ASIS INTERNATIONAL

Security and Resilience in Organizations and their Supply Chains—Requirements with Guidance

ASIS ORM.1-2017

STANDARD

The worldwide leader in security standards and guidelines development

ASIS INTERNATIONAL
Advancing Security Worldwide®

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 Center 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 the intelligence, resources, and technology needed within the business enterprise.

www.asisonline.org

ANSI/ASIS ORM.1-2017

(Revision, consolidation, redesignation of ASIS SPC.1-2009 and ASIS/BSI BCM.01-2010)

an American National Standard

SECURITY AND RESILIENCE IN ORGANIZATIONS AND THEIR SUPPLY CHAINS – REQUIREMENTS WITH GUIDANCE

An integrated risk-based management systems approach to manage risk and enhance resilience in organizations and their supply chains

Approved March 20, 2017

American National Standards Institute, Inc.

ASIS International

Abstract

This *Standard* recognizes the complex risk landscape facing organizations and their supply chains requires an integrated, comprehensive and systematic risk-based approach for managing risks to enhance sustainability, survivability and resilience, as well as identify and pursue opportunities for improvements. The *Standard* emphasizes proactive risk and business management to support a process of prevention, protection, preparedness, readiness, mitigation, response, continuity and recovery from undesirable and disruptive events. This *Standard* provides a single integrated management system to eliminate "siloing" of risk, enabling an organization to more efficiently anticipate and plan for naturally, accidentally, or intentionally caused events, using a single management system standard.

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 shall not be attributable to ASIS and is solely the responsibility of the certifier or maker of the statement.

ISBN: 978-1-934904-82-4

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.

This management systems standard provides generic auditable criteria and informative guidance.

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*.

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

Commission Members

Michael Knoke, CPP, Express Scripts, Inc., Chair
Bryan Leadbetter, CPP, Arconic.
Jose Miguel Sobron, United Nations
Roger Warwick, CPP, Pyramid International Temi Group
Allison Wylde, Cardiff University

At the time it approved this document, the ORM.1 Standards Committee, which is responsible for the development of this *Standard*, had the following members:

Committee Members

Committee Chairman: Marc H. Siegel, Ph.D., M. Siegel Associates
Commission Liaison: Lisa DuBrock, Radian Compliance
Committee Secretariat: Aivelis Opicka, ASIS International

Colin Ackroyd, Colin Ackroyd and Associates
Mark Baker, CPP, Macatoma Security Inc.
Mark Beaudry, CPP
John Bennett, Hospital Network Ventures, LLC
Dennis Blass, CPP, PSP, Children's of Alabama
Bruce Braes, CPP, CSyP, Optimal Risk Management
Hart Brown, HUB International
Herbert Calderon, CPP, PCI, PSP, Gloria Group
Werner Cooreman, CPP, PSP, Solvay
Britt Corra, Microsoft
Steven Dawson, Owens Corning
David Dodge, CPP, PCI, Temi Group, South Africa
Larry Dodson, CPP, University of Kansas
Jack Dowling, CPP, PSP, J. D. Security Consultants
James Drymiller, CPP
Eduard Emde, CPP, ESA European Space Agency
Thomas Frank, CPP, AbbVie
Shaun Fynes, CPP, PCI, PSP, Government Security Office (B.C.)
Francis Gallagher, PSP, Good Harbor Techmark
Jeffrey Gambrell, CPP, Absolute Software
Tareq Ghosheh, PalSafe
Robert Grieman, CPP, Securitas Security Services, USA
Andrew Griffiths, PCI, CEVA Logistics Uk Limited
Carlos Guzman, CPP, Security 101
Michael Heath, Diamond Security & Investigative Services
Christian Huenke, GENCO, A FedEx Company
Calvin Jaeger
Ben Jakubovic, CPP, PSP, CYBRA Corporation

Eduardo Jimenez-Granados, Procter & Gamble
UWE Klapproth, Euroclear SA/NV
Mukesh Lakhanpal, CPP, PSP, G4S Secure Solutions India
James Leflar, CPP, Zantech IT Services at the Federal Protective Service
Alessandro Lega, CPP
Victoria Leighton, Pierce College COE HSEM
Jeffrey LeMoine, CPP, General Mills
Rachelle Loyear
Ronald Martin, CPP, Open Security Exchange
Raida Mashal, JRMC (Jordan Risk Management Center for Training)
James McGuffey, CPP, PCI, PSP, A.C.E. Security Consultants
Murray Mills, CPP
William Minear, CPP, State of West Virginia
Dan Moe
Juan Munoz, CPP
Francisco Muñoz, CPP, Occidental Petroleum Corporation
Deyanira Murga, Executive Protection Institute
Normadene Murphy, BASF
Matthew Neely, CPP, SecureState
Vicki Nichols, Lockheed Martin
Peter Page, CPP, Al-Tayer Group
Juan Paredes, Socrates LTD.
Michael Payne, CPP, iJET International
Warren Petty, CPP, Wells Fargo
Russ Phillips, Coca-Cola Refreshments
Jose Piscione, CPP, PSP, Westcorp Argentina SA
Werner Preining, CPP, Interpool Security
Brandi Priest, Strategic Sustainable Solutionary Services Consulting
Stanley Ragen, CPP
Ronald Ronacher, PSP, Arup
Rick Saunders, Dynamis, Inc.
Ed Schlichtenmyer, StormGeo
Nancy Slotnick, Setracon
Jeffrey Slotnick, CPP, PSP, Setracon
Malcolm Smith, CPP
Jose-Miguel Sobron
Thomas Stephens, PCI, Rochester Research Associates, LLC
J. Kelly Stewart, Newcastle Consulting
Eduard Stor
Jason Teliszczak, CPP, JT Environmental Consulting
Rajeev Thykatt
Yoriko Tobishima, InterRisk Research Institute & Consulting, Inc.

Irvin Varkonyi, Supply Chain Ops Prep Edu.
Richard Widup, CPP, Mead Johnson Nutrition
Robert Wiest, CPP, CGI Group Inc.
William Wills, CPP, Briggs and Stratton Corporation
Allison Wylde, Regent's University London
Richard Zijdemans, Medtronic

Working Group Members

Working Group Chairman: Marc H. Siegel, Ph.D., M. Siegel Associates

Colin Ackroyd, Colin Ackroyd and Associates
Mark Beaudry, CPP
Dennis Blass, CPP, PSP, Children's of Alabama
Britt Corra, Microsoft
Thomas Frank, CPP, AbbVie
Shaun Fynes, CPP, PCI, PSP, Government Security Office (B.C.)
Robert Grieman, CPP, Securitas Security Services, USA
Andrew Griffiths, PCI, CEVA Logistics Uk Limited
Calvin Jaeger
James Leflar, CPP, Zantech IT Services at the Federal Protective Service
Alessandro Lega, CPP
William Minear, CPP, State of West Virginia
Dan Moe
Normadene Murphy, BASF
Michael Payne, CPP, iJET International
Russ Phillips, Coca-Cola Refreshments
Werner Preining, CPP, Interpool Security
Ronald Ronacher, PSP, Arup
Ed Schlichtenmyer, StormGeo
Jose-Miguel Sobron
Thomas Stephens, PCI, Rochester Research Associates, LLC
Jason Teliszczak, CPP, JT Environmental Consulting
Rajeev Thykatt
Robert Wiest, CPP, CGI Group Inc.
William Wills, CPP, Briggs and Stratton Corporation
Allison Wylde, Regent's University London
Richard Zijdemans, Medtronic

TABLE OF CONTENTS

TABLE OF FIGURES

0. INTRODUCTION

0.1 General

This *Standard* recognizes the complex risk landscape facing organizations and their supply chains requires an integrated, comprehensive and systematic risk-based approach for managing risks to enhance survivability, sustainability and resilience, as well as identify and pursue opportunities for improvements. The *Standard* emphasizes proactive risk and business management to support the pursuit of objectives and opportunities as well as a process of prevention, protection, preparedness, readiness, mitigation, response, continuity and recovery from undesirable and disruptive events. This *Standard* provides a single integrated management system to eliminate "siloing" of risk, enabling an organization to more efficiently anticipate and plan for naturally, accidentally, or intentionally caused events, using a single management system standard.

The *Standard* recognizes that organizations do not operate in isolation but rather as part of a complex and interconnected ecosystem. It is not sufficient to manage just internal organizational risks, but it is essential for organizations to take a systems approach and understand the risk characteristics and interactions with individuals, organisations, the community and society. To properly manage risk, organizations need to assess the internal and external context of their activities, functions, products and services. This includes the risk factors related to its end-to-end supply chain, interdependencies and dependencies.

This *Standard* takes a jurisdictional/country and discipline neutral approach to managing the uncertainties in achieving the organization's strategic, operational, tactical, and reputational objectives. Risk management is viewed from a proactive and forward-looking perspective to protect and create value for the organization and its stakeholders. In order to build resilience, organizations need to continually integrate and optimize their risk and business management processes. By fully integrating its risk management processes throughout its enterprise-wide business management activities, the organization is empowered to make informed decisions based on best available information.

Resilience, as defined in this *Standard* is: "The absorptive and adaptive capacity of an organization in a complex and changing environment." Therefore, resilience is about building capacity, rather than an end-point, and includes:

a) A convergence and integration of systems to manage its human, tangible and intangible assets (including addressing risks associated with information and communications technology products and services);
b) Building a capacity for proactive risk management which identifies indicators of opportunities, change and adversity to enable an organization to take pre-emptive measures to pursue positive outcomes and minimize negative outcomes;
c) An agility and flexibility capacity in risk and business management processes aligned with time dependencies and needs for change;

d) An absorptive, resistive and carrying capacity to resist being affected by an event or the ability to return to an acceptable level of performance in an acceptable period of time after being affected by an event;
e) The capability of a system to maintain its functions and structure in the face of internal and external change in order to pursue opportunities and/or to manage degradation of activities and functions when it must;
f) Proactively planning to reduce the magnitude and/or duration of undesirable and disruptive events by enhancing its ability to anticipate, absorb, adapt to, and/or rapidly recover from events;
g) Empower people to respond to change, opportunities, or adversity in an informed manner; and
h) Viewing the organization from a multidimensional, multi-disciplinary systems approach to optimize its management of interactions within its risk environment.

0.2 Proactive Management of Risk to Build Resilience

Resilience takes a forward-looking view of risk, fully integrating business and risk management into the organization's system of management. Risk is viewed as inevitable and having the potential for positive outcomes. People in a resilient organization ask themselves: "what are the positive changes we can make to strengthen the organization?" This means better understanding where you are to assist in knowing where you are going. It also means acknowledging weaknesses and threats in order to build strengths and opportunities.

Risk is the effect of uncertainty on the achievement of strategic, operational, tactical, and reputational objectives (ANSI/ASIS/RIMS RA.1-2015). All activities involve a certain amount of uncertainty. Uncertainty is the state where outcomes are unknown, undetermined, or undefined; or where there is a lack of sufficient information. Outcomes may be positive, negative, or neutral. Individuals, organizations, and communities must decide how much risk and uncertainty they are willing to accept or take in order to achieve their objectives and desired outcomes. Objectives may include short and long term strategic goals related to the whole or parts of the organization and its value chain (including its supply chains), as well as operational and tactical issues at all levels of the organization. The management of risks is a function of the organization's objectives, appetite for risk, and its desire to exploit an opportunity or minimize a potential negative consequence. There is no simple formula or standardized approach to managing risk and building resilience. It must be tailored to the organization and it context.

Resilience promotes a perspective of enterprise-wide agility and adaptability in a dynamic and uncertain environment. Resilient organizations fully integrate a holistic and proactive risk management perspective into good business management practice to enhance their buffering and adaptive capacity. Resilience requires both the convergence of risk disciplines as well as the elimination of and/or collaboration among organizational siloes to have a coordinated plan for managing risk throughout the enterprise.

Resilience is not something that is inherent to an organization but develops as organizations mature, learn from successes and mistakes, improve their management and decision making

skills, and gain better insights and more knowledge about the internal and external factors that may impact performance. Resilience also comes from supportive relationships, cultural perspectives, and individuals' ability to cope with stress and adversity. Therefore, resilience is a function of a variety of behaviours, thoughts, and actions that can be learned and developed over time.

Resilience in organizations is similar to resilience in people in that it is not a trait but rather a perspective of living with risk. Resilient organizations:

a) Recognize that change is constant;
b) Consider the organization's dependencies and interdependencies in assessing risk to the organization and its risks on others;
c) Integrate proactive risk management into all their decision-making processes;
d) Position the organization to identify and exploit opportunities emphasizing that adaption before a potential event provides efficiencies;
e) Promote situational awareness and monitoring with an emphasis on identifying indicators of change;
f) Develop a process of managing adversity to pre-emptively adapt, better absorb a blow, learn from its experiences and that of others to persevere and evolve into a stronger organization;
g) Cultivate problem-solving skills throughout the organization considering future outcomes and where the organization wants or needs to go;
h) Use a systems approach to management understanding the relationships between all the elements, disciplines and divisions that make up the whole;
i) Recognize that not all uncertainties and their outcomes can be identified or quantified, so they determine the criticality of assets, activities and services necessary to facilitate sustainable operations;
j) View recovery as an opportunity considering the context of the changed environment, determining where the organization can be best positioned; and
k) Foster meaning and purpose for their stakeholders to work for the common benefit of all.

Being a resilient organization means efficiently tapping into its human, tangible, and intangible resources. All organizations have resource and capability limitations. Understanding risk management within the context of these resource limitations enables an organization to better identify its strengths and leverage them. Resilient organizations develop strong networks and relationships with stakeholders, their supply chains, other organizations, and the community. The organization understands its position in the bigger picture and learns from observing others, sharing appropriate information, and knowing where to seek help when needed. Resilient organizations are resourceful and recognize that relationships with stakeholders are among their most important resources.

Improving communication and consultation skills is essential to building resilience. Risk is best managed with ongoing consultation and interactive communication among stakeholders. A resilient organization will build the mechanisms needed to support both a top-down and bottom-up flow of information.

Empowering people at all levels of the organization fosters the sense of inclusiveness and ownership that encourages the sharing of ideas. It helps to promote a risk culture where risk makers and risk takers understand that they are also risk owners and risk managers. An effective flow of information based on a sense of inclusion promotes informed decision making. By communicating that continual innovation, creativity, and information/knowledge acquisition are core values of the organization, persons working on behalf of the organization will be empowered to proactively identify and address concerns thereby enhancing agility and an adaptive capacity. People will sense that they are part of the solution and not the problem.

Being resilient does not mean an organization will not suffer the consequences of change and adversity, rather the organization is better positioned to quickly identify, learn, and adapt to change and adversity. It is an evolutionary process. Recognizing new opportunities and possibilities does not require abrupt or impulsive change; it requires a measured approached based on best available information.

0.3 An Integrated Management Systems Approach

The management systems approach encourages organizations to analyze organizational and stakeholder requirements and define processes that contribute to success. A management system provides the framework for continual improvement to increase the likelihood of achieving strategic, operational, tactical, and reputational objectives while enhancing the resilience of an organization and its supply chain. It provides confidence to both the organization and its stakeholders that the organization is able to manage its risks and meet legal, regulatory, and contractual requirements, as well as voluntary commitments.

For additional information on an integrated management systems approach, please see Annex E.

Figure 1 illustrates the management systems approach used in this *Standard*.

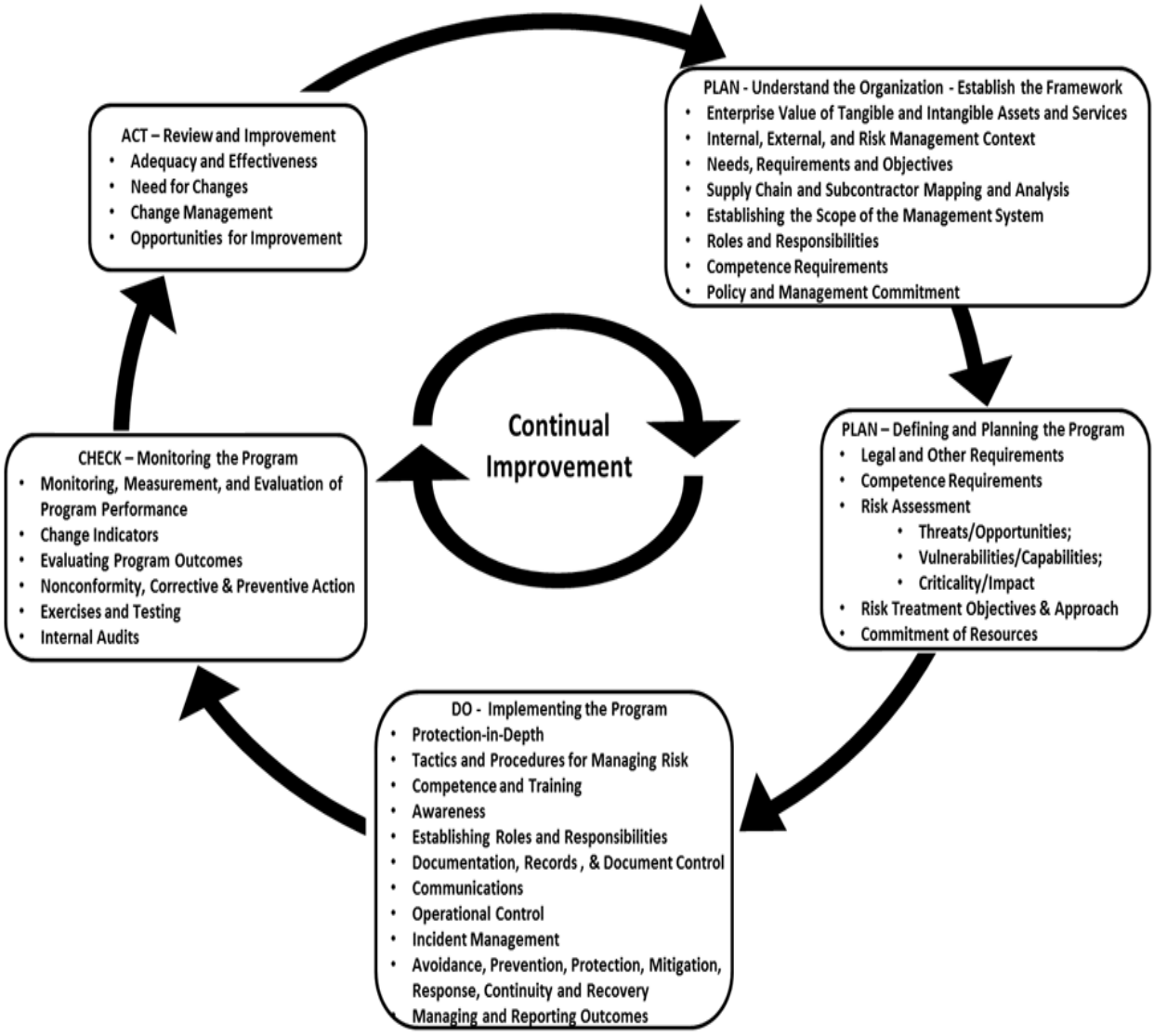

Figure 1: Management System for Security and Resilience in Organizations and their Supply Chains

Security and Resilience in Organizations and their Supply Chains – Requirements with Guidance

1. SCOPE

This *Standard* specifies requirements for an integrated management system for organizations and their supply chains. The organizational resilience management system (ORMS) enables an organization to identify, assess, and manage risks related to the achievement of its strategic, operational, tactical, and reputational objectives in the organization and its supply chains. It provides a holistic framework to develop and implement policies, objectives, and programs taking into account:

a) Context of the organization and its supply chains;
b) Legal, regulatory, and contractual obligations and voluntary commitments;
c) Needs of internal and external stakeholders;
d) Uncertainties in achieving its objectives; and
e) Protection of human, tangible and intangible assets.

This *Standard* applies to risks and/or their impacts that the organization identifies as those it can control, influence, reduce, or exploit. It does not itself state specific performance criteria.

This *Standard* is applicable to any organization that wishes to:

a) Establish, implement, maintain, and improve an ORMS;
b) Assure itself of its conformity with its stated ORMS;
c) Demonstrate conformity with this *Standard* by:
    i. Making a self-determination and self-declaration; or
    ii. Seeking confirmation of its conformance by parties having an interest in the organization (such as customers); or
    iii. Seeking confirmation of its self-declaration by a party external to the organization; or
    iv. Seeking certification/registration of its ORMS by an external organization.

All the requirements in this *Standard* are intended to be incorporated into any type of organization's management system. It provides all the elements required to integrate management, technology, facilities, processes, and people into the security and resilience culture, risk management, and ORMS of an organization. The extent of the application will depend on factors such as the risk appetite and policy of the organization; the nature of its activities, products, and services; and the location where, and the conditions in which, it functions.

This *Standard* provides generic requirements as a framework, applicable to all types of organizations (or parts thereof) regardless of size and nature of operation. It is applicable to all types of activities and decision-making processes. It provides guidance for organizations to develop their own specific performance criteria, enabling the organization to tailor and implement an ORMS appropriate to its needs and those of its stakeholders.

The *Standard* emphasizes resilience, the absorptive and adaptive capacity of an organization in a complex and changing environment. Risks are managed in a forward-looking proactive perspective to enable the organization to identify current and emerging threats and opportunities in its operations and in its supply chain. Applying this S*tandard* enhances the organization's absorptive and adaptive capacity to avoid, prevent, withstand and emerge stronger from all manner of intentional, unintentional, and/or naturally-caused events.

This *Standard* enables an organization to:

a) Develop an ORMS policy;
b) Establish objectives, procedures, and processes to achieve the policy commitments;
c) Develop processes to assure competency, awareness, and training;
d) Set metrics to measure performance and demonstrate success;
e) Take action as needed to improve performance;
f) Demonstrate conformity of the system to the requirements of this *Standard*; and
g) Establish and apply a process for continual improvement.

Annex A provides informative guidance on system planning, implementation, testing, maintenance, and improvement.

2. Normative References

The following document contains information which, through reference in this text, constitutes foundational knowledge for the use of this American National Standard. At the time of publication, the editions indicated were valid. All material is subject to revision, and parties are encouraged to investigate the possibility of applying the most recent editions of the material indicated below.

a) ANSI/ASIS/RIMS RA.1-2015 – Risk Assessment[1]

3. Terms and Definitions

For the purposes of this document, the terms and definitions given in ANSI/ASIS/RIMS RA.1-2015, *Risk Assessment*, and the following apply:

[1] This document is available at < http://www.asisonline.org >.