Making the SoA an Information Security Governance Tool

Do you have something to say about this article?
Visit the *Journal* pages of the ISACA® website *(www.isaca.org/journal)*, find the article and click on the Comments link to share your thoughts.

http://bit.ly/2wBsSUj

The International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC)'s ISO/IEC 27001:2013 standard has defined the requirements for an information security management system (ISMS). An ISMS simultaneously encompasses IT security management and exceeds the strict boundaries of IT infrastructure and software. Indeed, an ISMS spans all of an organization's activities. It broadens the security view to all assets including physical assets (e.g., documents, premises, offices) and human assets (e.g., employees, contractors, suppliers).

Broadening one's view allows for the organization to see the true state of all assets. Both physical and human assets may host, reflect or transmit sensitive information that may pose strategic, reputational, regulatory or financial risk if lost, deformed, breached or leaked.

Daniel Gnana, CISA, ISO/IEC 27001:2013 LA, PRINCE2
Is the founder of ISO27K Audit Consulting. He has more than 20 years of experience in IT, including audit and security governance. He also provides training courses in audit, and he helps IT providers in their journey to obtain ISO/IEC 27001:2013 certification. He can be reached at danielgnana@gmail.com.

To guarantee the awareness of every information security aspect, an ISMS requires any organization to focus on 14 control objectives, which are listed in **figure 1**. The numbering in **figure 1** starts at 5 so that each control objective number aligns with the related ISO chapter.

Introducing the SoA

The ISO/IEC 27001:2013 standard reveals the Statement of Applicability (SoA) as a requirement related to information security risk treatment. It states, "Produce a statement of applicability that contains the necessary controls and justification for inclusions, whether they are implemented or not, and the justification of exclusions of controls."[1]

The explanation provided in the standard shows how an SoA tightly links risk assessment and risk treatment. That said, detailing such a link assumes that the organization has previously performed a risk assessment and is conscious of the current stakes, vulnerabilities and countermeasures available.

Since an SoA covers 14 themes, as previously mentioned, the risk assessment is indirectly assumed to include these themes. Once again, this applies to more than just the IT realm.

What is next? Surprisingly, the SoA is only mentioned once in the ISO/IEC 27001:2013 standard, which leads to a frequent misunderstanding that the SoA is a supplementary document in place only to comply with the standard and nothing more.

Is the SoA a trivial addition in the ISO/IEC 27001:2013 standard? Certainly not. If an organization has the desire to utilize the real benefits of the ISO/IEC 27001:2013 standard, which is to install information security governance, then it must utilize the SoA in its full capacity. The SoA is a tool that allows top management to see the comprehensive strengths,

Figure 1—Control Objectives for an ISMS

Control Objective	Set of Measures	Number of Measures
5: Information Security Policies	5.1 Management direction for information security	2
6: Organization of Information Security	6.1 Internal organization	5
	6.2 Mobile devices and teleworking	2
7: Security of Human Resources	7.1 Prior to employment	2
	7.2 During employment	3
	7.3 Termination and change of employment	1
8: Asset Management	8.1 Responsibility for assets	4
	8.2 Information classification	3
	8.3 Media handling	3
9: Access Control	9.1 Business requirements of access control	2
	9.2 User access managment	6
	9.3 User responsibility	1
	9.4 System and application access control	5
10: Cryptography	10.1 Cryptographic controls	2
11: Environmental and Physical Security	11.1 Secure areas	6
	11.2 Equipment	9
12: Operations Security	12.1 Operational procedures and responsibilities	4
	12.2 Protection from malware	1
	12.3 Backup	1
	12.4 Logging and monitoring	4
	12.5 Control of operational software	1
	12.6 Technical vulnerability management	2
	12.7 Information systems audit cosiderations	1
13: Communications Security	13.1 Network security management	3
	13.2 Information transfer	4
14: System Acquisition, Development and Maintenance	14.1 Security equipment of information systems	3
	14.2 Security in development and support processes	9
	14.3 Test data	1
15: Supplier Relationships	15.1 Information security in supplier relationships	3
	15.2 Supplier service deilvery management	2
16: Information Security Incident Management	16.1 Management of information security incidents and improvements	7
17: Information Security Aspects of Business Continuity Management	17.1 Information security continuity	3
	17.2 Redundancies	1
18: Compliance	18.1 Compliance with legal and contractual requirements	5
	18.2 Information security reviews	3
		114

* Highlighted measures affect more than IT

weaknesses and paths to mitigate the organization's information risk. Even further, this tool allows for follow-up enhancements to be carried out for information security.

Stated in other terms, the SoA must be considered a dual-role instrument rather than a simple document. First, it can be used as a health diagnostic tool for the organization to protect its information, and second, it pilots the general paths to improve organizational health.

"The SoA is a difficult exercise and requires the person conducting it to have enough seniority and authority to determine the person who best knows about the enterprise's security controls."

Decisions to Make Before Implementing the SoA

Prior to carrying out the SoA, there are some decisions the organization's top management have to make:

- **Confirm the organizational perimeter**—Ensure the ISMS perimeter is well defined and approved by the head of the organization as the target to be ISO/IEC 27001:2013 certified. Which businesses are concerned? Are there specific activities to focus on within those businesses, and if so, in which countries? Who are the stakeholders?

  As an example, suppose a company whose main business is to provide services related to a data center. In such a case, the main concerns reside in this perimeter, regardless of whether the company has other premises or not. Concretely, when scanning the SoA, restrict the physical security (theme 11) to the data center only.

- **Aim for a quick-win SoA**—Decide on a preliminary simple, but nonetheless reachable, version of the SoA in a short period of time, e.g., within a quarter. For each ISO requirement to mitigate the information security risk, strive to first get a quick insight of the actions currently carried out that fit such a requirement. Getting a quick insight for each of every 114 requirements calls for discernment between completeness and efficiency. An outdated and obsolete SoA may not reflect the current situation anymore and does not help decision making.

- **Identify the appropriate employee level at which to implement the SoA**—Decide on the employee profile that will be capable of rolling out each measure. This role should be able to investigate with enough authority; here are some considerations to keep in mind:
  - Regarding the previously defined perimeter, are these control objectives (**figure 1**) and set of measures applicable to the ISMS?
  - After investigation, can the information obtained be considered reliable?
  - As calculated, can the coverage rate of such a measure be considered acceptable for the organization, given the risk level?
  - If the coverage rate is low and it could take considerable effort to increase coverage, can the organization afford to remain at this point and accept the risk?

Avoid having a small SoA with no substance or with no reliable results. An ineffective SoA can happen after assigning someone whose lack of authority will lead to run constantly after the right answers. The SoA is a difficult exercise and requires the person conducting it to have enough seniority and authority to determine the person who best knows about the enterprise's security controls. Authority and seniority are also important to convince interviewed people to cooperate to help the person making the SoA determine the level of reliability and completeness of each answer.

Implementing the SoA

Once the preliminary steps mentioned previously are completed, there are three major steps to build a realistic and effective SoA:

1. **Filter and keep only the control objectives and the measures corresponding to the organization's scope**—First, regarding the organization's activities aspiring to comply with the ISO/IEC 27001:2013 standard, select each control

objective and every set of measures addressing the scope; consequently, disregard any objective and set of measures that fall out of scope, i.e., those that are nonapplicable to the organization.

For example, consider a subsidiary company in which supplier relationships are handled by the headquarters' human resources (HR) department. In such a case, objective 15, "supplier relationships," may be out of scope for that organization, making it inapplicable in the organizational context.

However, there are control objectives (CO) running as universal constants that are applicable to any organization:

- CO 5 (Information Security Policies)
- CO 6 (Organization of Information Security)
- CO 7 (Security of Human Resources)
- CO 8 (Asset Management)

A careful reading of the ISO/IEC 27001:2013 standard helps clarify that the previously mentioned control objectives are compulsory. Indeed, any organization targeting such a standard has to fix at least one high-level information security policy and one set of responsibilities to control its application throughout the organization. Any organization has to manage the assets and the stakeholders; therefore, it is necessary to identify them.

2. **With the help of the risk assessment results, shed light on the priorities relating to every set of measures**—To be able to determine the minimum responses that correlate to each set of measures of the SoA, it is worth analyzing the organization-level risk assessment and ranking the corresponding priorities (e.g., 1 = low risk, low priority; 2 = medium risk, medium priority; 3 = high risk, high priority) to weigh every measure.

   Avoid waiting until the perfect risk assessment is complete. Perfection is a lure and a hurdle against a successful quick scan of the SoA. Rather, develop a first version by considering which control objective the organization considers a major risk. Should the enterprise take up the exercise again, the second version can widen the scope of the risk assessment.

3. **For each measure deemed applicable to the organization, detail it to understand how far the measure is currently applied**—The following guidelines are elaborated on with examples drawn from a subsidiary company's SoA, theme 7, "human resource security," domain 7.1, "prior to employment," requirement 7.1.1., "screening of candidates' background." The purpose of these excerpts is to provide a concrete view of what actions are possible. Each applicable measure is broken down into five items as follows:

"Avoid waiting until the perfect risk assessment is complete."

   - Scope of responsibilities. In this subsidiary context, two types of responsibilities are considered:
     - The HR department is responsible for hiring personnel for fixed or long-term contracts; candidate background screening is the HR department's responsibility.
     - Any department, including HR, that is willing to hire subcontractors is responsible for verifying a candidate's background.
   - Declining the ISO/IEC 27001:2013 requirement in the organizational context given the scope; declining one or more items to come later:
     - **Requirement 1 (responsibility of HR department)**—Before hiring personnel, the following verifications are to be performed for considered candidates: identity control, criminal record, education, professional credentials and contact of former employers.
     - **Requirement 2 (responsibility of all departments)**—Before hiring subcontractors, the same verifications previously mentioned should be performed.
   - Examining how much the concerned organization is complying with previous requirements:
     - Compliance with requirement 1: 1 (Full compliance)
     - Compliance with requirement 2: 0, 2 The organization has handled the personal

verification of the subcontractors' suppliers; however, the reality and the completeness of such verification is never checked by the organization.

- Calculating a requirements coverage rate:
  - In the organization context, the coverage rate is 60 percent (∑compliances=1,2/∑Requirements=2).
- Decision improvements and deadline:
  - **Improvements**—First, the organization shall indicate to their suppliers which control objectives are required (e.g., identity, education; credentials; references). Second, the organization shall require their subcontractors' suppliers to provide their verification process documentation to ensure it complies with the control objectives previously mentioned. Third, the organization shall take periodic control of the supplier's verification evidence.
  - **Deadline**—First quarter of 2018.

Serving Information Security Governance

By its very detailed nature, the SoA, with its 114 measures covering 14 control objectives, cannot be reasonably delivered for governance meetings. However, the SoA becomes a goldmine for a synthesis of the weaknesses and paths to achieve control objectives. **Figures 2** and **3** help show the possibilities of synthesis of coverage rates and decisions. **Figure 2** provides an example of mapping the coverage rate with each measure for control objective 7, HR security.

Figure 2—Coverage Rate for HR Security

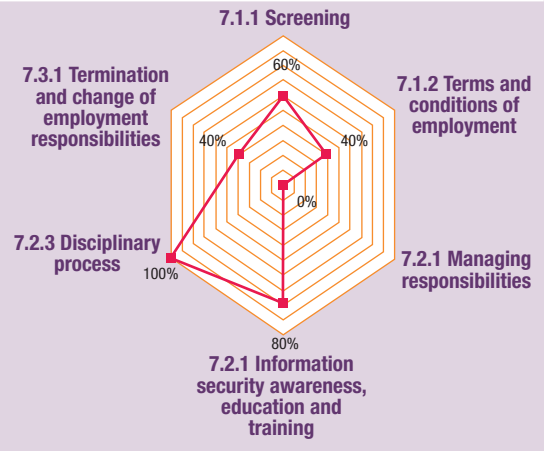

Figure 2 shows that when it comes to HR security, the sample organization has not yet provided an appropriate response to requirement 7.2.1 Managing Responsibilities, which most likely will

Figure 3—Organizational Decision-Making Response

Theme	Decision: No Additional Action	Decision: Additional Action	Total
5: Information Security Policies		1	1
6: Organization of Information Security		1	1
7: Security of Human Resources		2	2
8: Asset Management	1	3	4
9: Access Control	1	1	2
10: Cryptography		1	1
11: Environmental and Physical Security		4	4
12: Operations Seurity	1	6	7
13: Communications Security	1		1
14: Systems Acquisition, Development and Maintenance	1		1
15: Supplier Relationships	—	—	—
16: Information Security Incident Managment	1	3	4
17: Information Security Aspects of Business Continuity Management	1		1
18: Compliance		3	3
	7	**25**	**32**

be an obstacle to strengthen the other measures related to human resources.

By extension, such a synthesis can be applied to other control objectives and give an overview of risk areas concerning information and can consequently help determine risk mitigation strategy for the entire organization.

Figure 3 illustrates a specific area of concern: What is the next step after assessing a coverage rate as nonsatisfactory? In the example shown, there are 32 measures that are not covered enough, of which seven measures will not require additional action. These types of decisions are made considering the residual risk given the current action with regard to the ISO/IEC 27001:2013 measure recommended. Such a decision-making process cannot be undertaken in the dark; it requires the commitment of top management.

Conclusion

Since the SoA is compulsory, take advantage of it by gaining a quick insight of the controls coverage, not only in one's information system, but also in the weakest links of the security chain, such as some departments that care less about IT. Getting quick insight helps an enterprise set quick and efficient measures to mitigate major risk factors. All this insight helps achieve the ultimate objective of providing top management with a reasonable assurance of the continuing suitability, adequacy and effectiveness of their ISMS.

"However, the SoA becomes a goldmine for a synthesis of the weaknesses and paths to achieve control objectives."

Endnotes

1 International Organization for Standardization, ISO 27001:2013, subclause 6.1.3, d), *https://www.iso.org/isoiec-27001-information-security.html*