. The previous four strategic indicators are a prerequisite to presenting the state of and changes in the security program (**figure 6**).

> "NO INITIATIVE OR INVESTMENT CAN EXIST IF IT DOES NOT SUPPORT STRATEGY, RISK MITIGATION, CAPACITY IMPROVEMENT AND REDUCTION OF COMPLIANCE GAPS."

The goal is not to discuss project status because this is dealt with in other committees. However, if there are recurring problems in delivering the program, such as delays due to a chronic lack of resources or changes in priority, these issues must be clearly raised.

Governance

Presenting the strengths and weaknesses of governance in a report is not only a sign of high maturity, but also a means of communication and coordination among partners for continuous improvement. To assess gaps in the governance process, standards can be used, such as International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) ISO/IEC 27014:2013 *Information Technology—Security Techniques—Governance of Information Security*,[5] or some specific recommendations or code of good practices. A self-assessment result could thus be used to report on the adequacy of information security governance in the organization.

The example in **figure 7** presents a short summary of findings after an IS governance self-assessment exercise using the Three-Level Control Framework (TLCF).[6]

Figure 6—IS Program and Its Origins

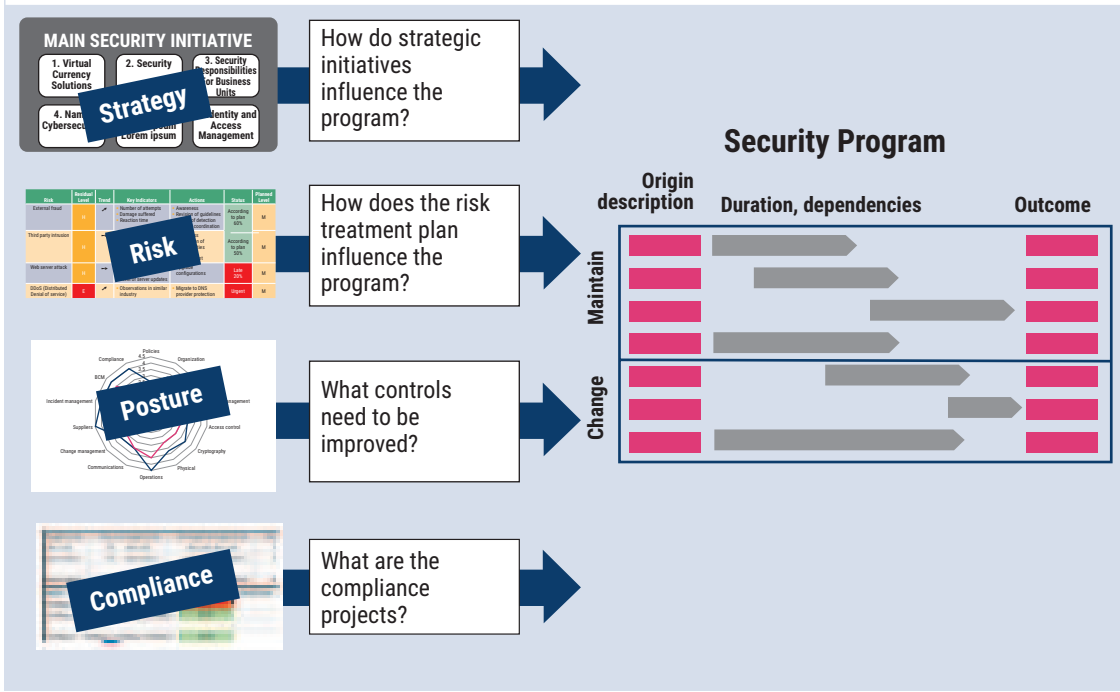


Figure 7—IS Governance Self-Assessment Result

Policies

Needed

- Review the documentary framework of the policies and guidelines and provide better readability.

Strategy

Strongly needed

- Review the security strategy.
- Align security initiatives with business objectives.

Organization

Strongly needed

- Appoint a security delegate in each business line to participate in quarterly security project review meetings.

Risk

No improvements needed

Program

Strongly needed

- Set up a committee to validate information security initiatives and projects.

Reporting

No improvements needed

Assets

Strongly needed

- Define data classes and categories and inventory them in a catalog.
- Identify data owners for each class/business line.

Compliance

Needed

Set up an employee awareness program regarding the legal and regulatory framework that impacts security.

Metrics

No improvements needed

To strengthen information security oversight, the organization should adopt some kind of information security governance self-assessment, revision process or consultancy commissioned by the board of directors or senior management. It should be noted that the issues concerning policies, organization (people) and asset management fall under this chapter. Some organizations may prefer to separate these issues and provide specific strategic indicators for them.

Costs

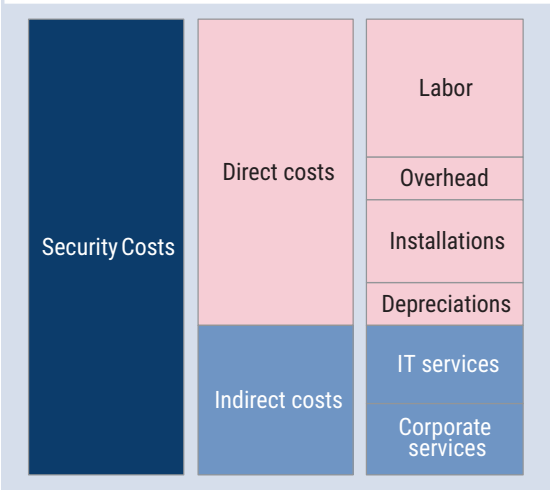
To present the structure of information security costs, standard cost accounting principles and the same formatting as in other units within the enterprise should be used. Data related to information security costs, combined with other indicators such as IT costs, financial results and number of employees, will enable the board of directors or governing body to better understand the information security footprint in regard to overall cost/benefit analyses.

Reporting on overall security costs should include a breakdown of direct and indirect costs. Direct costs are those generated by the activities of the security team itself. They can be further broken down into labor, overhead, and amortization or depreciation. Indirect costs are costs attributed to security but not generated directly by security team activities. Examples are IT operations related to security, human resources services, corporate functions or general services. These costs are often underestimated or neglected for information security precisely because of the absence of accounting methods to highlight them.

An example of a security cost breakdown is presented in **figure 8**.

> "AS THERE IS NO DEFINED STANDARD, SECURITY OFFICERS ARE INVITED TO FIRST LISTEN AND UNDERSTAND THE REAL NEEDS OF GOVERNING BODIES AND THEN PROPOSE SUITABLE METRICS AND REPORTING FORMATS TO SATISFY THEM."

Figure 8—IS Cost Breakdown



The following indicators can be included in the report as needed:

- Evolution of the costs of each category
- Evolution of costs compared with other indicators, such as turnover, number of employees and budget
- Breakdown of expenses among other business or geographic units
- Distribution of expenses by service provided within information security (business continuity, operations, physical security or safety)

Cost accounting needs defined coding standards for expense accounts within the organization. Only then can information security use the same standards to produce its own cost accounting report.

Goals

The last section of the report should give perspective on overall goals for information security for the next period. Based on everything that was mentioned previously, the governing body needs some perspective on achieved and new goals. The most common way to present and communicate on objectives is to use a balanced scorecard (BSC) for information security.[7] Metrics and targets must be associated to objectives to facilitate revision, communication and evaluation of achievements.

An example of a formal presentation of objectives is given in **figure 9**.

Figure 9—Example of Presentation of Objectives With Associated Metrics and Targets in a BSC Format

Perspective	Objectives	Metrics	Target	Projects
Finance	• Reduce, percentage	• Investments • Ratios	• Costs	• •
Operations	• Contribute • Improve	• Number/trend • Efficiency	• Operational KPI	• •
Customer	• Enable • Provide	• Time • Service	• Level of service	• •
Capacity	• Policies • Awareness • Controls	• Evaluation • Readiness • Gaps	• Maturity level	• •

Conclusion

Information security governing bodies and general management need reporting from security officers on a regular basis to assess the information security program and be able to fully exercise their responsibilities. In the absence of a clear vision on the costs, benefits, priorities and risk, senior managers cannot steer the security program and expose themselves to the risk of incidents, noncompliance and financial losses. Reporting also serves as a communication tool and reinforces a security culture among all the stakeholders. The few high-level or strategic indicators presented convey overall information on the state of information security for this purpose. However, strategic indicators must be previously accepted by the executives, because the indicators become an important support in the process of governance. As there is no defined standard, security officers are invited to first listen and understand the real needs of governing bodies and then propose suitable metrics and reporting formats to satisfy them.

Endnotes

1 Volchkov, A.; "Key Performance Indicators for Security Governance, Part 1," *ISACA® Journal*, vol. 6, 2020, *https://www.isaca.org/archives*

2 KPMG; "Connecting the Dots: A Proactive Approach to Cybersecurity Oversight in the Boardroom," 2016, *https://assets.kpmg/content/dam/kpmg/pdf/2016/01/cyber-security-oversight-in-the-boardroom-2016-au.pdf*

3 *Ibid.*

4 *Ibid.*

5 International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC), ISO/IEC 27014:2013 *Information Technology—Security Techniques—Governance of Information Security*, Switzerland, 2013, *www.iso.org/standard/43754.html*

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

7 Kaplan, R.; D. Norton; *The Balanced Scorecard: Translating Strategy Into Action*, Harvard Business Review Press, USA, 1996