Technical Guide

Requirements for Risk Assessment Methodologies

Technical Guide

Requirements for Risk Assessment Methodologies

ISBN: 1-931624-78-X

Document Number: G081

Published by The Open Group, January 2009.

Comments relating to the material contained in this document may be submitted to:

The Open Group
Thames Tower
37-45 Station Road
Reading
Berkshire, RG1 1LX
United Kingdom

or by electronic mail to:

ogspecs@opengroup.org

Contents

Preface

The Open Group

The Open Group is a vendor-neutral and technology-neutral consortium, whose vision of Boundaryless Information Flow™ will enable access to integrated information within and between enterprises based on open standards and global interoperability. The Open Group works with customers, suppliers, consortia, and other standards bodies. Its role is to capture, understand, and address current and emerging requirements, establish policies, and share best practices; to facilitate interoperability, develop consensus, and evolve and integrate specifications and Open Source technologies; to offer a comprehensive set of services to enhance the operational efficiency of consortia; and to operate the industry's premier certification service, including UNIX® certification.

Further information on The Open Group is available at www.opengroup.org.

The Open Group has over 15 years' experience in developing and operating certification programs and has extensive experience developing and facilitating industry adoption of test suites used to validate conformance to an open standard or specification.

More information is available at www.opengroup.org/certification.

The Open Group publishes a wide range of technical documentation, the main part of which is focused on development of Technical and Product Standards and Guides, but which also includes white papers, technical studies, branding and testing documentation, and business titles. Full details and a catalog are available at www.opengroup.org/bookstore.

This Document

This document is the Guide to the Requirements for Risk Assessment Methodologies. It has been developed and approved by The Open Group.

This Guide is the second of an initial set of three Open Group publications addressing Risk Management:

- **The Open Group Technical Standard: Risk Taxonomy** provides a rigorous set of definitions and a taxonomy for information security risk, as well as information regarding how to use the taxonomy. The intended audience for this document includes anyone who has the need to understand and/or analyze a risk condition. This includes, but is not limited to:
  - Information security and risk management professionals
  - Auditors and regulators
  - Technology professionals
  - Management

- **The Open Group Technical Guide: Requirements for Risk Assessment Methodologies** (this document) identifies and describes the key characteristics that make up any effective risk assessment methodology, thus providing a common set of criteria for evaluating any given risk assessment methodology against a clearly defined common set of essential requirements. In this way, it explains what features to look for when evaluating the capabilities of any given methodology, and the value those features represent.
- **The Open Group Technical Standard: Risk Assessment Methodology & Cookbook** describes in detail how to apply the FAIR (Factor Analysis for Information Risk) methodology to a selected risk management framework, in the form of an application paper. FAIR is complementary to other methodologies like COSO, ITIL, ISO/IEC 27002:2005, COBIT, OCTAVE, etc. – it provides the engine that can be used in other risk models. The Cookbook part of this document enables risk technology practitioners to follow by example how to create their own application to apply FAIR to other frameworks of their choice.

Trademarks

Boundaryless Information Flow™ and TOGAF™ are trademarks and Making Standards Work®, The Open Group®, UNIX®, and the "X" device are registered trademarks of The Open Group in the United States and other countries.

COBIT® is a registered trademark of the Information Systems Audit and Control Association and the IT Governance Institute.

ITIL® is a registered trademark of the Office of Government Commerce in the United Kingdom and other countries.

OCTAVE® (Operationally Critical Threat, Asset, and Vulnerability Evaluation) is a registered trademark of CERT at Carnegie Mellon University (see www.cert.org/octave).

The Open Group acknowledges that there may be other brand, company, and product names used in this document that may be covered by trademark protection and advises the reader to verify them independently.

Acknowledgements

The Open Group gratefully acknowledges the contribution of the following people in the development of this Guide:

- Alex Hutton, CEO, Risk Management Insight (www.riskmanagementinsight.com)
- Jack Jones, CTO, Risk Management Insight
- Members of the Security Forum who have contributed to the development of this Guide

Referenced Documents

The following documents are referenced in this Guide:

- COBIT (Control Objectives for Information and related Technology), Information Systems Audit and Control Association (ISACA); refer to www.isaca.org
- COSO (Committee of Sponsoring Organizations) Enterprise Risk Management Framework; refer to www.coso.org
- ISO/IEC 27002:2005: Information Technology – Security Techniques – Code of Practice for Information Security Management
- ITIL (Information Technology Infrastructure Library); refer to www.itil-officialsite.com/home
- OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation); refer to www.cert.org/octave
- Risk Taxonomy Technical Standard, January 2009 (ISBN: 1-931624-77-1, C081), published by The Open Group
- Risk Assessment Methodology & Cookbook Technical Standard (due Q2/2009), published by The Open Group

1 Introduction

Over time, the information security/risk management profession has developed a variety of methods for assessing risk within an organization. These methods often reflect the conditions and objectives of the organization being assessed (as understood by the assessor), the prevailing practices within the profession at the time, the experience and knowledge level of the assessor(s), as well as any bias or agenda the assessor(s) might bring to the table. Another important factor that has often played a role is the definition of "risk" as used within the methodology.

As a result of these variables, risk assessment results have varied widely in terms of consistency, accuracy, and utility to management. This Guide seeks to identify and articulate the characteristics that make up effective risk assessment methodologies, thus providing a standard set of guidelines for risk assessment methodologies.

1.1 Intended Audience

The intended audience for this Guide is anyone who is tasked with selecting, performing, evaluating, or developing a risk assessment methodology. This includes all stakeholders who have responsibilities covering these areas, including business managers, information security/risk management professionals, auditors, and regulators both acting as policy-makers and as law-makers.

1.2 Business Case

In the overall context of risk management, it is important to appreciate that our business objective in performing risk assessments is to identify and estimate levels of exposure to the likelihood of loss, so that business managers can make informed business decisions on how to manage those risks of loss – either by accepting each risk, or by mitigating it – through investing in appropriate internal protective measures judged sufficient to lower the potential loss to an acceptable level, or by investing in external indemnity. Critical to enabling good business decision-making therefore is to use risk assessment methods which give the most objective, meaningful, consistent results.

With this in mind, a number of challenges exist as a result of the current risk assessment methodology landscape, including:

- Assessment results can't reliably be compared, either between different organizations/scenarios or even amongst assessments performed on a single organization. Consequently, risk posture comparisons and trend analyses within and between industries are difficult if not impossible. Likewise, tracking risk posture improvement within an organization becomes challenging.

- Management and others needing to select and perform a risk assessment may not be able to differentiate more effective methodologies from less effective ones. As a result, their chosen methodology may not provide them with the information they need.
- Those developing risk assessment methodologies will continue to introduce variability into the landscape, exacerbating the current condition.

1.3 Scope

In order to provide guidance without unnecessarily limiting assessment methodology evolution or the ability to craft proprietary assessment practices, coverage in this Guide is limited to describing foundational characteristics that describe effective methodologies. This Guide does not describe a specific methodology.

1.4 Using this Guide

This Guide may be used to help:

- Evaluate whether a given risk assessment methodology meets management needs
- Distinguish between methodologies in order to choose the one that most closely meets management needs
- Evaluate whether a given methodology effectively assesses risk (rather than simply some sub-element of risk; e.g., control conditions)
- As a reference for developing or evolving risk assessment methodologies

1.5 Definition of Terms

This Guide leverages the terminology provided in The Open Group Technical Standard: Risk Taxonomy. Borrowing from that document, the following key definitions apply here:

Risk	The probable frequency and probable magnitude of future loss.
Threat	Anything that is capable of acting in a manner resulting in harm to an asset and/or organization; for example, acts of God (weather, geological events, etc.), malicious actors, errors, failures.
Vulnerability	The probability that threat capability exceeds the ability to resist the threat.
Asset	Any data, device, or other component of the environment that supports information-related activities, which can be illicitly accessed, used, disclosed, altered, destroyed, and/or stolen, resulting in loss.

2 Key Operating Assumptions

Before describing requirements, it is important to lay out the key operating assumptions that drive those requirements. Keeping in mind the adage that it's best to "begin with the end in mind", this Guide will describe assumptions regarding the fundamental purpose risk assessments serve (i.e., results). These assumptions regarding results will then drive assumptions and requirements regarding the methods used to achieve those results:

- An organization's management team is responsible for seeing that the organization's objectives are met.
- Management has a finite set of resources available in order to meet those objectives.
- There exists a broad spectrum of risk conditions that can interfere in meeting those objectives.
- Management needs accurate and useful information regarding the risk issues it faces and the options it has available so that it can cost-effectively apply its limited resources to the portfolio of risk issues.
- Risk management decisions may, on occasion, have to be defended to key stakeholders (e.g., auditors, regulators, business partners, judges/juries, investors, etc.).
- Risk assessments are intended to provide management with the accurate and useful information needed to make timely, well-informed, effective, and defensible risk management decisions.

3 What Makes a Good Risk Assessment Methodology?

It is important that the information provided by the risk assessment is meaningful to both IT and non-IT management. There is one key component and several key traits that can help a risk assessment methodology provide meaning to an organization.

3.1 Key Component: Taxonomy

First and foremost, the risk management framework should provide a taxonomy for risk. Taxonomies are used to help those who study a certain body of knowledge to describe and define their problem space. A taxonomy provides a means for categorizing the information around us and helps organize the volumes of information in the field, increase the effectiveness of communication, and develop standardization.

A taxonomy for risk should seek to remove the ambiguity from terms like threat, vulnerability, and risk (itself having valid but similar definitions to threat and vulnerability).

3.2 Key Risk Assessment Traits

This section describes the traits that are indicative of a good risk assessment methodology. The set of traits provided is by no means complete or comprehensive, but establishes the fundamental concepts that risk assessment methodology development should strive for.

3.2.1 Probabilistic

A study and analysis of risk is a difficult task. Such an analysis involves a discussion of potential states, and it commonly involves using information that contains some level of uncertainty. And so, therefore, an analyst cannot exactly know the risk in past, current, or future state with absolute certainty.

But ultimately a statement concerning risk is a belief statement – a belief statement that is simply the act of describing the issue currently at hand (sometimes referred to as a "state of nature") based on the evidence available at the time. The act of creating a belief statement based on evidence lends itself to using probabilistic methods. Treating risk as a probability problem can add needed rigor, scrutiny, and structure to the risk analysis process and outcome.

A good risk assessment methodology will be organized so as to assist the analyst in creating probabilities for risk and its component factors.

3.2.2 Accurate

A good risk assessment methodology should deliver accurate results. And while it seems self-evident that the results of the risk assessment should be accurate, many risk assessment

methodologies focus more on the technical aspects of system weakness instead of the probability of exploitation and resultant impact.

3.2.2.1 How can we Test for Accuracy?

The easiest way we can examine a risk statement for accuracy is by comparing past experience to what the assessment says is most probable in frequency and magnitude of loss. For example, if the risk assessment says that the current risk due to exposure of paper information is "high", an organization may be able to compare that result to a past history (i.e., have there been a significant number of past incidents? And if there are occurrences of such incidents, were the costs of those incidents in line with the expected loss amount given in the risk assessment?).

However, quality historical data may be difficult to obtain. In the absence of historical data of acceptable quality, accuracy may be established by:

- Treating risk in a probabilistic manner
- Making sure that variables aren't weighted (unless there is a logical and defensible rationale for doing so)
- Basing the analysis on a risk model that accounts for the reasons why critical aspects of risk exist (e.g., frequency, or the relative capability of the threat, or probable instead of worst-case impact, etc.)

3.2.2.2 Precision, Accuracy, and Meaningful Results

One of the greatest obstacles for adoption of risk in an organization is the notion that precision is required. Precision in measurement is desirable, but not as necessary as accuracy. Accuracy is best defined for use in risk analysis as "our capability to provide correct information". Precision, however, is defined as "exact, as in performance, execution, or amount". Because risk is a probability problem, it is extremely difficult to be precise in measurement, calculation, and expression. Accuracy may or may not be attainable.

Fortunately for most decisions in information risk management, precise expressions of probable frequency of loss or probable magnitude of loss are not necessary, especially when the risk assessment methodology is capable of consistently delivering accurate results. One of the goals in risk measurement and expression should be to achieve accuracy in the belief statements it creates.

3.2.2.3 Misrepresentation of Precision and Creating Accuracy

Because achieving high precision in risk assessments is extremely difficult, any assessment which uses falsely precise probability estimates can mislead the decision-maker into believing that there is more rigor in the risk assessment process than actually exists. Accuracy, however, can be provided in risk assessments by using ranges or distributions of estimates and measurements, and communicating the outcome probabilities in terms of ranges or distributions.

3.2.3 Consistent (Repeatable)

One significant indicator of a good risk assessment methodology is that it lends itself to repeatable results. That is, if two analysts were given the same information independently and performed a risk assessment, they would arrive at similar conclusions.

This consistency is important for two significant reasons. First, repeatable results validate a degree of rigor and logic within the assessment methodology and model. Second, consistency is critical in creating a defensible, credible belief statement.

3.2.4 Defensible

In order for risk assessment results to be defensible, the results have to be deemed accurate and logical. If the results or measurements of the risk assessment cannot be defended, the recommendation, assessment effort, and presenter all lose credibility.

3.2.5 Logical

One of the most common complaints about risk assessment frameworks is the lack of logic that goes into creating the relationships between the various factors they use to create a risk statement. A good risk assessment methodology will use a model that logically describes how the world works by establishing how the elements of the assessment affect each other and then culminate in that "state of nature" ultimately described as risk. It will not allow for contradictory or haphazard association of risk factors.

Nor will a good risk assessment framework allow for mathematical expression that is nonsensical. For example, many risk assessment frameworks that advocate the use of ordinal scales also advocate the use of arithmetic functions on those values, and as such their results are not logical, consistent, nor defensible.

3.2.6 Risk-Focused

The only metrics that really matter are the probable frequency of loss event, and the probable magnitude of loss. As a result, any assessment methodology whose end result cannot be expressed in these terms is not really measuring risk, and is not providing data owners with the information necessary to make a good risk decision. A risk-focused assessment methodology will result in end expressions that are concise and meaningful.

3.2.7 Concise and Meaningful

The risk expression must give the right information to the right audience; e.g., executive information must help executives identify their opportunity to mitigate, accept, or transfer risk, and technical information should be provided to enable technical stakeholders to implement selected solution sets. Risk assessment results should be expressed as concisely as possible to lessen the opportunity for confusion. Technical elaborations on controls and attack techniques should be used judiciously.

In order to be meaningful, recommendations from the results of an analyst must also be feasible and actionable in order to allow the data owner to make the best decision given the information at hand.

3.2.8 Feasible

Meaningful outcomes of a risk assessment will also provide feasible options to the decision-maker. Feasible options will be cost-effective, politically viable, and achievable from a technical and execution perspective. Feasible solution sets will also be actionable to give data owners a clear path to the solution under consideration.

3.2.9 Actionable

When confronted with a probability statement around risk, management can mitigate, transfer, or accept/tolerate the issue at hand. Risk assessment results should not only provide management with feasible solution sets, but also include a plan of action (should management decide that action is necessary). Actionable results expression will allow management to properly prioritize their resource allocations.

3.2.10 Prioritized

The results of a risk assessment should help management be efficient in applying finite resources to the portfolio of business opportunities and risk issues they face. Prioritization may be based on risk, resources required to address the issues, and/or some other criteria provided by management. The bottom line is that prioritization should meet the requirements laid forth by management in advance of report generation.

3.2.11 Important Note

No amount of risk information, regardless of how accurate or useful, will guarantee good risk decisions on the part of management. Good risk information simply informs business managers so they are in the best informed positions to make cost-effective risk management decisions that are based on consistent application of their corporate policy for managing risk.

4 Risk Assessment Methodology Considerations

Many risk assessment methodologies tend to focus on providing a step-by-step process for risk assessment without discussing how things should be measured, or at times even what the assessor should be using to create measurement. But even a good risk assessment methodology will provide poor results if some critical aspects of the measurement and calculation process are not considered.

These considerations, described in the following sections, generally boil down to understanding "what" and "how" to measure and calculate. When risk assessments, or risk assessment frameworks, fail it is often because the framework or assessor didn't fully comprehend the implications of what they were measuring and how they were going about measuring those things.

Understanding how the assessment should go about measuring, calculating, and expressing risk is critical to creating a logical, defensible assessment.

4.1 Use of Qualitative versus Quantitative Scales

Current approaches to risk assessment use either qualitative or quantitative means to measure, estimate, and express risk. Ideally, a risk assessment methodology will be useful regardless of which scale is chosen. Note that with quality information available to the assessor, the same risk assessment will produce acceptably similar results when both qualitative and quantitative assessments are performed.

The decision to use one means of expression over another is going to be primarily dependent on two factors:

1. Suitability within the organization
2. Quality of available information

Using qualitative scales requires a description of the boundaries across each level. This can be done using other qualitative words (e.g., "substantial" *versus* "moderate") or quantitative ranges. In the first case, the method is still vulnerable to analyst bias and perception, and mathematical functions can't be applied. In the second case, some math may be feasible depending on how the ranges are structured.

When is using Numbers not Quantitative?

The use of numbers in an ordinal scale (see Section 4.2) is actually a qualitative approach to risk expression.

If an analyst using a qualitative approach is pressured hard enough, they often reveal (many times to their own surprise) that they are in fact defining their qualitative values using quantitative ranges.

4.2 Measurement Scales

When information is being collected for the risk assessment, that information will invariably be ordered in some method of scale. One of the most significant issues with modern risk assessment frameworks is that they do not provide the assessor with an understanding of how to create scale, or the logical implications of their use of measurements in the context of the chosen scale. Data may be arranged in one of the following methods of scale.

4.2.1 Nominal Scale

Using a nominal scale, any number is used as a label. For example, in many sports, the number on a uniform gives no indication of performance and is simply used to identify the athlete. Applying mathematical functions to nominal values is nonsensical.

4.2.2 Ordinal Scale

In an ordinal scale, quantitative values are assigned to data, but the numbers are only indicative of some relative position of the information. The amount of difference between two points on the scale is undefined, and so using mathematical functions on an ordinal scale is meaningless.

A child arranging crayons in order of color preference is creating ordinal values.

4.2.3 Interval Scale

Using an interval scale, the quantitative values describe the position of data sets, but outside of any fixed point that can be called zero (zero can be an arbitrary point, however). Interval variables can express measurement, but multiplication (and division) cannot be performed (directly) on intervals because the creation of any ratio between measurement is meaningless.

Dates in most western calendars are interval values, as would be Celsius temperatures. They are measurements, but we are still unable to perform mathematical function outside of basic addition and subtraction on them (i.e., June 3rd multiplied by June 7th does not equal June 21st).

4.2.4 Ratio Scale

In a ratio scale, numbers indicate some amount of difference, using a fixed zero point. Unlike other scales, ratio variables can have statistical functions applied to them because the origin point is not arbitrary.

Examples of ratio values would be Kelvin temperatures, population distribution percentiles, two and three-dimensional space measurements, etc.

4.2.5 Important Note

In scales and measurement, only ratio or interval scales can be said to have units of measurement.

4.3 How Frequent is "Likely"?

Many approaches to risk assessment attempt to craft a probability expression using a "likelihood" factor. Unfortunately, it is not always evident what likelihood describes and what factors a likelihood expression takes into account. There are two critical flaws in using likelihood:

1. Likelihood usually doesn't describe timeframe (i.e., likely to happen this week, month, year, lifetime, etc.).
2. Likelihood doesn't allow distinctions between events likely to happen once *versus* many times.

A superior approach is to frame the probability in the context of a timeframe. By introducing the concept of frequency into the probability expression, the risk expression:

- Is framed using an actual measurement (time) allowing for the use of mathematic function
- Becomes more accurate by using time as a factor to refine the probability statement
- Helps simplify the prioritization effort due to clearer communication
- Helps the analyst better identify effective strategies in preventing, detecting, and responding to threat communities

Note: With some audiences, the absence of timeframing in a likelihood expression could call into question whether that expression is simply a discussion of what is possible, rather than a true expression of probability.

4.4 Risk and the Data Owners

Risk is not a security problem, it is a business problem that surrounds business processes and involves multiple stakeholders. Yet many risk management frameworks don't dive deeply enough into what creates real dollar loss to facilitate the involvement of other subject matter experts in the business. Quality information involves getting subject matter expert estimates and measurements, and many times this will require input from outside information technology. For example, a line of business owner is in the best position to provide estimates surrounding the losses an organization might encounter should a factory be unable to produce product. A marketing department might be the best source of information for dollar amounts that might need to be spent to repair reputation damage.

A good risk assessment effort may require the involvement from marketing, legal, and the data owners. A good risk assessment framework will facilitate the involvement of stakeholders outside of information technology.

5 Assessment Elements

When executing a risk assessment, the analyst performs two critical functions:

1. The *analysis* of a state of nature (the current observed state of what is being analyzed) using information and evidence to create a state of knowledge (meaning that can be logically arrived at from the evidence in the state of nature)
2. The *synthesis* of wisdom from the state of knowledge

There are five primary elements to an effective risk assessment:

- Identifying risk issues (analysis)
- Evaluating the severity/significance of risk issues (analysis)
- Identifying the root cause of risk issues (synthesis)
- Identifying cost-effective solution options (synthesis)
- Communicating the results to management (synthesis)

5.1 Identifying Risk Issues

The first element to performing an effective risk assessment is to identify the nature and scope of the assessment. Risk assessments can be performed for isolated business processes or systems, or on an aggregate level. There are several ways in which an analyst can establish evidence for use in risk analysis:

5.1.1 Interviews and Questionnaires

When developed from a good framework or inventory of controls, assets, business processes, etc., questionnaires can be used as a discovery mechanism for evidence concerning the current state of risk, as well as the organization's ability to manage risk.

5.1.1.1 Pros of Using Interviews and Questionnaires

Interviews and questionnaires can help analysts quickly identify areas of concern in an organization's ability to manage risk. The interview and questionnaire process can have less of an impact on organizational resources than more involved means of identifying risk issues such as "red team" or "blue team" testing exercise (and are generally less risky). Interviews and questionnaires are also the most useful way of establishing measurement ranges for use in risk analysis.

5.1.1.2 *Cons of Using Interviews and Questionnaires*

The difficulty of developing truly useful questions is widely underestimated. It is no small task to develop questions that protect against bias, encourage consistent and accurate answers, and result in useful measurement.

5.1.2 Testing

Testing can be used in two significant ways in the identification process.

First, testing may be used to uncover evidence of a risk issue. This is most commonly a result of a vulnerability management process like scanning systems and/or penetration testing. Testing, however, primarily uncovers evidence that equates to symptoms. Testing as a primary discovery method should be followed by interviews and questions developed to help uncover the root cause of the problem and the extent to which the problem exists.

Second, if interviews and/or questionnaires were the primary information gathering process, then testing can be used to help reinforce, or identify discrepancies from, the measurements created by answers to the questionnaire. This use of testing as verification can lead to increased accuracy in the measurement of factors that contribute to risk.

5.1.2.1 *Pros of Using Testing*

Testing uncovers evidence where the risk management processes may be less than ideal or deviates from the expectations set in policies. Testing can also give very good evidence of an organization's ability to resist a threat of some capability.

5.1.2.2 *Cons of Using Testing*

The data that testing establishes is rarely a direct correlation to current state of controls, and "passing" a test can lead to a false sense of security. Testing can have negative impacts when performed on an operating environment. Testing can be more expensive than other review options. Testing is often performed without defining a level of attack sophistication, so testing is performed with a significant level of attack sophistication which can result in discovering and exploiting a "long tail" issue. Testing can be resource-intensive.

5.1.3 Sampling

Sampling is the act of examining some subset of an overall population in order to extract key characteristics for analysis. Sampling can be useful when:

- Resource requirements to examine the entire population are infeasible.
- The bounds (or frame) of the population is uncertain.

The ability to extract useful information while limiting resource requirements can be a very attractive proposition, but in order to establish a meaningful data set, sampling must be performed well.

In order to sample, purpose must be well defined. Aspects of purpose definition include:

- The definition of the population should be as specific as possible.

- The unit of sample must be defined.
- The sampling performance should be as unbiased as possible.
- The measurement should be as accurate as possible.

5.1.4 Types of Sampling

There are two types of sampling: probability sampling and non-probability sampling. Probability sampling methods that "frame" the data set can greatly assist the organization's ability to organize its data sets. For example, an organization may use stratified sample framing to separate systems or business processes into areas that share characteristics.

5.2 Evaluating the Severity/Significance of Risk Issues

The severity of a risk issue is determined through risk analysis. A risk analysis is the process by which the analyst can establish probability statements concerning the frequency and impact of a loss event. These probabilities will be established using information collected by the analyst for the various risk factors.

For example, in order to use the Factor Analysis of Information Risk (FAIR) framework, the analyst will need to collect useful information concerning the frequency of threat events, the capabilities of the threat community in question, the organization's ability to resist the actions of the threat community, and where (and in what form) dollar losses can be expected to impact the organizational budgets.

Once that information is collected, the analyst then can create posterior (calculated) information concerning the ability of the organization to resist threat actions (i.e., its vulnerability), the probable frequency of loss events, and the probable magnitude of loss events. The combination of these elements is used to establish and communicate the current state of risk for the issue being analyzed.

5.3 Identifying the Root Cause of Risk Issues

In order to successfully address risk, an organization must identify the root causes of its risk issues. Root causes generally stem from either a problem in decision-making or execution of decisions that have been made. Root causes with their sources in organizational decision-making exist because of misalignment with management risk tolerances or because management was given inaccurate information regarding risk. Root causes stemming from execution failures exist because of inadequate awareness, capabilities, and/or motivation on the part of those responsible for protecting/managing assets. Identifying root causes is necessary in order for an organization to identify truly successful solution options.

5.4 Identifying Cost-Effective Solution Options

Risk assessments should present decision-makers with options for risk treatment (where reasonable options exist). This requires that analysts present decision-makers with a statement concerning the current state of risk, and either:

- Solutions that will bring the level of risk to an established desired level
- Solutions that will reduce the level of risk to various degrees of magnitude

In either case, the analyst should expect to perform several desired state analyses to allow for more than one solution option for decision-makers. Solutions should consider:

- Resources required to achieve desired or future state
- Comparison of proposed future state(s) with the current state
- Resources required to maintain their future state(s)

If possible, a "side by side" comparison of multiple solutions relative to the current state is desirable. Including the resources required for each solution allows for a cost/benefit comparison.

5.5 Communicating the Results to Management

5.5.1 What to Communicate

Results should communicate:

- Current risk
- Future desired state (if available)
- Root cause of variance between current state and desired state
- Various options (and their resource requirements) that will achieve and maintain desired state

Current and desired states of risk should be expressed using two key measurements:

- The probable frequency with which loss events may occur
- The probable magnitude of loss events

A worst-case loss magnitude may also be expressed to communicate the upper bounds of loss. Various risk reduction statistics can be created by comparing the investment needed and the benefits in either expected frequency or loss magnitude.

5.5.2 How to Communicate

The language of the business manager, regulator, legislator, policy-maker, and boardroom is well known to be markedly different to that used by IT technologists. Nowhere is this language gap more pronounced than when talking about “risk” and how to manage it.

This is the prime reason why a rigorous risk taxonomy is needed – to define specific meanings to the key words that all use when talking about risk, so that all can refer to this taxonomy and therefore be sure they mean the same thing.

An example of this language gap is that the business manager talks about “impact” of loss, not in terms of how many servers or operational IT systems will cease to provide normal service, but rather what will be the impact of losing normal service on the business’s ability to continue to trade normally and, if there is an impact, what is that when measured in terms of $-value.

The key lesson here is that even the best risk assessment is only of high value to its consumer – the business risk decision-makers – when it is presented in terms which the decision-makers understand and which therefore enable them to make the right decisions to manage the organization’s risk profile in line with their risk management policy and the applicable regulatory regime to which they wish to conform.

Many good risk assessments – like many good proposals for investment in information security – have failed to be accepted because one or both parties have not taken sufficient note of how to communicate effectively the key issues on cost of investment, exposure to risks, and return on investment (benefits).

Glossary

Control Strength (CS)

The strength of a control as compared to a standard measure of force.

Loss Event

A loss event occurs when a threat agent's action (threat event) is successful in negatively affecting an asset.

Loss Event Frequency (LEF)

The probable frequency, within a given timeframe, that a threat agent will inflict harm upon an asset.

Method

A rule or orderly procedure used in carrying out a task or accomplishing an aim.

Methodology

A system of methods and rules applied to work on a given subject.

Probable Loss Magnitude (PLM)

The probable magnitude of loss resulting from a loss event.

Risk

The probable frequency and probable magnitude of future loss.

Threat Agent

Any agent (e.g., object, substance, human, etc.) that is capable of acting against an asset in a manner that can result in harm.

Threat Capability (Tcap)

The probable level of force that a threat agent is capable of applying against an asset.

Threat Event

Occurs when a threat agent acts against an asset.

Threat Event Frequency (TEF)

The probable frequency, within a given timeframe, that a threat agent will act against an asset.

Vulnerability

The probability that an asset will be unable to resist the actions of a threat agent.

Index