ASIS INTERNATIONAL

Supply Chain Risk Management:

A Compilation of Best Practices

ANSI/ASIS SCRM.1-2014

STANDARD

The worldwide leader in security standards and guidelines development

ASIS INTERNATIONAL
Advancing Security Worldwide®

ANSI/ASIS SCRM.1-2014

an American National Standard

SUPPLY CHAIN RISK MANAGEMENT: A COMPILATION OF BEST PRACTICES

Approved March 28, 2014

American National Standards Institute, Inc.

ASIS International

Abstract

This *Standard*, developed in collaboration with the Supply Chain Risk Leadership Council, provides a framework for collecting, developing, understanding, and implementing current best practices for supply chain risk management (SCRM). It is a practitioner's guide to SCRM and associated processes for the management of risks within the organization and its end-to-end supply chain. This *Standard* provides some guidelines and possible approaches for an organization to consider, including examples of tools other organizations have used. It can serve as a baseline for helping enterprises assess and address supply chain risks and for documenting evolving practices.

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 International 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 does not accept or undertake a duty to any third party because it does not have the authority to enforce compliance with its standards or guidelines. It assumes no duty of care to the general public, because its works are not obligatory and because it does not monitor the use of them.

ASIS disclaims 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 disclaims and makes 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 does 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 is not undertaking to render professional or other services for or on behalf of any person or entity, nor is ASIS 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 has no power, nor does it undertake to police or enforce compliance with the contents of this document. ASIS has no control over which of its standards, if any, may be adopted by governmental regulatory agencies, or over any activity or conduct that purports to conform to its standards. ASIS does not list, certify, test, inspect, or approve any practices, products, materials, designs, or installations for compliance with its standards. It merely publishes 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 is solely the responsibility of the certifier or maker of the statement.

ISBN: 978-1-934904-56-5

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.

About ASIS

ASIS International (ASIS) is the leading organization for security professionals, with more than 38,000 members worldwide. ASIS is dedicated to increasing the effectiveness and productivity of security professionals by developing educational programs and materials that address broad security interests, such as the ASIS Annual Seminar and Exhibits, as well as specific security topics. ASIS also advocates the role and value of the security management profession to business, the media, government entities, and the public. By providing members and the security community with access to a full range of programs and services, and by publishing the industry's No. 1 magazine – *Security Management* - ASIS leads the way for advanced and improved security performance.

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. 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 the SCRLC

The SCRLC (http://www.scrlc.com) is a cross-industry organization including world-class manufacturing and services supply-chain organizations and academic institutions that work together to develop and share current best practices in supply-chain risk management. Its mission is to create supply-chain risk management standards, processes, capabilities, and metrics that reflect current best practices and can be widely adopted.

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 A. Baley, Farmers Insurance Group, Inc.
Jason L. Brown, Thales Australia
Michael Bouchard, Sterling Global Operations, Inc.
Cynthia P. Conlon, CPP, Conlon Consulting Corporation
William J. Daly, Control Risks Security Consulting
Lisa DuBrock, Radian Compliance
Eugene F. Ferraro, CPP, PCI, CFE, Convercent
F. Mark Geraci, CPP, Purdue Pharma L.P.
Bernard D. Greenawalt, CPP, Securitas Security Services USA, Inc.

Robert W. Jones, Socrates Ltd
Glen Kitteringham, CPP, Kitteringham Security Group Inc.
Michael E. Knoke, CPP, Express Scripts, Inc.
Bryan Leadbetter, CPP, CISSP
Marc H. Siegel, Ph.D., ASIS International, European Bureau
Jose Miguel Sobron, United Nations
Roger D. Warwick, Pyramid International
Allison Wylde, Researcher and Consultant

At the time it approved this document, the SCRM Standards Committee, which is responsible for the development of this *Standard*, had the following members:

Committee Members

Committee Co-Chair: Marc H. Siegel, Ph.D., Commissioner, ASIS Global Standards Initiative
Committee Co-Chair: John J. Brown, P.E., ARM-E, Thomson Reuters
Commission Liaison: Bernard D. Greenawalt, CPP, Securitas Security Services USA, Inc.
Committee Secretariat: Susan Carioti, ASIS International

Frank Amoyaw, LandMark Security Limited
Raymond Andersson, Australian Government - Department of Human Services
Edgard Ansola, CISA, CISSP, CEH, CCNA, Asepeyo
Ravi Anupindi, University of Michigan
Dennis Arter, ASQ Fellow, Certified Quality Auditor, American Society for Quality
Abrar Ashraf, CPP, PSP, Secure Options Group
Craig Babcock, Procter & Gamble
William Badertscher, CPP, PMP, GSEC, Georgetown University
Pradeep Bajaj, Professional Industrial Security Management Academy
Jay Beighley, CPP, CFE, Nationwide Mutual Insurance Company
Dennis Blass, CPP, PSP, CISSP, CFE, CSHP, Children's of Alabama
Michael Bouchard, CPP, Security Dynamics Group LLC
John Brown, CPP, Independent
Michael Brzozowski, PSP, Symcor
Terry Carrico, McKesson Corp.
John Casas, PSP, John Casas & Associates, LLC
Jim Castle, MSc, Corporate & Executive Solutions Ltd
Hugues Costes, DESS Information and Security - University Marne la Vallée, ArcelorMittal
John Coughlin, LoJack Supply Chain Integrity
Robert Day, CPP, PCI, CSP, CRSP, CHRP, Grad IOSH, CPMSIA, Office of Regulatory Change Management
Anthony DiSalvatore, CPP, PSP, PCI, Rocky Gap Casino Resort
Brian Dooley, CCP, CCSP, Brian T. Dooley & Associates
Jack Dowling, CPP, PSP, JD Security Consultants, LLC
Johan Du Plooy, CPP, TEMI Group
Meliha Dzirlo-Ayvaz, PMP, CBCP, CEM, Deloitte & Touche LLP

Mike Edgerton, CPP, Good Harbor Consulting, LLC
Thomas Engells, CPP, CPM, The University of Texas Medical Branch at Galveston
Richard J. Ferraro, Centanni Maritime, Inc.
Windom Fitzgerald, FitzgeraldTechnology Group
Charles Forsaith, Purdue Pharma
Thomas Frank, CPP, AbbVie Inc.
Jeremiah Frazier, CPP, Coca-Cola
Peter French, CPP, SSR Personnel
Robert Grieman, CPP, Securitas Security Services, USA, Inc.
Jeffrey Gruber, CPP, CHS-IV, Department of Defense, Department of the Army Civilian
Hector Grynberg, CPP, NOKIA
Phillip Guffey, CPP, Roche
Carlos Guzman, Security 101 Denver
Jon Hallaway, Harris Health Systems
Mark Hankewycz, CPP, The Protection Engineering Group, Inc.
Lloyd Hardy, JSI Logistics
Tom Holmes, Edinburgh International
Zahid Iqbal, MSc psn, Microsoft Corporation
Calvin Jaeger, PhD, Sandia National Laboratories
Ben Jakubovic, CPP, PSP, Avante International Technology
Mitchell Kemp, CPP, Cummins Filtration
David Kimmerly, CSC, AVSEC PM, WSP Middle East
Tami Kitajima, Competitive Insights, LLC
Timothy Klass, CPP, Amazon Web Services
Gerold Knight, The Coca-Cola Company
Otto Kocsis, Zurich Insurance Group
Stephen Krill, PMP, CEM, CBCP, SRA International
Alessandro Lega, CPP, Independent Consultant
Steven Lente, CPP, Securitas Security Services, USA, Inc.
Timothy Lindsey, CPP, Sidwell Protection Services
Charles Littler, American Bus Association
Anthony Macisco, CPP, The Densus Group
Charlie Maclean-Bristol, CPP, PlanB Consulting
Christopher Mark, American Sugar Refining/Domino Brands
Ronald Martin, CPP, Open Security Exchange
Pascal Matthey, PSP, XL Insurance Services Ltd
Jim McMahon, CPP, CISSP, McMahon & Associates
William Miller, MaCT USA
Michael Miller, American Broadcasting Companies, Inc.
David Moore, AcuTech Consulting Group
Rashon Moore, West-Ward Pharmaceutical
Joseph Nelson, CPP, State Street

Augustine Okereke, CPP, PZ Cussons Nigeria PLC
Philip Oppenheim, CBCP, Continuity Information Support Services
Russ Phillips, MMTS Group
Russell Price, Continuity Forum
Daniel Puente Pérez, Sociedad de Prevención de Asepeyo
Joseph Rector, CPP, PSP, PCI, USAF/11th Security Force Group
James Rice, MIT Center for Transportation and Logistics
Mark Riesinger, CPP, West Bend Mutual Insurance
Eric Rojo, USDOE, DOD, Magination Consulting International
John Schettino, CFS, DIAGEO
Gavriel Schneider, CPP, MTSEC, Dynamic Alternatives
Richard Sharpe, Competitive Insights, LLC
Jeffrey Slotnick, CPP, PSP, Setracon Inc.
Kevin Smith, CPP, Allied Insurance
Jose Miguel Sobron, United Nations
Jerzy W. Sobstel, SOSTEL
Scott Soltis, CPP, Actavis
Scott Taylor, CPP, Exact Security
Jason Teliszczak, CPP, JT Environmental Consulting, Inc.
Rajeev Thykatt, ISO 27001 Lead Auditor, BS 25999 Lead Auditor, Infosys BPO Ltd
Yoriko Tobishima, InterRisk Research Institute & Consulting, Inc.
Shawn VanDiver, CPP, AEM, CHS-V, CTT+, CHSM, CAS-PSM, VanDiver Consulting
Stephane Veilleux, CPP, Pharmascience
Carlos Velez, Johnson & Johnson
Erika Voss, CBCP, MBCI, Microsoft Corporation
Doug Weeks, PSP, Chevron
Renee Wentworth, Commonwealth of Virginia
Robert Weronik, CPP, Alexion
Nick Wildgoose, Zurich Insurance Group
Hunter Wright, CPP, Vestas Wind Systems
A. Dale Wunderlich, CPP, A. Dale Wunderlich & Associates, Inc.
Allison Wylde, University of Roe Hampton Business School

Working Group Members

Working Group Co-Chairs:

Marc H. Siegel, Ph.D., Commissioner, ASIS Global Standards Initiative
John J. Brown, P.E., ARM-E, Thomson Reuters

Frank Amoyaw, LandMark Security Limited
Ravi Anupindi, University of Michigan
Craig Babcock, Procter & Gamble

Pradeep Bajaj, Professional Industrial Security Management Academy
Dennis Blass, CPP, PSP, CISSP, CFE, CSHP, Children's of Alabama
John Casas, PSP, John Casas & Associates, LLC
Anthony DiSalvatore, CPP, PSP, PCI, Rocky Gap Casino Resort
Meliha Dzirlo-Ayvaz, PMP, CBCP, CEM, Deloitte & Touche LLP
Windom Fitzgerald, FitzgeraldTechnology Group
Charles Forsaith, Purdue Pharma
Thomas Frank, CPP, AbbVie Inc.
Robert Grieman, CPP, Securitas Security Services, USA, Inc.
Jeffrey Gruber, CPP, CHS-IV, Department of Defense, Department of the Army Civillian
Hector Grynberg, CPP, NOKIA
Lloyd Hardy, JSI Logistics
Tom Holmes, Edinburgh International
Zahid Iqbal, MSc psn, Microsoft Corporation
Calvin Jaeger, PhD, Sandia National Laboratories
Gerold Knight, The Coca-Cola Company
Alessandro Lega, CPP, Independent Consultant
Steven Lente, CPP, Securitas Security Services, USA, Inc.
Anthony Macisco, CPP, The Densus Group
Charlie Maclean-Bristol, CPP, PlanB Consulting
Pascal Matthey, PSP, XL Insurance Services Ltd
Jim McMahon, CPP, CISSP, McMahon & Associates
Philip Oppenheim, CBCP, Continuity Information Support Services
Russ Phillips, MMTS Group
Russell Price, Continuity Forum
Joseph Rector, CPP, PSP, PCI, USAF/11th Security Force Group
Eric Rojo, USDOE, DOD, Magination Consulting International
John Schettino, CFS, DIAGEO
Richard Sharpe, Competitive Insights, LLC
Jeffrey Slotnick, CPP, PSP, Setracon Inc.
Kevin Smith, CPP, Allied Insurance
Jerzy W. Sobstel, SOSTEL
Jason Teliszczak, CPP, JT Environmental Consulting, Inc.
Rajeev Thykatt, ISO 27001 Lead Auditor, BS 25999 Lead Auditor, Infosys BPO Ltd
Shawn VanDiver, CPP, AEM, CHS-V, CTT+, CHSM, CAS-PSM, VanDiver Consulting
Stephane Veilleux, CPP, Pharmascience
Doug Weeks, PSP, Chevron
Renee Wentworth, Commonwealth of Virginia
Hunter Wright, CPP, Vestas Wind Systems
Allison Wylde, University of Roe Hampton Business School

This page intentionally left blank.

TABLE OF CONTENTS

TABLE OF FIGURES

TABLE OF TABLES

0 Introduction

0.1 Supply Chain Risk Management: An Overview

This *Standard* defines supply chain risk as the uncertainty in achieving an organization's objectives throughout its supply chain. Organizations of all types and sizes face internal and external factors and influences that make it uncertain whether and when they will achieve their objectives. The effect this uncertainty has on an organization's objectives is "risk". Supply chain risk management (SCRM) involves the assessment and control of risk events at all points in an end-to-end supply chain, from sources of raw materials to end use by customers and consumers. SCRM is the systematic assessment and treatment of potential risk events across operations with the objective to exploit opportunities and/ or to reduce negative impacts on the performance of the organization and its supply chain. This includes the coordinated activities and practices an organization uses to manage its operational risks related to its end-to-end supply chain. Potential risk events can occur within and outside the supply chain. Risk events may be caused by:

a) Natural disasters;

b) Intentional acts (e.g., criminal acts, terrorism, industrial espionage, labor and social unrest, regulatory actions, etc.); and

c) Unintentional acts (e.g., accidents, process breakdowns, wrong materials, personnel issues, etc.).

SCRM is part of an integrated and multifaceted business management strategy, and therefore also takes into consideration the organization's image, reputation, and marketing, as well as the management of quality; environment, health and safety; purchasing; logistics; facilities; communications; human resources; and materials. SCRM integrates several different risk and resilience related disciplines, including, but not limited to security, cyber-security, crisis, business continuity, and emergency management, as well as asset conservation, insurance, and technology recovery. SCRM seeks to anticipate, prevent, protect, mitigate, manage, respond, and recover from potentially undesirable and disruptive events, as well as identify opportunities. The best strategy for addressing risk events will be determined by the organization's context of operations, its risk appetite, and results of risk assessments.

Supply chain risk management is a holistic component of the overall risk management framework for an organization. Therefore, this *Standard* should be used as a complement to existing risk management programs for enterprise or fiduciary risk. Adoption of this *Standard* should build on rather than supplant existing specialized risk programs.

0.2 The Need for Supply Chain Risk Management

SCRM is vital for organizations that increasingly rely on extended operations, both internal and external, for their success. This is primarily due to the advantages organizations have found in utilizing strategies such as globalization, outsourcing, off-shoring, specialized manufacturing,

supply-base rationalization, just-in-time deliveries, supplier consolidation and lean inventories. While these strategies offer many benefits in efficiency and effectiveness, they also make supply chains increasingly prone to risk and can increase the likelihood of supply-chain disruption.

Historic and recent events have proven the need to identify and manage supply chain risks.[1] These past events illustrate that a single event can disrupt multiple elements of supply chains around the world. Disruptions can impact any aspect of the supply chain, including critical infrastructure, communications, logistics, supply, manufacturing, and distribution. Therefore, to protect itself, an organization needs to develop proactive risk management strategies and plans. Additionally, they need to be fully cognizant of potential adverse consequences, opportunities, and impacts on financial performance.

SCRM is essential for all public or private organizations to manage risks associated with their dependencies and interdependencies in order to survive and thrive. Operational maturity levels vary between organizations. Some organizations have yet to realize the importance of SCRM while others have emerging or advanced SCRM programs[2] This *Standard* provides guidance on some current best practices that can be applied to any organization. An organization may select and use the appropriate guidance based on the maturity of its SCRM program.

In a globalized economy SCRM is critical for decision making and business planning of international operations and expansion of business. It is important that those responsible for analysis of international operations conduct a robust assessment of risk and resilience in their planning processes prior to domestic or international expansion, taking into account the local context and environment of operations. In the planning process the organization needs to understand the levels of control, exposure, and visibility it will have of the various tiers of its supply chain from end-to-end.

This guidance *Standard* is a compilation of evolving SCRM current best practices. It presents a generic approach to risk and resilience management that is intended to be applicable to all types of risk and all types of organizations. An organization's approach to SCRM should be tailored to meet its needs, context of operation, risk appetite, risk criteria, and its unique supply chain characteristics. There is no single path to success; therefore, this *Standard* offers a collection of SCRM current best practices, tools and approaches that any organization can review, and use or customize to meet its unique needs. Illustrative examples of SCRM current best practices have been included. Organizations should modify and adapt the concepts and examples included in this *Standard* to fit their distinctive requirements, characteristics, and culture.

---

[1] In 2011 and 2012 alone, economic losses around the world have been reported in the hundreds of billions of dollars in disruptive losses from natural disasters (e.g., Tohoku earthquake and tsunami, Thailand floods, Hurricane Sandy, droughts and other extreme weather events, etc.) and man-made catastrophes (political instability, power outages, cyber-crime, etc.).

[2] See Annex K for an example of the Supply Chain Risk Leadership Council's (SCRLC) maturity model.

This *Standard* addresses operational risks in the supply chain and includes risks to tangible assets (e.g., human, physical, and financial) as well as intangible assets (e.g., brand, reputation, competitive position or intellectual property). Each organization should define the scope of its SCRM program consistent with its risk criteria. It presents SCRM current best practices as models and/or options to improve operational risk management performance in the organization and its supply chain based on empirical experience.

SCRM is an evolving field. The challenges faced by organizations and their supply chains are constantly changing, therefore SCRM is a dynamic discipline that in order to achieve maximum effectiveness should be integrated into business management and business planning processes of the organization.[3] The contents of this *Standard* should be seen as a snapshot in time reflecting a collection of current best practices. Continual monitoring of risks is essential due to their dynamic nature and the manner in which they may impact the operations of organizations and their supply chains. When using this *Standard*, organizations should consider the concepts for their organization against their current operating environment to determine how best to structure SCRM to promote resiliency within their organization and its supply chain.

[3] See Figure 13

This page intentionally left blank.

Supply Chain Risk Management: A Compilation of Best Practices

1 SCOPE

This *Standard* provides guidance and current best practices for developing and embedding a framework and process of risk management in supply chain management. It can be applied to any type of organization, and its supply chain, regardless of size. This *Standard* adopts the risk management framework and process described in the ISO 31000:2009 - *Risk management -- Principles and guidelines* as the framework and process of Supply Chain Risk Management (SCRM). It provides current best practices to:

a) Identify internal and external environments (including dependencies and interdependencies);

b) Define risk criteria;

c) Assess risk (identify, analyze, and evaluate);

d) Consider and implement risk treatments and controls; and

e) Continually monitor and review risks and their treatment.

2 NORMATIVE REFERENCES

The following standard(s) contain provisions which, through reference in this text, constitute fundamental knowledge for the use of this American National Standard. At the time of publication, the edition(s) 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 edition(s) of the standard(s) indicated below.

a) ISO 31000:2009, *Risk management -- Principles and guidelines*.

3 TERMS AND DEFINITIONS

For the purposes of this *Standard*, the following terms and definitions apply:

	Term	Definition
3.1	**consequence**	Outcome of an event affecting objectives. NOTE 1: An event can lead to a range of consequences. NOTE 2: A consequence can be certain or uncertain and can have positive or negative effects on objectives. NOTE 3: Consequences can be expressed qualitatively or quantitatively. NOTE 4: Initial consequences can escalate through cumulative effects