6.5 Risk Determination

Risk determination is the final stage of a risk-assessment process, and incorporates the results from an asset valuation, a threat assessment and a vulnerability assessment. Using the input of these patterns, the enterprise is able to evaluate and prioritize the risks to its assets.

Also Known As

Risk Evaluation

Example

The museum has identified the following assets as part of the its risk assessment:

Information asset types

- Museum employee data
- Museum financial/insurance data, partner financial data
- Museum contractual data and business planning
- Museum research and associated data
- Museum advertisements and other public data
- Museum database of collections information

Physical assets

- Museum building
- Museum staff
- Museum collections and exhibits
- Museum transport vehicles

It has also completed the three major steps in a risk assessment, as defined by ASSET VALUATION (103), THREAT ASSESSMENT (113), and VULNERABILITY ASSESSMENT (125). It must now assimilate this information, evaluate the overall risk, and present the results.

Context

An enterprise has defined the assets to be included in a risk assessment and has evaluated the importance of those assets in an asset valuation table. As well, it has performed a threat assessment and vulnerability assessment and collected unique combinations of threats and vulnerabilities in a threat-vulnerability table.

Problem

Once the work has been done to determine an asset's worth and assess the threats and vulnerabilities that affect it, its overall risk needs to be determined. Without a formal method for determining risk, how can one be assured that effort expended in protecting an asset is too high or too low?

How does an enterprise evaluate the risks posed to its assets?

An enterprise must resolve the following forces:

- The results of the risk assessment must be understood by the executive team if they are to address risk in the enterprise effectively.
- Determination of risk is directly related to asset value, threat likelihood, and vulnerability severity.
- Conducting a risk assessment requires resources such as time, people and project funding, as well as a commitment to follow up the results.
- Quantitative risk measures imply greater precision and are therefore preferred over qualitative indicators, but only if the quantitative scores are based on adequate measurements: false precision in risk levels is misleading.

Solution

Systematically determine the risk that is posed to each enterprise asset. This process involves the following four steps:

1. Collect results from ASSET VALUATION (103), THREAT ASSESSMENT (113) and VULNERABILITY ASSESSMENT (125).

   Recall that the previous stages of the risk assessment are the asset valuation, threat assessment and vulnerability assessment. Apply those patterns and collect the following:

   - The asset valuation table: this table shows the overall value of enterprise assets.
   - The threat-vulnerability table: this table is a catalog of threats and their associated vulnerabilities. Each threat includes a likelihood rating, and each vulnerability includes a severity rating.

2. Associate threat-vulnerability pairs with assets.

   Using the threat-vulnerability table, identify all threat-vulnerability pairs that pose a direct risk to each asset separately.

3. Evaluate risk.

   Evaluate a risk equation using the numerical values for asset valuation, threat likelihood and vulnerability severity. The result will represent the final risk posed to each asset.

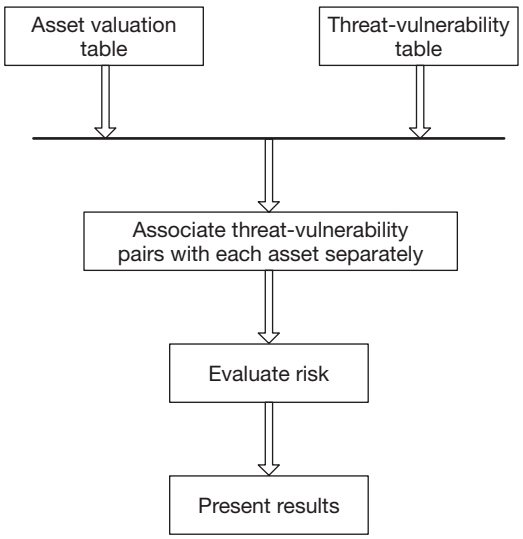
4. Present the results.

   Sort the results in order of decreasing risk. Use qualitative terms, a color scale or other scale system (as appropriate) to display the results.

Dynamics

The allowable sequence for performing RISK DETERMINATION (137) is shown in the figure:

- First, collect the asset valuation and threat-vulnerability tables from ASSET VALUATION (103) and VULNERABILITY ASSESSMENT (125), respectively.
- Use a risk equation to calculate the risk posed to each asset.
- Finally, sort and present the results in descending order.



Risk determination sequence constraints

Implementation

The implementation of the process for risk determination is described below.

1. Collect results from ASSET VALUATION (103), THREAT ASSESSMENT (113) and VULNERABILITY ASSESSMENT (125). Apply these three patterns and collect the asset valuation and threat-vulnerability tables.
2. Associate threat-vulnerability pairs with assets.

   In both THREAT ASSESSMENT (113) and VULNERABILITY ASSESSMENT (125), we grouped assets by either physical or information type, rather than individually. At this stage of RISK DETERMINATION (137), we now need to consider the threat-vulnerability pairs for each asset separately.

   The threat-vulnerability table lists all threat actions and their corresponding vulnerabilities. Each of these pairs may pose a risk to one or more informational or physical assets. Therefore, identify all the threat-vulnerability pairs that affect each asset directly. The condition of 'affecting directly' is important, because to associate all threat-vulnerability pairs for every asset would lead to identical and, ultimately, meaningless results. However, a single threat-vulnerability pair may certainly affect multiple assets directly.
3. Evaluate risk.

   Regardless of the actual equation or method used to evaluate risk, it must consider the following properties:

   - The more vulnerabilities that exist in an asset and the systems that enable access to it, the greater the risk.
   - The more severe the vulnerabilities, the greater the risk.
   - The greater number of threats that could exploit a vulnerability, the greater the risk.
   - The more likely the threats, the greater the risk.
   - The more valuable an asset, the greater the risk.
   - The risk to an asset is zero if no threats or vulnerabilities exist for that asset.

   Any number of equations could be used to calculate a risk value, including those presented in the Variants and Known Uses sections. For the purposes of this pattern, we will use the following equation for each asset included in the scope of the risk assessment:

   $$\text{Risk}(A) = \text{SUM}[\text{Threat} * \text{Vulnerability}](A) * \text{Asset Value}(A)$$

This can be read as, 'the risk to asset 'A' is the sum of all unique combinations of threat likelihood, multiplied by the vulnerability severity, multiplied by the asset value.'

4. Present the results.

   Present the results in order of descending risk. The greatest risk will have the highest numerical value, whereas the lowest risk will have the lowest numerical value. All values will be greater than zero, and the numbers will most certainly vary from one risk assessment to another.

   If necessary, the raw numerical values can be presented in a table. However, a more intuitive effect can be achieved by using qualitative terms, consistent with those used throughout the risk assessment pattern set. First, on a scale of 1 (representing the lowest possible risk value) to the highest risk value, create 6 equal ranges, labeled as: Negligible, Low, Medium, High, Very high and Extreme. Then group each asset according to its qualitative value.

   4.1. Understanding and presenting the results.

   The importance of sorting and clearly presenting the results to a senior management team cannot be overemphasized. It is their task to interpret the results and develop plans to mitigate, transfer or accept the risk, often as part of an overall risk management strategy. Generally, this senior management team will only be interested in the risk values relative to other assets, so the actual value itself is not important. An exception to this is when the results from one assessment are compared with those from another assessment, perhaps from previous years. A declining value, for example, would demonstrate a reduction in risk, either due to fewer or less likely threats, more effective security controls, or declining asset value.

   4.2. Qualitative versus quantitative risk determination.

   Although the final results can be given in numerical terms, RISK DETERMINATION (137) (as with ASSET VALUATION (103), THREAT ASSESSMENT (113) and VULNERABILITY ASSESSMENT (125)) is very much a qualitative process. The values used in these patterns reflect the relative numerical values, rather than objective, quantifiable numbers.

Example Resolved

Using the asset valuation table and threat-vulnerability table as input to RISK DETERMINATION (137), the museum has evaluated and prioritized the risks to its assets. The complete results of the risk equation for three museum assets are presented below, and the remaining results are summarized in Table 6.22.

Evaluation of Risk Equation

1. Risk evaluation for museum building.

   From the threat-vulnerability table of VULNERABILITY ASSESSMENT (125), the museum has identified three threat-vulnerability pairs that affect the museum building, as shown in Table 6.19.

   ASSET VALUATION (103) identified the museum building as having a value of 6. The risk equation can therefore be written as follows:

   $$\text{Risk} = (3*6 + 3*5 + 3*4) * 6$$
   $$\text{Risk} = (18 + 15 + 12) * 6$$
   $$\text{Risk} = (45) * 6$$
   $$\text{Risk (museum building)} = 270$$

Table 6.19 Threat-vulnerability pairs for museum building

THREAT ACTION (FREQUENCY)	VULNERABILITY (SEVERITY)
Natural	
Museum fire (3)	Failure of fire alarm system (6) Failure of fire suppression system (5)
Fatigue of support fixtures, building structural failure (3)	Lack of regularly scheduled inspections (4)

2. Risk evaluation for museum collections and exhibits.

   The museum collections and exhibits asset has an asset value of 6, with the threat-vulnerability pairs as shown in Table 6.20.

   $$\text{Risk} = (33 + 12 + 16 + 12 + 12 + 8 + 20 + 12 + 6) * 6$$
   $$\text{Risk} = (131) * 6$$
   $$\text{Risk (museum collections and exhibits)} = 786$$

3. Risk evaluation for museum employee data.

   $$\text{Risk} = (12 + 12 + 21 + 15 + 10 + 9) * 5$$
   $$\text{Risk} = 79 * 5$$
   $$\text{Risk (museum employee data)} = 395$$

Table 6.20 Threat-vulnerability pairs for museum collections and exhibits

THREAT ACTION (FREQUENCY)	VULNERABILITY (SEVERITY)
Natural	
Museum fire (3)	Failure of fire alarm system (6) Failure of fire suppression system (5)
Fatigue of support fixtures, building structural failure (3)	Lack of regularly scheduled inspections (4)
Failure of monitoring and alarm systems (4)	Lack of regularly scheduled inspections (4)
Professional criminals	
Theft of museum collections and exhibits (2)	Lack of regular alarm testing procedures (3) Lack of adequate storage and protection of physical assets (3)
Physical attack against employees (3)	Lack of security training for employees (4)
Employees	
Accidental damage to museum collections and exhibits (4)	Carelessness of employees when handling/cleaning exhibits (2)
Theft of museum collections and exhibits (2)	Lack of regular alarm testing procedures (3) Lack of adequate storage and protection of physical assets (3) Susceptibility of employees to bribery (4)
Misconfiguration of monitoring and alarm systems (4)	Lack of regular alarm testing procedures (3)
Museum patrons	
Accidental damage to museum collections and exhibits (3)	Carelessness of museum patrons when viewing exhibits (2)

Table 6.21 Threat-vulnerability pairs for museum employee data

Natural	
Electrical spike in computer room (3)	Lack of surge protection, uninterruptible power system (UPS) (4)
Loss of electronic documents (3)	Incomplete or corrupt data backups (4)
Professional criminals	
Theft of information assets (3)	Susceptibility of employees to bribery (3) Lack of proper physical controls for document storage (locks, safe) (4)
Employees	
Unauthorized access of informational assets (5)	Weak information security controls enabling unauthorized access (3)
Data entry errors (5)	Lack of data validation during form input (2)
Leaking confidential information (3)	Exposure of information assets (3)

4. Complete results.

   Risk values have been calculated for the remaining assets and are presented in Table 6.22.

Table 6.22 Prioritized risks for museum assets

ASSET	RISK VALUE
Museum collections and exhibits	786
Museum employee data	395
Museum staff	342
Museum financial/insurance data, partner financial data	316
Museum building	270
Museum contractual data and business planning	232
Museum database of collections information	232
Museum research and associated data	147
Museum transport vehicles	120
Museum advertisements and other public data	98

Presentation of results

6 equal ranges (from 1 to 786) have been created, as shown in Table 6.23, and the final qualitative results are presented in Table 6.24.

Table 6.23 Qualitative risk translation

RATING	RANGE
Extreme	656–786
Very high	525–655
High	394–524
Medium	263–393
Low	132–262
Negligible	1–131

Table 6.24 Qualitative risks for museum assets

ASSET	RISK
Museum collections and exhibits	Extreme
Museum employee data	High
Museum staff	Medium
Museum financial/insurance data, partner financial data	Medium
Museum building	Medium
Museum contractual data and business planning	Low
Museum database of collections information	Low
Museum research and associated data	Low
Museum transport vehicles	Negligible
Museum advertisements and other public data	Negligible

Variants

An alternative formula for risk determination is provided by [Mei03]:

Risk = Probability * Damage Potential

in which both the probability and damage potential variables are represented numerically as values from 1 to 10, giving a minimum and maximum risk value of 1 and 100 respectively. To achieve qualitative results, 'low' represents any risk from 1 to 33, 'medium' represents risks from 34 to 66, and 'high' represents risks from 67 to 100. Note that because this method is threat- based, it gives the risk of a particular threat, as opposed to the risk posed to an asset.

Appendix E of [ISO13335-3] provides a number of examples of the use of matrices to evaluate risk, in which each example places emphasis differently. One example offers an asset-based evaluation, whereas another assesses the risk of given threats. While these examples recognize the inherent relationship between threats and vulnerabilities, they do not provide a formal way of accounting for them.

Known Uses

[NIST800-30] uses a 3x3 matrix made up of threat likelihood and threat impact. Qualitative values of threat likelihood (high, medium, low) are converted numerically to ratings of 1.0, 0.5, and 0.1 respectively. Qualitative values of threat impact (high, medium, low) are converted numerically to ratings of 100, 50, and 10 respectively. Risk is then computed by multiplying the threat likelihood by threat impact for each identified threat-vulnerability. The resulting value represents the 'degree or level to which an IT system, facility or procedure might be exposed if a given vulnerability were exercised.' Note that while this method is clear and straightforward, it does not provide an overall risk rating to a given asset, but simply the risk of a single threat-vulnerability pair.

[Pel01] describes an Annual Loss Exposure (ALE)—an equation that provides a quantitative method for calculating loss. The ALE is calculated from the value of an asset (A) multiplied by the likelihood of a threat occurrence (L) as follows: ALE = A * L. The likelihood value used is calculated from a multiplier table in which an occurrence of once a day is 365, once a month is 12, once a year is 1, once every 5 years is 1/5, and so on.

Consequences

This pattern has the following benefits:

- The enterprise is now able to identify and address the risks posed to its assets, as part of a risk mitigation effort.

- The qualitative results provided are much easier to calculate, prioritize and interpret.
- The results can be archived and used to track the progress of asset risk among consecutive risk assessments.

As well as the following liabilities:

- The risk equation may not account for all the properties of the relationship between threat, vulnerability, and asset value.
- The results are based on the completeness and subjectivity of ASSET VALUATION (103), THREAT ASSESSMENT (113) and VULNERABILITY ASSESSMENT (125), and therefore cannot be objectively verified or guaranteed.
- Because of the various methods for calculating an actual risk value, an enterprise may find it difficult to identify the particular equation that meets their risk assessment needs.