IT Asset Valuation, Risk Assessment and Control Implementation Model

The first steps in information security strategic planning in any form of business are risk management and risk evaluation. This is necessarily broad, including business processes, people and physical infrastructure, as well as the information system. The security risk evaluation needs to assess the asset value to predict the impact and consequence of any damages, but it is difficult to apply this approach to systems built using knowledge-based architectures. Knowledge-based systems attempt to represent knowledge explicitly via tools, such as ontologies and rules, rather than implicitly via procedural code, the way a conventional computer program does. Usually, professionals face challenges to give assurance for organizations on asset valuation, risk management and control implementation practices due to the nonexistence of clear and agreed-on models and procedures. The main objective of this article is to propose simple and applicable models for professionals to measure, manage and follow up on assets, risk and controls implementation in the organization.

An ISACA® Journal volume 5, 2016, article titled “Information Systems Security Audit: An Ontological Framework” briefly describes the fundamental concepts (owner, asset, security objectives, vulnerability, threat, attack, risk, control and security audit) and their relationships to the whole security audit activities/process. This article proposes different models that help to measure and implement concepts objectively by using the previously proposed ontological framework and empirical study. The objectives are to identify risk-based auditable areas required to carry out asset valuation and to help measure risk and identification of the existing control gap of the company’s IT assets for regulatory, management and audit purposes.

The previous ontological framework briefly presents concepts hierarchically from asset valuation to control implementation processes for a specific asset based on the summarized steps. This article shows how to take the steps sensibly:

1. Identify the owner and custody of the asset.
2. Identify and list information systems assets of the organization. (List all interfacing applications, people, hardware or other containers for each asset.)
3. Containers are the place where an information asset or data “lives” or any type of information asset (data) is stored transported or processed.
4. Identify the security objectives of confidentiality, integrity and availability (CIA) and a weighting of the asset to conduct an impact assessment based upon the criticality of the asset to the operation of the company.
5. Identify the asset’s security categories and its estimated value.
6. Determine the threat and vulnerability’s quantitative value and rates.
7. Estimate the probability of occurrence/likelihood of impact.
8. Identify existing controls and perform a gap analysis.

Asset Identification, Valuation and Categorization

Identification, valuation and categorization of information systems assets are critical tasks of the process to properly develop and deploy the required security control for the specified IT assets (indicate data and container). Organizations or individuals able to implement security for assets by using this model must first identify and categorize the organization’s IT assets that need to be protected in the security process.
Mapping an information asset (such as data) to all of its critical containers leads to the technology assets, physical records and people that are important to storing, transporting and processing the asset. The map of information assets will be used to determine all of the information assets that reside on a specific container. In addition, the value of a container depends on the data that are processed and transported (through the network) or stored (reside) within that specific container. Security audits should look into how the data or information is processed, transferred and stored in a secured manner.

### Risk Assessment and Management

The risk assessment comprises the qualitative assessment and quantitative measurement of individual risk, including the interrelationship of their effects. Risk management constitutes a strategy to avoid losses and use available opportunities or, rather, opportunities potentially arising from risk areas. Normally, no single strategy will be able to cover all IT asset risk, but a balanced set of strategies will usually provide the best solutions. Once the risk is identified, it can be evaluated as acceptable or not. If it is acceptable, no further actions are required other than communicating and monitoring the risk, but if the risk is not acceptable, it must be controlled through four separate options of prevention and/or mitigation measures:

1. Reduce the impact.
2. Reduce the likelihood.
3. Transfer the risk (to insurance or a subcontractor).
4. Avoid the risk. (Temporarily distancing the target from the threat summarizes the potential impact definitions for the CIA security objectives.)

This article discusses risk mitigation strategy based on the CIA security objectives.

The overall objective of this section is to quantitatively measure risk impacts of an organization’s specific IT assets and to propose a proper mitigation strategy. Concepts from the International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) ISO/IEC 27001:2013, *Information technology—Security techniques—Information security management systems—Requirements,* and empirical analysis results taken from interviews with professionals are used to illustrate various conclusions and approaches to implementation. Hence, quantitative measurement of risk impact is implemented based on the following formula:

\[
\text{Risk Impact} = \text{Potential Risk} \times \text{Probability of Occurrence}
\]

### Potential Risk

This could be any type of risk that is conceivable for a business or any risk associated with an action that is possible in certain circumstances. This risk also refers to a threat or damage that may occur on operations of the business. When a business...
undertakes any operations within a particular industry and in specific markets, it faces potential risk. Risk potential should be estimated without a detailed consideration of the individual risk, at as little expense as possible. Potential risk is a product of total asset value, severity of vulnerability and severity of threat:

\[ \text{Potential Risk} = \text{Total Asset Value} \times \text{Severity of Vulnerability} \times \text{Severity of Threat} \]

**Probability of Occurrence**
This is an estimate of how often a hazardous event occurs. The likelihood can be expressed in terms of the frequency of occurrence. A review of historic events assists with this determination. Each hazard is rated in accordance with the numerical ratings and definitions shown in figure 1.

**Asset Valuation**
This is a method of assessing the worth of the organization’s information system assets based on its CIA security.

\[ \text{Total Asset Value} = \text{Asset Value} \times \text{Weight of Asset} \]

Assumptions for asset valuation include:
- The value of an asset depends on the sensitivity of data inside the container and their potential impact on CIA.
- CIA of information will have a minimum value of 1 for each.
- The value of levels for CIA are as follows: A rating of 3 is high, 2 is medium and 1 is low.
- The value of the information asset is determined by the sum of the three (C + I + A) attributes.

Based on the model, it is possible to create a matrix for value of an asset as illustrated in figure 2.

**Weight of Asset**
From interviews and the author’s practical experience, it can be concluded that the actual value of an asset is determined by the sensitivity value of data in the container. The reason is that all similar containers are not equally important to the organization, and the value of a container is determined by the data it holds, processes or transfers. For example, servers with equal capacity, technology and cost may have different weights due to the data they hold, process or transfer. A database containing employee information may have less value than one containing customer transactions. Equally, data on prominent customers may have more value than data on ordinary/walk-in customers, based on business/organizational objectives.

<table>
<thead>
<tr>
<th>Security Objective</th>
<th>Low (Rating of 1)</th>
<th>Medium (Rating of 2)</th>
<th>High (Rating of 3)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Confidentiality</strong></td>
<td>Limited adverse effect on organizational operations, assets or individuals.</td>
<td>Serious adverse effect on organizational operations, assets or individuals.</td>
<td>Severe or catastrophic adverse effect on organizational operations, assets or individuals.</td>
</tr>
<tr>
<td><strong>Integrity</strong></td>
<td>Limited adverse effect on organizational operations, assets or individuals.</td>
<td>Serious adverse effect on organizational operations, assets or individuals.</td>
<td>Severe or catastrophic adverse effect on organizational operations, assets or individuals.</td>
</tr>
<tr>
<td><strong>Availability</strong></td>
<td>Limited adverse effect on organizational operations, assets or individuals.</td>
<td>Serious adverse effect on organizational operations, assets or individuals.</td>
<td>Severe or catastrophic adverse effect on organizational operations, assets or individuals.</td>
</tr>
</tbody>
</table>

*Source: Shemise Gebremedhin Kassa. Reprinted with permission.*

Enjoying this article?
- Read COBIT® 5 for Risk. [www.isaca.org/cobit-risk](http://www.isaca.org/cobit-risk)
- Learn more about, discuss and collaborate on risk management in the Knowledge Center. [www.isaca.org/risk-management](http://www.isaca.org/risk-management)
Therefore, to evaluate the sensitivity of assets, the concept of “weight” or “weighting” was developed, which helps to measure each asset’s value based on the data it holds/processes compared to other assets. To measure the value of the asset’s weight, the rating concepts shown in Figure 3 can be used—3 for high, 2 for medium and 1 for low—to show value of a specific asset as compared to the another asset, based on business objectives. This concept differentiates this approach for the asset valuation concept.

Therefore, according to the CIA matrix and the weight of an asset model, it is possible to determine the following total asset value using an asset weight matrix table as shown in Figure 4.
standards, poorly managed flammable liquids and poor circuit insulation are some of the weaknesses (vulnerabilities) or factors that help the fire threat to happen and cause damage.

Exposure (attacker access to the flow) is the potential exposure to loss, resulting from the occurrence of one or more threat events. It may be disseminated across other system components. Figure 5 depicts a model to rate the susceptibility and exposure of a flow or vulnerability of an asset.

To measure the overall value of the severity of a vulnerability, the combination of the value of susceptibility and exposure rating must first be decided, as shown in Figure 7. (Note: This rating table is similarly used for threat factors [impact and capability rating] in the following threat assessment section.)

Vulnerability and threat valuation assumptions include:
- The same 1 to 3 rating scale will be used, in which a specific vulnerability or threat rated as high is assigned a 3, medium a 2 and low a 1 (figure 5).
- The severity of the threat and the vulnerability is graded as very low (1), low (2), medium (3), high (4) and very high (5) (figure 6).

**Vulnerability Rating Factors**

Vulnerability is the intersection of three elements: a system susceptibility or flaw, attacker access to the flaw, and attacker capability to exploit the flaw.13

Susceptibility is simply to measure the effort required to successfully exploit a given weakness. For example, fire is a threat. Poor fire prevention standards, poorly managed flammable liquids and poor circuit insulation are some of the weaknesses (vulnerabilities) or factors that help the fire threat to happen and cause damage.

<table>
<thead>
<tr>
<th>SUSCEPTIBILITY</th>
<th>Rating</th>
<th>EXPOSURE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Minor susceptibility: Vulnerability requires significant resources to exploit with little potential for loss.</td>
<td>1</td>
<td>Minor exposure: Effects of the vulnerability are tightly contained and do not increase the probability of additional vulnerabilities being exploited.</td>
</tr>
<tr>
<td>Moderate susceptibility: Vulnerability requires significant resources to exploit with significant potential for loss. Or, vulnerability requires little resources to exploit, moderate potential for loss.</td>
<td>2</td>
<td>Moderate exposure: Vulnerability can be expected to affect more than one system element or component. Exploitation increases the probability of additional vulnerabilities being exploited.</td>
</tr>
<tr>
<td>High susceptibility: Vulnerability requires few resources to exploit with significant potential for loss.</td>
<td>3</td>
<td>High exposure: Vulnerability affects a majority of system components. Exploitation significantly increases the probability of additional vulnerabilities being exploited.</td>
</tr>
</tbody>
</table>

Source: Shemlse Gebremedhin Kassa. Reprinted with permission.

<table>
<thead>
<tr>
<th>Rating</th>
<th>Grade</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Very low (VL)</td>
<td>Minor exposure, minor susceptibility</td>
</tr>
<tr>
<td>2</td>
<td>Low (L)</td>
<td>Minor exposure, moderate susceptibility; or moderate exposure, minor susceptibility</td>
</tr>
<tr>
<td>3</td>
<td>Medium (M)</td>
<td>Highly exposed, minor susceptibility; or minor exposure, high susceptibility; or moderate exposure, moderate susceptibility</td>
</tr>
<tr>
<td>4</td>
<td>High (H)</td>
<td>Highly exposed, moderate susceptibility; or moderate exposure, high susceptibility</td>
</tr>
<tr>
<td>5</td>
<td>Very high (VH)</td>
<td>Highly exposed, high susceptibility</td>
</tr>
</tbody>
</table>

Source: Shemlse Gebremedhin Kassa. Reprinted with permission.
the threat agent’s technical ability, knowledge and available material to exploit the vulnerability.

As with vulnerability measurement elements (susceptibility and exposure), rating, capability and impact should also be considered for threat measurement. Figure 8 shows how to use capability and impact for threat ratings.

The model for grading the severity of the threat uses impact and capability of the threat, similar to the severity of vulnerability matrix in Figure 6 and Figure 7. The only difference is susceptibility and exposure for vulnerabilities are replaced with impact and capability for threat.

**Risk Impact Measurement**

Risk management is the act of determining what threats the organization faces, analyzing the vulnerabilities to assess the threat level and determining how to deal with the risk. Security risk management is a strategy of management to reduce the possible risk from an unacceptable to an acceptable level. There are four basic strategies for managing risk: transference, acceptance, avoidance and mitigation.

**Threats Assessment and Rating Methodology**

A general list of threats should be compiled, which is then reviewed by those most knowledgeable about the system, organization or industry to identify those threats that apply to the system. Each threat is derived from a specific vulnerability, rather than identifying threats generally without considering vulnerability. Measuring the value of a threat depends on the rating value of its impact and capability. Impacts are a forceful consequence or a strong effect of the launch of a threat on the business.

Capability is a measure of a threat agent's ability (including the level of effort required) to successfully attack an asset by exploiting its vulnerabilities, e.g.,
Risk assessment requires individuals to take charge of the risk management process. Risk assessment is the determination of a quantitative or qualitative estimate of risk related to a well-defined situation and a recognized threat (also called a hazard). Quantitative risk assessment requires calculations of two components of risk: the magnitude of the potential risk and the probability that the loss will occur.\textsuperscript{18}

Risk Impact = Potential Risk \times Probability

### Probability or Likelihood of Risk

A likelihood assessment estimates the frequency of a threat happening. With this type of assessment, it is necessary to observe the circumstances that will affect the probability of the risk occurring. The likelihood can be expressed in terms of the frequency of occurrence,\textsuperscript{19} which are depicted in figure 9.

**Figure 9—Model for Probability or Likelihood of Risk**

<table>
<thead>
<tr>
<th>Value</th>
<th>Description of Probability</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Never happened (has not happened in the past three years)</td>
</tr>
<tr>
<td>2</td>
<td>Rare (happens once in year)</td>
</tr>
<tr>
<td>3</td>
<td>Periodic (happens once in a quarter)</td>
</tr>
<tr>
<td>4</td>
<td>Regular (takes place once in a fortnight)</td>
</tr>
<tr>
<td>5</td>
<td>Frequent (happens once in a week)</td>
</tr>
</tbody>
</table>

Source: Adapted from ISO 27001 implementers forum. Reprinted with permission.

Based on the previously discussed risk analysis concepts, risk mitigation options are acceptable, tolerable and intolerable risk, the values of which follow.

**Figure 10—Examples for Potential Risk and Risk Impact**

<table>
<thead>
<tr>
<th>Total Asset Value</th>
<th>Vulnerability Severity Value</th>
<th>Threat Severity Value</th>
<th>Potential Risk</th>
<th>Probability</th>
<th>Risk Impact Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>1 (VL)</td>
<td>1 (VL)</td>
<td>3\times1\times1=3</td>
<td>3 (Periodic)</td>
<td>3\times3 = 9</td>
</tr>
<tr>
<td>9</td>
<td>3 (M)</td>
<td>3 (M)</td>
<td>9\times3\times3=81</td>
<td>4 (Regular)</td>
<td>81\times4 = 324</td>
</tr>
<tr>
<td>20</td>
<td>4 (H)</td>
<td>4 (H)</td>
<td>20\times4\times4=320</td>
<td>2 (Rare)</td>
<td>320\times2 = 640</td>
</tr>
<tr>
<td>27</td>
<td>5 (VH)</td>
<td>5 (VH)</td>
<td>27\times5\times5=675</td>
<td>5 (Frequent)</td>
<td>675\times5 = 3375</td>
</tr>
</tbody>
</table>

Source: Shemlse Gebremedhin Kassa. Reprinted with permission.
The value of the control implementation is determined by the sum of the three attributes.

Based on figure 10, a control matrix is presented in figure 11.

![Figure 11—Model for Rating CIA Control Implementation](image)

<table>
<thead>
<tr>
<th>Rate</th>
<th>Security Objective</th>
</tr>
</thead>
<tbody>
<tr>
<td>None (0)</td>
<td>CIA is not implemented for the company asset, operation or individuals.</td>
</tr>
<tr>
<td>Low (1)</td>
<td>CIA is limited or is at a low level of implementation for the company asset, operation or individuals.</td>
</tr>
<tr>
<td>Medium (2)</td>
<td>CIA is at an intermediary level of practicability for the company asset, operation or individuals.</td>
</tr>
<tr>
<td>High (3)</td>
<td>CIA is at a strong level of achievability for the company asset, operation or individuals.</td>
</tr>
</tbody>
</table>

Source: Shemlse Gebremedhin Kassa. Reprinted with permission.

Figure 12 shows calculations for existing controls and risk mitigation.

Adding controls to mitigate the risk impact first requires identification of the existing control (the total amount of control measured by adding the value of CIA for each asset), then identification of the possible control (the sum of a control value of CIA derived by considering the maximum technology applied to that specific asset and the conditions to satisfy adoption of that additional control).

The following formulas will calculate the “to be controlled risk” and the “mitigated risk”:

\[
\text{To Be C} = \text{Maximum Possible Control} - \text{Existing Control}
\]

\[
\text{Mitigated Risk} = \frac{\text{Risk Impact}}{\text{Existing Control}}
\]

No organization can ever be 100 percent secure or free of risk. There will always be remaining, or residual, risk. In the first example shown in figure 13, the possible control is equal to the existing control (which is high for CIA). Therefore, the remaining risk, 375, is residual, not mitigated further because it already represents the maximum possible control. As per the risk analysis concepts described in this article, the 375 risk is acceptable because it is less than the maximum acceptable risk level of 540.

**Conclusion**

Managing the risk and valuation of an organization’s valuable IT assets is the first and critical stage of information security planning and security control implementation. Objectively measuring concepts like vulnerability, threat, risk impact, mitigated risk...
and implemented control of an asset is relatively the most difficult task in the process, because of a lack of uniformity on subjective judgments during the rating selection (high, low, medium) and the quality and accuracy of the results are highly dependent on the assessors' professional experience. The models described in this article can minimize error and introduce uniformity of activities and process results carried out by different individuals/organizations. Generally, information security risk management/evaluation is still a very complex field of research, with a lot of unexplored areas. More research is needed to explore essentials. This research work can be based on the model proposed in this article and perhaps could be focused on creating mechanical or robotic techniques to implement quantitative measurement, thus avoiding subjective judgments of high, low or medium.

Endnotes

6 Op cit, Foroughi
8 Op cit, Foroughi
9 Ibid.
12 Op cit, Shemlse
13 Kiyuna, A.; L. Conyers; Cyberwarfare Source Book, Lulu.com, 14 April 2015, p. 42
15 Gregg, M.; CISSP Exam Cram 2, Pearson IT Certification, USA, 2005
16 Op cit, Elky
17 Ibid.
19 Op cit, Kamat
20 Ibid.
21 Op cit, Gregg
22 Ibid.