Communicating Information Security Risk Simply and Effectively, Part 2

A Three-Step Process for Top Management

The ability to answer top management's questions is the first step to being successful in presenting information security risk effectively. In enterprise risk management, the difficulty is to combine different data and, at the same time, be able to provide the necessary details without relying on overly specialized arguments, as discussed in "Communicating Information Security Risk Simply and Effectively, Part 1."[1] In the case of enterprise communication, the loss or deviation from specialist detail is counterbalanced by a gain in expository clarity. The correct assessment of information security resources is a benefit for the effectiveness of the whole information and communication technology (ICT) process.

From Threats to Enterprise Risk

Many of the risk factors of ICT processes are at the operational level, while the decisions to counter them are made at the top level of the enterprise. This means that after having illustrated the severity of the threats for each process impacted to management, with respect to enterprise objectives, it is necessary to expand on the discussion, providing a more detailed level of exposure to clarify the risk scenario and describe the consequences of acting or not acting. The ultimate decision maker is often in an organizational position that does not have detailed knowledge of specialist operations.

The description of the risk context of each relevant resource is the first level of detail required, and it should be focused on the importance it has for the business and for all related processes. Detailed technological discussions of the topics should be avoided. Once the presentation of the risk scenario has been completed, if additional details are requested, an organizational description of the actions involved is used, describing the roles impacted, the attributions of responsibility and the links with the other processes. This way of balancing organizational, operational aspects and overall references creates a contextual perspective that facilitates understanding of the topics without requiring too much technical detail.

Exposing the Context of Risk

The in-depth analysis of the threat scenario should focus on one single risk at a time and should be connected to the processes involved, including the

Luigi Sbriz, CISM, CRISC, CDPSE, ISO/IEC 27001 LA, ITIL v4, UNI 11697:2017 DPO
Has been the risk monitoring manager at a multinational automotive company for more than seven years. Previously, he was responsible for information and communications operations and resources in the Asia and Pacific Countries (APAC) region (China, Japan and Malaysia) and was the worldwide information security officer for more than seven years. He developed an original methodology for internal risk monitoring, merging an operational risk analysis with a subsequent risk assessment driven by the maturity level of the controls. He also designed a cybermonitoring tool and an integrated system involving risk monitoring, maturity modeling and internal auditing. Sbriz was a consultant for business intelligence systems for several years. He can be contacted on LinkedIn (*https://it.linkedin.com/in/luigisbriz*) or at *http://sbriz.tel*.

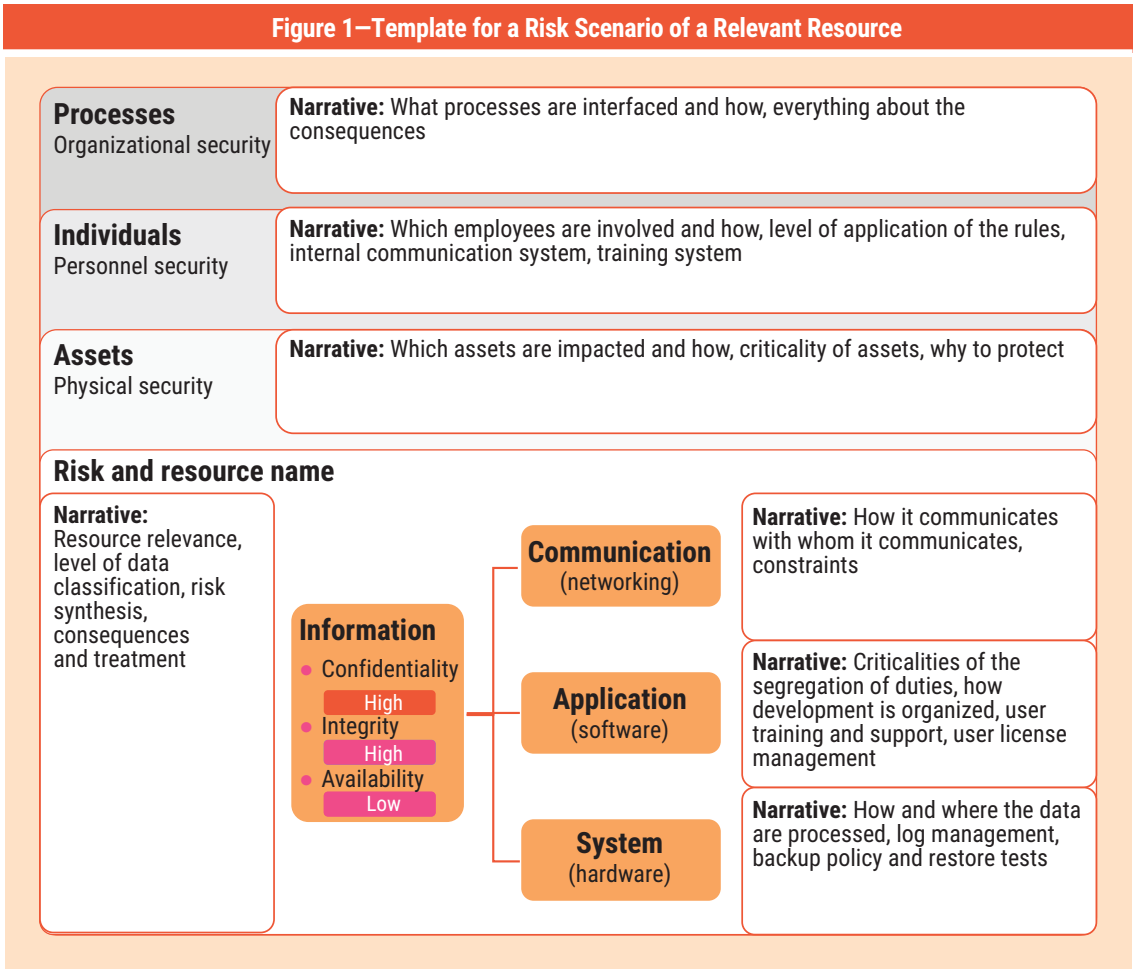
human resources involved and the assets used. It should also contain a description of the value of the resource to be protected. Finally, all the information summarized in this prospectus should be presented in a way that can be understood by top management. A template for this prospectus is shown in **figure 1**. Attention is drawn to the center of the chart, where the resource to be protected is described.

A report that provides risk information for a specific resource can be thought of as consisting of two parts: The central part describes the resource (or group of homogeneous resources), the reasons for protecting it and its critical implementation elements, and the outer part briefly describes the business context that will suffer consequences if risk mitigation measures are not taken.

The business context is defined by three areas—processes, individuals and assets—each of which describes its current state, with an emphasis on requirements, criticalities and the severity of consequences. This information is presented in narrative form. Because the three narratives of the business context are on the same level and must be considered together, there is no need to highlight one area over another, such as with the use of colors. The three areas and the main issues that must be dealt with are:

- **Processes**—With a focus on organizational security. The narrative describes the importance of the interfunctional relationships between the processes involved and any business continuity problems in the event one of these processes is compromised. It indicates any critical issues related to the quality of the process governance system (set of procedures).
- **Individuals**—With a focus on personnel security. The narrative describes the importance of the assigned rules and adherence to the training plan to spread knowledge and ensure compliance. Compliance with the rules and the scheme for assigning responsibilities should be verified.

Figure 1—Template for a Risk Scenario of a Relevant Resource



Critical issues related to the internal climate, the lack of skills, the need to increase the workforce or the risk of losing know-how should be addressed. In general, behavioral rules for physical environments, individual equipment, interpersonal relationships and activity on digital platforms should be implemented.

- **Assets**—With a focus on physical security. The narrative describes the importance of the assets used to support the resource to be protected and the methods of accessing and using it. This includes the control measures for physical access, the necessary infrastructure and equipment, the importance of physical areas with limited access, and the purposes of the video surveillance system. The critical functional services related to the resource or its protection should be highlighted.

The resource to be protected is assessed based on compliance with the objectives of the confidentiality, integrity and availability (CIA) triad[2] and the functional requirements of communication, applications and systems. The resource can be any asset, either tangible or intangible, or a group of homogeneous assets in terms of risk management.

The narrative briefly highlights the resource's importance, the classification of data, the risk of failure to meet objectives, the potential consequences and the treatment proposal. Data classification is expressed through the CIA triad using a color that indicates an expected deviation from the objective based on current risk. Additional information can be inserted, creating a kind of to-do list (e.g., a schematic business plan for risk treatment, relevant clauses of the service-level agreement [SLA] in outsourcing contracts[3] or escalation rules for incident management).

The operational areas of the resource are divided into three parts, each with its own brief description. The aim is to describe the functionalities or highlight the critical issues. The narrative area can be left empty if it is not relevant to that particular resource.

Networking is part of the communication and data sharing process. Typical issues include segregation of the network; use of virtual private networks (VPNs), encrypted channels, email and chats; behavior on social networks; design of the network with continuity solutions; organization of remote work; network traffic control; data sharing methods; and network authentication policies.

"THE WHOLE WRITTEN PRESENTATION SHOULD HAVE A CLEAR, CONCISE LOOK, WITH SOME COLOR RELATED TO DATA CLASSIFICATION."

In the context of application and development features, software is involved. The most relevant issues include whether to acquire or develop applications, the rules of segregation of duties (SoD),[4] management of an application change, management of user licenses, rules of patch management, database administration, organization of the user ticketing service, source control, application obsolescence and vulnerability assessment.

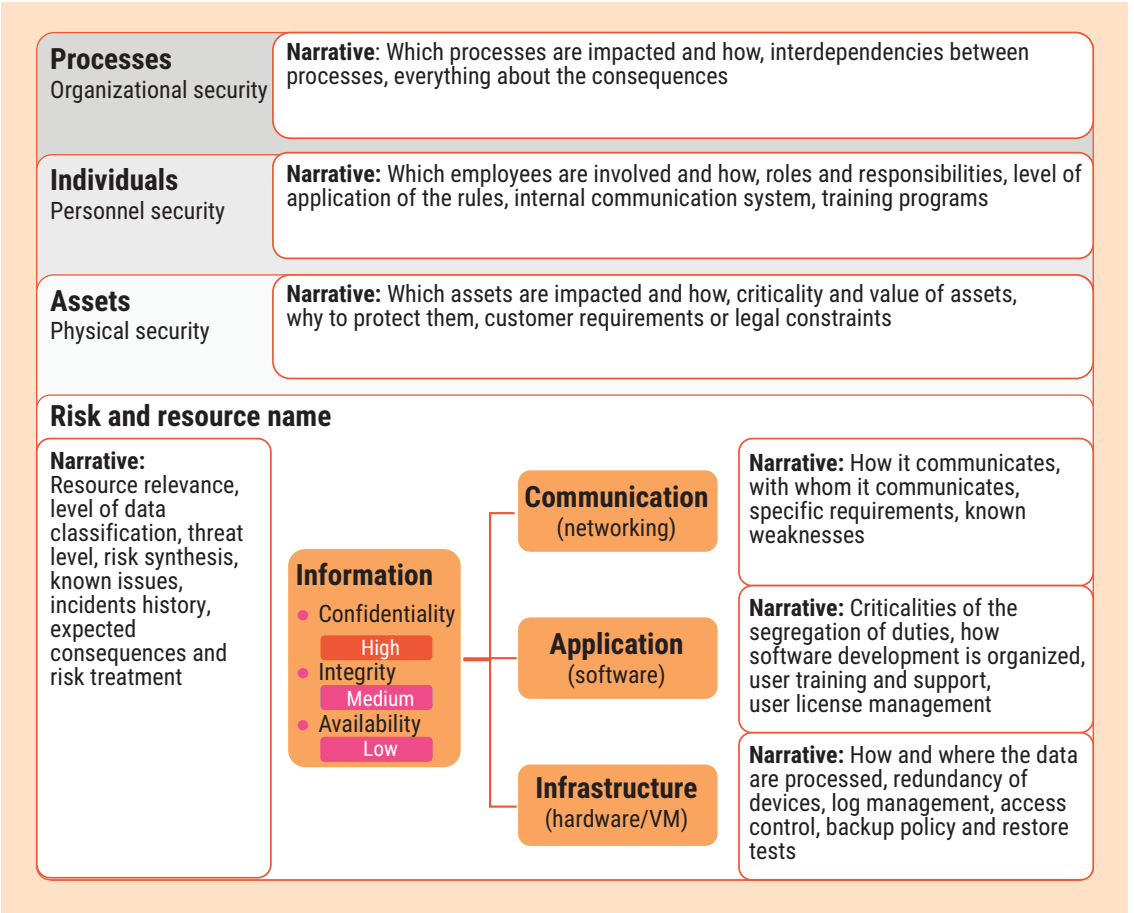
Hardware and virtualization are part of the management of data processing and data storage systems (IT infrastructure), both internal and external. The relevant issues in this area include redundancy systems to improve the resilience of equipment, system performance, use of cloud or physical systems, protection against natural events or unauthorized access, methods of surveillance of critical areas, log control procedures, and requirements and tests for historical archiving. An example of a filled-in template is shown in **figure 2**.

When writing narratives, a deliberately nontechnical style is recommended. The whole written presentation should have a clear, concise look, with some color related to data classification. The aim is to communicate the implications of the proposed actions by describing the themes from the perspective of interaction between processes and activities, rather than presenting a monothematic and technical narration of the solution. Organizational information describing business processes is balanced with activities related to the resource to be protected.

Communicating the Solution's Impact on Business Processes

If a different level of detail is necessary to better understand the organizational scenario and the involvement of individuals in addressing the risk, a

Figure 2—Risk Scenario for a Suspected Network Intrusion



new prospectus can be developed. At this stage, it is not advisable to use a Gantt chart[5] because it would be premature to thoroughly detail a solution that might not be implemented. A responsible, accountable, supports, consulted, informed (RASCI) matrix[6] is also not appropriate for the same reason—that is, many elements are still missing.

However, it is possible to use a matrix similar to RASCI that is revised for macroresponsibilities and subprocesses (**figure 3**), with some illustrative elements to emphasize the most critical activities. In this phase, there is no need to demonstrate the feasibility or the benefits of the proposed solution; the goal is to outline the level of involvement of some organizational roles in carrying out the subprocesses. The degree of detail is low, and the focus is on correlations and commitment. The matrix should be read in columns, from top to bottom. Each column is dedicated to a subprocess, and different colors represent the roles and key activities.

The lower part of the template provides space to summarize primary tasks by role, indicating which ones are most critical to the success of the risk mitigation action:

- **Management**—Managers provide implementation guidelines, improve training processes or modify organizational aspects. They are also responsible for ensuring compliance with the assigned rules and measuring the performance of processes.
- **Personnel**—Employees are assigned various tasks to deal with threats. These individuals must operate within the scope of the operating instructions received, maintain a level of

Figure 3—Template for ICT Subprocess Activities and Responsibilities

Who should do what?	Design and Development	Policies and Classification	Awareness and Training	Identify and Access	Ticketing and Charge	Reviews and Audit
		Management		Personnel	ICT Department	Auditors
Management		Key Actions	Key Actions			
Personnel		Key Actions	Key Actions	Key Actions	Key Actions	
ICT Department	Key Actions	Key Actions	Key Actions	Key Actions	Key Actions	Key Actions
Auditors						Key Actions

competence adequate to carry out their duties and operate in compliance with the SoD, as these activities must be traceable. If staff members detect problems or see possibilities for improvement, they must be proactive and report their findings (by opening a ticket).

- **ICT**—The ICT role is assigned to the information management service provider. If this function is internal, a formal SLA is generally not established. Through policies and a set of internal procedures, both the implementation method and the level of service delivery are defined. The ICT function has exclusive responsibility for managing all phases from design to the release of solutions, continuously monitoring all activities, measuring performance, supporting users, and modifying applications or infrastructure, when necessary.
- **Auditor**—The auditor intervenes in the auditing phase when an independent opinion is required to ensure compliance with the rules. Internal or external auditing personnel may be involved, and this must be specified. An internal auditor might be used for planned institutional activities, and an external auditor, presumably at a higher cost but with specialized skills, might be engaged on an *ad hoc* basis for specific needs.

Key actions (tasks) are summarized in short lists and provide the correct assignment of activities with respect to who is responsible. An example of a completed prospectus, indicating critical activities, is shown in **figure 4**.

The final result is a map of actions, localized by the coordinates of the subprocesses and responsibilities. This helps top management better understand the extent of the effort required to implement the entire process. It is an alternative to the use of classic tables to present content, emphasizing critical organizational factors without the use of numbers.

Conclusion

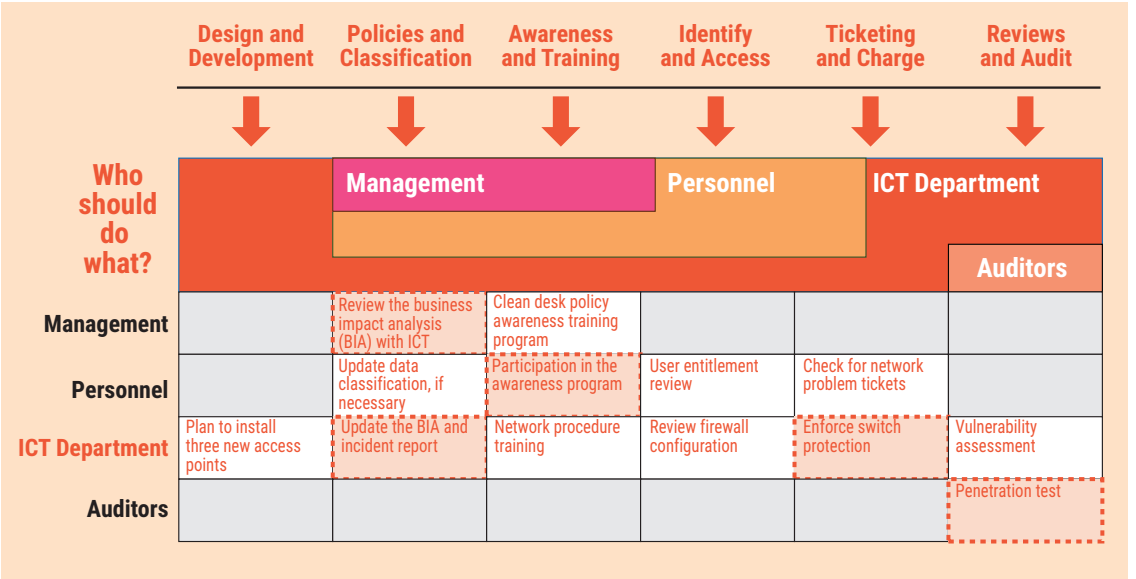
With the templates presented, it is possible to draw attention to those events with a high level of risk. To get top management fully involved in the actions that need to be taken, it is necessary to use methods that focus on the topics most closely linked to the organizational context. By introducing a different perspective, it is possible to focus on concepts that otherwise would not be communicated clearly.

The different spheres of competence and sensitivity, and the different perspectives of process experts and top managers, make it necessary to find common ground to improve communication,

Enjoying this article?

- Read *Reporting Cybersecurity Risk to the Board of Directors. www.isaca.org/reporting-cyberrisk-to-bod*
- Learn more about, discuss and collaborate on information and cybersecurity in ISACA's Online Forums. *https://engage.isaca.org/onlineforums*

Figure 4—Example of ICT Subprocess Activities and Responsibilities



maximize understanding of relevant issues and allow for truly informed decision making. When the level of risk is understood, it is easier to develop effective solutions.

A three-step process can be used to present the results of information security risk to top management to help understand the scenario of information security threats, describe the risk events of specific critical resources, and define the relationship between activities and responsibilities in the treatment of risk. The immediate goal is simple and nontechnical communication to the extent possible. The technical context of the solution remains inside a black box, where threats in the input operational context are transformed into output in the expected level of protection, emphasizing only the interactions between processes, not the technical details of the solutions.

Communication is effective only if all stakeholders understand the issue. The expectation is a conscious choice, always oriented toward business objectives. Communication tools can be unconventional, but this does not mean an abandonment of methodological standards. These standards are simply enriched with components that suit the needs of each enterprise.

> "THE IMMEDIATE GOAL IS SIMPLE AND NONTECHNICAL COMMUNICATION TO THE EXTENT POSSIBLE."

Endnotes

1 ISACA®, "Communicating Information Security Risk Simply and Effectively, Part 1," *ISACA® Journal*, vol. 6 2021, *https://www.isaca.org/archives*

2 ISACA, "Information Security," ISACA Glossary, *https://www.isaca.org/resources/glossary*

3 ISACA, "Service Level Agreement (SLA)," ISACA Glossary, *https://www.isaca.org/resources/glossary*

4 ISACA, *CISA Review Manual, 26th Edition*, USA, 2015, *https://www.isaca.org/resources*

5 Weaver, P.; "Henry L. Gantt, 1861–1919: A Retrospective View of His Work," Mosaic Projects, 2012, *https://www.mosaicprojects.com.au/PDF_Papers/P158_Henry_L_Gantt.pdf*

6 Baker, D. A.; *Multi-Company Project Management: Maximizing Business Results Through Strategic Collaboration*, J. Ross Publishing, USA, 2009