# Limitations of the Information Security Management System Assessment Approaches in the Context of Information Security Policy Assessment

Maria Soto Corpuz
Information Security Institute, Queensland University of Technology
Brisbane, Queensland/4000, Australia

**ABSTRACT**

Organizations develop information security policies to provide direction in implementing their information security management programs. These information security policies require assessment relative to the security assurance requirements of the organization to maintain its capability to handle security risks according to evolving business objectives. This paper provides a brief literature review on information security policy assessment by first providing an overview on the general considerations and mechanics for assessing information security policies. This is followed by a short discussion of existing research and industry best practice on assessment approaches commonly utilized for information security management systems. The review evaluates information security assessment approaches based on the defined assessment considerations and mechanics under two main categories: the process-based assessment methods and the product-based assessment methods. It is shown that there are limitations on the literature on information security assessment when reviewed in the context of information security policy assessment.

## 1 General Considerations for Information Security Policy Assessment

Information security policies define the goals, responsibilities and security control requirements that are continually reassessed and updated based on evolving corporate business and risk management objectives. Information security policies may be presented as a collective set of organizational statements consisting of an overarching high level strategic statement of security assurance goals, a lower level of operational policies and procedures and a more detailed technical layer of IT application and system security policies. The acknowledged drivers for information security policy management include the corporate requirements for ICT risk management and governance and regulatory compliance, and the need for coordinated and integrated policies for coherent security management.

Effective information security policy management requires policy review activities in addition to policy development and implementation. The International Standards Organization standard Information technology -- Security techniques -- A framework for IT security assurance -- Part 1: Overview and framework ISO/IEC15443-1 defines security assessment as "*the verification of a security deliverable against a security standard using the corresponding security method to establish compliance and determine the security assurance"*. The ISO/IEC15443-1 further defines that the target object of a security assessment may be an information technology security product system, service, process, or environmental factor such as personnel.

The elements of any assessment activity usually consist of a defined purpose and method of measurement which includes the metrics approach. The purpose or requirement for assessment must define the method of measurement and the metrics approach. As management of information security policies require both the establishment of a policy development process and the effective implementation of the product set of security policies, a security policy assessment method may be classified as either a process-based approach if the primary assessment objective is business process improvement, or a product-based approach if effectiveness of security policy implementation is the primary concern.

In addition, the assessment should consider the following characteristics based on the derived definitions and drivers for security policies discussed earlier:

(1) Risk-based development – policy development process should be based on business and/or organizational requirements to manage risks;
(2) Security policy structure - product set of security policies, practices and procedures should be coordinated and integrated and implemented at different levels;
(3) Cost efficiencies – security policies should be balanced against both cost efficiencies and benefits; and
(4) Review and assessment – development process should facilitate policies to be continually reassessed and updated to address evolving risks.

### 1.1 Process-based Assessment

The major driver for utilizing process-based assessment is the requirement for business improvement drawn from the corporate need for cost-cutting in operations and improving business performance and productivity. Such requirements are usually brought about by organisational changes in corporate structure, strategic business direction and overall corporate objectives. To address the requirement for security policy assurance through process

improvement, the mechanics for process-based assessment involve the process quality elements of consistency, repeatability, predictability of outcomes and continuous optimization. These quality elements are the main assessment considerations defined in the capability maturity models initially developed for software development.

### 1.2 Product-based Assessment

The other major focus of security policy assessment is on the effectiveness of the security policies as internal controls for achieving and maintaining organizational security assurance. In this perspective, the main considerations for product-based assessment are the policy quality elements that address the need for security policies to be based on business and/or organizational requirements to manage risks (business alignment); coordinated and integrated and should be implemented at different levels (integrated policy structure); and balanced against both cost efficiencies (cost efficiency).

## 2 Assessment Approaches in Information Security Management

Information security assessment are required to maintain organizational security assurance. Although vast majority of organizations conduct security audits, the tools and methods of assessment used for security is far from universal. Depending on the business objective for security assessment which is commonly for compliance and certification purposes, the traditional methods of assessment involve auditing of security technologies and controls against checklists provided by industry standards and best practices. These checklists of controls have progressed to include elements that define the state of maturity of processes as adapted from the assessment approach of the capability maturity model for developed by the Software Engineering Institute for evaluating software development.

### 2.1 Traditional Assessment Methods

The multipart standard ISO/IEC 15408, also known as the Common Criteria, (CC) is one of the earliest tools used for security assessment. The CC defines the criteria to be used as evaluation basis for the security properties of IT products and systems and is mainly used as a guide for the development of products and systems. The CC guidelines provide checklists of requirements that are applied to IT security measures in hardware, firmware and software implementation. Essentially, the evaluation process provides a confidence level that the security functions of the products and systems meet the security assurance requirements.

The Information Protection Assessment Kit (IPAK), another early assessment tool, is used to measure the state of the information protection program of an organization. It presents an assessment criteria checklist that contains basic categories providing internal controls statements for compliance. Other similar but more prominent assessment checklists are provided by the industry and best practice standards.

Among the most widely used information security management standards are the ISO/IEC 27001 Information technology – Security techniques – Information security management systems – Requirements, the National Institute of Standards and Technology (NIST) Generally Accepted Principles and Practices for Securing Information Technology Systems Special Publication 800-14 and the Information Technology Infrastructure Library Best Practice for Security Management (ITIL). Also used is the governance standard COBIT Control Objectives Management Guidelines. These standards and best practice guidelines provide general checklists for security auditing. Suggestive definitions and characteristics for consideration in developing security policies are also provided as reference for policy audit.

### 2.2 Capability Maturity Assessment Methods

The maturity assessment model defines a 5-level maturity categorization to assess capability based on process maturity and uses metrics to measure process and productivity of the software development life cycle. The maturity assessment model was adopted and adapted for information security through assessment checklists presented by industry standards such as the Information technology-Systems Security Engineering-Capability Maturity Model SSE-CMM (ISO/IEC 21827) and the Federal Information Technology Security Assessment Framework (NIST_2000) used to evaluate the information security management system within the organization. Also used is the governance standard COBIT Control Objectives Management Guidelines. COBIT Maturity Models (COBIT).

Table 1 presents a summary of the checklist-type of assessment provided by the maturity assessments in the industry standards.

| Levels | NIST_2000 | ISO/IEC 21827 | COBIT |
|---|---|---|---|
| Level 1 | policy developed and implemented | not performed | ***Non-existent:*** There is no recognition of the need to establish a set of policies |
| Level 2 | documented procedures must be in place | performed informally | ***Initial/Ad Hoc:*** Policy development are ad hoc and driven by issues |
| Level 3 | procedures and controls must be implemented | well defined | ***Repeatable:*** Policy development is left to the discretion of the managers |
| Level 4 | procedures and controls must be tested and reviewed | quantitatively controlled | ***Defined process:*** Management has developed a framework for policy development |
| Level 5 | procedures and controls must be fully integrated | continuously improving | ***Managed and Measurable:*** A complete set of policies has been developed, maintained and communicated ***Optimised:*** The control environment is aligned with the strategic management framework and is regularly reviewed, updated and improved |

Table 1 Levels of Maturity Assessment Models

The levels of the maturity assessment checklist in Table 1 may be considered to be addressing some of the process quality elements to an extent. However, there is a lack of presentation on the measurement method and metric approach which renders the assessment approach

inadequate for assessing overall organizational security posture. The checklist approach is usually employed for high-level security audit for purposes of meeting certification against the standard or meeting compliance requirements.

## 3 Evaluating Assessment Approaches in the Context of Information Security Policy Assessment

The relevant factors in evaluating the existing assessment approaches in the context of information security policy assessment are: first the nature of assessment based on the requirement (process-based or product-based) and second the set of quality elements according to the nature of assessment. In Table 2, both the traditional and maturity assessment methods are checked against every quality element required by the nature of the assessment. Each of the assessment methods is also checked against the factors such as the method of measurement and metrics approach as part of each of the assessment approach. A check means the assessment method provides a means to address the quality element requirement either through the presence of a checklist method of assessment or a method of measurement which includes a metrics approach.

| Nature of assessment | Quality elements | Traditional assessment methods | | Capability maturity assessment methods | |
|---|---|---|---|---|---|
| | | checklist | method of measurement and metrics | checklist | method of measurement and metrics |
| Process-based | | | | ✓ | |
| | Consistency | | | ✓ | |
| | Repeatability | | | ✓ | |
| | Predictability of outcomes | | | ✓ | |
| | Continuous optimization | | | ✓ | |
| Product-based | | ✓ | | | |
| | Business alignment | ✓ | | | |
| | Integrated policy structure | ✓ | | | |
| | Cost efficiency | ✓ | | | |

Table 2 Evaluation of Assessment Approaches Matrix

Based on this presentation, it is shown that there are limitations on the traditional and capability maturity assessment methods when reviewed in the context of information security policy assessment as formal measurement methods have not been provided. The traditional assessment tools are used mainly in the conduct of a security audit to assess the extent of security implementation in an organization and not necessarily the security posture of the organization. These tools, using the checklist type of assessment do not define levels of maturity by which an organization can assess itself thus leaving a gap by which to base improvement. The lack of a progressive assessment scheme in traditional assessment methods presents a challenge to the organization in implementing an improvement approach to escalate to a higher level of maturity pertinent to their organizational policy processes, much less their policies structures. On the other hand, maturity assessment approaches concentrate attention on the process itself, usually losing sight of the product that the process is producing. By itself, the capability maturity assessment approach will not provide sufficient assessment results to provide an understanding of the effectiveness of the security policies.

## 4 Conclusion and Recommendation

It is concluded that the current literature on security management assessment greatly utilizes the process-centric method of assessment based on the maturity assessment model and that there is limited literature on other aspects of assessment such as product-centric methods. The main contribution of the paper is that it presents a comparison of the assessment methods in the context of security policy assessment to facilitate policy review and development as part of information security policy management. The paper provides a basis for comparing assessment approaches to facilitate method selection for assessing security policies based on the required nature of assessment . Related future work that can be pursued may involve the development of a framework for security policy assessment.