Chapter 10

IA OM® as an Enterprise Risk Management Metric

David R. Comings and Wendy W. Ting

Additional information is available at the end of the chapter

http://dx.doi.org/10.5772/50880

1. Introduction

Ting and Comings [1] described how to use the Information Assurance (IA) Object Measurement (OM®) metric as a tool to measure the monitoring step (Step 6) described in the United States (U.S.) National Institute of Standards and Technology's (NIST) Risk Management Framework (RMF)[1] [2]. This chapter expands the applicability of the IA OM® metric and shows how it may be used as an enterprise-wide information security risk management metric.

Risk management is concerned with the identification of risks, the avoidance, mitigation, transference, or sharing of unacceptable risks, and the acceptance of risks that are within an organization's risk tolerance. However, just as with information system controls within NIST's RMF, it is necessary to monitor the risk posture of systems, maintaining an ongoing assessment of the level of risk they represent within and to an organization. This risk posture changes with changes to the hardware and software employed by the organization, as well as when patches and updates are released that are intended to be applied to deployed software. Changes can also occur from vulnerabilities identified with no patch available, or when new types of information are allowed on a previously authorized or accredited information system. Different types of information are of varying interest to an organization or adversary. More valuable information generally has a higher impact on the organization when it is compromised[2], and can increase the threat level of an information system. From an information system perspective, many of the monitoring activities, conducted to ensure the systems remain operational and maintain an acceptable security posture, are also activities involved in the management of information system risks.

[1] The RMF is described in detail in NIST Special Publication (SP) 800-37, available from: http://csrc.nist.gov/publications/nistpubs/800-37-rev1/sp800-37-rev1-final.pdf

[2] Compromise is used in this chapter to indicate a loss of confidentiality, integrity, or availability of the information.

The IA OM® metric is a good choice for use as an enterprise risk management metric, as described in this chapter, due to its versatility as a management metric. This metric:

- Measures information security risk management activities within an organization;
- Shows organizational senior management where their organization currently stands with respect to its risk management strategy, and its monitoring plan; and
- Demonstrates to senior management how such metrics can be used over time to track and improve their organization's ability to meet its overall risk management strategy and risk monitoring plan.

2. Risk management

Risk management focuses on understanding and managing risks to an organization. This chapter focuses on information security (also referred to as information assurance (IA)) risks. Wheeler [3] in his book on risk management stated that "The goal of risk management is to maximize the output of the organization (in terms of services, products, revenue, [mission accomplishment], and so on), while minimizing the chance for unexpected outcomes". This goal is best accomplished through the use of an established, proven framework for managing information security risks to organizations. This chapter proposes an approach based on the structure provided by the NIST.

The approach described by the NIST is used in this chapter due to several factors. First, the NIST approach has been developed to be consistent with and harmonize with international standards to the extent appropriate. These international standards include those of the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) [3]. This approach is also being adopted and used by the U.S. government for virtually all government organizations, as well as other private organizations regulated by the U.S. government.

The approach described by the NIST is based on a 4-step process, used within a 3-tiered structure. The 3-tiered structure is used to depict the principal functional areas within an organization as they relate to risk management decision-making – the organization, mission/business process, and information systems Tiers – described in Section 2.2. The risk management process and the 4-steps in the process – frame, assess, respond, and monitor – are described in Section 2.3.

2.1. Risk management overview

Information security practitioners are transitioning from a compliance-based, checklist type of approach to a more risk managed approach to security [3]. This is being done largely due to practicality and resource constraints [3]. It is not possible to eliminate risk in an

[3] The NIST risk management structure is aligned with ISO/IEC 3100, *Risk Management – Principles and Guidelines*; 31010, *Risk Management – Risk Assessment Techniques*; 27001, *Information technology – Security techniques – Information Security Management Systems – Requirements*; and 27005, *Information Technology – Security Techniques – Information Security Risk Management Systems*.

information system, and is resource intensive to try [3, 4]. In order to effectively manage resources and maintain usability of the system, it is necessary to implement a risk managed approach to securing Information Technology (IT) systems.

To understand this change, it is important to start with a good definition of risk. A good definition in this case is one that can be understood operationally and can be easily used to clarify the process. Not surprisingly, there are many different definitions of risk. Wheeler [3] defines risk as: "the probable frequency and probable magnitude of future loss of confidentiality, integrity, availability or accountability". Accountability is not commonly accepted as being a part of the definition of risk, is not included in the definition of risk used by the NIST[4], and thus will not be included in the definition of risk used in this chapter. The definition of risk used for this chapter is therefore:

Risk: The probable frequency and probable magnitude of future loss of an organization's operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation resulting from a loss of confidentiality, integrity, or availability.

There are two fundamentally different approaches to Information security risk management activities used by organizations:

1. Compliance-based; and
2. Risk management-based.

Each of these approaches, while working toward the overall objective of ensuring the confidentiality, integrity, and availability of the organization's information and information systems, attempts to meet that objective in a fundamentally different way. Compliance-based approaches default to including controls from the best practice or other framework they are implementing – not including a prescribed control is the exception [5]. On the other hand, risk management-based approaches default to not including a control unless its need and utility can be justified by a risk analysis [5].

2.1.1. Compliance and best practice frameworks

Failure to comply with the legal and regulatory structures confronting an organization can result in penalties, loss of contracts, loss of confidence, loss of business, and stock price declines [6]. Some of the requirements that organizations may need to maintain compliance with include:

- U.S. Legal requirements (e.g., the Sarbanes-Oxley Act, the Health Insurance Portability and Accountability Act (HIPAA), Gramm-Leach-Bliley Act (GLBA);

[4] The definition of risk provided by the NIST is: "A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence. [Note: Information system-related security risks are those risks that arise from the loss of confidentiality, integrity, or availability of information or information systems and reflect the potential adverse impacts to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation]" [17].

- Non-U.S. Legal requirements for organizations operating outside the United States;
- International frameworks (e.g., Basel, Basel II); and
- Industry standards (e.g., the Payment Card Industry Data Security Standard (PCI or PCI-DSS)).

Compliance with these requirements is often a part of an organization's due diligence [7]. The focus on best practice frameworks frequently focuses on satisfying the auditor/examiner, helping to meet compliance requirements rather than the organizations genuine information security needs [8, 9]. Unfortunately, these checklist or compliance-based approaches to information security risk management provide static, "one-size-fits-all" information security "solutions" [3]. One result of this approach is the common perception among information security practitioners that "if you are secure you *may* be compliant, but if you are only compliant you are certainly not secure" [6].

There are a number of best practice frameworks for information security, including the Information Technology Infrastructure Library (ITIL) [10], COBIT [11], and the ISO/IEC 27001 [12], 27002 [13], and 27005 [14]. Unfortunately, these approaches are dated almost as soon as they are published due to the speed of change on the Internet and within the IT security arena [15]. Attackers are very adaptable, and change their tactics quickly. In addition, a checklist or compliance-based approach assumes that every system requires the same protection as every other system, without regard for cost, information sensitivity, and mission or business impact [3]. However, there are often considerable differences in the types of systems deployed in an enterprise, and the information they contain. Since the information contained in the IT system is normally the critical asset requiring protection, the protective mechanisms that should be implemented will depend largely on the sensitivity of the information processed, stored, or transmitted by the system [8].

However, best practice frameworks do provide a useful method for ensuring that all aspects of an IT information security program are considered when using a risk managed approach to IT information security requirements development. Due to the need of organizations to remain compliant with respect to specific legal requirements and industry frameworks some form of compliance-based approach is likely to remain necessary.

2.1.2. Risk managed approaches

Risk-based approaches to securing information systems allow organizations to customize their information security protections, based in the needs of their organization. Using a risk-based approach requires consideration of the information processed, stored, or transmitted by the information system, as well as consideration of the IT system's environment, connectivity, and threat environment [7, 16]. Other considerations include the cost of implementing security controls weighted against the impact on the mission and business operations of the organization should a loss of confidentiality, integrity, or availability of the information occur [7].

A risk-based approach to information security is what the U.S. government is transitioning to with the release of the NIST Special Publication (SP) 800-37 [2] and SP 800-39 [3, 17]. The NIST has developed a series of SPs to focus on information security risk management, starting with an enterprise view in SP 800-39 [17], an information system view in SP 800-37 [2], and by providing an approach for performing risk assessments in SP 800-30 [18]. NIST SP 800-53 [19] provides a catalog of security controls, and recommends "baselines" of security controls based on the sensitivity of the information on the system. These baselines are intended to be customized, or "tailored" to meet the needs of the information and the information system when consideration of the system's environment, connectivity, and threats are considered [19].

2.2. 3-Tiered risk management structure

When addressing information security risk management activities, the NIST and other authors divide organizations into three levels [17, 20]. The NIST [17] identifies these tiers as the:

1. Organization;
2. Mission/Business Process; and
3. Information Systems.

Each tier has different organizational risk management responsibilities. However, despite their different perspectives and roles, they all use the same 4-step risk management process described in Section 2.3 for risk management actives within their Tier. This 3-tiered structure is depicted in Figure 1.

Figure 1. Risk Management Tiers[5]

[5] This figure is adapted from Figure 2 on page 9 of NIST SP 800-39 [17].

2.2.1. Organization tier

At the organization tier, risk to the entire organization is considered and managed. Part of the responsibility for managing risk throughout the organization is the process of "risk framing", establishing the context within which all organizational risk management activities will be conducted [17]. Risk framing establishes the governance framework from which are derived the risk management activities and the risk tolerance of the organization. Other activities occurring at Tier 1 include:

- Establishment and prioritization of activities and programs at the Mission/Business Tier;
- Determination of organization-wide common controls[6]; and
- The Risk Executive (Function)[7] recommended by the NIST is established in and is located within the organization at this level [17].

The Risk Executive (Function) (REF) is an individual or group within the organization that serves in an advisory role to organizational decision makers at all 3-tiers. The REF does not make decisions for the organization; rather it informs decision makers about the risks to the system, network, and the organization that may result from a particular risk decision. The REF considers risk from a holistic perspective, considering mission and business risks, in addition to security risks. This risk consideration is done with an organization-wide perspective, allowing the REF's recommendations to evaluate the potential impact of accepting risks in one area or system on other systems or the organization.

2.2.2. Mission/business process tier

Tier 2 is where the mission/business processes necessary to implement the strategic goals and objectives established at Tier 1 are defined and prioritized [17]. This is also where the types of information required, the information sensitivity, and information flows necessary to support the Tier 1 goals and objectives is determined [17]. The IT enterprise architecture is defined and established at this tier, to include the implementation of the common controls identified in Tier 1. The decisions and activities at this tier have a direct effect on the activities undertaken at Tier 3.

2.2.3. Information systems tier

Tier 3 is where the information systems that support the organization reside. The decisions and prioritizations established in Tiers 1 and 2 are implemented in information systems at this tier. The activities required for each of the steps in the Risk Management Framework

[6] Common controls are security controls implemented in a way that they are available to information systems across the organization. Common controls can be "inherited" by a system, meaning that the system itself does not need to implement the control the system can leverage/use the control as implemented by the organization.

[7] The Risk Executive (Function) is an individual or office responsible for considering risk across the organization, to include mission, business, and security risks, balancing them appropriately for the organization, and making recommendations to decision-makers within the organization based on their risk determinations.

(RMF)[8] and the system development life cycle [9] are performed here, to ensure each information system meets its technical, mission, and security requirements. In this tier, "information system owners, common control providers, system and security engineers, and information system security officers make risk-based decisions regarding the implementation, operation, and monitoring of organizational information systems" [17].

2.3. Risk management process

The risk management process is comprised of a number of discrete steps. These steps take place at different times within the process, and possibly at multiple times in the process due the iterative nature of risk management activities. It is important that all of the steps are completed for a risk management program to be fully effective. These steps apply to risk management activities taking place at each tier within the organization, so this process is equally applicable to risk management activities taking place at Tier 1 as it is at Tier 2 or 3.

NIST describes four distinct steps in the risk management process. These steps are:

1. Risk Framing
2. Risk Assessment
3. Risk Response
4. Risk Monitoring

2.3.1. Risk framing

Risk framing is a governance activity that is performed at Tier 1. Its principal output is a risk management strategy "that addresses how organizations intend to assess risk, respond to risk, and monitor risk" [17]. The risk management strategy is created as a joint effort between an organization's senior management and/or executives in conjunction with the risk executive (function) [17]. The risk management strategy explicitly states the assumptions, constraints, risk tolerances, and priorities or trade-offs used in making investment and operational decisions for the organization [17]. It also details what types of risk responses are supported, how risk is assessed, and how risk is monitored for the organization [17].

2.3.2. Risk assessment

Risk assessment is the process of:

1. Identifying risks (threats and associated vulnerabilities) to an organizational asset, activity, or operation;
2. Estimating the potential impact and likelihood of the risk materializing, and

[8] The RMF is described in detail in NIST Special Publication (SP) 800-37, available from: http://csrc.nist.gov/publications/nistpubs/800-37-rev1/sp800-37-rev1-final.pdf

[9] The system development life cycle established by the NIST is described in NIST SP 800-64, *Security Considerations in the System Development Life Cycle*, Oct. 2008 [23].

3. Prioritizing the identified risks according to their severity to the organization [3, 17].

Risk assessments can and should be conducted at every Tier of the organization. However, the objectives of risk assessments conducted at different Tiers will reflect the differences in responsibility and objectives for the Tier being assessed [17]. For example, a risk assessment at Tier 3, the Information Systems Tier, will go into considerable technical detail on a specific information system and the risks involved in its operation. Whereas a risk assessment at Tier 1, the Organization Tier, may address information systems from the perspective of the organization's enterprise architecture or common control framework, but will not go into significant technical detail, nor will it address a specific information system. However, a Tier 1 risk assessment will address business risks, and the risks involved in investing in particular missions or business areas.

2.3.3. Risk response

Responding to risk involves deciding on and implementing a course of action to address the risk within the organization. The options available to the organization for risk response are defined in the organization's risk management strategy. The courses of action available to address risk as identified in NIST SP 800-39 [17] are:

1. Accept – take no action when the risk is within the organization's risk tolerance;
2. Avoid – eliminate the activities or technologies resulting in risk that exceeds the organization's risk tolerance, or reposition the activities or technologies into areas or positions where the risk is avoided;
3. Mitigate – apply security controls, safeguards, or process re-engineering to reduce the risk to a level acceptable to the organization;
4. Transfer or Share – shifting all or part of the liability for risk, respectively, to another organization.

2.3.4. Risk monitoring

Risk monitoring is conducted on an ongoing basis to ensure that the organization's risk posture remains within the organization's risk tolerance. The risk monitoring process allows an organization to:

- Ensure compliance with national laws, regulations, organizational policies, and mission/business functions;
- Determine how effective its risk response measures are;
- Identify changes to organizational assets or their operating environments that result in changes their risk postures [17].

Risk monitoring activities are normally conducted on a periodic basis, with the period determined in accordance with the organization's risk management strategy and the sensitivity of the information or business process being protected [16, 17]. Monitoring risk and changes to operating environments includes identifying changes to the threat environment, and determining whether a change in the threat environment requires a

reassessment of the risk posture of an organizational asset, activity, or operation earlier than normally scheduled [3].

These risk monitoring activities can be implemented at any tier in the organization [17]. The objectives and process for each tier will differ according to their respective needs, and, particularly at Tiers 1 and 2, are likely to involve cross-tier monitoring – as the upper tiers are directly affected by operational or process-level changes to the organization's risk posture at the lower levels [17]. An example of cross-tier monitoring would involve the monitoring of the risk posture of an information system authorized to operate within an organization. The organizational official responsible for the authorization decision will want to monitor the risk posture of the information system to ensure it continues to operate within an acceptable level of risk, and that any changes to the risk posture of the system or its environment are properly evaluated and addressed.

3. IA OM®

The metrics or results derived from the IA OM® methodology are meaningful to the organization because the measurements themselves are "tied directly to questions that are important to the organization"[21] . The results are also useful to organizational management since they indicate the degree to which specific information security risk management goals are being met as action is taken to improve an organization's overall information security posture in terms of its information security objectives [1]. In this instance IA OM® can be conceptually expressed as providing a measure of the degree to which the organization's information security risk management objectives are being met [1].

The creators of the OM® methodology, Donaldson and Siegel [21, 22], have 20+ years of professional software engineering experience at Science Applications International Corporation (SAIC) and in the Department of Defense (DoD). The OM® methodology enables one "to measure software products and software systems development processes in everyday terms familiar and – therefore meaningful – to your organization" [21]. The OM® methodology measures software products and software systems development processes as part of a continual process improvement exercise. The OM® framework derives its effectiveness as a "management process" tool in that the OM® Index, akin to the Consumer Price Index, folds in a number of individual measurements into a single overall value [1, 22]. The OM® Index can also be deconstructed to gain insight into the elements comprising the index value. By looking at trends in the index values, it is possible to determine the effect or outcome of changes within the organization.

The OM® quantifies software *product* "goodness" and software *process* "goodness", where an object (i.e., an attribute, component, or activity) is measured through its characteristics. "For products, these characteristics are called attributes; for processes, these characteristics are called components and activities" [22]. Software product "goodness" is the degree to which the product satisfies the customer and meets the customer's requirements. Software process "goodness" is a measure of the product creation process' ability to consistently and reliably create good quality products within budget [1].

The IA OM® metric can be used with existing organizational objectives or industry best practices. However, industry best practices are not appropriate for many organizations, and as described in Section 2.1.1, are often not sufficient in and of themselves to meet the an organization's requirements. Each organization must determine what is most appropriate for its needs. This is best accomplished when requirements are evaluated in the context of their budget and a thorough risk analysis [7]. Evaluating an organization's information security risk management posture, based on how well its systems comply with the organization's information security risk management objectives, provides a metric with greater versatility and applicability across a wider range of organizations [1].

Implementing IA OM® at an organizational level provides Senior Management with a high-level or strategic-level view of where its organization's risk management program stands and how well it is meeting its stated information security risk management objectives. IA OM® is the OM®[10] metric created by Donaldson and Siegel [21] adapted to information security and information security risk management activities as IA OM®[11]. The IA OM® metric can be used to:

- Quantitatively determine the degree of risk identified within an organization's information security risk management program;
- Characterize the organization's risk management policy elements as they are applied to its information security risk management program for IA OM® evaluation;
- Determine the weighting factors, based on a determination of the relative importance of each component, for the identified characteristics of the organization's risk management strategy and policy;
- Periodically present the results of the evaluation, the current risk management posture of the enterprise, in a balanced scorecard-like format that is familiar and easy to understand and interpret by Senior Management;
- Analyze the metrics data, identify the strengths and weaknesses of proposed metrics approaches; and
- Suggest areas for future assessment and evaluation.

IA OM® will help answer Senior Management's questions regarding the state of their organization's information security risk management program enabling them to determine their organization's current risk posture, identify areas needing improvement, and prioritize the allocation of organizational resources in addressing identified risks.

Any effective risk management program requires periodic monitoring and re-assessment, including risk monitoring at the organization, mission/business process, and, information systems Tiers. The components of risk management at these multiple-tier levels are specifically identified[12] and encompass the following:

---

[10] OM® was developed by Donaldson and Siegel, SAIC, [21] to evaluate system development life cycle (SDLC) processes.

[11] See Ting and Comings [1] for a complete description of IA OM®.

[12] NIST SP 800-39 [17], *Managing Information Security Risk*, describes the fundamentals of risk management in Chapter 2 and the process for framing, assessing, responding and monitoring risk in Chapter 3.

- Tier 1 – Addresses risk from an organizational perspective by establishing and implementing governance structures including: 1) Establishment and implementation of a risk executive (function); 2) Establishment of a risk management strategy including a determination of organizational risk tolerance; and 3) Development of organization-wide investment strategies for information resources and information security.
- Tier 2 – Addresses risk from mission/business process perspective by designing, developing, and implementing the processes supporting the mission/business functions defined at Tier 1 including: 1) Risk aware processes designed to manage risk according to the risk management strategy defined at Tier 1 and explicitly accounting for risk in evaluating the mission/business activities and decisions at Tier 2; 2) Implementing an enterprise architecture, and, 3) Establishing an information security architecture as an integral part of the organization's enterprise architecture.
- Tier 3 – Addresses risk from an information system perspective, guided by risk context, risk decisions and risk activities at Tiers 1 and 2, risk management activities (i.e. activities at each step of the Risk Management Framework (NIST SP 800-37 [2]) and in the systems development life cycle (NIST SP 800-64 [23])

These three Tiers, properly integrated, provide the capability to establish a strong, risk-based security infrastructure for an organization.

Risk management monitoring must be conducted at all three Tiers, making sure that all key activities are performed properly within each Tier and across Tiers [17]. Monitoring at the information systems level must take into account those controls that are "common" to an organization or enterprise [2]. Common controls are those controls that are established by an organization itself, or an element within an organization, and are made available for use by other elements and information systems within the organization. It is often not possible for an individual system owner to monitor common controls – such monitoring must be provided by the Common Control Provider.

With monitoring taking place at many levels within the organization, the need for an enterprise-wide risk management solution is even greater. Without a big-picture view of the information security risk posture of the systems within an organization, there may be systems operating that are creating significant risks to the organization without anyone in a position to address the problems realizing a problem exists.

At the Tier 1 and 2 levels, the concept of common controls is not the same as at Tier 3, however, there is still the need to ensure that organizational guidance and organizational functions remain aligned. When strategies, policies, and other organization-level guidance changes, the changes need to ripple through the organization – updating policies, programs, investments, etc. to ensure they remain in alignment with the top-level guidance.

IA OM® addresses these needs by aggregating the results of risk monitoring programs occurring throughout the organization, rolling them up, and presenting them as a set of summary statistics indicating where an organization stands with respect to remaining within its:

- Overall risk tolerance
- Risk tolerance within organizational elements
- Risk tolerance for individual systems

Applied this way, IA OM® allows Senior Management to readily assess their current information security risk management posture and determine whether it fits within their risk tolerance. It also identifies those areas, programs, and systems of greatest risk to the organization – allowing Senior Management to quickly and easily prioritize their remediation efforts.

4. Using IA OM® as an enterprise risk management metric

The process for using IA OM® as an enterprise risk management metric involves a number of steps. The overall steps in the process, as adapted from the OM® process, are:

1. Decide what questions you need or want answers to regarding your organization's risk management program;
2. Identify the organizational assets, processes, or operations that need to be measured to answer the questions from step 1;
3. Identify any characteristics and sub-activities of the organizational assets, processes, or operations to be measured from step 2;
4. Define an activity value scale for each activity or sub-activity in terms that make sense within the organization;
5. Determine the current value (or location along the value scale) for each activity or sub-activity being measured;
6. Calculate the value for each asset, process, or operation identified in Step 2 using the formulas provided in Section 4.4 and the activity (or sub-activity) values from step 5. Weighting factors are selected based on the organization's determination of the relative importance of the activities;
7. Combine the values for each activity (asset, process, or operation) into an overall IA OM® index value to be reported and analyzed.

These steps and activities are applied to organizational risk management using IA OM®, resulting in a metric that provides:

- The ability to evaluate the risk posture of a specific organizational asset, process, or operation;
- A set of organizational assets;
- All activities within a risk management tier; or
- Risk management activities across tiers.

This process is shown in Figure 2 [24] using an activity from an organization's personnel security process as an example. The individual process steps are examined in more detail in Sections 4.1 – 4.7.

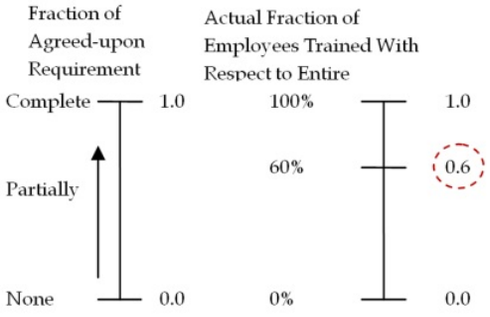
IA OM® Process[13]	
Steps	**Examples**
1. Decide what questions you want answered	Am I complying with my organization's personnel security policy?
2. Identify the organizational assets, processes, or operations that need to be measured to answer the questions from step 1	1) Employee job description 2) Employee information security training
3. Identify any characteristics or sub-activities of the organizational assets, processes, or operations to be measured from step 2	1) Extent to which security in job definition and resourcing are met 2) Actual fraction of employees trained with respect to entire organization
4. Define an activity value scale for each activity or sub-activity 5. Determine the current value (or location along the value scale) for each activity or sub-activity	
Associate observable events with value scale numbers	1) Number of requirements fulfilled in employees' job description 2) Date that employee trained records in training log that employee received
Measure each characteristic	1) Filled positions addressed 7 of the 10 employee's security requirements called out (Value = 0.7) 2) The employees' training log showed that 1 employee did not receive training
6. Calculate an index by substituting measured values into the appropriate IA OM® equation	$PersonnelSecurityComplianceIndex = \frac{\sqrt{0.7^2 + 0.6^2}}{\sqrt{2}} = 0.65$
7. Combine the values for each activity (asset, process, or operation) into an overall IAIndex value[14] to be reported and analyzed	$IARMIndex = \frac{\sqrt{\sum_{i=1}^{n} w_i^2 da_i^2}}{\sqrt{\sum_{i=1}^{n} w_i^2 (\max[da_i])^2}}$

Figure 2. IA OM Process with Personnel Security Process Example

[13] Adapted from interview with Stanley G. Siegel on Jan. 7, 2004 [24].

[14] This equation and its components are described in Section 4.5.

4.1. Step 1 – Ask questions

IA OM® is like other investigative ventures – the first step in the process is determining what you want or need to know. This chapter focuses on evaluating and understanding the ongoing risk management activities within an organization. As a result, the questions framed for use with IA OM® in this chapter focus on what the organization's executives, program managers, or system-level managers want or need to know about the risk posture of the portion of the organization they are responsible for. As such, the questions to be addressed by IA OM® need not to be restricted to Tier 1 – they can, and ultimately should, be spread across all three tiers so that the managers at each tier have the answers they need to be successful in the organization's risk management program.

Examples of questions that might be asked at each Tier are presented in Table 1:

Tier 1	Tier 2	Tier 3
Is our risk management strategy aligned with our organizational goals and objectives?	How well do our mission/business processes align with our organization's risk management strategy?	Are our information systems properly operating within the risk tolerance of our organization's mission/business processes?
How well aligned is our risk management strategy with our mission and business programs?	How well does my mission program align with our organization's risk management strategy?	Is the risk posture of this system within established boundaries to support this mission?
Is our common control strategy effective?	Which common controls are cost effective?	How fully am I using the common controls available to me?

Table 1. Example questions by Tier

4.2. Steps 2 and 3 – Identify assets, processes, or operations to measure

Now that the questions to be answered have been identified, the next step is to identify the assets, processes, or operations that can be measured to obtain answers to those questions. For example, to determine the effectiveness of an organization's common control strategy, you could examine:

- The common controls called for in the common controls strategy/policy;
- Their alignment with current organizational goals and objectives; and
- Their utilization.

An example analysis of Tier 1 risk monitoring activities, their components, and their subcomponents is provided in Figure 3. The common controls assets are presented as $Characteristic_n$ in the right hand branch of the figure. These characteristics and subcharacteristics will also be referred to as diagnostic areas, where diagnostic area 1 (da_1) is equivalent to $characteristic_1$; da_2 is equivalent to $characteristic_2$; and so forth. The

subcharacteristics for each area follow a similar numbering scheme where, for example, subcharacteristic11 is equivalent to da11 and so forth. This is done to simplify the abbreviations used in the equations in Steps 6 and 7.

It is important to remember that the identification of organizational assets, processes, and operations are organization-specific. This is one of the strengths of the IA OM® process, since it enables the abstraction of these key activities – specifically identified by the organization as being of interest – into a metric that shows Senior Management where their organization stands with respect to its risk management strategy and policies. If low level technical metrics exist, they can be combined and abstracted into the IA OM® process. Metrics produced through the use of the IA OM® process can be deconstructed into their component areas, allowing Senior Management to identify the areas needing attention. If further improvement in their risk management program is required, the IA OM® and its component measures can be used to track and improve the organization's risk posture over time.

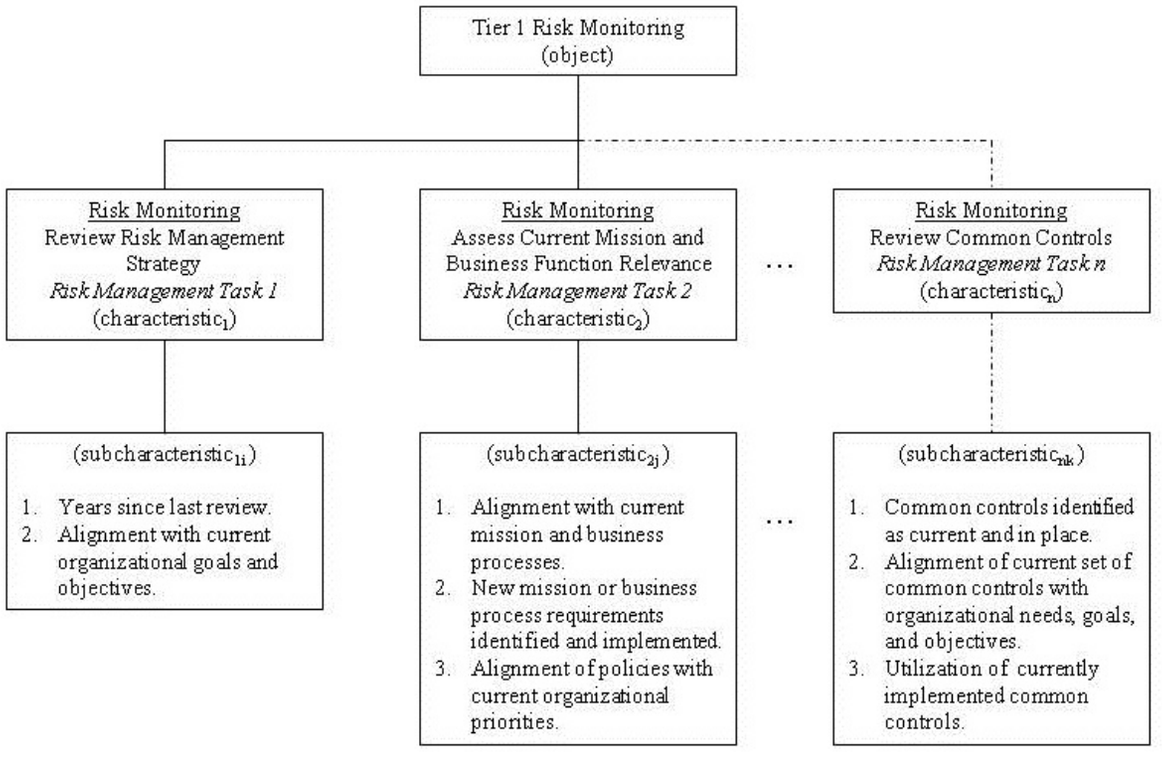


Figure 3. Example analysis of risk monitoring activities and their subcomponents

4.3. Steps 4 and 5 – Define activity value scales and determine activity values

Activity value scales used for IA OM® activities are normally scoped to range between 0 and 1. This makes comparison easy and allows them to be aggregated and rolled-up into measures that are easy to use and understand. Also, these values can be readily seen as percentages to further enhance their understanding. However it is perfectly acceptable to have more important characteristics have values greater than 1 if desired to indicate their

relative importance to the organization. Alternatively, the relative importance of different characteristics/subcharacteristics can be accounted for using the weighting factors discussed in Steps 6 and 7.

For activities that can only assume a specific set of values (e.g., Yes/No, or high, moderate, and low), the value scales can be adapted to accommodate them. For example, with a binary set, like Yes and No, it is common to use Yes = 1, and No = 0. Sets like high, moderate, and low could be represented with high = 1, moderate = 0.5, and low = 0. It would also be possible to decide that high = 0.9 (since even high is not definite like "yes"), moderate = 0.5, and low = 0.1 (since low is also not definite like "no"). The decision on value scales is made by the organization and is made to maximize the utility and understandability of the measurements in the context of their organization.

Continuing with the example of the effectiveness of an organization's common controls strategy, value scales for each of the three subcomponents can be defined, and values determined for each of the subcharacteristics assigned as shown in Figure 4. Each subcharacteristic/diagnostic area (da_{ij}) will be evaluated separately and then combined in Step 6 to provide an overall value for each characteristic or top-level diagnostic area (da_i). These values are then combined in Step 7 to provide an overall IA OM Index Value.

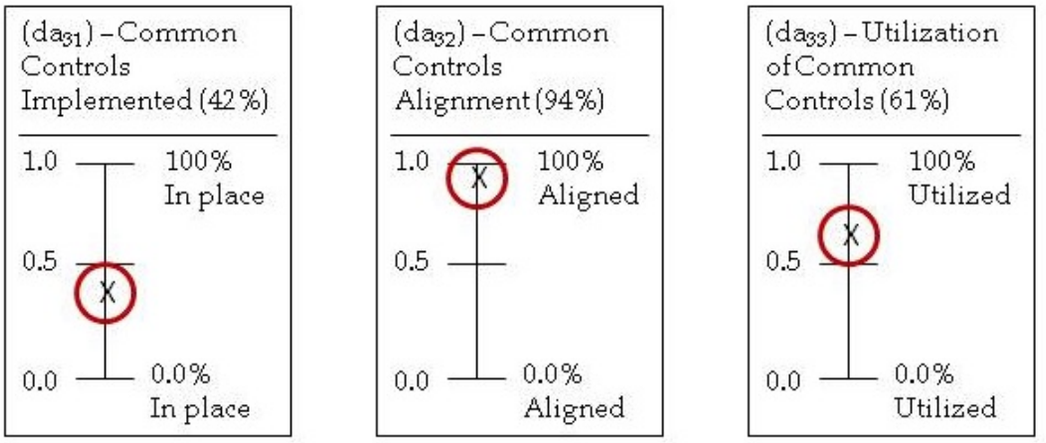


Figure 4. Common Control Value Scales Example

4.4. Step 6 – Calculate an asset, process, or operation index

Steps 3 through 5 have shown how to derive values for each of the assets, processes, and operations identified in Step 2. Each of these values represents a characteristic or subcharacteristic for an asset, process or operation. In this step, any values for subcharacteristics (da_{ij}) will be combined with weighting factors and aggregated to provide values for each characteristic (da_i).

The weighting factor value (w_{ij}) for each subcharacteristic (da_{ij}) is assigned by organizational management to represent the organization's determination of the relative importance of each subcharacteristic to the characteristic being evaluated.

Equation 1 – Calculating diagnostic area (characteristic) values:

$$da_i = \frac{\sqrt{\sum_{j=1}^{ni} w_{ij}^2 da_{ij}^2}}{\sqrt{\sum_{j=1}^{ni} w_{ij}^2 (\max[da_{ij}])^2}}$$

Where:

n_i= number of diagnostic criteria for diagnostic area da_i
w_{ij} = weighting factor for diagnostic da_{ij} of diagnostic area da_i
da_{ij} = the j^{th} diagnostic criterion of the of the i^{th} diagnostic area da_i
max [da_{ij}] = maximum value of da_{ij}

For the common control example, using organizationally determined weightings and subcharacteristics/diagnostic areas values provided in Table 2:

Weightings	Subcharacteristics/ diagnostic areas
$w_{31} = 1$	$da_{31} = 0.42$
$w_{32} = 1$	$da_{32} = 0.94$
$w_{33} = 2$	$da_{33} = 0.61$

Table 2. Weightings and Subcharacteristics Values

The equation works out to:

$$Characteristic_3 = \frac{\sqrt{(1^2 \times 0.42^2) + (1^2 \times 0.94^2) + (2^2 \times 0.61^2)}}{\sqrt{(1^2 \times 1.0^2) + (1^2 \times 1.0^2) + (2^2 \times 1.0^2)}}$$

Thus:

$$\text{Characteristic}_3 = \frac{\sqrt{2.55}}{\sqrt{6}} = .65$$

Inserting values for the other characteristics, and arranging all of the values into a fishbone diagram for clarity of presentation provides breakdown of the process as shown in Figure 5.

4.5. Step 7 – Calculate the IA OM® index

Calculating an IA OM® index provides a concise, high-level assessment of the enterprise risk management posture of the organization. The IA OM index, in this case referred to as the IA risk management index, or IARMIndex, is defined in terms of:

1. Diagnostic areas
2. Diagnostic criteria for each diagnostic area
3. Diagnostic criterion value scales

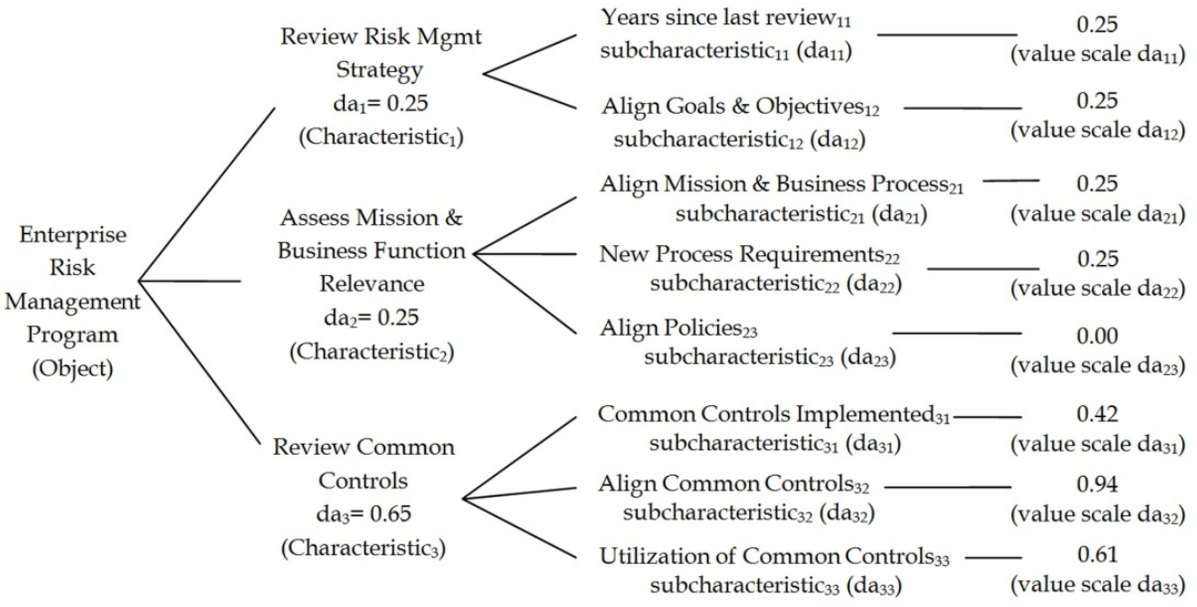


Figure 5. Fishbone Diagram with All Risk Monitoring Characteristics and Subcharacteristics Values

All of these items are provided in the fishbone diagram provided as Figure 5. A weighting factor can be applied to each characteristic/diagnostic area. As noted above, the weighting factor is an organizationally defined value indicating the relative importance to the organization of the particular characteristic. In this example the IARMIndex is normalized to one (i.e., ranges between zero and one). In all cases, value scales are defined in terms familiar to corporate management.

The process for calculating the IARMIndex is shown in Equation 2. For activity element characteristics, the IARMIndex[15] is normalized to one:

Equation 1 – Calculating the IARMIndex value:

$$IARMIndex = \frac{\sqrt{\sum_{i=1}^{n} w_i^2 da_i^2}}{\sqrt{\sum_{i=1}^{n} w_i^2 (\max[da_i])^2}}$$

Where:

da_i = diagnostic area (characteristic)
n = number of attributes
w_i = weighting factor for attribute da_i
max $[da_i]$ = maximum value of da_i

Using the values from above and the organizationally defined weightings as shown in Table 3:

[15] Taken and adapted from Donaldson & Siegel [22] (p. 420).

Weightings	Characteristics/ diagnostic areas
$w_1 = 2$	$da_1 = 0.25$
$w_2 = 1$	$da_2 = 0.25$
$w_3 = 1$	$da_3 = 0.65$

Table 3. Weightings and Characteristics Values

Results in a value for **IARMIndex = 0.35**

4.6. Evaluating the IA OM® index

The following steps describe the analysis process allowing organizational management to quickly uncover areas needing attention and prioritize which area(s) to address first to obtain the greatest benefit:

1. The IARMIndex value is examined to determine whether it is within the range determined by the organization to correspond to its risk tolerance;
2. If the IARMIndex value is within the risk tolerance of the organization, the current values are included in the trending information and no further action is required until the next review cycle is initiated.
3. If the IARMIndex value is not within the risk tolerance of the organization:

a. The individual component index values that were aggregated to derive the IARMIndex value are examined and the value(s) furthest from the normalized value of 1.0 (the values closest to 0) is singled out for further analysis;
b. The selected component index value(s) is then unfolded (if applicable) to find the subcomponent(s) with the lowest value(s);
c. The component(s)/subcomponent(s) with the lowest value(s) is analyzed and a method for improving it is identified and implemented;
d. At management's discretion, reassess and recalculate the characteristic(s) (and any applicable subcharacteristic(s)) value(s) for the component(s) that was addressed and update the IARMIndex value to assess the impact of the changes made.

4. By looking at trends in the IARMIndex values, and the component index values compiled over time, the organization may determine the overall improvement resulting from addressing these components.
5. By looking at the IA OM® mapping and measurement trends in the component values, leadership or management can see which areas have had the greatest improvement, and which areas are most in need of attention.

Continuing with the example from above, the IARMIndex value = 0.35. Assuming the organization has determined that any value under 0.70 is outside of its risk tolerance, the next step is to determine which component(s) to single out for further analysis. Using the values in Table 4, we find that characteristics da_1 and da_2 have the lowest values. However, if we also consider the weightings we see that $w_1 = 1.0$ indicates that it is a higher priority item to the organization than w_2, suggesting that if we cannot address both areas, priority

should be given to characteristic1, reviewing and updating the organization's risk management strategy.

Weightings	Characteristics/ diagnostic areas
$w_1 = 2$	$da_1 = 0.25$
$w_2 = 1$	$da_2 = 0.25$
$w_3 = 1$	$da_3 = 0.65$

Table 4. Component Values and Their Weightings

5. Conclusion

The need to initially assess, and then conduct ongoing monitoring of an organization's overall risk posture, the risk posture of its assets, processes, and systems has been clearly established. The more valuable the information, asset, activity, or operation, the greater the need to increase the frequency of monitoring activities to ensure these resources are not compromised, or to identify and respond to any compromises as quickly as possible. This chapter shows how the IA OM® metric herein described provides an enterprise-wide risk management metric that can integrate synergistically with other risk management tools and efforts within an organization to provide monitoring personnel and decision-makers with the timely, accurate, and useful information they need to perform their functions and ensure their organization's mission and business functions are protected. IA OM® not only provides a metric targeted to organizational senior management, but one that can be used by decision-makers at all levels in the organization to ensure the processes and assets they are responsible for are protected in a way that aligns with the risk management strategy of the organization.

Author details

David R. Comings
Tenacity Solutions, Inc., United States of America

Wendy W. Ting
Department of Defense, United States of America

Acknowledgement

David R. Comings, Ph.D., CISSP, CRISC, *Tenacity Solutions, Inc., United States of America*, Dr. Comings specializes in information security, risk management, and strategic planning particularly for customers within the U.S. Government. Dr. Comings earned his doctorate at the University of Fairfax and his Master of Arts at the University of Pittsburgh.

Wendy W. Ting, Ph.D., CISSP, CISM, *Department of Defense, United States of America*, Dr. Ting specializes in performance metrics, cross domain information-sharing solutions, information security and systems security engineering. Dr. Ting earned her doctorate at the University of Fairfax and her Master of Science at the University of Maryland.

6. References

[1] Ting WW, Comings DR. Information Assurance Metric for Assessing NIST's Monitoring Step in the Risk Management Framework. Information Security Journal: A Global Perspective. 2010; 19(5): 253-62.

[2] NIST. SP 800-37, Revision 1: Guide for Applying the Risk Management Framework to Federal Information Systems. In: Commerce Do, ed.: National Institute of Standards and Technology 2010: 93.

[3] Wheeler E. Security Risk Management: Building an Information Security Risk Management Program from the Ground Up. Waltham, MA: Syngress 2011.

[4] Olivia LM, ed. IT Solutions Series: IT Security Advice from Experts. Hershey, PA: CyberTech Publishing 2004.

[5] Straub DW, Goodman S, Baskerville RL, eds. Information Security: Policy, Processes, and Practices. Armonk, NY M E Sharpe Inc. 2008.

[6] DeLuccia IV JJ. IT Compliance and Controls: Best Practices for Implementation. Hoboken, NJ: John Wiley & Sons, Inc. 2008.

[7] LeVeque V. Information Security: A Strategic Approach. Hoboken, NJ: John Wiley & Sons, Inc. 2006.

[8] Pironti JP. Changing the Mind-set - Creating a Risk-conscious and Security-aware Culture. ISACA Journal. 2012 2012; 2: 13-9.

[9] Johnson ME, Goetz E. Embedding Information Security into the Organization. IEEE Security & Privacy. 2007 (May/June): 16-24.

[10] HM Government. ITIL. 2012 [cited 2012 4/17/2012]; Available from: http://www.itil-officialsite.com/

[11] ISACA. COBIT 5: A Business Framework for the Governance and Management of Enterprise IT. 2012 [cited 2012 4/17/2012]; Available from: http://www.isaca.org/ COBIT/Pages/ default.aspx

[12] ISO/IEC. ISO/IEC 27001:2005 Information technology -- Security techniques -- Information security management systems -- Requirements. 2012 [cited 2012 4/17/2012]; Available from: http://www.iso.org/iso/catalogue_detail?csnumber=42103

[13] ISO/IEC. ISO/IEC 27002:2005 Information technology -- Security techniques -- Code of practice for information security management. 2012 [cited 2012 4/17/2012]; Available from: http://www.iso.org/iso/catalogue_detail?csnumber=50297

[14] ISO/IEC. ISO/IEC 27005:2011 Information technology -- Security techniques -- Information security risk management. Information Technology 2012 [cited 2012 4/17/2012]; Available from: http://www.iso.org/iso/iso_catalogue/catalogue_tc/ catalogue_detail.htm?csnumber=56742

[15] Johnson ME, ed. Managing Information Risk and the Economics of Security. New York, NY: Springer Science+Business Media, LLC 2009.
[16] Slay J, Koronios A. Information Technology Security & Risk Management. 3rd. ed. Milton, Qld: John Wiley & Sons Australia, LTD 2006.
[17] NIST. SP 800-39, Managing Information Security Risk: Organization, Mission, and Information System View. In: Commerce Do, ed.: National Institute of Standards and Technology 2011: 88.
[18] NIST. SP 800-30, Risk Management Guide for Information Technology Systems. In: Commerce Do, ed.: National Institute of Standards and Technology 2002.
[19] NIST. SP 800-53, Revision 3: Recommended Security Controls for Federal Information Systems and Organizations Gaithersburg, MD: National Institute of Standards & Technology; 2009.
[20] Jones A, Ashenden D. Risk Management for Computer Security. New York: Butterworth-Heinemann 2005.
[21] Donaldson SE, Siegel SG. Cultivating Successful Software Development. 1st ed. Upper Saddle River, NJ: Prentice Hall 1997.
[22] Donaldson SE, Siegel SG. Successful Software Development. 2nd ed. Upper Saddle River, NJ: Prentice Hall 2001.
[23] NIST. SP 800-64, Revision 2: Security Considerations in the System Development Life Cycle. In: Commerce Do, ed.: National Institute of Standards and Technology 2008.
[24] Ting WW. Interview with Stanley G. Siegel. Arlington, VA 2004.