Risk Assessment

ANSI/ASIS/RIMS RA.1-2015

Supply Chain Risk Management: A Compilation of Best Practices

ASIS INTERNATIONAL

The worldwide leader in security standards and guidelines development

1625 Prince Street
Alexandria, Virginia 22314-2818
USA
+1.703.519.6200
Fax: +1.703.519.6299
www.asisonline.org
# Table of Contents

0 INTRODUCTION .......................................................................................................................... XV

0.1 GENERAL ................................................................................................................................. XV
0.2 DEFINITION OF RISK ASSESSMENT .................................................................................... XVI
0.3 QUANTITATIVE AND QUALITATIVE ANALYSIS .................................................................... XVII
0.4 MANAGING ORGANIZATIONAL AND SPECIFIC RISK ASSESSMENTS .................................... XVIII
0.5 PLAN-DO-CHECK-ACT MODEL .............................................................................................. XIX

1 SCOPE ....................................................................................................................................... 1

2 NORMATIVE REFERENCES ....................................................................................................... 1

3 TERMS AND DEFINITIONS ........................................................................................................ 2

3.1 DEFINITIONS .......................................................................................................................... 2

4 PRINCIPLES .............................................................................................................................. 8

4.1 GENERAL ............................................................................................................................... 8
4.2 IMPARTIALITY, INDEPENDENCE, AND OBJECTIVITY ............................................................. 9
4.3 TRUST, COMPETENCE, AND DUE PROFESSIONAL CARE .................................................... 9
4.4 HONEST AND FAIR REPRESENTATION .................................................................................. 10
4.5 RESPONSIBILITY AND AUTHORITY ...................................................................................... 10
4.6 CONSULTATIVE APPROACH .................................................................................................. 10
4.7 FACT-BASED APPROACH ...................................................................................................... 10
4.8 CONFIDENTIALITY ................................................................................................................ 11
4.9 CHANGE MANAGEMENT ......................................................................................................... 11
4.10 CONTINUOUS IMPROVEMENT ............................................................................................ 11

5 MANAGING A RISK ASSESSMENT PROGRAM ....................................................................... 11

5.1 GENERAL .............................................................................................................................. 11
5.2 UNDERSTANDING THE ORGANIZATION AND ITS OBJECTIVES .......................................... 12
5.3 ESTABLISHING THE FRAMEWORK ..................................................................................... 16
5.4 ESTABLISHING THE PROGRAM ........................................................................................... 22
5.5 IMPLEMENTING THE RISK ASSESSMENT PROGRAM ............................................................ 28
5.6 MONITORING THE RISK ASSESSMENT PROGRAM ............................................................... 38
5.7 REVIEW AND IMPROVEMENT ............................................................................................... 39

6 PERFORMING INDIVIDUAL RISK ASSESSMENTS ................................................................ 40

6.1 GENERAL .............................................................................................................................. 40
6.2 COMMENCING THE RISK ASSESSMENT ............................................................................. 40
6.3 PLANNING RISK ASSESSMENT ACTIVITIES ....................................................................... 45
6.4 CONDUCTING RISK ASSESSMENT ACTIVITIES ................................................................ 56
6.5 POST RISK ASSESSMENT ACTIVITIES ............................................................................... 79

7 CONFIRMING THE COMPETENCE OF RISK ASSESSORS ..................................................... 82

7.1 GENERAL .............................................................................................................................. 82
7.2 COMPETENCE ...................................................................................................................... 82

A RISK ASSESSMENT METHODS, DATA COLLECTION, AND SAMPLING .................................. 88

A.1 GENERAL .............................................................................................................................. 88
A.2 TYPES OF INTERACTIONS ..................................................................................................... 88
A.3 ASSESSMENT PATHS ............................................................................................................. 89
A.4 SAMPLING .............................................................................................................................. 89

B ROOT CAUSE ANALYSIS .......................................................................................................... 93
ANSI/ASIS/RIMS RA.1-2015

B.1 GENERAL ................................................................................................................................. 93
B.2 APPLYING ROOT CAUSE TECHNIQUES ................................................................................. 93
B.3 TEN STEPS FOR EFFECTIVE ROOT CAUSE ANALYSIS ....................................................... 94
C  BACKGROUND SCREENING AND SECURITY CLEARANCES .................................................. 97
C.1 GENERAL ................................................................................................................................. 97
C.2 BACKGROUND CHECKS ......................................................................................................... 97
C.3 INTERVIEWS ............................................................................................................................ 98
C.4 PRIVACY PROTECTION .......................................................................................................... 99
D  CONTENTS OF THE RISK ASSESSMENT REPORT ................................................................ 100
E  CONFIDENTIALITY AND DOCUMENT PROTECTION ................................................................. 102
F  EXAMPLES OF RISK TREATMENT PROCEDURES THAT ENHANCE RESILIENCE OF THE ORGANIZATION ........................................................................................................... 103
F.1 GENERAL ................................................................................................................................. 103
F.2 PREVENTION AND MITIGATION PROCEDURES ................................................................. 103
F.3 RESPONSE PROCEDURES ...................................................................................................... 104
F.4 CONTINUITY PROCEDURES .................................................................................................. 105
F.5 RECOVERY PROCEDURES ....................................................................................................... 106
G  BUSINESS IMPACT ANALYSIS ................................................................................................. 113
H  BIBLIOGRAPHY .......................................................................................................................... 116

---

TABLE OF FIGURES

FIGURE 1: RISK MANAGEMENT PROCESS (BASED ON ISO 31000) .................................................. XVI
FIGURE 2: PLAN-DO-CHECK-ACT MODEL .................................................................................... XIX
FIGURE 3: FORMAL VS. INFORMAL RISK ASSESSMENTS ................................................................ 30
FIGURE 4: INFLUENCE DIAGRAM EXAMPLE .............................................................................. 37
FIGURE 5: RISK PORTFOLIO DESIGN FORMAT .......................................................................... 47
FIGURE 6: MANAGING UNCERTAINTY IN CONTEXT ................................................................. 48
FIGURE 7: ELEMENTS OF THREAT ............................................................................................... 65
FIGURE 8: DETERMINING THREAT LEVELS ............................................................................... 66
FIGURE 9: CRITICALITY AND CONSEQUENCE ANALYSIS ....................................................... 70
FIGURE 10: DETERMINING THE LEVEL OF RISK .................................................................... 71
FIGURE 11: RISK EVALUATION FUNNEL ..................................................................................... 74
FIGURE 12: CONCEPTUAL RISK “FRONTIER” ............................................................................ 75
FIGURE 13: SAMPLE MATRIX ....................................................................................................... 76
FIGURE 14: SAMPLING PROCESS .................................................................................................. 90
FIGURE 15: DEFINE, ANALYZE AND SOLVE ........................................................................... 94
FIGURE 16: BUSINESS IMPACT ANALYSIS (BIA) .................................................................. 114
FIGURE 17: EXAMPLE OF BIA METHODOLOGY .................................................................... 115
FIGURE 18: EXAMPLE OF BIA PROCESS ..................................................................................... 115

xiv
0 INTRODUCTION

0.1 General

A risk assessment provides the analytical foundation for risk management, therefore, a risk assessment step of the overall risk assessment process is used to inform decision-making. By using a logical, structured and consistent approach to assessing risk, persons responsible for decision-making can systematically select from possible choices that are based on reason and best available information. In order to achieve the organization’s overall and risk management objectives, those responsible for conducting the risk assessment should follow a structured approach to review and analyze relevant facts, observations, and possible outcomes. The output of the risk assessment process provides a basis for informed decision-making to determine a particular course or courses of action.

The risk management process of an organization should support enterprise-wide strategic and operational activities, as well as program and project-related activities. A risk assessment provides the cornerstone for informed decision-making about how to address uncertainties in achieving an organization’s objectives. Therefore, a comprehensive risk assessment is designed to consider the organization’s vision, mission, values, and culture, as well as strategic and tactical objectives. It may consider an organization’s broader objectives and activities or some specific goals and objectives but in all cases it assesses what can affect the achievement of these both positively or negatively.

In this Standard, we focus on risk assessments from the viewpoint that risk – the effect of uncertainty on achieving objectives (particularly uncertainty with respect to future outcomes) – is a dynamic concept. Therefore, risk assessments require proactive and ongoing monitoring of the internal and external context of the organization, as well as its risks and treatment measures. Uncertainty is inseparable from likelihood: the future plays out in various and differing scenarios, some more likely than others. Throughout this Standard, risk is considered from the perspective of achievement of objectives and outcomes; therefore, the effect of uncertainty on objectives may result in opportunities with potential gains (“improving”), as well as threats that may result in potential losses (“worsening”). Risk assumes that things will change, whether in the environment or in other circumstances.

This risk assessment standard provides guidance on developing and sustaining a coherent and effective risk assessment program, including principles, managing an overall risk assessment program, and performing individual risk assessments, along with confirming the competencies of risk assessors. This standard is complementary to the standards noted in the normative references and follows the risk assessment process outlined in the ISO 31000:2009 Risk management — Principles and guidelines and illustrated in Figure 1. A well-defined risk assessment program and individual assessments provide the foundation for the risk management process.

This Standard provides a generic model for conducting risk assessments (including impact analyses) for risk management decision-making and for use with risk-based management system standards. Risk-based management system standards require a defined, repeatable, and documented risk assessment process. It provides the foundation for planning the management of issues addressed by a management system standard, as well as identifies opportunities for improvements. Therefore, following the approach described in this Standard, meets the requirements for the risk assessment process in management system standards.
0.2 Definition of Risk Assessment

Risk assessment is the identification, analysis, and evaluation of uncertainties to objectives and outcomes. It provides a comparison between the desired/undesired outcomes and expected rewards/losses of organizational objectives. The risk assessment analyzes whether the uncertainty is within acceptable boundaries and within the organization’s capacity to manage risk. The results of the risk assessment inform the responsible and accountable decision maker(s) of choices available to effectively manage risk to achieve the organization’s objectives. A risk assessment is a careful and methodical examination of what could cause uncertainty, providing the basis to determine whether sufficient actions have been taken to prevent negative outcomes, or enhance the opportunities to generate positive outcomes. It is not possible to eliminate all risk and uncertainty, so the risk assessment helps prioritize the risks that impact the quest to achieve organizational objectives. The context of the organization and risk assessment provide the foundational information for:

- Calculating the effects of uncertainty which impact desired outcomes;
- Protecting an organization’s tangible and intangible assets including people; tangible assets that are physical (i.e., site, building, equipment); intangible assets that are intellectual (i.e., information, processes, trade secrets); and abstract (i.e., image, reputation);
- Safeguarding the integrity and continuity of its supply chain, services, and activities;
- Understanding of the relative exposure to risk for current and planned activities;
- Enhancing the achievement of objectives and identifying untapped opportunities;
- Providing a mechanism for understanding the impact of a possible event;
• Complying with the law and regulations; and
• Identifying reasonable control measures needed to treat risk and their associated cost/benefit.

The risk assessment is conducted in order to determine whether if, how, and to what extent the organization’s objectives, desired outcomes, and assets may be impacted. A risk assessment is tailored to the context in which the organization operates.

0.3 Quantitative and Qualitative Analysis

Risk assessments can be accomplished in varying degrees of detail. The level of detail is dependent upon the type of risk, purpose of the analysis, resource limitations, the information available to the assessor, and communicating the risk assessment findings. Risk may be assessed using a quantitative computational approach or a qualitative subjective approach, or a combination of both. In all cases the underlying assumptions should be understood and documented. The types of analysis and context for use are:

a) Qualitative analysis – relies on the reasoning and experiential judgment of assessment team members and subject matter experts using terms, words, and images as descriptors of risk;

b) Quantitative analysis – relies on probabilities and statistics using mathematical formulas and calculations to interpret numbers, data, and estimates; and

c) Combined approaches – can be complementary when the risk is better described and communicated by a combination of subjective and numerical values.

In some cases, a qualitative analysis precedes a quantitative analysis in order to obtain an indication of the level of risk and to identify principal risk factors as well as existing controls.

When choosing a qualitative analysis, quantitative analysis, or a combination of both, the reliability and validity of the available data should be considered. The nature of the risk factors and if they are quantifiable should also be considered. For example, the value of intangible assets and likelihood of a threat are often difficult to quantify and require qualitative analysis. Furthermore, consideration should be given to the target audience for the receipt of the risk assessment outputs. Decision-makers respond to the presentation of risk assessment outputs differently, depending on the type of analysis. Quantitative assessments can be translated into qualitative terms for communicating with stakeholders and management. Therefore, the analysis method should consider if one analysis method is more understandable and usable than another method.

0.3.1 Qualitative Analysis

A qualitative analysis uses descriptive terms and phrases such as “minor”, “moderate”, “major”, or “critical” to describe potential likelihoods and consequences of risk events, and the possibility of the consequences occurring. The terms used to describe different risks and consequences should be clearly defined, recognizing the same phrase may not be understood the same way when describing different risks or by different people. Qualitative analyses can be used when numerical data is inadequate, uncertain, or unavailable to properly describe the risk. They can also be implemented when an empirical method of analysis for decision-making is appropriate, and when initial risk screening is deemed acceptable in lieu of quantifiable methods.
A qualitative risk assessment may have advantages when:

a) Management and the governance body will better understand a descriptive presentation of risk;

b) Communicating and consulting risk with internal and external stakeholders will be more effective verbalizing or visualizing the risk information;

c) Underlying or historical data are not available or uncertain;

d) Resources limitations make quantitative data gathering impractical;

e) A risk is not well-defined or understood;

f) Quantification would be unnecessarily complex and may be based on potentially erroneous assumptions;

g) Multiple risks may drive business objectives; and

h) Addressing strategic risks, which tend to be harder to quantify than operational or financial risks.

0.3.2 Quantitative Analysis

Quantitative analysis uses numeric comparisons to describe potential likelihoods and consequences (including the likelihood of the consequences/impact occurring). The goal is to calculate objective numeric values for each of the components of risk evaluated in the risk assessment (e.g., threat, vulnerability, consequence). A cost/benefit analysis may also be included in the quantitative analysis. More than a single numerical value may be used in this method of analysis, as the analysis may apply to more than one category of risk or consequence.

A quantitative risk assessment may have advantages when:

a) The risk lends itself to quantification in numerical terms;

b) Numerical precision and presentation is required for a particular decision;

c) Quantitative metrics are used to measure performance and success in the organization;

d) Sufficient and appropriate data is available or can be readily obtained and is relevant for predictive assessments;

e) Risk can be better communicated and understood through quantitative comparisons; and

f) There is general agreement on underlying assumptions.

0.4 Managing Organizational and Specific Risk Assessments

Organizational risk assessments encompass the overarching organizational structure, resources, commitment, and documented methods used to plan and execute risk assessments. An effective program is built by clearly defining the risk assessment objectives. A competent person with the appropriate knowledge and experience should manage the risk assessment program and the organization should be committed to allocating the necessary resources, people, and time to effectively administer the program and its objectives. Priority should be given to assessing risks significant to the mission of the organization.
and the uncertainties in achieving desired outcomes (e.g., exploiting an opportunity, meeting obligations, or managing risk-related events).

A comprehensive risk assessment program may comprise many different strategic and tactical risk assessments—either ad-hoc or conducted at defined intervals or change(s) in circumstance(s). Individual assessments within the overall risk assessment program are conducted within a clearly defined scope and consistent with achieving the objectives of the overall risk assessment program. This Standard also provides guidance on the preparation for and the execution of individual risk assessments.

0.5 Plan-Do-Check-Act Model

Similar to ISO 31000, this Standard utilizes the "Plan-Do-Check-Act" (PDCA) model for both the overall risk assessment program as well as individual risk assessments. Figure 2 illustrates the PDCA model.

![Plan-Do-Check-Act Model](image)

**Figure 2: Plan-Do-Check-Act Model**

The PDCA model is a clear, systematic, and documented approach to:

a) Set measurable policies, objectives, and targets;

b) Methodically implement the program;

c) Monitor, measure, and evaluate progress;

d) Identify, prevent, or remedy problems as they occur;

e) Assess competence requirements and train persons working on the organization’s behalf;
f) Provide top management with a feedback loop to assess progress and make appropriate changes to the risk assessment program; and

g) Manage information within the organization, thereby improving operational efficiency.

In conjunction with the PDCA model, this Standard uses a process approach for the risk assessment program. A risk assessment program is a compilation of a system of interrelated activities; their identification, linkages, and interactions can be referred to as a “process approach”. When designing a risk assessment program, it is necessary to identify and manage many activities in order to function effectively. Any activity using resources and managed in order to enable the transformation of inputs into outputs can be considered to be a process. In developing the risk assessment program and individual risk assessments, it is important to recognize that often the output from one process directly influences the input of another process.
Risk Assessment

1 Scope

This Standard:

a) Provides guidance for establishing a risk assessment program and conducting individual risk assessments consistent with ISO 31000:2009 Risk management — Principles and guidelines, and the Committee of Sponsoring Organizations of the Treadway Commission (COSO) Enterprise Risk Management (ERM) framework;

b) Provides guidance on conducting risk assessments for risk- and resilience-based management system standards for the disciplines of risk, resilience, security, crisis, continuity, and recovery management, including principles of risk assessments, managing the risk assessment program, and conducting risk assessments, as well as evaluation of competence of persons involved in the risk assessment process;

c) Describes the process for conducting risk assessments consistent with the Plan-Do-Check-Act Model; and

d) Provides the informational basis necessary for decision-makers to make informed decisions about managing risks in the organization and its supply chain.

Organizations of all types and sizes can use the concepts and guidance of this Standard to conduct risk assessments supporting their risk management activities. It is recommended that organizations implementing risk- and resilience-based management system standards use the procedures described in this Standard in conjunction with ISO 31000:2009 to conduct their risk management activities (see Figure 1).

This Standard is a guidance document and not intended as a specification for third-party certification. It provides a comprehensive approach to establishing a risk assessment program and the conduct of individual assessments. Implementation of this Standard should be tailored to the needs of the organization.

2 Normative References

The following standards contain provisions which, through reference in this text, constitute provisions of this American National Standard. At the time of publication, the editions indicated were valid. All standards are subject to revision, and parties to agreements based on this American National Standard are encouraged to investigate the possibility of applying the most recent editions of the standards indicated below.

a) ISO 31000:2009, Risk management — Principles and guidelines;

b) ISO/IEC 31010:2009, Risk management — Risk assessment techniques; and