RISK ASSESSMENT

Approved August 3, 2015
American National Standards Institute, Inc.

ASIS International and The Risk and Insurance Management Society, Inc.

Abstract
This 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 and understanding biases. This Standard describes a well-defined risk assessment program and individual assessments to provide the foundation for the risk management process. Seven annexes provide additional guidance for applying risk assessments and potential treatments.
NOTICE AND DISCLAIMER

The information in this publication was considered technically sound by the consensus of those who engaged in the development and approval of the document at the time of its creation. Consensus does not necessarily mean that there is unanimous agreement among the participants in the development of this document.

ASIS and RIMS standards and guideline publications, of which the document contained herein is one, are developed through a voluntary consensus standards development process. This process brings together volunteers and/or seeks out the views of persons who have an interest and knowledge in the topic covered by this publication. While ASIS administers the process and establishes rules to promote fairness in the development of consensus, it does not write the document and it does not independently test, evaluate, or verify the accuracy or completeness of any information or the soundness of any judgments contained in its standards and guideline publications.

ASIS is a volunteer, nonprofit professional society with no regulatory, licensing or enforcement power over its members or anyone else. ASIS and RIMS do not accept or undertake a duty to any third party because they do not have the authority to enforce compliance with their standards or guidelines. They assume no duty of care to the general public, because their works are not obligatory and because they do not monitor the use of them.

ASIS and RIMS disclaim liability for any personal injury, property, or other damages of any nature whatsoever, whether special, indirect, consequential, or compensatory, directly or indirectly resulting from the publication, use of, application, or reliance on this document. ASIS and RIMS disclaim and make no guaranty or warranty, expressed or implied, as to the accuracy or completeness of any information published herein, and disclaims and makes no warranty that the information in this document will fulfill any person’s or entity’s particular purposes or needs. ASIS and RIMS do not undertake to guarantee the performance of any individual manufacturer or seller’s products or services by virtue of this standard or guide.

In publishing and making this document available, ASIS and RIMS are not undertaking to render professional or other services for or on behalf of any person or entity, nor are ASIS and RIMS undertaking to perform any duty owed by any person or entity to someone else. Anyone using this document should rely on his or her own independent judgment or, as appropriate, seek the advice of a competent professional in determining the exercise of reasonable care in any given circumstances. Information and other standards on the topic covered by this publication may be available from other sources, which the user may wish to consult for additional views or information not covered by this publication.

ASIS and RIMS have no power, nor do they undertake to police or enforce compliance with the contents of this document. ASIS and RIMS have no control over which of their standards, if any, may be adopted by governmental regulatory agencies, or over any activity or conduct that purports to conform to their standards. ASIS and RIMS do not list, certify, test, inspect, or approve any practices, products, materials, designs, or installations for compliance with its standards. They merely publish standards to be used as guidelines that third parties may or may not choose to adopt, modify, or reject. Any certification or other statement of compliance with any information in this document should not be attributable to ASIS and RIMS and is solely the responsibility of the certifier or maker of the statement.

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, without the prior written consent of the copyright owner.

Copyright © 2015 ASIS International and The Risk and Insurance Management Society, Inc. All rights reserved.

ISBN: 978-1-934904-75-6
FOREWORD

The information contained in this Foreword is not part of this American National Standard (ANS) and has not been processed in accordance with ANSI's requirements for an ANS. As such, this Foreword may contain material that has not been subjected to public review or a consensus process. In addition, it does not contain requirements necessary for conformance to the Standard.

ANSI guidelines specify two categories of requirements: mandatory and recommendation. The mandatory requirements are designated by the word shall and recommendations by the word should. Where both a mandatory requirement and a recommendation are specified for the same criterion, the recommendation represents a goal currently identifiable as having distinct compatibility or performance advantages.

ASIS International and The Risk Management Society, Inc. collaborated in the development of this Risk Assessment standard.

About ASIS

ASIS International (ASIS) is the largest membership organization for security management professionals that crosses industry sectors, embracing every discipline along the security spectrum from operational to cybersecurity. Founded in 1955, ASIS is dedicated to increasing the effectiveness of security professionals at all levels.

With membership and chapters around the globe, ASIS develops and delivers board certifications and industry standards, hosts networking opportunities, publishes the award-winning Security Management magazine, and offers educational programs, including the Annual Seminar and Exhibits—the security industry’s most influential event. Whether providing thought leadership through the CSO Roundtable for the industry’s most senior executives or advocating before business, government, or the media, ASIS is focused on advancing the profession, and ensuring that the security community has access to intelligence, resources, and technology needed within the business enterprise. www.asisonline.org

The work of preparing standards and guidelines is carried out through the ASIS International Standards and Guidelines Committees, and governed by the ASIS Commission on Standards and Guidelines. An ANSI accredited Standards Development Organization (SDO), ASIS actively participates in the International Organization for Standardization (ISO). The mission of the ASIS Standards and Guidelines Commission is to advance the practice of security management through the development of standards and guidelines within a voluntary, nonproprietary, and consensus-based process, utilizing to the fullest extent possible the knowledge, experience, and expertise of ASIS membership, security professionals, and the global security industry.

About RIMS

As the preeminent organization dedicated to advancing the practice of risk management, RIMS, the risk management society™, is a global not-for-profit organization representing more than 3,500 industrial, service, nonprofit, charitable and government entities throughout the world. Founded in 1950, RIMS brings networking, professional development and education opportunities to its membership of more than 11,000 risk management professionals who are located in more than 60 countries.

Suggestions for improvement of this document are welcome. They should be sent to ASIS International, 1625 Prince Street, Alexandria, VA 22314-2818.

Commission Members

Charles Baley, Farmers Insurance Group, Inc.
Michael Bouchard, Sterling Global Operations, Inc.
Cynthia P. Conlon, CPP, Conlon Consulting Corporation
William Daly, Control Risks Security Consulting
Lisa DuBrock, Radian Compliance LLC
Eugene Ferraro, CPP, CFE, PCI, SPHR, Convercent, Inc.
F. Mark Geraci, CPP, Purdue Pharma L.P., Chair
Bernard Greenawalt, CPP, Securitas Security Services USA, Inc.
Robert Jones, Socrates Ltd
Glen Kitteringham, CPP, Kitteringham Security Group Inc.
Michael Knoke, CPP, Express Scripts, Inc., Vice Chair
Bryan Leadbetter, CPP, Alcoa Inc.
Marc Siegel, Ph.D., Commissioner, ASIS Global Standards Initiative
Jose Miguel Sobron, United Nations
Roger Warwick, CPP, Pyramid International Temi Group
Allison Wylde, Consultant

At the time it approved this document, RA, which is responsible for the development of this Standard, had the following members:

Committee Members

Committee Co-Chair: Carol Fox, ARM, Director of Strategic and Enterprise Practice, RIMS
Committee Co-Chair: Marc Siegel, Ph.D., Commissioner, ASIS Global Standards Initiative
Commission Liaison: Glen Kitteringham, CPP, Kitteringham Security Group Inc.
Committee Secretariat: Sue Carioti, ASIS Secretariat

Kaleem Ahmed, Independent
Sean Ahrens, M.A., CPP, BSCP, CSC, Aon Corporation
Ian Alderson, CPP, Independent
Christopher Aldous, Dip SP&C (Open), CPP, PSP, Design Security Ltd
Lyle Alexander, CPP, A.R.M. Specialists Ltd
Rex Alexander, HeliExperts International LLC
Kanch Algama, DynCorp International, LLC
Frank Amoyaw, LandMark Security Limited
Edgard Ansola, CISA, CISSP, CEH, CCNA, Asepeyo MATEPSS nº151
Gina Arbeau, Cadillac Fairview Ltd.
Julie Ashley, The MITRE Corporation
Paul Aube, CPP, Dessau
Don Aviv, CPP, PSP, PCI, Interfor Inc.
Pradeep Bajaj, Eagle Hunter Solutions Limited
Mark Baker, CPP, Macatoma Security Inc.
Guillaume Banville, PSP, Bell Canada
Serge Barbeau, CPP, Chartand-Barbeau
Shayne Bates, CPP, LMC Consulting Group
Mark Beaudry, CPP, Independent
Jay Beighley, CPP, CFE, Nationwide Insurance
Dan Belai, CPP, PSP, Independent
Frank Bellomo, Business Risks International
Ray Bernard, PSP, RBCS, Inc.
Russell Hunt, Independent
Adam Incher, CPP, ACT Government, Shared Services
Scott Jack, CPP, Baylor Health Care System
Calvin Jaeger, Independent
Celia Jarvis, SPHR, MCR, LLC
Katherine Johnson, Harsco Corporation
Tyson Johnson, CPP, Independent
Roger Johnston, CPP, Argonne National Laboratory
Nicholas Jones, CPP, Independent
Edward Jopec, Independent
Matthew Jordan, CPP, Parsons Corporation
Richard Kibbey, CPP, PSP, Independent
Glen Kitteringham, CPP, Kitteringham Security Group, Inc.
Kelly Klatt, CPP, Loews Hotels
Don Knox, CPP, CITRMS, Caterpillar Inc.
Daniel Kropp, CPP, Towers Watson
Ellen Ku, CBCP, Association of Contingency Planners (ACP)
Michael Kuras, CBCP, CHP, AIM Specialty Health
Keith Kushner, TRC Corporation
Eliot Kushner, CPP, CHS-V, NICET, Pacific Gas & Electric
Henrik Laidlow-Petersen, Siemens Wind Power
Mukesh Lakhanpal, CPP, G4S Secure Services India Pvt. Ltd.
Ronald Lander, CPP, Ultrasafe Security Solutions
Robert Lang, Kennesaw State University
Laura Langone, JD, Juniper Networks, Inc.
Russell Law, PSP, Gralion, LLC
Donald Lee, Jr., CPP, First Citizens Bank of North Carolina
James Leflar, Jr., CPP, CBCP, MBCI, Zantech IT Services
Vickie Leighton, AMBCI, Avanade Inc.
Jeffrey Leonard, CPP, PSP, Securitas Critical Infrastructure Services, Inc.
Vincent Lombardi, Jr., E*TRADE Financial
Christopher Lowery, Celgene Corporation
James Lukaszewski, Risdall Public Relations
Grant Lundberg, First Citizens Bank of North Carolina
Ashley MacDonald, NCSO (ACSA) CPO (IFPO), United Protection Services, Inc.
Anthony Macisco, CPP, The Densus Group
Virginia MacSuibhne, J.D., CCEP, Roche Molecular Systems
Tracy Male, CFCP, CBCA, Independent
Peter Marotto, M.Ed., Independent
Ronald Martin, CPP, Open Security Exchange
Jan Mattingly, CRM, RF, CIP, RiskResults Consulting Inc.
Christopher Mayer, Department of Defense
Joe Mazza, CHPP, Independent
Brett Reddock, M.Sc., ABCP, SEM, Unparalleled Technologies
James Reese, TigerSwan
Vince Regan, CPP, PSP, PCI, Anixter, Inc.
Shawn Reilly, CPP, CHPA, Tech Systems, Inc.
John Richardson, Initiative for Human Rights in Business
Thomas Rohr Sr., CPP, Carestream Health, Inc.
Ronald Ronacher, PSP, Arup
Craig Rydalch, CISSP, CISM, PMP, AIM Specialty Health
Michael Saad, CPP, Gane Security Solutions
Ed Schlichtenmyer, ABCP, ImpactWeather
Brian Schmidt, CPP, Independent
Michael Schroeder, CBCP, MBCI, US Equities Asset Management
Josh Schubring, CPP, Mulva International Inc.
Michael Severin, Independent
Alister Shepherd, Allen & Overy LLP
Maya Siegel, M. Siegel Associates
Jeffrey Slotnick, CPP, PSP, Setracon Inc.
Jeff Snider, The MITRE Corporation
Jose Miguel Sobron, United Nations
Christopher Spillman, PSP, Port Authority of NY & NJ, Office of Emergency Management
Gregory Staisiunas, CPP, CTI, FISSM, Independent
Teresa Stanford, CPP, Security Engineers, Inc.
Barry Stanford, CPP, Independent
J. Kelly Stewart, Newcastle Consulting LLC
Peter Stiernstedt, CPP, Cikraitz AB
John St-Ilma, PSP, NCSPF, Health Canada
Jeremy Sturgeon, CPP, CFE, Apple
Robert Summers, CPP, Summers Associates, LLC
Timothy Sutton, CPP, CHSS, Sorensen, Wilder & Associates (SWA)
Kenneth Szalontay, CPP, AlliedBarton Security Services
Scott Taylor, CPP, Exact Security Pty Ltd.
Scott Tezak, Professional Engineer, TRC Corporation
Rajeev Thykatt, Infosys BPO Ltd.
Yoriko Tobishima, InterRisk Research Institute & Consulting, Inc.
Lina Tsakiris, CPP, TD Bank
Ruth Unks, ARM, Maricopa County Community College District
Karim Vellani, CPP, Threat Analysis Group, LLC
Joop Verdonk, CPP, CPOI, European Security Academy
Heather Viccione, PSP, (RBS) Citizens Bank
Corey Vitello, Ph.D., Visa Inc.
Taz Wake, CISSP, CISM, CRISC, Halkyn Consulting
Todd Warren, Spring Hill College
Andrew Weaver, PSP, PMP, Markon, Inc.
Jerry Werries, First Citizens Bank of South Carolina
ANSI/ASIS/RIMS RA.1-2015

Working Group Members

Committee Co-Chair: Carol Fox, ARM, Director of Strategic and Enterprise Practice, RIMS
Committee Co-Chair: Marc Siegel, Ph.D., Commissioner, ASIS Global Standards Initiative
Anthony Macisco, CPP, The Densus Group
Jan Mattingly, CRM, RF, CIP, RiskResults Consulting Inc.
William Minear, II, CPP, West Virginia Military Authority
Curtis Noffsinger, CPP, PSP, Independent
Kevin Peterson, CPP, CPOI, Innovative Protection Solutions, LLC
Vince Regan, CPP, PSP, PCI, Anixter, Inc.
Jeffrey Slotnick, CPP, PSP, Setracon Inc.
J. Kelly Stewart, Newcastle Consulting LLC
Jeremy Sturgeon, CPP, CFE, Apple
Andrew Weaver, PSP, PMP, Markon, Inc.
William Wills, CPP, Independent
This page intentionally left blank.
# Table of Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>0 Introduction</td>
<td>XV</td>
</tr>
<tr>
<td>1 Scope</td>
<td>1</td>
</tr>
<tr>
<td>2 Normative References</td>
<td>2</td>
</tr>
<tr>
<td>3 Terms and Definitions</td>
<td>2</td>
</tr>
<tr>
<td>4 Principles</td>
<td>8</td>
</tr>
<tr>
<td>5 Managing a Risk Assessment Program</td>
<td>11</td>
</tr>
<tr>
<td>6 Performing Individual Risk Assessments</td>
<td>40</td>
</tr>
<tr>
<td>7 Confirming the Competence of Risk Assessors</td>
<td>82</td>
</tr>
<tr>
<td>A Risk Assessment Methods, Data Collection, and Sampling</td>
<td>88</td>
</tr>
<tr>
<td>B Root Cause Analysis</td>
<td>93</td>
</tr>
</tbody>
</table>
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;
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