



Make a Match for Your Organization: Security roles and job definitions

By Sekar Sethuraman

Part of an effective solution to the problem of Information Security requirements is to specify security roles and responsibilities within job definitions as early as possible, and to use this strategy to build a culture of accountability.

Success in Information Security is a business priority in today's interconnected world. Compelling reasons such as regulatory compliance mandates and customer demands should drive an organization to take up an Information Security Program as a major business initiative, and to implement a suitable Information Security Management System (ISMS) as a properly funded project. However, in many organizations, business managers and employees often view Information Security (IS) responsibilities as requirements over and above their job requirements; and the IS manager finds it an onerous task to keep the organization engaged in the initiative.

Part of an effective solution to this problem is to specify security roles and responsibilities within job definitions as early as possible – for example, when the positions are created, or when the ISMS is implemented as a management-sponsored project – and to use this strategy to build a culture of accountability. This article discusses the various considerations for integrating security roles and responsibilities in job definition.

Why integrate security roles and responsibilities?

People, process and technology are the three components of an Information Security Program that, when orchestrated appropriately, will realize business objectives. Security roles and responsibilities in job definition represent formal guiding rules, because management can specify them among the first steps ensuring that employees follows expectations. This is as relevant and crucial as conducting security awareness for a new employee.

Documented and clear job definition enables an employee to understand and work toward the expectations in his or her job. Communicating the security roles and responsibilities to employees right at the time of joining helps them understand the expectations for them in respect to the security program. This also demonstrates the importance management attaches to information security.

Every activity that needs to be performed in implementation, ongoing maintenance and enhancement should figure appropriately in the job definition of the right person at the right level, across the organization.

Inclusion of security responsibilities in job definition should be undertaken for all positions that are required for the implementation of an IS program. Every activity that needs to be performed in implementation, ongoing maintenance and enhancement should figure appropriately in the job definition of the right person at the right level, across the organization. These definitions also need to be continuously enhanced so as to make the program successful on a continuing basis.

Such relevant positions include:

- CISO/ISO/Information Security Manager
- Network Security Manager
- Physical Security Manager and associated staff
- HR Manager and associated staff
- Legal Manager and associated staff
- Information Security Analyst
- Network/Systems Administrator
- Internal Audit members
- General users
- Business Managers
- Senior Management (especially that of Information Security Management Forum)

The advantages of specifying security roles and responsibilities are manifold:

- Defining security responsibilities in job definition helps in appropriate resourcing for the IS Program and in carrying IS activities on an ongoing basis
- Accountability for the various security expectations is clearly identified, which again helps in better execution
- As the IS Program matures in the organization, these job definitions can be enhanced and new job definitions created as required; this enables proper task distribution and meeting requirements
- Documented job definitions with security responsibilities across the organization enable work to be carried out via better coordination of work organization-wide

- Documented job definitions for security also demonstrate management's commitment to security controls, which, in addition to utility, shows external auditors a proper internal control system. Even if there are gaps, job definitions can be suitably modified to reflect requirements
- In the growing context of outsourcing and like options, documented job definitions for security are quite valuable, establishing accountability and ensuring better coordination
- IS processes cut across the organization; success in IS comes only from effective participation by all key members

In short, specifying security roles and responsibilities in all job definitions (and measuring performance) institutionalizes security activities, shows organizational maturity, and leads to greater success and cost-effective security.

Specifying security responsibilities

Here are the steps to take:

1. The first step is to identify the various tasks to be carried out within the IS Program. If an ISMS is implemented as per frameworks/standards such as ISO 177799 / ISO 27001, the tasks are readily identifiable from the policies, processes and guidelines formalized for the frameworks or standards. Map these tasks to the various positions in the organization as responsibilities. Enhance existing job definitions to include these security responsibilities, and create new positions if needed.
-
- Specifying security roles and responsibilities in all job definitions... leads to greater success and cost-effective security.**
-
2. Identify and implement suitable methods for measurement, reporting and review of performance via a performance management system.
 3. Identify customer perceptions about the IS Program; use these to correct or improve job definitions.
 4. Establish methods to enhance job definitions or create new ones as the IS implementation matures in the organization, and also to take care of changes and new requirements.

Mapping security responsibilities to jobs

There are four basic types of responsibility for IS in an organization:

- Responsibilities to lead IS Governance and to be accountable to external bodies such as regulatory compliance authorities
- Responsibilities to lead the IS Program and proactively make security happen
- Responsibilities to participate in implementation and resolve issues/incidents as per IS Policy and Program
- Responsibilities as a general user of information in the organization

These can be mapped to the various job positions as in Figure 1.

| Positions in Organization and Nature of Responsibilities | | | | |
|--|---|--|---|--|
| Position/Level | Responsibility to lead IS Governance, and be accountable to external bodies | Responsibility to lead IS Program, proactively make security happen, and implement IS Policy and Program | Responsibility to participate in implementation, and resolve issues/ incidents as per IS Policy and Program | Responsibility as "general user," and as expected by IS Policy and Program |
| Senior Management | Primary | Yes | Yes | Yes |
| CISO/ISO/IS Manager | Supportive | Primary | Yes | Yes |
| Business Managers | Supportive | Primary from business perspective | Yes | Yes |
| Network/Security Manager | Supportive | Yes | Primary | Yes |
| Network/Security Administrator | Supportive | Yes | Primary | Yes |
| Information Security Analyst | Supportive | Supportive | Primary | Yes |
| Physical Security Manager | Supportive | Member of the core IS team | Primary | Yes |
| Legal Manager | Supportive | Member of the core IS team | Primary | Yes |
| HR Manager | Supportive | Member of the core IS team | Yes | Yes |
| Internal auditors | Supportive | Member of the core IS team | Yes | Yes |
| General users | — | — | Yes | Primary |

Table 1 - Positions in Organization and Nature of Responsibilities

These security responsibilities can be elaborated based on the IS Program and associated security policies, processes, procedures, standards and guidelines.

Challenges

Information security is still in early stages in most organizations. A Gartner study of Global 2000 organizations shows¹:

- As many as 30% of the organizations are still in the “blissful ignorance” stage
- 50% of the organizations are still in the “awareness” stage and are in the process of establishing the teams
- 15% of the organizations are in the “corrective” stage and are carrying out corrective projects
- Only 5% of the organizations are in the “operational excellence” stage

Maturity in IS follows a multi-stage model, as elaborated by the System Security Engineering Capability Maturity Model² (SSE-CMM). The model appears in adapted form in Figure 2. The stages are:

- Level 0 – Not performed
- Level 1 – Performed informally
- Level 2 – Planned and tracked
- Level 3 – Well defined
- Level 4 – Quantitatively controlled
- Level 5 – Continuously improving

Security roles and responsibilities start appearing in job definitions formally when the organization is at Level 2, and become well defined as the organization reaches Level 3.

The usual practice is to specify, to begin with, the security responsibilities for the job definitions of the key positions in an IS program. Security responsibilities are specified for the other positions depending on the program’s comprehensiveness and effectiveness. This, in fact, shapes one of the factors by which the organization can move forward quickly, and also clearly shows that security is no longer treated just as IT Security, but as Information Security.

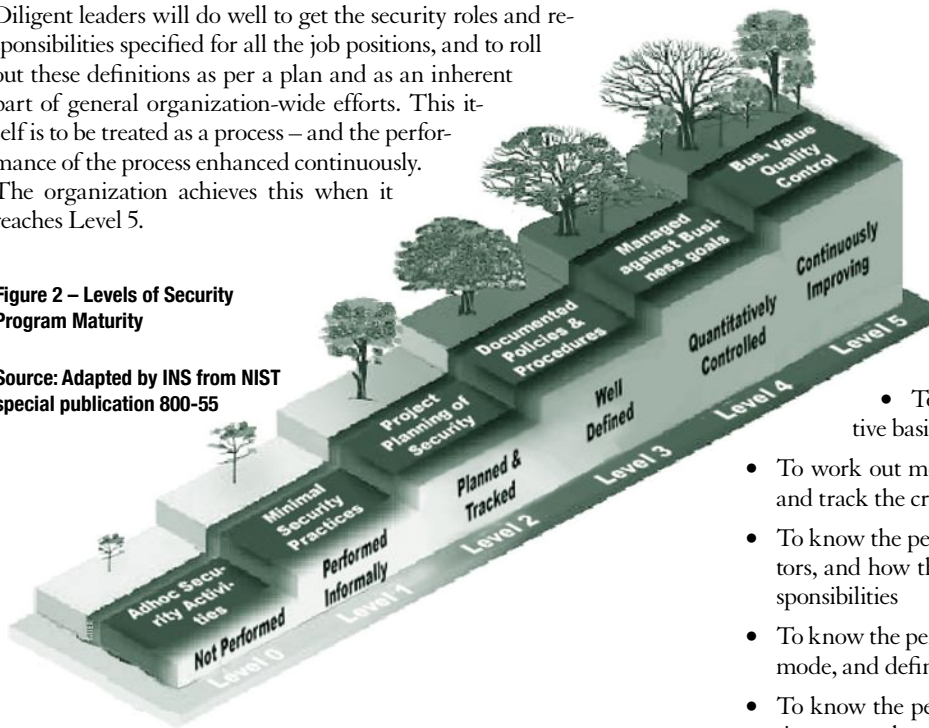
¹ Ouellet, Eric, et al., “The Evolving Role of the Chief Information Security Officer,” January 23, 2006. <http://www.gartner.com>

² <http://sse-cmm.org/>

Diligent leaders will do well to get the security roles and responsibilities specified for all the job positions, and to roll out these definitions as per a plan and as an inherent part of general organization-wide efforts. This itself is to be treated as a process – and the performance of the process enhanced continuously. The organization achieves this when it reaches Level 5.

Figure 2 – Levels of Security Program Maturity

Source: Adapted by INS from NIST special publication 800-55



- To use interested parties' requirements and expectations to determine the "critical success factors" for identifying and implementing appropriate job definitions
- To specify, to start with, security roles and responsibilities for essential members (CISO/ISO, Network/Systems Administrator, Business Manager, Senior Management)
- To specify security roles and responsibilities as required for general users
- To approach other job definitions on a reactive basis
- To work out measures to verify successful implementation and track the critical success factors identified above
- To know the percentage of jobs meeting critical success factors, and how they are specified with security roles and responsibilities
- To know the percentage of jobs specified within the reactive mode, and define and implement them well in time
- To know the percentage of general users whose job definitions carry the complete security responsibilities
- To formalize methods for tracking, reporting and review of these metrics, and for taking appropriate corrective and preventive actions

Measuring and managing the process

Based on a range of experiences, the author proposes the following as crucial aspects of this process:

Interested parties' requirements and expectations

Overall Process for Specifying Job Definitions

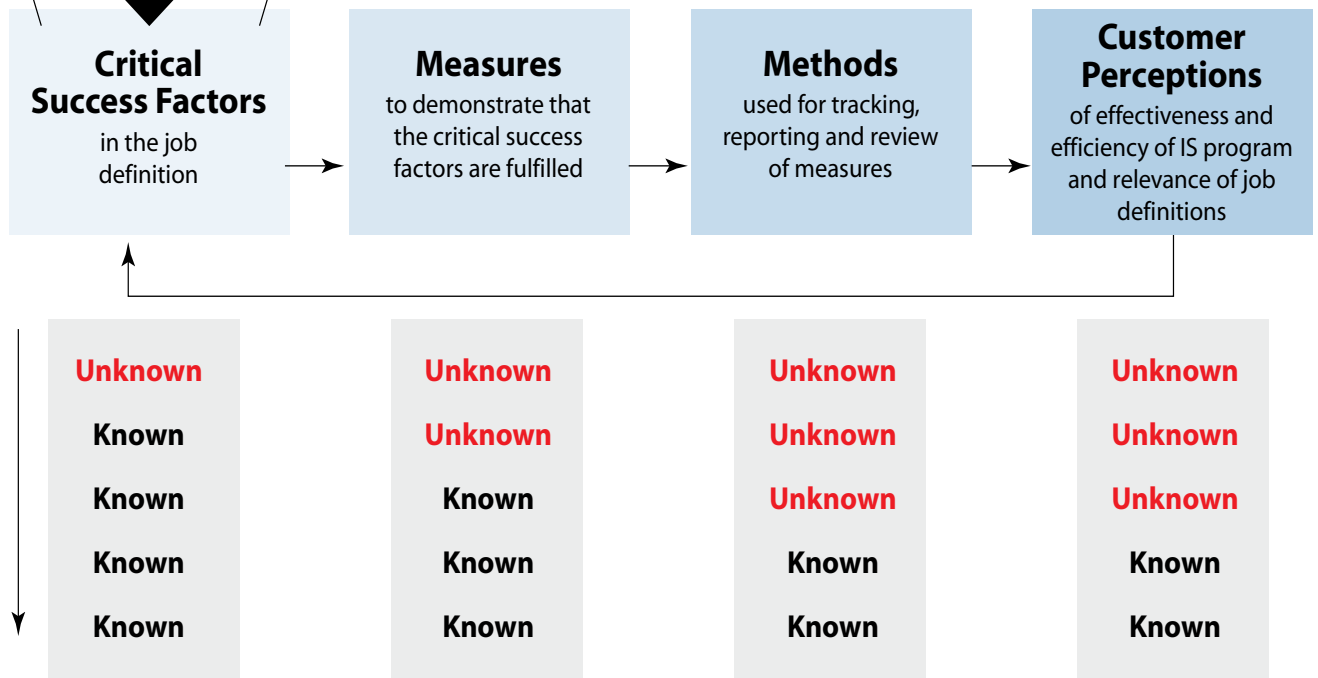


Figure 3 – Overall process for specifying job definitions

- To obtain customers' perceptions of the IS Program's effectiveness and efficiency, and in particular the job definitions vis-à-vis the program
- To shepherd the entire process through any changes, commensurate with the perceptions and adjustments needed

Figure 3 shows the overall process of this proposed method. For each category the parameters are likely to be “unknown” in the early stages; as the organization matures in Information Security, all the parameters will be “known” – and well-defined and assessed.

Driving accountability and responsibility

In building a proper security culture in the organization, it becomes important to understand the difference between “accountability” and “responsibility.”

integrating security roles and responsibilities in job definitions across the organization should be among the key moves you consider

When someone feels accountable, he is too driven to meet expectations imposed from outside, as he is answerable to someone beyond

him. When, on the other hand, someone feels responsible, she is driven by factors from within, and an innate desire to do what she considers right.

Integrating security roles and responsibilities in job definitions leads to a more effective *accountable* culture. But achieving this with an accompanied effort to enhance *responsibility* within the organization really leads to long-term advantage.

This kind of balanced approach in the culture will be especially aided by a Security Awareness program delivered well on time, and kept current to changing demands; and by Senior Management support of the IS Program.

In summary, integrating security roles and responsibilities in job definitions across the organization should be among the key moves you consider – do it effectively as a part of an Information Security Program, and do it as early as possible. Since this process has substantial implications for the organizational culture and the “people” component, managing it well on an ongoing basis will make you succeed.

About the Author

Sekar Sethuraman is a CISSP, CISM, CISA, CIA, CSQA and BS 7799 L.A. He is currently Head - IT Security (Greater Asia) with LexisNexis. He has over 25 years' experience and has implemented information security systems for large organizations to fulfill the requirements of international standards such as ISO 17799 / BS 7799 / ISO 27001. He can be reached at sekar.sethuraman@lexisnexis.com.au.