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
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

Charles Baley, Farmers Insurance Group, Inc.

Cynthia P. Conlon, CPP, Conlon Consulting Corporation

William Daly, Control Risks Security Consulting

Lisa DuBrock, Radian Compliance LLC

Eugene Ferraro, CPP, PCI, ForensicPathways, Inc.

Bernard Greenawalt, CPP, Securitas Security Services USA, Inc., Vice Chair

Robert Jones, Socrates Ltd

Glen Kitteringham, CPP, Kitteringham Security Group Inc.

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

0. INTRODUCTION XV
0.1 GENERAL XV
0.2 PROACTIVE MANAGEMENT OF RISK TO BUILD RESILIENCE XVI
0.3 AN INTEGRATED MANAGEMENT SYSTEMS APPROACH XVIII

1. SCOPE 1

2. NORMATIVE REFERENCES 2

3. TERMS AND DEFINITIONS 2

4. GENERAL PRINCIPLES 8
4.1 LEADERSHIP AND VISION 9
4.2 GOVERNANCE 9
4.3 FACTUAL BASIS FOR DECISION MAKING 9
4.4 OUTCOMES ORIENTED 9
4.5 NEEDS ORIENTED TAKING HUMAN AND CULTURAL FACTORS INTO ACCOUNT 9
4.6 OVERALL ORGANIZATIONAL RISK AND BUSINESS MANAGEMENT STRATEGY 10
4.7 SYSTEMS APPROACH 10
4.8 ADAPTABILITY AND FLEXIBILITY 10
4.9 MANAGING UNCERTAINTY 11
4.10 CULTURAL CHANGE AND COMMUNICATION 11
4.11 CONTINUAL IMPROVEMENT 11

5. ESTABLISHING THE FRAMEWORK 11
5.1 GENERAL 11
5.2 CONTEXT OF THE ORGANIZATION 12
5.3 NEEDS AND REQUIREMENTS 13
5.4 DEFINING RISK CRITERIA 14
5.5 SCOPE OF THE MANAGEMENT SYSTEM 14

6. LEADERSHIP 15
6.1 GENERAL 15
6.2 MANAGEMENT COMMITMENT 15
6.3 POLICY 16
6.4 ORGANIZATIONAL ROLES, RESPONSIBILITIES, AND AUTHORITIES FOR THE ORMS 16

7. PLANNING 17
7.1 LEGAL AND OTHER REQUIREMENTS 17
7.2 RISK ASSESSMENT 17
7.3 OBJECTIVES AND PLANS TO ACHIEVE THEM 19
7.4 ACTIONS TO ACHIEVE RISK AND BUSINESS MANAGEMENT OBJECTIVES 20

8. STRUCTURAL REQUIREMENTS 21
8.1 GENERAL 21
8.2 ORGANIZATIONAL STRUCTURE 21
8.3 FINANCIAL AND ADMINISTRATIVE PROCEDURES 21
8.4 INSURANCE 21
8.5 OUTSOURCING AND SUBCONTRACTING 21
8.6 DOCUMENTED INFORMATION 22

9. OPERATION AND IMPLEMENTATION 23
9.1 OPERATIONAL CONTROL 23
9.2 RESOURCES, ROLES, RESPONSIBILITY, AND AUTHORITY 24
9.3 COMPETENCE, TRAINING, AND AWARENESS 27

9.4 COMMUNICATION 28
9.5 PREVENTION AND MANAGEMENT OF UNDESIRABLE OR DISRUPTIVE EVENTS 29

10. PERFORMANCE EVALUATION 33
10.1 GENERAL 33
10.2 MONITORING AND MEASUREMENT 33
10.3 EVALUATION OF COMPLIANCE 33
10.4 EXERCISES AND TESTING 33
10.5 INTERNAL AUDIT 34
10.6 MANAGEMENT REVIEW 35

11. CONTINUAL IMPROVEMENT 36
11.1 GENERAL 36
11.2 NONCONFORMITIES, CORRECTIVE AND PREVENTIVE ACTION 36
11.3 CHANGE MANAGEMENT 36
11.4 OPPORTUNITIES FOR IMPROVEMENT 36

A GUIDANCE ON THE USE OF THE STANDARD 38
A.1 INTRODUCTION 38
A.2 GENERAL REQUIREMENTS 40
A.3 MANAGEMENT SYSTEM 42
A.4 GENERAL PRINCIPLES 42
A.5 ESTABLISHING THE FRAMEWORK 43
A.6 LEADERSHIP 46
A.7 PLANNING 48
A.8 STRUCTURAL REQUIREMENTS 56
A.9 OPERATION AND IMPLEMENTATION 59
A.10 PERFORMANCE EVALUATION 78
A.11 MATURITY MODEL FOR THE PHASED IMPLEMENTATION 83

B EXAMPLES OF INCIDENT PREVENTION, PREPAREDNESS, AND RESPONSE 85

C EXAMPLES OF RISK TREATMENT PROCEDURES THAT ENHANCE RESILIENCE OF THE ORGANIZATION 92
C.1 GENERAL 92
C.2 PREVENTION AND MITIGATION PROCEDURES 92
C.3 RESPONSE PROCEDURES 93
C.4 CONTINUITY PROCEDURES 94
C.5 RECOVERY PROCEDURES 95

D BUSINESS IMPACT ANALYSIS 102

E AN INTEGRATED MANAGEMENT SYSTEMS APPROACH 106
E.1 GENERAL 106
E.2 SCOPE OF THE ORMS 108

F QUALIFIERS TO APPLICATION 110

G BIBLIOGRAPHY 112
G.1 ASIS INTERNATIONAL PUBLICATIONS 112
G.2 NATIONAL STANDARDS PUBLICATIONS 112

H REFERENCES 113
H.1 GOVERNMENT PUBLICATIONS 113

TABLE OF FIGURES

FIGURE 1: MANAGEMENT SYSTEM FOR SECURITY AND RESILIENCE IN ORGANIZATIONS AND THEIR SUPPLY CHAINS xix
FIGURE 2: PROCESS FOR MANAGING RISK (BASED IN ISO 31000) 50
FIGURE 3: BUSINESS IMPACT ANALYSIS (BIA)..104
FIGURE 4: EXAMPLE OF BIA METHODOLOGY..104
FIGURE 5: TYPICAL BIA ACTIVITIES 105
FIGURE 6: PLAN-DO-CHECK-ACT MODEL 107

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*.

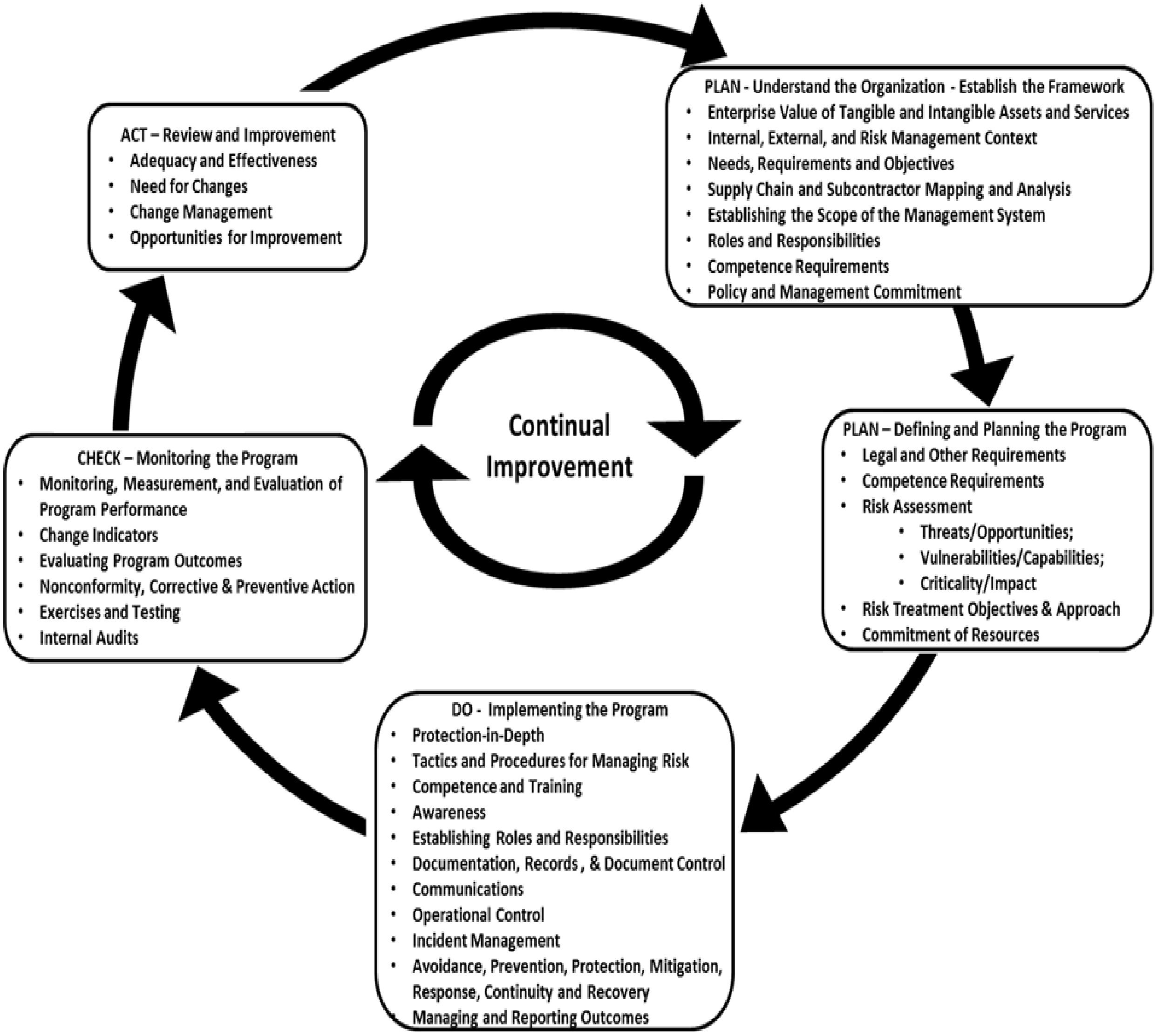
PLAN - Understand the Organization - Establish the Framework
Enterprise Value of Tangible and Intangible Assets and Services
Internal, External, and Risk Management Context
Needs, Requirements and Objectives
Supply Chain and Subcontractor Mapping and Analysis
Establishing the Scope of the Management System
Roles and Responsibilities
Competence Requirements
Policy and Management Commitment
PLAN – Defining and Planning the Program
Legal and Other Requirements
Competence Requirements
Risk Assessment
Threats/Opportunities;
Vulnerabilities/Capabilities;
Criticality/Impact
Risk Treatment Objectives & Approach
Commitment of Resources
DO - Implementing the Program
Protection-in-Depth
Tactics and Procedures for Managing Risk
Competence and Training
Awareness
Establishing Roles and Responsibilities
Documentation, Records , & Document Control
Communications
Operational Control
Incident Management
Avoidance, Prevention, Protection, Mitigation, Response, Continuity and Recovery
Managing and Reporting Outcomes
CHECK – Monitoring the Program
Monitoring, Measurement, and Evaluation of Program Performance
Change Indicators
Evaluating Program Outcomes
Nonconformity, Corrective & Preventive Action
Exercises and Testing
Internal Audits
ACT – Review and Improvement
Adequacy and Effectiveness
Need for Changes
Change Management
Opportunities for Improvement
Continual Improvement

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 >.

	Term	Definition
3.1	**acceptable downtime**	Maximum elapsed time between a disruption and restoration of needed operational capacity or capability.
3.2	**activity**	Process or set of processes undertaken by an organization (or on its behalf) that produces or supports one or more products or services. NOTE: Examples of such processes include accounting, call center, information services, manufacturing, distribution, and other services.
3.3	**alternate worksite**	A work location, other than the primary location, to be used when the primary location is not accessible. [ASIS International Business Continuity Guideline: 2004]
3.4	**auditor**	A person with the competence to conduct an audit.
3.5	**business continuity**	Ability of an organization to operate at predefined levels following a disruptive event.
3.6	**business continuity management (BCM)**	Proactive set of planning, preparedness and related activities which are intended to restore an organization's critical business functions to pre-determined levels enabling the organization to operate despite serious disruptive events and recover to an operational state expeditiously.
3.7	**business continuity plan (BCP)**	A collection of procedures and information which is developed, tested and maintained in preparation for use in a disruptive event to continue operations at predefined levels following the event.
3.8	**continual improvement**	Recurring process of enhancing the security, preparedness, and continuity (SPC) management system in order to achieve improvements in overall SPC management performance consistent with the organization's SPC management policy NOTE: The process need not take place in all areas of activity simultaneously.
3.9	**conformity**	Fulfillment of a requirement.
3.10	**crisis**	An unstable condition involving an impending abrupt or significant change that requires urgent attention and action to protect life, assets, property, or the environment.

	Term	Definition
3.11	**crisis management**	Holistic management process that identifies potential impacts that threaten an organization and provides a framework for building resilience, with the capability for an effective response that safeguards the interests of its key stakeholders, reputation, brand, and value-creating activities -- as well as effectively restoring operational capabilities. NOTE: Crisis management also involves the management of preparedness, mitigation response, continuity or recovery in the event of an incident -- as well as management of the overall program through training, rehearsals, and reviews to ensure the preparedness, response, and continuity plans stays current and up-to-date.
3.12	**crisis management team**	Group of individuals functionally responsible for directing the development and execution of the response and operational continuity plan, declaring an operational disruption or emergency/crisis situation and providing direction during the recovery process, both pre-and post-disruptive incident. NOTE: The crisis management team may include individuals from the organization as well as immediate and first responders, stakeholders, and other interested parties.
3.13	**disaster**	Event that causes significant damage to assets or loss of life.
3.14	**disruption**	An event that interrupts normal business, functions, operations, or processes, whether anticipated (e.g., hurricane, political unrest) or unanticipated (e.g., a blackout, terror attack, technology failure, or earthquake). NOTE: A disruption can be caused by either positive or negative factors that will disrupt normal functions, operations or processes.
3.15	**downtime**	Period of time when something is not in operation. NOTE: The allowable period of downtime is determined by the organizations obligations (e.g., customer and regulatory requirements).
3.16	**emergency**	Serious, unexpected, and precarious situation requiring immediate action.
3.17	**evacuation**	Organized, phased, and supervised dispersal of people from dangerous or potentially dangerous areas. [ASIS International Business Continuity Guideline: 2004]

	Term	Definition
3.18	**exercises**	Evaluating management programs, rehearsing the roles of team members and staff, and testing the recovery or continuity of an organization's systems (e.g., technology, telephony, administration) to demonstrate management competence and capability. NOTE 1: Exercises include activities performed for the purpose of training and conditioning team members and personnel in appropriate responses with the goal of achieving maximum performance. NOTE 2: An exercise can involve invoking response and operational continuity procedures, but is more likely to involve the simulation of a response and/or operational continuity incident, announced or unannounced, in which participants role-play in order to assess what issues might arise, prior to a real invocation.
3.19	**facility (infrastructure)**	Plant, machinery, equipment, property, buildings, vehicles, information systems, transportation facilities, and other items of infrastructure or plant and related systems that have a distinct and quantifiable function or service.
3.20	**first responder**	A member of an emergency service who is first on the scene at a disruptive incident NOTE 1: Emergency services include any public or private service that deals with disruptions, such as the initial responding law enforcement officers, other public safety officials, emergency medical personnel, rescuers and/or other emergency response service providers.
3.21	**hazard**	Possible source of danger or conditions (physical or operational) that have a capacity to produce a particular type of adverse effect.
3.22	**internal audit**	Systematic, independent, and documented process for obtaining audit evidence and evaluating it objectively to determine the extent to which the management system audit criteria set by the organization are fulfilled. NOTE: In many cases, particularly in smaller organizations, independence can be demonstrated by the freedom from responsibility for the activity being audited.
3.23	**key performance indicator (KPI)**	Metric used to evaluate factors that are crucial to the success of an organization or of a particular activity in which it engages. NOTE: A KPI is a metric which indicates how an organization is performing against its objectives.
3.24	**loss**	Being deprived of someone or something, of value.
3.25	**management plan**	Clearly defined and documented plan of action, typically covering the key personnel, resources, services, and actions needed to implement the incident management process.

	Term	Definition
3.26	**mitigation**	Limitation of any negative consequence of a particular incident.
3.27	**mutual aid agreement**	Written agreement between agencies, organizations, or jurisdictions to lend assistance across jurisdictional boundaries.
3.28	**ORMS**	Organizational resilience management system - Coordinated activities to direct and control an organization with regard to managing risk to enhance resilience and security in the organization and its supply chain. NOTE: Direction and control with regard to ORMS generally includes establishment of the policy, planning, and objectives directing operational processes and continual improvement.
3.29	**ORMS objective**	Something sought, or aimed for, related to managing risk to enhance resilience and security in the organization and its supply chain. NOTE 1: Quality objectives are generally based on the organization's quality policy. NOTE 2: Quality objectives are generally specified for relevant functions and levels in the organization.
3.30	**ORMS policy**	Overall intentions and direction of an organization related to managing risk to enhance resilience and security in the organization and its supply chain as formally expressed by top management. NOTE 1: Generally, the security and resilience policy is consistent with the overall policy of the organization, and provides a framework for the setting of security and resilience objectives. NOTE 2: ORMS principles presented in this Standard can form a basis for the establishment of a quality policy.
3.31	**policy**	Overall intentions and direction of an organization, as formally expressed by top management. [ANSI/ASIS/RIMS RA.1-2015]
3.32	**preparedness (readiness)**	Activities, programs, and systems developed and implemented prior to an incident that may be used to support and enhance mitigation of, response to, and recovery from disruptions, disasters, or emergencies.
3.33	**probability**	A number between zero and one that shows how likely a certain event is.
3.34	**procedure**	An established or specified way to conduct an activity or a process. [ANSI/ASIS/RIMS RA.1-2015]
3.35	**process**	Actions, changes or steps taken in order to achieve a particular end.
3.36	**product**	Goods and services that are the result of a process. NOTE: Typically, a product is an item or service that is produced to create value.

	Term	Definition
3.37	**recovery point objective**	Point in time to which data or capacity of a process is in a known and valid or integral state can be restored from. This should be less than the maximum amount of loss tolerance and may be defined in hours or days.
3.38	**recovery time objective (RTO)**	Time goal for the restoration and recovery of functions or resources based on the acceptable down time and acceptable level of performance in case of a disruption of operations.
3.39	**resilience**	Absorptive and adaptive capacity in a complex and changing environment.
3.40	**resources**	Any asset (human, physical, information, or intangible), facilities, equipment, materials, products, or waste that has potential value and can be used.
3.41	**response plan**	Documented collection of procedures and information that is developed, compiled, and maintained in readiness for use in an incident.
3.42	**response team**	Group of individuals responsible for developing, executing, rehearsing, and maintaining the response plan, including the processes and procedures.
3.43	**safety**	Freedom from danger, risk, or injury.
3.44	**security**	The condition of being protected against risks, hazards, threats, or loss. NOTE 1: In the general sense, security is a concept similar to safety. The distinction between the two is an added emphasis on being protected from dangers that originate from outside. NOTE 2: The term security means that something not only is secure, but that it has been secured.
3.45	**target**	Something you are trying to do or achieve with defined metrics.
3.46	**testing**	Activities performed to evaluate the effectiveness or capabilities of a plan relative to specified objectives or measurement criteria. Testing usually involves exercises designed to keep teams and employees effective in their duties, and to reveal weaknesses in the preparedness and response/continuity/recovery plans. [ASIS International Business Continuity Guideline: 2004]
3.47	**threat**	Potential cause of an unwanted incident, which may result in harm to individuals, assets, a system or organization, the environment, or the community.

	Term	Definition
3.48	top management	Directors, managers, and officers of an organization that can ensure effective management systems -- including financial monitoring and control systems -- have been put in place to protect assets, earning capacity, and the reputation of the organization.
3.49	vulnerability	State of being susceptible to harm or injury. NOTE: Susceptibility to negative outcomes of a risk.
3.50	vulnerability analysis	Process of identifying and quantifying something that creates susceptibility to a source of risk that can lead to a consequence.

NOTE: The reader is encouraged to read through the terms and definitions provided in the ANSI/ASIS/RIMS RA.1-2015, prior to reading the body of this document.

4. General Principles

The goal of an ORMS is to support the achievement of strategic, operational, tactical, and reputational objectives. Organizations need to anticipate and manage circumstances related to human, technical, or naturally caused events that may have positive or negative outcomes for the organization and its supply chains. Organizations need to manage risks to its stakeholders, including persons working on its behalf, supply chain partners, clients, shareholders, and affected communities. They have a duty-of-care responsibility to enhance human safety and security as well as the protection of tangible and intangible assets while maintaining respect for laws and obligations as well as rights and interests of stakeholders. This is accomplished by fully integrating the management of risks into decision-making and business management processes throughout the organization and its supply chain.

The intent is to:

a) Provide an information-driven approach to decision-making and management;
b) Identify and pursue potential opportunities;
c) Minimize the likelihood and consequences of an undesirable or disruptive event by prevention, when possible; mitigating the impact of an event; through effectively and efficiently responding when an event occurs; by maintaining an agreed level of performance; by assuring accountability and implementing lessons learned after the event; and by taking measures to prevent a recurrence; and
d) Promote a culture in the organization that recognizes the role and responsibility of every person working on behalf of the organization in managing risks.

An ORMS is achieved by developing, designing, documenting, deploying and evaluating fit-for-purpose proactive management strategies needed to achieve current objectives and identify indicators for potential needs for changes. The elements for the management system are detailed in clauses 5-11 and the annexes of this Standard. In developing, applying and improving a ORMS, top management/decision-makers should apply the following general principles.

4.1 Leadership and Vision

Top management (which refers to the person or persons responsible for decision making, that have authorization for the implementation of the decisions) establishes the vision, sets objectives, and provides direction for the organization. They promote a culture of ownership within the organization where everyone views managing the risks as part of their contribution to achieving the organization's goals and objectives. They encourage a top-down/bottom-up approach to identify needs for change to pursue opportunities as well as to prevent and manage undesirable and disruptive events. Top management demonstrates a commitment to promote a culture of respect for relevant jurisdictional laws, contractual obligations, and the rights of individuals, as well as effective leadership in the implementation and maintenance of this Standard.

4.2 Governance

Enhanced security and resilience is viewed as part of an overall good governance strategy and an enterprise-wide responsibility. Transparency and inclusiveness of risk management processes provide the foundation for good governance. Decision-making and the provision of goods and services in line with compliance with relevant jurisdictional laws, contractual obligations, protection of human rights and the creation of value are part of the organization's ethos and values. The protection of human life and safety in the course of achieving the mission's objectives is a primary concern of managing the risks of undesirable and disruptive events.

4.3 Factual Basis for Decision Making

Identifying, assessing and managing risks provides the basis for making informed decisions at all levels of the organization and its supply chain. Assessing and managing risk drives decision making, and dictates the actions that will be taken based on factual analysis – balanced with experience and accepted industry best practices. The ORMS increases the ability to review, challenge, and change opinions and decisions; enhances problem-solving capacity; increases the ability to demonstrate effectiveness of past decisions through reference to factual records; and ensures that data and information are accurate, reliable, and timely – in line with company policy.

4.4 Outcomes Oriented

A management system is more than a set of management processes; it is a tool to achieve desired outcomes. The desired outcome of the ORMS is to enhance security and resilience of the organization and its supply chain to facilitate the achievement of strategic, operational, tactical, and reputational objectives. Key Performance Indicators (KPI) are defined to support achievement of objectives. KPIs drive a culture of management by measurement for continual monitoring and performance improvement.

4.5 Needs Oriented Taking Human and Cultural Factors into Account

In order to create and protect value, the ORMS identifies, understands and is responsive to the needs and expectations of internal and external stakeholders – such as persons working on behalf of the organization, supply chain partners, affected communities, and its clients and customers.

Objectives of the organization are linked to internal and external stakeholder needs and expectations. Stakeholder relationships are systematically managed using a balanced approach between the needs of the organization and its stakeholders. This requires an understanding of the security and resilience needs and expectations of individuals, organizations, industry sectors, communities and society that may impact and be impacted by the organization. The ORMS considers and takes into account the variability of human and cultural factors that impact and may be impacted by its activities. Understanding bias, human, cultural and temporal factors are essential for understanding and adequately managing risk.

4.6 Overall Organizational Risk and Business Management Strategy

Security and resilience assurance are part of an organization's overall risk and business management strategy. Unless risk is managed effectively, organizations cannot maximize opportunities and minimize negative outcomes. Therefore, the risk management process requires a clear understanding of the organization's internal and external contexts to proactively identify opportunities and minimize the uncertainty in achieving its strategic, operational, tactical, and reputational objectives. Risk management is viewed as integral to business management, decisions, activities, functions and change-making processes throughout the organization. Assessing and understanding an organization's acceptable level of risk is critical for the organization to develop a preemptive and effective risk management strategy that matches the needs and expectations of its internal and external stakeholders within the context of the operating environment's level of risk.

4.7 Systems Approach

A ORMS requires a multi-dimensional, dynamic and iterative approach. Identifying, understanding, and managing interrelated processes and elements contribute to the organization's effective and efficient control of its risks. The systems approach examines the linkages and interactions between the elements that compose the entirety of the system. Component parts of a system can best be understood in the context of their interrelationships, rather than in isolation, and must be treated as a whole.

4.8 Adaptability and Flexibility

The ORMS is aligned with internal and external factors (context), and therefore, is tailored to the needs and risk profile of the organization and its supply chain. Organization's need to recognize that they operate in dynamic environments that are subject to change. Organizations need to conduct on-going monitoring of the risk and market environment to identify changes and implement effective change control strategies. Organizations need to be agile and adaptable: able and willing to evolve – continually responding and adapting to reflect the changing operating environment. The ORMS should be seen as a management framework, rather than a set of activities. As missions, budgets, priorities, and staff continue to change, the structure of the framework will remain predictable when particular applications change.

4.9 Managing Uncertainty

The management of risks explicitly takes account of uncertainty, the nature of that uncertainty, and how it should be addressed. It promotes the concept that decision-making is based on best available information. Management is not always based on predictable threats and quantifiable risks. Estimates and assumptions need to be understood in analyzing the positive and negative outcomes of sources of risk, both known and unknown, within a changing environment.

4.10 Cultural Change and Communication

In order to support a security and resilience culture in the organization and its supply chain, it is essential for top management to establish a well-defined strategy, including communications, training, and awareness programs to ensure all levels of management and persons working on its behalf, understand the goals of the management system. The ORMS supports cultural and perceptual change in the organization where risk makers and risk takers are the risk owners at all levels. Communicating a shared vision, purpose and core values supporting strategic, operational, tactical, and reputational objectives provides direction for decision-making at all levels. Stakeholders are empowered to participate in inclusive consultative processes to identify, assess and proactively manage risk to pursue opportunities and improvements as well as mitigate potential weaknesses and vulnerabilities. Cultivating leadership skills at all levels enhances resilience, builds trust and contributes to protecting the image and reputation of the organization. The ORMS must be fully understood and supported at the top level in the enterprise and communicated to all persons who work on behalf of the organization as part of the core culture of the organization.

4.11 Continual Improvement

Recognizing the dynamic risk, market and operating environment coupled with resource availability considerations an ORMS is an on-going process of continual improvement. All organizations need to be cognizant of their resource constraints in order to prioritize the allocation of resources when managing risks. The ORMS provides a framework for understanding the context, assessing risks, and prioritizing the allocation of resources to facilitate the achievement of objectives. The ORMS provides the basis for monitoring, measurement, review, and subsequent modification of ORMS processes, procedures, capabilities, and information within a continual improvement cycle. Formal, documented reviews are conducted regularly. The findings of such reviews are considered by top management, and action taken where necessary to identify opportunities for improvement.

5. ESTABLISHING THE FRAMEWORK

5.1 General

The organization shall establish, document, implement, maintain, and continually improve a ORMS in accordance with the requirements of this *Standard*, and determine how it will fulfil these requirements. In developing the ORMS the organization shall consider its strategic, operational, tactical, and reputational objectives. The organization shall establish intended outcomes and performance metrics for an outcomes-driven ORMS. The organization shall continually improve its effectiveness in accordance with the requirements set out in this *Standard*.

Where the organization chooses to subcontract or outsource any process or an activity that affects the conformity with the requirements of this Standard, the organization shall ensure and accept control and accountability over the operations of subcontractors or outsource partners in the performance of such processes. Control of such subcontracted or outsourced process or activity shall be identified and managed within the ORMS. Subcontractors of outsourced processes or services are also responsible and accountable for all client, legal, regulatory, contractual, ethical, and industry obligations.

5.2 Context of the Organization

The design and implementation of a management system framework is based on an understanding of the organization and its internal and external context of operation. Therefore, the organization shall define and document its internal and external context, including its supply chain and subcontractors. These factors shall be taken into account when establishing, implementing, and maintaining the organization's ORMS, and assigning priorities.

The organization shall evaluate internal and external factors that can influence the way in which the organization will manage risk.

5.2.1 Internal Context

The organization shall identify, evaluate, and document its internal context, including:

a) Mission, strategies, policies, objectives, plans, and guidelines to achieve objectives;
b) Governance, roles and responsibilities, and accountabilities;
c) Values, ethos, and culture;
d) Overall risk management strategy;
e) Information flow and decision-making processes;
f) Capabilities, resources, and assets;
g) Procedures and practices;
h) Activities, functions, services, and products; and
i) Brand and reputation.

The organization shall identify relevant internal stakeholders that may impact or be impacted by its activities, functions, goods and services, and thereby contribute to the risk profile.

5.2.2 External Context

The organization shall define and document its external context, including:

a) The cultural, social and political context;
b) Legal, regulatory, contractual, technological, economic, natural, and competitive environment;
c) Contractual agreements, including other organizations within the contract scope;

d) Infrastructure dependencies and operational interdependencies;
e) Perceptions of time and time sensitivities;
f) Supply chain, outsourcing, and contractor relationships and commitments;
g) Key issues and trends that may impact on the processes and/or objectives of the organization;
h) Perceptions, values, needs, and interests of external stakeholders (including local communities in areas of operation); and
i) Operational forces and lines of authority.

The organization shall identify relevant external stakeholders that may impact or be impacted by its activities, functions, goods and services, and thereby contribute to the risk profile. In establishing its external context, the organization shall ensure that the objectives and concerns of external stakeholders are considered when developing ORMS criteria.

5.2.3 Enterprise Value of Tangible and Intangible Assets and Services

In order to understand the organization's value chain, it is necessary to identify people, assets and services that provide tangible and intangible value. The value of an asset and service shall be considered within the context of how the assets contribute to the organization's achievement of its objectives. While organizations may have a myriad of assets, products and services, typically not all are critical. Therefore, in addition to considering the monetary value of assets, valuation shall consider how the asset fits within the value chain of the organization and its relative value in achieving objectives.

5.2.4 Supply Chain and Subcontractor Node Analysis

Managing risks in the supply chain, including subcontractors, requires an understanding of the organization's culture and environment as well as the context of the global environment of its supply chain. Each upstream and downstream node of the organization's supply chain involves a set of risks and management processes.

The organization shall identify and document its upstream and downstream supply chain, particularly its use of subcontractors, to identify significant risks that present opportunities or have the potential to cause an undesirable or disruptive event. Managing supply chain risk shall be included in an organization's overall ORMS program where risks have been identified which have a potential to cause an undesirable or disruptive event, or provide an opportunity. The organization shall define and document the level in their supply chain and subcontractors to include in their ORMS program.

5.3 Needs and Requirements

Top management shall ensure that stakeholder needs and requirements are identified, evaluated, continually monitored, and met to achieve its objectives and minimize risks.

When identifying stakeholder needs and requirements, the organization shall determine:

a) Requirements and obligations specified by stakeholders (e.g. client, customers, etc.);
b) Legal, regulatory, and contractual obligations, as well as other voluntary commitments;

c) Human rights responsibilities and impacts relevant to its activities;
d) Needs of the local and impacted communities and other stakeholders,
e) Impact on and interactions with other organizations and stakeholders;
f) Records and documentation requirements for delivery of services and non-conformances; and
g) Risk management requirements, including stakeholder risk appetite.

5.4 Defining Risk Criteria

The organization shall define and document criteria to evaluate the significance of risk. The risk criteria shall reflect the organization's values, objectives and resources. When defining the risk criteria, the organization shall consider:

a) Critical activities, functions, services, products, and stakeholder relationships;
b) The operating environment and inherent uncertainty in locations of operations;
c) The potential impact related to an undesirable or disruptive event;
d) Legal, regulatory, and contractual requirements, as well as other voluntary commitments to which the organization subscribes;
e) The organization's overall risk management policy;
f) The nature and types of threats and consequences that can occur to its assets, business, and operations;
g) Time factors and time dependencies;
h) Dependencies and interdependencies;
i) How the likelihood, consequences, and level of risk will be determined;
j) Needs of and impacts on stakeholders – particularly life, safety, and human rights;
k) Reputational and perceived risk;
l) Risk appetite and perspective (pursue, retain, take or not accept risk) of the organization and its clients; and
m) How combinations and the sequence of multiple risks will be taken into account.

5.5 Scope of the Management System

The organization shall define and document the scope of its ORMS, including the boundaries of the organization to be included in the ORMS – i.e., the whole organization, or one or more of its constituent parts, locations, value chain, or functions. The organization shall define the scope of the ORMS in terms of and appropriate to its size, nature, and complexity from a perspective of continual improvement.

In defining the scope, the organization shall consider:

a) The organization's objectives, activities, internal and external obligations (including those related to stakeholders), and legal responsibilities;
b) The internal and external context of its activities, functions and operations; and
c) The uncertainty in achieving its strategic, operational, tactical, and reputational objectives including factors that could adversely affect the operations and activities of the organization within the context of their potential likelihood and consequences.

The organization shall define the scope consistent with the need to manage risk and preserve the integrity of the organization. Where an organization chooses to subcontract or outsource any process that affects conformity with the requirements of this *Standard*, the organization shall ensure that such processes are controlled. The controls and responsibilities of such outsourced processes shall be identified within the scope of the ORMS. The organization retains responsibility to oversee compliance with jurisdictional, legal, and regulatory requirements as well as adherence to its voluntary commitments (e.g., human rights, labor practices) of its subcontract and outsourced partners.

A "Statement of Applicability" shall define the relevant risks that apply to the organization's scope, legal, regulatory, and contractual obligations, and operating environment based on its risk assessment. The organization shall implement adaptive, proactive and/or reactive measures to manage risk that apply to the organization's scope, legal, regulatory, and contractual obligations and operating environment. Specific exclusions and their justifications shall be documented.

6. LEADERSHIP

6.1 General

Top management shall provide evidence of active leadership for the ORMS by overseeing its establishment and implementation, and motivating individuals to integrate security and resilience as a central part of the mission of the organization and its culture.

6.2 Management Commitment

Top management shall provide evidence of its mandate and commitment to the development and implementation of the ORMS to achieve intended outcomes and continually improving its effectiveness by:

a) Identifying strategic, operational, tactical, and reputational objectives;
b) Establishing the ORMS policy;
c) Articulating a shared sense of joint purpose and values underlying decision-making processes;
d) Instilling a sense of ownership in the ORMS to persons working on behalf of the organization and recognizing their contributions;
e) Establishing risk criteria including risk appetite;
f) Reviewing risk assessment and performance assessment outcomes;
g) Communicating to the organization the importance of meeting ORMS objectives and conforming to the ORMS policy;
h) Communicating to persons working on behalf of the organization the importance of adhering to legal obligations and voluntary commitments;
i) Providing sufficient resources to establish, implement, operate, monitor, review, maintain, and improve the ORMS. Internal and external resources include but are not

limited to people with specialized skills, equipment, infrastructure, technology, information, and financial resources;

j) Encouraging and supporting management at all levels and other persons working on behalf of the organization to integrate a security, risk, and resilience culture and awareness into their areas of responsibilities;
k) Aligning organizational incentives in a manner consistent with ORMS objectives;
l) Conducting at planned intervals, management reviews of the ORMS; and
m) Promoting the need for continual improvement.

6.3 Policy

Top management shall establish a ORMS policy. The policy shall:

a) Provide a clarity of purpose and shared vision for the ORMS;
b) Provide a framework for setting and reviewing ORMS objectives, targets, and programs;
c) Be consistent with the organization's other policies;
d) Empower persons working on behalf of the organization to recognize their role in the ORMS and achievement of objectives;
e) Provide a commitment to comply with applicable legal, regulatory, and contractual requirements as well as voluntary commitments;
f) Include a commitment to human rights and public safety as a top priority;
g) Provide a commitment to avoid, prevent, and reduce the likelihood and consequences of undesirable or disruptive events;
h) Be documented, implemented, and maintained;
i) Be communicated to all appropriate people working for or on behalf of the organization;
j) Be available to stakeholders;
k) Be visibly endorsed by top management;
l) Include a commitment to continual improvement; and
m) Be reviewed at planned intervals and when significant changes occur.

6.4 Organizational Roles, Responsibilities, and Authorities for the ORMS

Top management shall ensure that the responsibilities and authorities for relevant ORMS roles are designated and communicated within the organization.

The organization shall appoint one or more individuals within the organization who – irrespective of other responsibilities – shall have defined competencies, roles, responsibilities, and authority for:

a) Ensuring that a ORMS is established, communicated, implemented, and maintained in accordance with the requirements of this *Standard*;
b) Identifying and monitoring the needs and expectations of the organization's internal and external stakeholders, and take appropriate action to manage these needs and expectations;
c) Ensuring that adequate resources are made available;

d) Promoting awareness of ORMS requirements throughout the organization; and
e) Reporting on the performance of the ORMS to top managers for review and as a basis for continuous improvement.

Top management shall ensure those responsible for the ORMS have the authority and competence to be accountable for the implementation and maintenance of the management system.

7. PLANNING

7.1 Legal and Other Requirements

The organization shall establish, implement, and maintain procedures to:

a) Identify legal, regulatory, contractual and other requirements in the jurisdictions in which it operates that are relevant to its personnel, facilities, activities, functions, products, services, supply chain, subcontractors, the environment, and stakeholders;
b) Identify relevant contractual and voluntary obligations; and
c) Determine how these requirements apply to its operations.

The organization shall document this information and keep it up to date. It shall communicate relevant information on legal and other requirements to persons working on its behalf and other relevant third parties, including subcontractors.

Any legal, regulatory, contractual, and other requirements applicable to the organization's activities shall be identified and incorporated into the management of the organization's activities. Statutory requirements will vary between countries and jurisdictions. Organizations have an overriding duty-of-care obligation to minimize risk to human and public safety, and abide by jurisdictional laws, contractual, and voluntary obligations.

The organization shall consider applicable legal, regulatory, contractual, and other requirements as well as voluntary obligations in developing, implementing and maintaining its ORMS.

7.2 Risk Assessment

7.2.1 General

The organization shall establish, implement and maintain a formal and documented risk assessment process for its activities, functions and operations, including its relevant supply chain and subcontractor activities.

7.2.2 Internal and External Risk Communication and Consultation

The organization shall establish, implement, and maintain a formal and documented communication and consultation process with internal and external stakeholders in the risk assessment process to ensure that:

a) Objectives and interests of internal and external stakeholders are understood;
b) Risks are adequately identified and communicated;

c) Risk appetite of internal and external stakeholders are understood;
d) Dependencies and linkages with subcontractors and within the supply chain are understood;
e) Security and resilience processes interface with other management disciplines; and
f) Risk assessment is being conducted within the appropriate internal and external context and parameters relevant to the organization and its contractors and supply chain.

7.2.3 Risk Assessment Process

The organization shall establish, implement and maintain a formal and documented risk assessment process, including its relevant supply chain partners and subcontractor activities. The risk assessment process shall include:

a) Asset identification, valuation and characterization - identify people, assets and services that provide tangible and intangible value. Valuation and characterization includes criticality in achieving objectives and mission of the organization. Consideration is given to financial, operational, temporal, and reputational characteristics of tangible and intangible assets, activities, functions and services;
b) Risk identification – identify sources of strategic, operational, tactical, and reputational risk to assess threats and opportunities; vulnerabilities and capabilities; and consequences and criticalities due to intentional, unintentional and natural events that have a potential for direct or indirect consequences on the organization's activities, assets, operations, functions and impacted stakeholders, as well as its ability to abide by principles articulated in its ORMS policy;
c) Risk analysis – systematically analyze risk (likelihood and consequence analysis, including supply chain risk analysis) to determine those risks that have a significant impact on activities, functions, services, products, supply chain, subcontractors, stakeholder relationships, local populations and the environment; and
d) Risk evaluation – systematically evaluate and prioritize risk controls and treatments, and their related costs to determine how to bring risk within an acceptable level consistent with risk criteria.

Note 1: Additional information on conducting a risk assessment can be found in the ANSI/ASIS/RIMS RA.1-2015, *Risk Assessment* Standard.

Note 2: Many methodologies exist for conducting risk assessments. The method selected should align with the organization's management, complexity of the risks needing to be assessed, and be applicable to the organizational culture. For example, the criticality analysis includes estimating allowable downtimes, potential impacts over time, and recovery time objectives; therefore, the organization may integrate a business impact analysis (BIA) into its risk assessment process. Where major variations in recovery priorities and/or complex interdependencies are present, the organization should consider conducting the BIA as a separate analysis.

The organization shall:

a) Integrate and implement the risk assessment outcomes in the ORMS processes;
b) Ensure that top management reviews the inputs and outputs of the risk assessment;
c) Document and keep this information up-to-date and secure;
d) Monitor, assess, evaluate and respond to changes in the risk environment;

e) Periodically review whether the ORMS scope, policy, risk criteria and risk assessment are still appropriate given the organization's internal and external context;
f) Re-evaluate risks within the context of changes within the organization or made to the organization's operating environment, procedures, functions, services, partnerships, and supply chains;
g) Evaluate the direct and indirect benefits and costs of options to manage risk, exploit opportunities, and enhance reliability and resilience;
h) Evaluate the actual effectiveness of risk treatment options post-incident and after exercises;
i) Ensure that the prioritized risks and impacts are taken into account in establishing, implementing, and operating its ORMS; and
j) Monitor and evaluate the effectiveness of risk controls and treatments.

The risk assessment shall identify activities, operations, and processes that need to be managed, outputs shall include:

a) A prioritized risk register identifying treatments to manage risk;
b) Justification for risk acceptance;
c) Identification of critical control points (CCP); and
d) Requirements for supplier, distributor, outsourcing and subcontractor controls.

7.3 Objectives and Plans to Achieve Them

The organization shall establish, implement, and maintain documented objectives and targets to manage risks in order to pursue opportunities, as well as to anticipate, avoid, prevent, deter, mitigate, respond to, and recover from undesirable or disruptive events. Documented objectives and targets shall establish internal and external expectations for the organization, its contractors, and supply chain that are critical to mission accomplishment, product and service delivery, and functional operations.

Objectives shall be derived from and consistent with the ORMS policy and risk assessment, including the commitments to:

a) Minimize risk by reducing likelihood and consequence;
b) Respecting jurisdictional laws, contractual requirements, and human rights;
c) Financial, operational, and business requirements (including contractor and supply chain commitments); and
d) Continual improvement.

When establishing and reviewing its objectives and targets, an organization shall consider:

a) Consistency with the ORMS policy;
b) Significant risks;
c) Creation of value;
d) Brand, reputational and human rights impacts;
e) Integrity of information;

f) Financial, operational, and business requirements;
g) Legal, regulatory, contractual and other requirements;
h) Technological options; and
i) Views of stakeholders and other interested parties.

Targets shall be measurable qualitatively and/or quantitatively. Targets shall be derived from and consistent with the ORMS objectives and shall be:

a) To an appropriate level of detail;
b) Commensurate to the risk assessment;
c) Specific, measurable, achievable, relevant, and time-based (where practicable);
d) Identify what will be done by whom, including how this will be accomplished using what resources and in what timeframe;
e) Communicated to all appropriate persons working on behalf of the organization and third parties including subcontractors and supply chain partners with the intent that these persons are made aware of their individual obligations; and
f) Monitored and reviewed periodically, and when any significant changes occur, to ensure that they remain relevant and consistent with the ORMS objectives and amended accordingly.

7.4 Actions to Achieve Risk and Business Management Objectives

The organization shall establish, implement, and maintain security and resilience programs for achieving its objectives and risk management goals. The programs shall be optimized and prioritized in order to control and treat risks associated with its operations, subcontractors, and supply chain. The organization shall establish, implement, and maintain a formal and documented risk treatment process, which considers the various risk treatment options:

a) Pursuing an opportunity;
b) Removing the risk source, where possible;
c) Removing or reducing the likelihood of an event and its consequences;
d) Removing, reducing or mitigating consequences of an event with a negative outcome;
e) Spreading the risk across assets and functions;
f) Sharing the risk with other parties, including risk insurance;
g) Accepting risk through informed decision; and
h) Avoiding activities that give rise to the risk.

Top management shall:

a) Review and approve selected risk treatment options to determine if they meet risk appetite objectives;
b) Assess the benefits and costs of options to remove, reduce, or retain risk;
c) Evaluate its security and resilience programs to determine if these measures have introduced new risks; and
d) Periodically review the risk treatment to reflect changes to the external environment, including legal, regulatory, contractual, and other requirements, and changes to the

organization's policy, facilities, information management system(s), activities, functions, products, services, and supply chain.

8. Structural Requirements

8.1 General

The organization shall be a legal entity, or a defined part of a legal entity, with transparent ownership such that it can be held legally accountable for all its activities.

8.2 Organizational Structure

A clearly defined management structure shall identify roles, responsibilities, authorities, and accountabilities for its operations and services. The organization shall:

a) Document its organizational structure, showing sub-divisions, duties, responsibilities, and authorities of management;
b) Identify information and value chain flows and interactions; and
c) Define and document if the organization is a defined part of a legal entity and the relationship to other parts of the same legal entity.

8.3 Financial and Administrative Procedures

The organization shall develop financial and administrative procedures and controls to support the provision of effective risk management and security and resilience programs. Financial procedures should consider normal operation conditions as well as procedures in anticipation and in response to an undesirable or disruptive event. Procedures shall be established:

a) Clearly defining authorization requirements;
b) To expedite fiscal decisions;
c) In accordance with authority levels and accounting principles; and
d) In consultation and coordination with appropriate stakeholders

8.4 Insurance

The organization shall demonstrate that it has sufficient insurance to cover risks and associated liabilities arising from its operations and activities consistent with its risk assessment. When outsourcing or subcontracting services, activities, functions, or operations, the organization shall ensure sufficient insurance coverage for the subcontracted activities.

8.5 Outsourcing and Subcontracting

The organization shall have a clearly defined process wherein it describes the conditions under which it outsources activities, functions, or operations. The organization shall take responsibility for all activities outsourced to another entity. The organization shall have a legally enforceable agreement covering outsourcing arrangements including:

a) Commitment by subcontractors to abide by the same obligations as held by the organization and as described in this *Standard*;
b) Confidentiality and conflict of interest agreements;
c) Clear definition of provision of goods and services; and
d) Conformance to the applicable provisions of this *Standard*.

8.6 Documented Information

8.6.1 General

The ORMS documentation shall be consistent with the complexity, size and type of organization and include:

a) The ORMS policy, objectives, and targets;
b) A description of the scope of the ORMS including Statement of Applicability;
c) A description of the main elements of the ORMS and their interaction, and reference to related documents;
d) Documented information required for the effective implementation, operation, and performance of the ORMS; and
e) Documents, including records, required by this *Standard*.

8.6.2 Records

The organization shall establish and maintain records to demonstrate conformity to the requirements of its ORMS.

Records include, among others:

a) Records required by this *Standard*;
b) Personnel screening;
c) Training records;
d) Process monitoring records;
e) Inspection, maintenance, and calibration records;
f) Pertinent subcontractor and supplier records;
g) Incident reports;
h) Records of incident investigations and their disposition;
i) Performance indicators, including exercise, testing and audit results;
j) Management review results;
k) External communications decision;
l) Records of applicable legal requirements;
m) Records of significant risk and impacts;
n) Records of management systems meetings;
o) Risk management, security, and resilience performance information;
p) Legal, regulatory, and contractual compliance;
q) Human rights performance information; and
r) Communications with stakeholders.

The organization shall establish, implement, and maintain procedures to protect the sensitivity, confidentiality, and integrity of records including access to, identification, storage, protection, retrieval, retention, and disposal of records. Records shall be retained for a minimum of seven years or as otherwise required or limited by law or contract.

8.6.3 Control of Documented Information

Documents required by the ORMS and by this *Standard* shall be controlled. The organization shall establish, implement, and maintain procedures to:

a) Approve documents for adequacy prior to issue;
b) Protect sensitivity and confidentiality of information;
c) Review, update as necessary, and re-approve documents;
d) Record amendments to documents;
e) Make updated and approved documents readily available;
f) Ensure that documents remain legible and readily identifiable;
g) Ensure that documents of external origin are identified and their distribution controlled;
h) Prevent the unintended use of obsolete documents; and
i) Ensure the appropriate, lawful, and transparent destruction of obsolete documents.

Organizations shall ensure the integrity of documents by rendering them securely backed-up, accessible only to authorized personnel, and protected from unauthorized disclosure, modification, deletion, damage, deterioration, or loss.

9. Operation and Implementation

9.1 Operational Control

9.1.1 General

The organization shall identify the activities that are associated with the identified significant risks and consistent with its ORMS policy, risk assessment, objectives, and targets, in order to ensure that they are carried out under specified conditions, which will enable it to:

a) Comply with legal, regulatory, and contractual requirements, and voluntary commitments;
b) Accomplish the mission while protecting the organization's reputation;
c) Ensure the security, well-being, and rights of both persons working on its behalf as well as those impacted by its activities;
d) Implement risk management controls to pursue opportunities and minimize the likelihood and consequences of an undesirable or disruptive event; and
e) Achieve its risk management, security and resilience objectives and targets.

The organization shall establish, implement, and maintain documented procedures to control situations where their absence could lead to deviation from the ORMS policy, objectives, and targets.

9.1.2 Establishing Norms of Behavior and Codes of Ethical Conduct

The organization shall establish, implement, and maintain a Code of Ethics for norms of behavior for all persons working on its behalf, including employees, subcontractors, and outsource partners. The Code of Ethics shall be documented and clearly communicate the importance of compliance with legal, regulatory, contractual obligations, and voluntary commitments. The Code of Ethics shall ensure that all persons working on its behalf understand their responsibilities within the context of managing and reporting risks and non-conformances.

The organization shall communicate and document its Code of Ethics to all persons working on its behalf, as well as appropriate stakeholders.

9.2 Resources, Roles, Responsibility, and Authority

9.2.1 General

Top management shall make available resources essential to establish, implement, maintain, and improve the ORMS. Resources shall include information, management tools, human resources (including people with specialist skills and knowledge), and financial support.

Roles, responsibilities, and authorities shall be defined, documented, and communicated in order to facilitate effective ORMS, including control, coordination, and command responsibility with a defined line of succession.

To effectively pursue opportunities and deal with undesirable and disruptive events, the organization shall establish planning, security, incident management, response and/or recovery team(s) with defined roles, appropriate authority, adequate resources, and rehearsed operational plans and procedures.

9.2.2 Personnel

The organization shall retain sufficient personnel with the appropriate competence to fulfill its contractual obligations. Personnel shall be provided with adequate pay and remuneration arrangements, including insurance, commensurate to their responsibilities. The organization shall protect the confidentiality of this information as appropriate and provide personnel with relevant documents in language that is readily comprehensible for all parties.

The organization shall maintain documented information on all personnel:

a) As required by legal, regulatory, and contractual obligations;
b) To maintain contact with individuals and their immediate families;
c) To assist in personnel recovery in event of an incident; and
d) Needed for family notification of injury or death.

9.2.3 Response Structure

The organization shall establish, document, and implement procedures and a management structure to anticipate, prevent, prepare for, mitigate, and respond to an undesirable or disruptive event using personnel with the necessary authority, experience, and competence.

The response structure shall:

a) Identify incident indicators and impact thresholds that justify initiation of a formal response;
b) Assess the nature and extent of a potential undesirable or disruptive event and its impacts;
c) Initiate an appropriate response to avoid, protect, mitigate, or manage a potential undesirable or disruptive event;
d) Have plans, processes, and procedures for the activation, operation, coordination, and communication of the response;
e) Have resources available to support the plans, processes and procedures to manage a disruptive event or work to minimize impact before realized;
f) Communicate with stakeholders and authorities, as well as the media; and
g) Post-incident analysis to identify opportunities for improvement.

9.2.4 Selection, Background Screening, and Vetting of Personnel

The organization shall establish, document, implement, and maintain procedures for background screening and vetting of all persons working on its behalf to ensure they are fit and proper for the tasks they will conduct. Wherever possible and consistent with jurisdictional laws, regulations, and contractual requirements, screening processes shall include:

a) Consistency with legal, regulatory, and contractual requirements;
b) Identity, minimum age and personal history verification;
c) Education and employment history review;
d) Personal references;
e) Military and security services records check;
f) Review of possible criminal records;
g) Evaluation for substance abuse;
h) Physical and mental evaluation for fitness with assigned activities; and
i) Evaluation for suitability to perform their duties.

Background screening involves the disclosure of highly sensitive information; therefore, the organization shall develop procedures to appropriately and strictly secure the confidentiality of information both internally and externally. Records shall be maintained consistent with relevant statutes of limitations.

Selection of qualified personnel shall be based on defined competencies including knowledge, skills, abilities, and attributes. Both the screening and selection measures shall be consistent with legal, regulatory, and contractual requirements.

9.2.5 Selection, Background Screening, and Vetting of Subcontractors

When the organization subcontracts activities, functions, and operations on a temporary or continuing basis, this work shall be placed with a competent subcontractor. The organization is responsible for the subcontractor’s work and is liable, as appropriate and within applicable law, for the conduct of these subcontractors. The organization shall:

a) Ensure appropriate written contractual agreements with the subcontractor;
b) Advise and obtain consent in writing from stakeholders, when appropriate;

c) Maintain a register of all subcontractors it uses;
d) Communicate the responsibilities of this *Standard* to the subcontractor; and
e) Maintain a record of evidence of conformance with this *Standard* for work subcontracted.

9.2.6 Internal and External Complaint and Grievance Procedures

The organization shall establish procedures to document and address grievances received from internal and external stakeholders (including, supply chain partners, clients and other affected parties). The procedures shall be communicated to internal and external stakeholders to facilitate reporting by individuals of potential and actual nonconformances with this *Standard*, or violations of laws, voluntary obligations or human rights. The organization shall investigate allegations expeditiously and impartially, with due consideration to confidentiality and restrictions imposed by jurisdictional laws. The organization shall establish and document procedures for:

a) Receiving and addressing complaints and grievances;
b) Establishing hierarchical steps for the resolution process;
c) The investigation of the grievances, including procedures to;
    i. Cooperate with official external investigation mechanisms;
    ii. Prevent the intimidation of witnesses or inhibiting the gathering of evidence; and
    iii. Protect individuals submitting a complaint or grievance in good faith from retaliation.
d) Identification of the root causes;
e) Corrective and preventative actions taken, including disciplinary action commeasurable with any infractions;
f) Document the outcomes of the investigation; and
g) Communications with appropriate authorities.

Grievances alleging criminal acts, violations of human rights, or imminent danger to individuals shall be dealt with immediately by the organization, and other authorities as appropriate.

9.2.7 Procurement and Management of Materials

The organization shall establish documented procedures and records for procurement and management of materials required for its processes to manage risks, based on jurisdictional legal, regulatory, and contractual requirements, as well as mission objectives and risks identified. Management of materials may include:

a) Compliance with registrations, certifications, and permits;
b) Acquisition;
c) Secure storage;
d) Controls over their identification, issue, use, maintenance, return, and loss;
e) Records regarding to whom and when materials are issued;
f) Identification and accounting of materials; and
g) Proper disposal with verification.

9.3 Competence, Training, and Awareness

9.3.1 General

The organization shall ensure that all persons performing tasks on its behalf, including employees, subcontractors, and outsource partners, who have the potential to prevent, cause, respond to, mitigate, or be affected by identified risks are competent (on the basis of appropriate education, training, and experience), and shall retain associated records.

The organization shall identify competencies and training needs associated with ORMS, particularly the performance of each individual's functions, consistent with respect for legal, regulatory, and contractual requirements, and voluntary commitments. It shall provide training or take other action to meet these needs, and shall retain associated records.

9.3.2 Competence Identification

The organization shall identify competencies, level of competency and training needs associated with its activities, operations and the management of risks. The organization shall establish, implement, and maintain procedures to ensure all persons performing tasks on its behalf are aware of:

a) The ORMS policy;
b) The parameters of performance of their functions;
c) The benefits of conformance to the ORMS and improved performance;
d) Their roles and responsibilities in achieving conformity with the requirements of the ORMS;
e) Assessing risks;
f) Managing risks identified in the risk assessment and associated with their work;
g) Applicable jurisdictional laws, regulations and voluntary commitments including but not limited to:

    i. Compliance issues related to their activities and functions;
    ii. Prohibition of degrading treatment of others;
    iii. Prohibition and awareness of discriminatory and exploitative practices;
    iv. Recognition and prevention of verbal and physical abuse; and
    v. Measures against bribery, corruption, fraud and similar crimes.

h) The procedures to reduce the likelihood and/or consequences of an undesirable or disruptive event, including procedures to respond to and report events;
i) Communications protocols and procedures;
j) Incident reporting and documentation procedures;
k) First-aid, health, environmental, safety and security procedures;
l) The culture, such as customs and religion, of the environment in which they are operating;
m) Receiving and reporting complaints; and
n) The potential consequences of departure from specified procedures.

9.3.3 Training and Competence Evaluation

The organization shall provide for training and establish a means to measure degrees of proficiency or levels of competency. Persons working on behalf of the organization shall be trained to demonstrate the level of competence and proficiency required.

The organization shall:

a) Establish competence-based metrics for its training programs;
b) Promote a ORMS culture by instilling an understanding that risk management, security and resilience cultures are part of the organization's core values and governance;
c) Identify other competencies that require periodic refresher training to maintain the required level of performance or to incorporate new requirements; and
d) Provide training on the importance of conformity with the ORMS policy and procedures and with the requirements of the ORMS, as well as potential consequences of departure from specified procedures for the ORMS, operations and the management of risk.

9.4 Communication

9.4.1 General

The organization shall establish, implement, and maintain procedures for:

a) Communicating with persons working on its behalf;
b) Communicating with external stakeholders including its clients, subcontractors, supply chain partners, government authorities, local and emergency services authorities, members of the community in which it operates, and the media;
c) Receiving, documenting, and responding to communications from internal and external stakeholders;
d) Defining and assuring availability of the means of communication during atypical situations and disruptions; and
e) Regular testing of communications system for normal and abnormal conditions.

Communication procedures shall consider the sensitive nature of operational information and legal restrictions on information sharing.

9.4.2 Operational Communications

The organization shall develop standardized communication procedures to share information protecting its integrity and level of confidentiality, including information related to:

a) Its operations, functions and activities;
b) Its chain of command, organizational hierarchy, and custody of information;
c) Relevant risk and threat information;
d) Logistics and supply chain management;
e) Incident reporting, internally and externally; and
f) Requests for assistance.

The organization shall ensure that spoken and written communications can be received and understood by all levels and operators and that all levels can respond in a language or means that can be understood by appropriate, internal and external stakeholders.

9.4.3 Risk Communications

The organization shall decide, based on safeguarding life as a top priority and in consultation with stakeholders, whether to communicate externally about significant risks and impacts to stakeholders and document its decision. If the decision is to communicate, the organization shall establish and implement methods for this external communication, alerts, and warnings (including with the media).

9.4.4 Communicating Complaint and Grievance Procedures

Complaint and grievance procedures shall be communicated to internal and external stakeholders. Procedures shall minimize obstacles to access caused by language, educational level, or fear of reprisal, as well as consider needs for confidentiality and privacy.

9.4.5 Whistleblower Policy

The organization shall communicate to people working on its behalf, who have reasonable belief that a nonconformance of this *Standard* has occurred, their right to anonymously report the nonconformance internally, as well as externally to appropriate authorities. The organization shall not take any adverse action against any individual for the act of making a report in good faith.

9.5 Prevention and Management of Undesirable or Disruptive Events

9.5.1 General

The organization shall establish, implement, and maintain procedures (plans) to prevent and manage potential undesirable and disruptive events based on its risk assessment and its recovery time objectives. The procedures shall document how the organization will anticipate, prevent, prepare for, and respond to undesirable and disruptive events. In preparing incident prevention and management procedures, the organization considers each of the following actions:

a) Safeguard life and assure the safety of internal and external stakeholders;
b) Protect assets;
c) Prevent further escalation of the incident;
d) Minimize disruption to operations;
e) Restore critical operational continuity;
f) Recover normal operations (including evaluating improvements);
g) Notification of appropriate authorities;
h) Protect image and reputation (including media coverage and stakeholder relationships); and
i) Corrective and preventative actions (including root cause analysis to remediate the situation and prevent a recurrence).

The following costs are assessed when developing incident prevention and management plans:

a) Human cost: Physical and psychological harm to clients, persons working on its behalf, suppliers, local communities and other stakeholders.
b) Financial cost: Equipment and property replacement, downtime, overtime pay, stock devaluation, lost sales/business, lawsuits, regulatory fines/penalties, etc.
c) Image cost: Reputation, standing in the community, negative press, loss of clients, etc.
d) Human rights impacts: Actual and potential adverse human rights impacts on specific people and groups, in particular vulnerable or marginalized groups, within the specific context of operations.
e) Indirect impacts: On the regional economy and reduction in the regional net economy, etc.
f) Environmental impacts: Degradation to the quality of the environment or to endangered species.

9.5.2 Risk Treatment Functions

The organization shall establish, implement and maintain procedures to support pursuit of opportunities and the protection of people, tangible and intangible assets, and other risk-related functions, including but not limited to:

a) Managing risks identified in the risk assessment;
b) Specific functions required to conduct activities and functions; and
c) Supply chain tasks and context specific functions.

9.5.2.1 Design of Controls and Countermeasures

The organization should establish, implement, and maintain procedures for controls and countermeasures to pursue opportunities and manage its risks that have the potential to harm the organization, its assets, supply chain and stakeholders, in order to:

a) Comply with legal, regulatory and contractual requirements, and voluntary commitments;
b) Meet its obligations to its internal and external stakeholders;
c) Deliver its ORMS programs (risk treatment and countermeasure action plans); and
d) Achieve its ORMS objectives and targets.

The control procedures shall document how the organization will:

a) Exploit potential opportunities;
b) Provide adequate protection of assets (tangible and intangible) based on the risk assessment;
c) Avoid, remove or reduce the likelihood of an incident;
d) Reduce and manage the consequences of an incident;
e) Maintain continuity of operations and services based on predetermined levels of performance and recovery time objectives;
f) Ensure the integrity of the controls if an incident takes place; and
g) Recover from an incident.

The organization shall adopt a "protection-in-depth" or layered protection strategy to develop a cost-effective and robust approach to deter, detect, delay, and respond, from risks and threats to the organization and its assets. Based on its risk assessment, the organization should consider layered controls that:

a) Promote risk awareness and situational awareness;
b) Eliminate the risk by complete removal of the risk exposure;
c) Reduce the risk by modifying activities, processes, equipment, or materials;
d) Isolate or separate the assets from risk;
e) Deploy engineering controls to deter, detect, delay, and respond from a potential hazard or threat agent;
f) Apply administrative controls such as work practices or procedures that reduce risk; and
g) Provide protection of the asset if the risk cannot be eliminated or reduced.

The value of the asset, the output from the risk assessment, the organization's risk appetite, and the relative cost-benefit of the control measures will determine the number and types of layers needed to adequately protect the asset. Evaluation of interdependencies is critical to a successful protection-in-depth strategy given the reliance and interactions of many countermeasures on human, physical, electronic, telecommunications and information systems.

9.5.2.2 Incident Management Procedures and Plans

The organization shall establish, implement, and maintain procedures (plans) to identify undesirable and disruptive events that can impact the organization, its activities, services, stakeholders, human rights, and the environment. The procedures shall document how the organization will proactively prevent, mitigate, and respond to events.

Where existing arrangements are revised and new arrangements introduced that could impact operations and activities, the organization should consider the associated risks before their implementation, and the potential to create new or modify existing risks.

The operational control procedures shall define:

a) Purpose and scope;
b) Objectives and measures of success;
c) Implementation procedures (including phases and sequences);
d) Roles, responsibilities, and authorities;
e) Technology requirements (including maintenance and calibration);
f) Communication requirements and procedures;
g) Internal and external interdependencies and interactions;
h) Resource requirements; and
i) Information flow and documentation processes.

The incident management procedures shall ensure:

a) Supply and demand requirements (demand signals) are comprehended in capacity planning;
b) Contingencies and appropriate redundancies provide protection-in-depth and address single point failures;
c) Processes are in place to validate supply chain responses (e.g., validate site/process/product time to recover);

d) There is a feedback loop to know if past risk control and countermeasures are changing as part of design, engineering or process changes, or a decision to outsource certain activities;
e) That planned changes are controlled, and that unintended changes are reviewed and appropriate action is taken; and
f) Procedures are periodically reviewed and, where necessary the ORMS is revised and documented.

9.5.3 Occupational Health and Safety

The organization shall establish, implement, and maintain procedures to promote a safe and healthy working environment including reasonable precautions to protect people working on its behalf in high-risk, hazardous or life threatening operations consistent with jurisdictional laws and regulations, as well as contractual obligations. Procedures shall include:

a) Assessing occupational health and safety risks to people working on its behalf as well as the risks to external parties;
b) High risk environment training (if appropriate);
c) Provision of personal protective equipment;
d) Medical and psychological health awareness training, care, and support; and
e) Guidelines to identify and address workplace violence, misconduct, alcohol and drug abuse, sexual harassment, and other improper behavior.

9.5.4 Incident Monitoring, Reporting, and Investigations

The organization shall establish, implement, and maintain procedures for incident monitoring reporting, investigations, disciplinary arrangements, and remediation. Incidents involving any casualties, physical injuries, allegations of abuse, loss of sensitive information or equipment, substance abuse, or nonconformance with the principles of ORMS, as well as applicable laws and regulations, shall be reported and investigated with the following steps taken, including:

a) Documentation of the incident;
b) Notification of appropriate authorities;
c) Steps taken to investigate the incident;
d) Identification of the root causes;
e) Corrective and preventative actions taken; and
f) Any compensation and redress given to the affected parties.

The organization shall assure all persons working on its behalf are aware of their responsibilities and the mechanisms to monitor and report non-conformances and incidents.

Records of non-conformances and incidents shall be maintained and retained for a minimum of seven years or as specified by legal, regulatory, and contractual requirements.

10. PERFORMANCE EVALUATION

10.1 General

The organization shall assess the performance and effectiveness of the ORMS by evaluating plans, procedures, and capabilities through periodic assessments, testing, post-incident reports, lessons learned, performance evaluations, and exercises. Significant changes in these factors should be reflected immediately in the procedures.

Performance evaluation considers:

a) Elements of the ORMS to monitor and evaluate;
b) Evaluation metrics and methodologies to accurately reflect performance and identify opportunities for improvement;
c) Frequency of monitoring, assessments and evaluations; and
d) Changes in the risk environment.

The organization shall keep records of the results of the periodic evaluations.

10.2 Monitoring and Measurement

The organization shall establish, implement, and maintain performance metrics and procedures to monitor and measure, those characteristics of its operations that have material impact on its performance (including partnerships, subcontracts, and supply chain relationships). Procedures are responsive to changes in the risk environment. The procedures shall include the documenting of information to monitor performance, applicable operational controls, and conformity with the organization's ORMS objectives and targets.

The organization shall evaluate and document the performance of the systems which protect its human, tangible and intangible assets, as well as its communications and information systems.

10.3 Evaluation of Compliance

Consistent with its commitment to compliance, the organization shall establish, implement, and maintain procedures for periodically evaluating compliance with applicable legal, regulatory, and contractual obligations and voluntary commitments. The organization shall evaluate any gaps in compliance and/or assess any changes in the compliance environment to develop a continual improvement strategy.

10.4 Exercises and Testing

The organization shall use exercises and other means to test the appropriateness and efficacy of its ORMS and risk treatment plans, processes, and procedures, including stakeholder relationships and subcontractor interdependencies. Exercises should be designed and conducted in a manner that limits disruption to operations and exposes people, assets and information to minimum risk.

Exercises shall be conducted regularly (at least annually), or following significant changes to the organization's mission and/or structure, or following significant changes to the risk environment. A formal report shall be written after each exercise. The report shall assess the appropriateness and efficacy of the organization’s ORMS plans, processes, and procedures including nonconformities, and should propose corrective and preventative action.

Actions shall be taken without undue delay to eliminate detected nonconformities and their causes. Follow-up activities shall include the verification of the actions taken and the reporting of verification results.

Post-exercise reports should form part of top management reviews.

10.5 Internal Audit

The organization shall establish, implement, and maintain a ORMS audit program and ensure that internal audits of the ORMS are conducted at planned intervals.

Internal audits shall assess whether the ORMS:

a) Meets the requirements of this *Standard*;
b) Meets relevant legal, regulatory, and contractual obligations as well as voluntary commitments;
c) Risk treatments and operational planning and controls have adequately and effectively addressed issues identified in the risk assessment;
d) Has been properly implemented, maintained and performing as expected;
e) Reflects the dynamic nature of the risk context and environment; and
f) Has been effective in achieving the organization’s ORMS policy and objectives.

The organization shall:

a) Plan, establish, implement, and maintain an audit program(s), taking into consideration the status and importance of the processes and areas to be audited, as well as the results of previous audits;
b) Define the audit criteria, scope, frequency, methods, responsibilities, planning requirements, and reporting;
c) Select auditors and conduct audits to ensure objectivity and the impartiality of the audit process (e.g., auditors should not audit their own work);
d) Ensure that the results of the audits are reported to the management responsible for the area being audited; and
e) Retain relevant documented information as evidence of the results.

The management responsible for the area being audited shall ensure that actions are taken without undue delay to eliminate detected nonconformities and their causes. Follow-up activities shall include the verification of the actions taken and the reporting of verification results.

NOTE: Additional information on conducting management system audits can be found in ANSI/ASIS SPC.2-2014, Auditing Management Systems: Risk, Resilience, Security, and Continuity—Guidance for Application.

10.6 Management Review

10.6.1 General

Management shall review the organization's ORMS at documented specified intervals (at least annually) to confirm its continuing suitability, adequacy, and effectiveness. This review shall include assessing opportunities for improvement and the need for changes to the ORMS, including the ORMS policy and objectives. The results of the reviews shall be clearly documented and records shall be maintained.

10.6.2 Review Input

The input to a management review shall include:

a) Results of ORMS audits and reviews;
b) Feedback from interested parties;
c) Techniques, products, or procedures that could be used in the organization to improve the ORMS performance and effectiveness;
d) Status of preventive and corrective actions;
e) Results of exercises and testing;
f) Risks not adequately addressed in the previous risk assessment;
g) Incident reports;
h) Results from effectiveness measurements;
i) Follow-up actions from previous management reviews;
j) Any changes that could affect the ORMS;
k) Adequacy of policy and objectives; and
l) Recommendations for improvement.

10.6.3 Review Output

The outputs from top management reviews shall include decisions and actions related to possible changes to policy, objectives, targets, and other elements of the ORMS, with the aim of promoting continuous improvement, including:

a) Improvement of the effectiveness of the ORMS;
b) Update of the risk assessment and risk management plans;
c) Modification of procedures and controls that effect risks, as necessary, to respond to internal or external events that may affect the ORMS;
d) Changes needed to promote risk management culture and maturity;
e) Resource needs; and
f) Improvement of how the effectiveness of controls is being measured.

11. Continual Improvement

11.1 General

The organization shall continually improve the effectiveness of the ORMS through the use of the ORMS policy, objectives, audit results, analysis of monitored events, corrective and preventive actions, and management review.

11.2 Nonconformities, Corrective and Preventive Action

The organization shall establish, implement, and maintain procedures for dealing with nonconformities and for taking corrective and preventive action. The procedures shall define requirements for:

a) Identifying and correcting nonconformities and taking actions to mitigate their consequences;
b) Evaluating the need for actions to prevent nonconformities and implementing appropriate actions designed to avoid their occurrence;
c) Investigating nonconformities, determining their root causes, and taking actions in order to avoid their recurrence;
d) Recording the results of corrective and preventive actions taken;
e) Assess how corrective and preventive actions modify risk; and
f) Reviewing the effectiveness of corrective and preventive actions taken.

The organization shall ensure that proposed changes are made to the ORMS documentation.

11.3 Change Management

The organization shall establish a defined and documented change management program to ensure that any internal or external changes that impact the organization are reviewed in relation to the ORMS. It shall identify any new critical activities that need to be included in the ORMS change management program.

11.4 Opportunities for Improvement

The organization shall monitor, evaluate, and exploit opportunities for improvement in ORMS performance and eliminate the causes of potential problems, including:

a) Ongoing monitoring of the operational and risk landscape to identify potential problems and opportunities for improvement;
b) Determining and implementing action needed to improve risk management and security and resilience performance; and
c) Reviewing the effectiveness of the action taken to improve performance.

Actions taken shall be appropriate to the impact of the potential problems, and the organization's obligations and resource realities.

Top management, in collaboration with key risk stakeholders, shall ensure that actions are taken without undue delay to exploit opportunities for improvement. Where existing arrangements are revised and new arrangements introduced that could impact on the management of risk, operations and activities, the organization shall consider the associated risks before their implementation.

The results of the reviews and actions taken shall be clearly documented and records shall be maintained. Follow-up activities shall include the verification of the actions taken and the reporting of verification results.

Annex A

(informative)

A GUIDANCE ON THE USE OF THE *STANDARD*

NOTE: The additional text given in this annex is strictly informative and is provided to assist in understanding and implementing the requirements contained in this *Standard*. While this information addresses and is consistent with the requirements of this *Standard*, it is not intended to add to, subtract from, or in any way modify those requirements.

A.1 Introduction

Organizations need to manage their uncertainties in achieving their strategic, operational, tactical, and reputational objectives to identify and pursue opportunities and minimize the likelihood and consequences of natural, intentional and unintentional events. Natural disasters, environmental accidents, technology mishaps, and man-made crises have historically demonstrated that undesirable and disruptive events can happen, impacting the public and private sectors alike. The challenge goes beyond merely reacting to adversity but rather identifying and modifying risk factors before they manifest themselves. Organizations need to engage in a comprehensive and systematic process of anticipation, avoidance, prevention, preparedness, readiness, mitigation, response, continuity, and recovery. Managing risks requires the creation of an on-going, dynamic, and interactive process supporting proactive risk management, assuring the continuation of an organization's core activities and functions before, during and after an undesirable or disruptive event.

This *Standard* provides organizations of all sizes and types with the elements needed to achieve and demonstrate proactive risk management and enhanced organizational resilience performance related to their physical facilities, services, activities, products, supply chains, and operations. They do so within the context of:

a) Increasing risks and threats in a dynamic global risk environment;
b) Increased dependencies and interdependencies, including supply chain volatility;
c) Increased threats that do not recognize physical or jurisdictional boundaries (e.g. cyber threats);
d) More stringent legislation and regulation;
e) More competitive business realities;
f) Increasing interdependencies in society due to a global economy (on an organizational, functional, or jurisdictional level);
g) Heightened awareness of the need for adequate security, safety, environmental, emergency response and remediation planning;
h) Concerns of interested and affected parties; and
i) The need to assure continuity and resilience of operations and supply chains.

An undesirable event not properly managed can rapidly escalate into a disruptive incident (emergency, crisis, or even a disaster). Preparing for a risk event before it occurs can identify opportunities and/or minimize its impact. An unmanaged event can taint an organization's image, reputation, or brand in addition to resulting in significant physical or environmental damage, injury, or loss of life. This *Standard* provides a framework to aid organizations in successfully managing risks by developing a strategy and action plan to safeguard its interests and those of its stakeholders.

Proactive planning and preparation for potential risk events can leverage an opportunity, avoid an undesirable event, mitigate event impacts and minimize length of a disruption. The holistic, integrated, discipline-neutral approach to risk management of adopting adaptive, proactive and reactive risk treatment measures can help avoid a disruption and minimize the suspension of critical services and operations, thereby allowing return to normal services and operations as rapidly as possible.

This *Standard* provides guidance or recommendations for any organization in the private, not-for-profit, and public sectors to identify and develop best practices to assist and foster action in:

a) Reducing risks throughout the organization and its supply chain;
b) Providing top management driven vision and leadership for strategies to protect human, tangible and intangible assets and assure the resilience of the organization;
c) Identifying, evaluating and managing risks critical to its short- and long-term success;
d) Minimizing the likelihood and consequences of a wide variety of hazards and threats;
e) Mitigating the impact of a wide variety of hazards and threats, including natural disasters, technological and environmental accidents, and man-made disasters (terrorism and crime);
f) Understanding the roles and responsibilities needed to protect assets and further the mission and achievement of objectives;
g) Managing incident response measures and resources;
h) Developing strategic alliances and mutual aid agreements;
i) Developing, testing and maintaining incident prevention and response plans, and associated operational procedures;
j) Developing and conducting training and exercises to support and evaluate incident/emergency preparedness, response plans, and operational procedures;
k) Developing and conducting training and exercises to support and evaluate prevention, protection, preparedness, mitigation, response, recovery and operational procedures;
l) Ensuring that relevant employees, supply chain partners, customers, suppliers, and other stakeholders are aware of the risk management arrangements and have confidence in their application;
m) Developing internal and external communications procedures, including response to requests for information from the media or the public;
n) Establishing metrics for measuring and demonstrating success;
o) Documenting the key resources, infrastructure, tasks, and responsibilities required to support critical operational functions; and

p) Establishing processes that ensure the information remains current and relevant to the changing risk and operational environments.

It is simply good business for an organization to protect its physical, virtual, and human assets. The success of the management system depends on the commitment of all levels and functions in the organization, especially the organization's top management. Decision makers must be prepared to budget for and secure the necessary resources to make this happen. It is necessary that an appropriate administrative structure be put in place to effectively deal with prevention, mitigation, and management. This will ensure that all concerned understand who makes decisions, how the decisions are implemented, and what are the roles and responsibilities of all persons working on behalf of the organization. The *Standard* drives a risk management culture within the organization at all levels. Personnel used for incident management should be assigned to perform these roles as part of their job description and not be expected to perform them on a voluntary basis. Regardless of the organization – for profit, not for profit, faith-based, non-governmental – its leadership has a duty to stakeholders to plan for its survival.

Adaptive and preemptive planning and preparation for potential undesirable and disruptive events will help reduce the likelihood and consequences of an event. The holistic management process can help avoid or minimize the interruption or suspension of mission critical services and operations.

A.2 General Requirements

The implementation of an ORMS specified by this *Standard* is intended to result in enhanced agility and resilience including improved security, preparedness, response, continuity, and recovery performance. Therefore, this *Standard* is based on the premise that the organization will periodically review and evaluate its ORMS to identify opportunities for improvement and their implementation. The rate, extent and timescale of this continual improvement process are determined by the organization in the light of its risk profile, economic objectives, and other circumstances. Improvements in its ORMS are intended to support the integration of risk and business management thereby supported improving resilience. This *Standard* requires an organization to:

a) Establish an appropriate ORMS policy;

b) Identify the sources or risk (hazards and threats) related to the organization's past, existing, or planned activities, functions, products, and services to determine the level of risk and necessary control measures;

c) Identify applicable legal, regulatory and contractual requirements and voluntary commitments to which the organization subscribes;

d) Identify priorities and set appropriate ORMS objectives and targets;

e) Establish a structure and programs to implement the policy and achieve objectives and meet targets;

f) Facilitate planning, control, monitoring, preventive and corrective action, and auditing and review activities to ensure both that the policy is complied with and that the ORMS remains appropriate; and

g) Be capable of adapting to changing circumstances.

Consideration should be given to normal and abnormal operations and functions within the organization, its relationships with relevant stakeholders, and to potential undesirable and disruptive conditions. Tools and methods for undertaking a review might include checklists, conducting interviews, direct inspection and measurement, or results of previous audits or other reviews, depending on the nature of the activities.

An organization has the freedom and flexibility to define its boundaries, and may choose to implement this *Standard* with respect to the entire organization or to specific operating units of the organization. The organization should define and document the scope of its ORMS.

Scoping is intended to clarify the boundaries of the organization to which the ORMS will apply, especially if the organization is a part of a larger organization at a given location. Once the scope is defined, all activities, products, and services of the organization within that scope need to be included in the ORMS system. In setting the scope, the credibility of the ORMS will depend upon the choice of organizational boundaries. Where a part of an organization is excluded from the scope of its ORMS, the organization should be able to explain and document the exclusion.

If this *Standard* is implemented for a specific operating unit, policies and procedures developed by other parts of the organization can be used to meet the requirements of this *Standard*, provided that they are applicable to the specific operating unit that will be subject to it.

Risk management involves issues and actions before, during, and after a disruptive incident. Therefore, this *Standard* encompasses avoidance, prevention, deterrence, readiness, mitigation, response, continuity, and recovery. The risk environment, as well as business/operational realities, focuses different strategic weights on each of these components; however, no component should be weighted zero. The Statement of Applicability should explain the strategic weighting of security management, preparedness, emergency management, disaster management, crisis management, and business continuity management in developing the management system, based on the risk assessment and context.

An organization with no existing ORMS should establish its current position with regard to risk management and its capabilities to manage potential risk scenarios by means of a gap analysis. A gap analysis will enable the organization to compare its actual performance with the potential performance needed to meet its objectives. The analysis should consider the organization's risks (including potential impacts) as a basis for establishing the ORMS.

The gap analysis should cover five key areas:

a) Identification of risks, including those associated with operating conditions, emergency situations, accidents, and potential undesirable and disruptive events;
b) The capacity to identify and pursue opportunities;
c) Identification of applicable legal, regulatory, contractual and other requirements to which the organization subscribes;
d) Evaluation of existing risk management practices and procedures, including those associated with subcontracting activities; and

e) Evaluation of previous emergency situations, and accidents, as well as previous measures taken to prevent and respond to undesirable and disruptive events.

In all cases, consideration should be given to operations and functions within the organization, its relationships with its relevant stakeholders (e.g., clients, supply chain partners, subcontractors, and the local community), and to potentially undesirable, disruptive and emergency conditions. Tools and methods for undertaking a gap analysis may include checklists, conducting interviews, direct inspection and measurement, benchmarking against best practices, or results of previous audits or other reviews, depending on the nature of the activities.

A.3 Management System

A management system is a dynamic and multifaceted process, with each element interacting as a structured set of functional units. It provides a framework that is based on the premise that the component parts of a system can best be understood when viewed in the context of relationships with each other and with other systems, rather than in isolation. The only way to fully understand and implement the elements of a management system is to understand the parts in relation to the whole. Therefore, it should be noted that a management system is not a simple cycle, but rather a complex set of interrelated elements interacting with each other. This results in an iterative process where establishing the context and policy, risk assessment, implementation, operation, evaluation, and review are not a series of consecutive steps, but rather a network of interacting functions.

The management systems approach is characterized by:

a) Understanding the context and environment within which the system operates;
b) Identifying the core elements of the system, as well as the system boundary;
c) Understanding the role or function of each element in the system; and
d) Understanding the dynamic interaction between elements of the system.

The systems approach ensures that holistic strategies and policies are developed. It provides a sound analytical basis for developing strategies and policies that are to be implemented in the complex and changing environment in which the organization operates. Establishing a framework for assessing the risks and effectiveness of strategies and policies prior to and during implementation provides a feedback loop for decision-making throughout the process.

The implementation of the ORMS specified by this *Standard* is intended to result in:

a) Improved provision of goods, products and services;
b) Security and safety of internal and external stakeholders; and
c) A culture of risk management within the organization and its supply chain.

A.4 General Principles

Organizations should integrate all the principles described in Clause 4 of this *Standard* into the design of its management system for the ORMS to be successful. The goal is to achieve the organization’s objectives and protect assets (human, tangible, and intangible) while enhancing the resilience of the organization and its supply chain. ORMS will depend on the effectiveness of integrating these principles into the management framework, which drives a risk management culture throughout all levels of the organization. Use of these principles should establish an environment where information is adequately reported and used as a basis for decision-making and accountability at all relevant organizational levels.

The ORMS framework provides key principles, a common language, and clear direction and guidance for decision making. Managing risks is not just the responsibility of management. For a ORMS program to be effective, it needs to be implemented by every person working on behalf of the organization. It is a top-down, bottom-up approach. Managing risk must become an integral part of the organization's culture. Therefore, all risk-makers and risk-takers should be the risk-managers.

All organizations face a certain amount of uncertainty and risk. In order to assure sustainability of operations and maintain competitiveness and performance, organizations must have a system to manage their risks. The challenge is to assess, evaluate, and treat risk in order to cost effectively manage the risk and uncertainty while meeting the organization's, and stakeholder's, strategic and operational objectives. Given the finite resources of organizations, it is imperative that they build a robust management system to address any array of risks they may face.

A.5 Establishing the Framework

A.5.1 Understanding the Organization and its Context

The organization establishes the context of its ORMS by identifying and understanding the internal and external influences and environment in which it operates. By establishing the context, an organization can define the scope of its ORMS and design a fit-for-purpose framework for ORMS. This should help assure that the organization meets the objectives, needs, and concerns of internal and external stakeholders (e.g., clients, supply chain partners, subcontractors, local communities). The context will determine the criteria for managing the risk to the organization, clients, and impacted communities thereby providing a basis for setting risk criteria and parameters for the risk assessment and treatment processes.

External context includes:

a) Social, socio-economic, environmental, geographic, political, cultural, competitive, business, financial, supply chain, interdependencies, and community factors;
b) Key drivers and trends having impact on objectives;
c) Client and supply chain needs and requirements; and
d) Needs, interests, and perceptions of external stakeholders.

Internal context includes:

a) Policies, processes, and business mission;
b) Capabilities, resources and knowledge (people, processes, systems, technology, time, and capital);
c) Overall risk management strategy;
d) Information – systems, flows, and decision making processes;
e) Nature of internal supply chains;

f) Internal stakeholders;
g) Objectives and strategies of the organization;
h) Perception, values, and culture;
i) Policies and processes; and
j) Governance, roles, and accountabilities.

During the process of establishing the internal and external context, the organization should identify the significant tangible and intangible assets of the organization. This includes identifying the relative importance of various types of assets to the viability and success of the organization.

A.5.2 Enterprise Value of Tangible and Intangible Assets and Services

In order to understand the organization, it is necessary to identify the people, assets, and services that provide the enterprise tangible and intangible value. People involved in or affected by the organization include employees, customers, visitors, vendors, patients, guests, passengers, tenants, contract employees, and any other persons who are lawfully present on the property being assessed. Unauthorized persons (such as trespassers) need to be considered in the risk assessment. Property includes real estate, land and buildings, facilities; transport mechanisms; tangible property such as cash, precious metals, and stones; monitoring, control, data, and communication systems; support infrastructure, instruments; materials (e.g., raw materials, process materials, finished goods, and hazardous materials); high theft items (e.g., drugs, securities, cash, etc.); as well as almost anything that can provide value, be stolen, damaged, or otherwise affected.

Intangible assets include the brand, goodwill, or reputation of an enterprise that could be impacted. Another high value intangible asset is information. Information includes intellectual property, export controlled technology, and proprietary data (e.g. trade secrets, marketing plans, social media interaction, business expansion plans, plant closings, confidential personal information about employees, customer lists, and other data) that if stolen, altered, or destroyed could cause harm to the organization).

Services provided to the internal and external stakeholders are important parts of the organization's value chain and may be affected. For example, non-availability of IT or accounting services may have an impact on the organization; its operations and assets.

The enterprise value of assets and services should be considered within the context of:

a) Value relative to critical mission activities, services, and products;
b) Exclusive possession;
c) Utility;
d) Cost of creation or re-creation;
e) Criticality and competitive edge;
f) Critical human resources and knowledge;
g) Operational and business impact (including dependencies and interdependencies);
h) Cost of lost opportunity;
i) Shelf life of the asset;

j) Reputation and brand impact; and
k) Other considerations important to management or clients.

The value of an asset and service should be considered within the context of how the assets contribute to the organization's achievement of its objectives. While organizations may have a myriad of assets, products and services, typically not all are mission critical. Therefore, in addition to considering the monetary value of assets, valuation should consider how the asset fits within the value chain of the organization and its relative value in achieving strategic, tactical, operational, and reputational objectives.

A.5.3 Supply Chain and Subcontractor Node Analysis

Supply chains and the use of subcontractors are typically integral parts of any organizations operations. While there is significant interdependence within a supply chain, each individual node of a supply chain is unique in certain respects. This uniqueness may require unique approaches to the management of the risks involved. Therefore, to manage the risks within a supply chain, the organization needs to identify:

a) The role of organizations and individuals at each tier or level of its upstream and downstream supply chain or network;
b) Understand the interdependencies and supporting infrastructure critical to mission success;
c) How each node plays a role in adding value to the performance of other members of the chain, directly or indirectly;
d) Determine how each node has the potential to contribute to the risk profile of the organization, both positively and negatively; and
e) Evaluate how each node exerts some influence on the success of minimizing risk implementation of the management system.

When conducting node analysis, the organization should recognize the decisions taken at the individual node which has potential chain-wide implications. Therefore, the risk factors throughout the supply chain need to be understood and controlled for successful implementation of the ORMS.

A.5.4 Scope of ORMS System

An organization has the freedom to define the boundaries for implementing its ORMS. It may choose to implement the ORMS across the entire organization, specific operating units, discrete geographic locations, or clearly defined supply chain flows. These scoping boundaries reflect top management objectives for the ORMS, and the size, nature, and complexity of the organization and its activities. Once top management defines the ORMS scope, all assets, activities, products, and services within that scope become elements of concern within the ORMS.

The organization should justify all exclusions from the scope of the ORMS using the risk assessment in the justification. Exclusions may include the inability of an organization to control certain services or operations; however, exclusions do not negate the organization's responsibilities to value the sanctity of human life or its obligations to respect human rights, laws, and its voluntary commitments. The scope should ensure the integrity of the organization and its supply chain. The credibility of the ORMS depends on the choice of organizational boundaries defined in the scope.

Outsourced and subcontracted activities remain the organization's responsibility and should be within the ORMS. If an outsourced or subcontracted product, service, activity, or part of the organization's supply chain remains under the organization's risk accountability and management control, then top management should place it within the scope of the ORMS. The organization should make appropriate agreements and take appropriate measures to assure effective ORMS agreements are in place with its subcontractors and outsource partners.

The level of detail and complexity of the ORMS, the extent of documentation required, and resources committed to the ORMS should guide the ORMS scope statement. When the organization implements the *Standard* for a specific operating unit, then the organization may use applicable policies, plans, and procedures developed by other parts of the organization to satisfy the requirements of this *Standard*.

A *Statement of Applicability* defines the strategic weighting of risk-related disciplines such as security management, preparedness, information security management, emergency management, disaster management, crisis management, and business continuity management in developing the management system, based on the risk assessment.

A.6 Leadership

A.6.1 Management Commitment

The top management of the organization (such as the managing director or chief executive) should demonstrate commitment and resolve to implement the ORMS in the organization. Without top management commitment, no management system can succeed. Top management should demonstrate to its internal and external stakeholders a visible commitment to managing risks and promoting a culture facilitating good business management and enhanced resilience. To initiate and sustain the ORMS effort, top management should communicate to all persons working on behalf of the organization the importance of:

a) Making organizational and individual competence inherent in everything the organization does;
b) Emphasizing that respect for laws, regulations and contractual obligations and voluntary commitments is an integral component of ORMS;
c) Integrating ORMS throughout the organization; and
d) Looking at problems as opportunities for improvement.

The top management should provide evidence of its commitment to the development and implementation of the ORMS and continually improve its effectiveness by:

a) Communicating to the organization the importance of meeting the requirements of this *Standard*;
b) Setting and communicating the policy and risk criteria;

c) Validating risk appetite and the outcomes of the risk assessment process are within set levels of risk tolerance;
d) Ensuring that ORMS objectives are established at all levels and functions;
e) Appointing one or more individuals within the organization to be responsible for the management system;
f) Ensuring that the responsibilities and authorities for relevant management system roles are assigned and communicated within the organization;
g) Allocating appropriate resources for the management system;
h) Demonstrating commitment to the management system and risk minimization;
i) Promoting awareness of risk and ORMS requirements throughout the organization;
j) Leading by example; and
k) Participating in reviews and driving the continual improvement process.

It is essential that top management of the organization sponsors, provides the necessary resources, and takes responsibility for creating, maintaining, testing, and implementing a comprehensive ORMS. This will insure that management and staff at all levels within the organization understand that the ORMS is a critical top management priority and are empowered to support risk and business decision-making processes. It is equally essential that top management engage a "top down" approach to the ORMS so that management at all levels of the organization understand accountability for system maintenance as part of the overall governance priorities.

A.6.2 ORMS Policy

The ORMS policy is the driver for implementing and improving an organization's ORMS. This policy should therefore reflect the commitment of top management to:

a) The sanctity of human life and safety as a top priority;
b) The pursuit of opportunities;
c) Avoid, prevent, and reduce the likelihood and consequences of undesirable and disruptive events;
d) Comply with applicable legal, regulatory, contractual and voluntary commitments and other requirements;
e) Respect human rights (including commitments to social responsibility and minimizing the organization's adverse impacts on stakeholders, the environment and the community); and
f) Continual improvement.

The ORMS policy is the framework that forms the basis upon which the organization sets its objectives and targets. The ORMS policy should be sufficiently clear to be capable of being understood by internal and external stakeholders and should be periodically reviewed and revised to reflect changing conditions and information. Its area of application (i.e., scope) should be clearly identifiable and should reflect the unique nature, scale, and impacts of the risks of its activities, functions, products, and services.

The ORMS policy should be communicated to all persons who work for or on behalf of the organization, including its clients, customers, supply chain partners, subcontractors, and relevant members of the local community. Communication to subcontractors and other external parties can be in alternative forms to the policy statement itself, such as rules, directives, and procedures. The organization's ORMS policy should be defined and documented by its top management within the context of the ORMS policy of any broader corporate body of which it is a part and with the endorsement of that body.

A ORMS planning team – including senior leaders from all major organizational functions and support groups – should be appointed to ensure wide-spread acceptance of the ORMS.

A.6.3 Resources, Roles, Responsibilities, and Authorities

The resources needed for the ORMS should be identified. These include human resources and specialized skills, equipment, internal infrastructure, technology, information, intelligence, and financial resources. Top management should ensure the availability of resources essential for the establishment, implementation, control, testing, and maintenance of the ORMS.

The management system is implemented by people within the organization. One or more qualified persons should be appointed and empowered to implement, test or exercise, and maintain the ORMS. Top management should conduct its own periodic reviews and audits of the overall ORMS. A ORMS planning team, including senior leaders from all major organizational functions and support groups, may be appointed to ensure wide-spread acceptance of the ORMS.

A.7 Planning

A.7.1 Legal and Other Requirements

The organization should identify and understand legal, regulatory, and contractual requirements that affect the achievement of its objectives. Jurisdictional requirements may include international, national, state, local, legal, and regulatory requirements. Identifying and understanding these requirements should help to ensure legal compliance, prevent litigation, minimize liability, and improve the organization's image.

Examples of other requirements to which the organization may subscribe include, if applicable:

a) Business and other contractual obligations;
b) Agreements with public authorities, community groups, or non-governmental organizations;
c) Agreements with clients;
d) Non-regulatory guidelines;
e) Voluntary principles or codes of practice;
f) Product or service stewardship commitments (e.g., warranties);
g) Requirements of trade associations;
h) Public commitments of the organization or its parent organization;
i) Non-binding protocols;
j) Healthcare requirements;

k) Financial obligations;
l) Social responsibility and environmental commitments; and
m) Identity information and privacy requirements.

Specific legal obligations vary by jurisdiction; geographic location; the type and nature of operations; and the location, type, and nature of the organization's customers. Therefore, it is important that the organization be aware of its obligations within the context of its operating environment.

The organization should identify all relevant statutory, regulatory, contractual, and other requirements and communicate this information to appropriate stakeholders. The organization should evaluate which requirements apply and where they apply, and identify who should receive this information. The organization should explicitly define, document, and keep current its approach to accessing and addressing these requirements. Similarly, the organization should define and document specific operational controls as well as individual responsibilities to meet these requirements.

A.7.2 Internal and External Risk Communication and Consultation

The organization should establish a formal communication and consultation process with appropriate stakeholders both for the collection of risk assessment input information and for the controlled dissemination of the outcomes. Sensitivity and integrity of the information should be considered in the risk communication and consultation processes.

A.7.3 Risk Assessment and Monitoring

Organizations typically operate in inherently dynamic risk environments. They must manage risk to internal and external stakeholders while also managing risk to the organization. The organization needs to achieve its strategic, operational, tactical, and reputational objectives within the context of protecting and creating value. Respecting laws and rights of individuals creates tangible and intangible value for the organization, and therefore is intrinsically a business objective requiring due diligence. The risk assessment provides a clear understanding of the risk environment in order for the organization to make informed decisions in prioritizing its risks and their treatment.

The risk assessment process provides an understanding of the risks that could affect the organization's achievement of its strategic, operational, tactical, and reputational objectives. The risk assessment should consider both positive and negative outcomes. It is intended to create a systematic process for an organization to identify, analyze, and evaluate risks to determine those that are significant to the organization and its stakeholders. The risk assessment provides a basis for evaluating the adequacy and effectiveness of current controls in place, as well as decisions on the most appropriate approaches to be used in managing and treating risks. It identifies those risks that should be addressed as a priority by the organization's ORMS. The risk assessment provides the foundation for setting objectives, targets and programs within the management system, as well as measuring the efficacy of the ORMS.

The organization should apply the ANSI/ASIS/RIMS RA.1-2015: *Risk Assessment*.

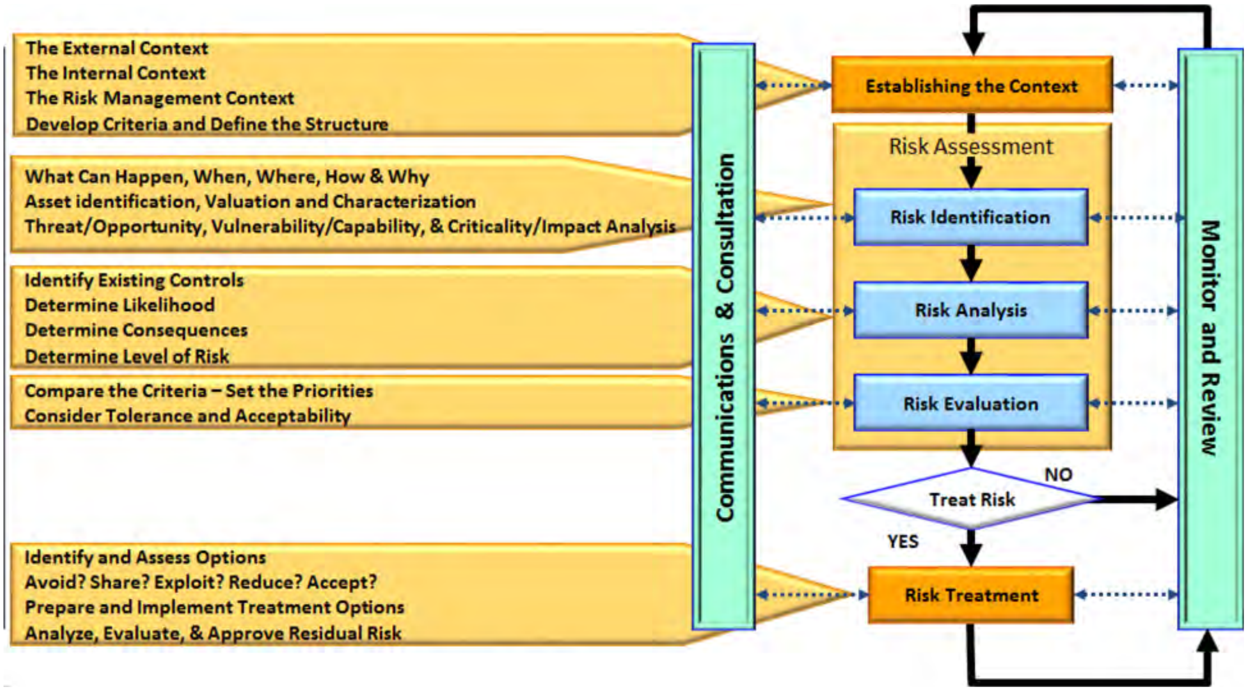
The External Context
The Internal Context
The Risk Management Context
Develop Criteria and Define the Structure
What Can Happen, When, Where, How & Why
Asset identification, Valuation and Characterization
Threat/Opportunity, Vulnerability/Capability, & Criticality/Impact Analysis
Identify Existing Controls
Determine Likelihood
Determine Consequences
Determine Level of Risk
Compare the Criteria – Set the Priorities
Consider Tolerance and Acceptability
Identify and Assess Options
Avoid? Share? Exploit? Reduce? Accept?
Prepare and Implement Treatment Options
Analyze, Evaluate, & Approve Residual Risk
Communications & Consultation
Establishing the Context
Risk Assessment
Risk Identification
Risk Analysis
Risk Evaluation
Treat Risk
NO
YES
Risk Treatment
Monitor and Review

Figure 2: Process for Managing Risk (based in ISO 31000)

The risk assessment process is conducted within the internal and external context of the organization. Risk assessment is the overall process of risk identification, risk analysis, and risk evaluation:

a) *Risk Identification*: The process of identifying, grading and documenting risks by means of threat/opportunity analysis, criticality/impact analysis, vulnerability/capability analysis and supply chain analysis. The process considers the causes and sources of risks, as well as events, situations and circumstances that could impact the organization and its stakeholders.

   The identification should include of all sources of risk that may present an opportunity and/or deter the organization from achieving its strategic, operational, tactical, and reputational objectives, including the rights, security and safety of internal and external stakeholders.

b) *Risk Analysis*: The process of developing an understanding of risk and level of risk. It provides the basis for determining which risks should be treated and the most appropriate method for treating them. It considers the sources of risk, their consequences, and the likelihood that the incident and associated consequences can occur.

   An organization should determine what the consequences of an event upon stakeholders will be if a threat materializes. The level of risk is a function of threat/opportunity analysis, criticality/impact analysis, vulnerability/capability analysis and supply chain analysis as well as the efficacy of existing controls. The level of risk determination considers the likelihood of an event, the likelihood of consequences, and the magnitude of the consequences. It provides the basis for prioritizing the risks that need to be treated;

c) *Risk Evaluation*: The process of comparing the estimated levels of risk with the risk criteria defined when the context was established. It determines the significance of the level and type of risk. The risk evaluation uses the understanding of the risk obtained in the risk analysis to make decisions about the strategies required for risk prioritization, control and treatment.

The risk assessment provides an understanding of risks, their causes, likelihood and consequences. Therefore, an organization should conduct a comprehensive risk assessment within the scope of its ORMS, taking into account the inputs and outputs (both intended and unintended) associated with:

a) Its activities, products, and services;

b) Interactions with the environment and community;

c) Relations with internal and external stakeholders (e.g., clients, subcontractors, local government); and

d) Infrastructure and interdependencies.

The risk assessment should include a detailed analysis and evaluation of the uncertainties associated with the successful achievement of the organization’s strategical, tactical, operational and reputational objectives – for example (but not limited to):

a) Tactical risks related to the activities, functions and operations;

b) Risks related to the reputation of the organization and stakeholders;

c) Political and social implications of the organization’s activities;

d) Threats, vulnerabilities, and consequences affecting persons working on behalf of the organization;

e) Threats, vulnerabilities, and consequences affecting local communities and other stakeholders, and the potential impact of operations;

f) Risks related to business relationships, such as the use of subcontractors, outsource partners and interactions with other organizations; and

g) The interrelationships between tactical and operational risks and the need to respect human life and rights.

Many methodologies exist for risk assessments. The organization should establish, implement, and maintain a formal methodology that is documented and repeatable. Assumptions, scope, evaluation criteria, and results should be clearly defined and reviewed by top management.

Since an organization might have many risks, it should establish and document criteria and a methodology to determine those that it will consider significant. There is no single method for determining significant risks. The method used should provide consistent results and include the establishment and application of evaluation criteria, such as those related to exploiting opportunities, protection of life and human rights, the severity of adverse impacts, its leverage to prevent or mitigate adverse impacts, criticality of activities and functions, downtimes and time frames for recovery, legal issues and the concerns of internal and external stakeholders. An organization should analyze likelihood, severity and consequences of undesirable and disruptive events to its operations and stakeholders, and identify critical operations that are given high priority for developing response and recovery times and objectives.

When assessing consequences, the organizations should consider the following.

a) Human cost: Physical and psychological harm to clients, persons working on its behalf, suppliers, local communities, and other stakeholders;
b) Financial cost: Equipment and property replacement, downtime, overtime pay, stock devaluation, lost sales/business, lawsuits, regulatory fines/penalties, etc.;
c) Image cost: Reputation, standing in the community, negative press, loss of clients, etc.;
d) Human rights impacts: Actual and potential adverse human rights impacts on specific people and groups, in particular vulnerable or marginalized groups, within the specific context of operations;
e) Indirect impacts: On the regional economy and reduction in the regional net economy, etc.; and
f) Environmental impacts: Degradation to the quality of the environment or to endangered species.

The risk assessment is an inclusive process taking into account the input of internal and external stakeholders. The risk and impact identification, analysis, and evaluation processes are framed within the operating environment of the organization; therefore, they should take into account the internal and external context and legal and other requirements.

To achieve results that accurately reflect the risk profile of the organization, data for the risk assessment should be gathered by a competent and experienced team. The sampling techniques for the collection of administrative, financial, technical, and physical data should be selected to assure representative samples. The risk assessment is not an exact science; therefore, assumptions and reliability of information should be documented. All operational units of the organization within scope of the ORMS should be directly consulted during the data-gathering process. Results of the risk assessment should be reported and reviewed by top management in order to establish the ORMS objectives, targets, and strategies. The organization should define the scope of the risk assessment based on:

a) ORMS scope (products, services, and activities);
b) Client expectations and obligations;
c) Legal, regulatory, and contractual requirements;
d) Respect for human rights;
e) Impacted communities' expectations;
f) Risk appetite;
g) Interdependencies and infrastructure requirements; and
h) Data/information requirements.

The risk assessment process should consider routine and atypical operating conditions, as well as reasonably foreseeable disruptive situations, in order to better understand and control undesirable and disruptive events. It should be kept in mind that it is not possible to foresee all undesirable and disruptive situations, so the organization should also consider the consequences of an event on critical assets, activities, and functions, as well as impacted communities, regardless of the nature of an event in order to preemptively manage its risks.

The risk assessment should:

a) Use a documented quantitative and/or qualitative methodology to estimate likelihood or probability of the identified potential risks and significance of their consequences if an event materializes;

b) Be based on reasonable and defined criteria;

c) Consider the reliability and confidence of information sources;

d) Give due consideration to all potential risks it recognizes to its operations;

e) Consider its dependencies on others and others dependencies on the organization, including client, community, and supply chain dependencies and obligations;

f) Evaluate the consequences of legal and other obligations which govern the organization's activities;

g) Consider risks associated with stakeholders, contractors, suppliers, and other affected parties;

h) Analyze information on risks, and select those risks which may cause significant consequences and/or those risks whose consequence is hard to be determined in terms of significance;

i) Analyze and evaluate the costs, benefits, and resources needed to manage risks; and

j) Evaluate risks and impacts it can control and influence.

NOTE: It is the organization that determines the degree of control and its strategies for risk acceptance, avoidance, management, minimization, tolerance transfer, and/or treatment.

In some locations, critical infrastructure, community assets, and cultural heritage may be an important element of the surroundings in which an organization operates, and therefore should be taken into account in the understanding of its risks and impact on surroundings.

When developing information relating to its significant risks, the organization should consider the need to retain the information for historical purposes, as well as how to use it in designing and implementing its ORMS.

The process of identification and evaluation of risks should take into account the location of activities, cost and time of undertaking the analysis, and the availability of reliable data. Information already developed for business planning, regulatory, or other purposes may be used in this process.

The organization should revisit its risk assessment to address changing operating conditions and processes after response to events. Changes that may elicit a revisit of the reassessment include changes in:

a) Risk landscape;

b) Leadership and partnerships;

c) Contractual and industry trends;

d) Regulatory requirements;
e) Political environment;
f) Conditions due to an event; and
g) Performance based test/exercise results.

This process of identifying and evaluating risks is not intended to change or increase an organization's legal obligations.

A.7.4 Objectives and Plans to Achieve Them

Objectives and targets are established to meet the goals and commitments of the organization's ORMS policy. By setting the security and resilience objectives and targets, the organization can translate the policy into action plans it describes in the risk treatment strategies. The objectives and targets should be specific and measurable in order to track progress and ascertain how the ORMS is performing in improving overall management of risk and organizational resilience.

ORMS "objectives" are overriding considerations such as minimizing accidents. ORMS "targets" are specific metrics for the reduction of accidents. Objectives and targets should be proportionate to the risk, cost effective, realistic, and informed by the risk assessment. The objectives and targets should reflect what the organization does, what it wants to achieve, and how effective the entity is in managing risk. Appropriate levels of management should define the objectives and targets. Objectives and targets should be periodically reviewed and revised.

When the objectives and targets are set, the organization should consider establishing measurable risk and business management performance indicators. These indicators can be used as the basis for performance evaluation system and can provide information on the ORMS and specific prevention, mitigation, response, and recovery strategies.

In establishing its objectives and targets the organization should consider:

a) Policy commitments;
b) Alignment with strategic objectives;
c) Outcomes of the risk assessment;
d) Risk appetite and tolerance;
e) Legal, regulatory, contractual, and other requirements;
f) Internal and external context;
g) Performance criteria;
h) Infrastructure requirements and interdependencies;
i) Interests of stakeholders (e.g., clients, communities, and supply chain partners);
j) Technology options;
k) Financial, operational, and other organizational considerations; and
l) Actions, resources, and timescales needed to achieve objectives.

When considering its technological options, an organization should consider the use of best available technologies where economically viable, cost-effective, and judged appropriate. Technology options should consider changes to the risk profile and if it introduces new risks.

The reference to the financial requirements of the organization is not intended to imply that organizations are obliged to use specific cost-accounting methodologies. The organization may choose to consider direct, indirect, and hidden costs.

A.7.5 Actions to Achieve Risk and Business Management Objectives

The risk management strategies and action plans are documented approaches to achieve the organization's objectives and targets. Strategies should be coordinated or integrated with other organizational plans, strategies, and budgets. Action plans may be subdivided to address specific elements of the organization's operations.

To ensure its success, the ORMS strategies and action plans should define:

a) Responsibilities for achieving goals (who will do it? where will it be done?);
b) Means and resources for achieving goals (how to do it?); and
c) Timeframe for achieving those goals (when will it be done?).

The strategies may be subdivided to address specific elements of the organization's operations. The organization may use several action plans as long as the key responsibilities, tactical steps, resource needs, and schedules are adequately defined in each of the documented plans.

The strategies should include – where appropriate and practical – consideration of all stages of an organization's activities related to planning, design, construction, commissioning, operation, retrofitting, production, marketing, outsourcing, and decommissioning. Strategy development may be undertaken for current activities and new activities, products, and/or services.

The organization should establish, implement, and maintain a formal and documented risk treatment and countermeasure selection process, which should consider:

a) Removing the risk source, where possible;
b) Removing or reducing the likelihood of an event and its consequences;
c) Removing or reducing harmful consequences;
d) Sharing or transferring the risk with other parties, including risk insurance;
e) Spreading the risk across assets and functions;
f) Retaining risk by informed decision; and
g) Avoiding the risk by temporarily halting activities that give rise to the risk.

The organization's planning should take into account pursuing opportunities, the priority of activities, contractual obligations, internal and external stakeholder needs, and operational continuity.

Strategies should be dynamic and monitored and modified when:

a) Outcomes of the risk assessment change;
b) Objectives and targets are modified or added;
c) Relevant legal requirements are introduced or changed;
d) Substantial progress in achieving the objectives and targets has been made (or has not been made); or

e) Activities, products, services, processes, or facilities change or other issues arise.

Determining the risk management strategy enables the organization to evaluate a range of options. The organization may choose an appropriate approach for each activity, such that it can operate at an acceptable level. The most appropriate strategy or strategies should depend on a range of factors such as the:

a) Results of the organization's risk assessment;
b) Costs of implementing a strategy or strategies; and
c) Consequences of inaction.

The organization should minimize the likelihood of implementing a solution that might be affected by the same event that causes a disruption.

Top management should approve documented strategies to confirm that the determination of risk treatment strategies has been properly undertaken, that they have addressed the likely causes and effects of an undesirable or disruptive event, and that the chosen strategies are appropriate to meet the organization's objectives within the organizations risk appetite.

The strategies should also consider the organization's relationships, interdependencies, and obligations with external stakeholders. These stakeholders include supply chain partners, clients, suppliers, and outsource partners – as well as public authorities and others in the community. The organization should establish and maintain strategies that first and foremost protect life and safety of stakeholders while respecting human rights and preserving the integrity of its delivery of products and services. In addition, interactions and coordination with public authorities and others in the community should be determined and included in strategy development. These strategic arrangements with external stakeholders should support the achievement of ORMS objectives and be clearly defined and documented.

A.8 Structural Requirements

A.8.1 Organizational Structure

A clearly defined management structure is necessary to establish the roles, responsibilities, and accountability of the contract. The organization entering into a contract should be a legal entity and signatures for the organization should be clearly authorized to enter into contracts on the organization's behalf.

A.8.2 Insurance

The organization should seek insurance coverage sufficient to meet any liability for damages to any person with respect to personal injury, death, or damage to property consistent with its risk assessment. The limit of such coverage should at least be at the minimum level as prescribed by the client or recognized as best industry practice. Insurance should include employer's liability and public liability coverage. Personnel should be provided with health and life insurance policies appropriate to their wage structure and the level of risk of their service as required by law or regulations.

When seeking insurance coverage, the organization should consider:

a) The policies and limits to be held by the organization should be specified in the contract;
b) The jurisdiction of the policy and in the event of a dispute;
c) The territorial limitations;
d) Limitations of indemnity;
e) Coverage of all activities, including use of weapons;
f) Medical coverage and treatment of persons working on behalf of the organization and impacted communities;
g) Activities of subcontractors; and
h) Contractual obligations.

Examples of the types of coverage to consider include (but are not limited to):

a) Liability;
b) Workers compensation;
c) Accident;
d) Property damage;
e) Kidnapping, ransom and/or captive;
f) Sensitive risk (e.g. evacuations); and
g) Key personnel.

A.8.3 Financial and Administrative Procedures

It is necessary that the organization put in place appropriate administrative and financial structures to effectively support the ORMS, before, during, and after an undesirable or disruptive event. Procedures should be established and documented to ensure transparency with regard to authorizations, consistent with generally accepted accounting procedures and industry good practices. Therefore, a management structure, authorities, and responsibility delegation for decision-making – including spending limitations, authorities, and responsibility for implementation – should be clearly defined.

A.8.4 Outsourcing and Subcontracting

A contract should provide the legal basis for the relationship between the contractor and subcontractor. The organization is responsible for all activities outsourced to another entity. The contract should specify the responsibilities, terms, and conditions under which the subcontractor is to perform, including a clearly defined:

a) Commitment to abide by the same obligations as held by the organization and described in the *Standard*;
b) Specification of the appropriate flow-down of conformance to applicable provisions of the *Standard*;
c) Confidentiality and conflict of interest requirements;
d) Process for reporting of risks, as well as the occurrence and response to undesirable and disruptive events;
e) Definition of the support relationship between the contractor and the subcontractor; and
f) Description of the service performed by subcontractor personnel.

For transparency, the organization should understand commitments to first, second and third parties, including how they relate to organizational priorities.

A.8.5 Documented Information

The level of detail of the documentation should be sufficient to describe the ORMS and how the parts work together. The documentation should also provide direction on where to obtain more detailed information on the operation of specific parts of the ORMS. This documentation may be integrated with documentation of other management systems implemented by the organization. It does not have to be in the form of a manual.

The extent of the ORMS documentation can differ from one organization to another due to the:

a) Size and type of organization and its activities, products, or services;
b) Complexity of processes and their interactions; and
c) Competence of personnel.

Examples of documents include:

a) Policy, objectives, and targets;
b) Statement of conformance;
c) Information on significant risks and impacts;
d) Procedures;
e) Process information;
f) Organizational charts;
g) Internal and external standards;
h) Incident response, mitigation, emergency, and crisis plans; and
i) Records.

Any decision to document procedures should be based on the:

a) Consequences, including those to tangible and intangible assets, of not doing so;
b) Need to demonstrate compliance with legal, regulatory, and contractual obligations as well as voluntary commitments;
c) Need to ensure that the activity is undertaken consistently; and
d) Requirements of this *Standard*.

The advantages of effective documentation include:

a) Easier implementation through communication and training;
b) Easier maintenance and revision;
c) Less risk of ambiguity and deviations; and
d) Demonstrability and visibility.

Documents originally created for purposes other than the ORMS may be used as part of this management system, and (if so used) should be referenced in the system.

A.8.5.1 Records

In addition to the records required by this *Standard*, records can include (among others):

a) Compliance records;
b) Roles, responsibilities, and authorities;
c) Accountability for serialized and sensitive equipment;
d) Reports for fuel, and training materials;
e) Authorization and tracking of controlled materials, vehicles, and hazardous materials;
f) Contract compliance audit reports;
g) Export/import compliance reports;
h) Audit trail documentation;
i) Licensing;
j) Exercise and testing results;
k) Access control records; and
l) Subcontractor documentation.

A.8.5.2 Control of Documented Information

The organization should create and maintain documents in a manner sufficient to implement the ORMS. The primary focus of the organization should be on the effective implementation of the ORMS and on ORMS performance and not on a complex document control system.

Proper account should be taken of confidential information. Procedures should be established, communicated, and maintained for the handling of classified information. This information should be clearly graded and labeled to protect the:

a) Sensitivity of the information;
b) Privacy, life, and safety of individuals; and
c) Image and reputation of the client.

The organization should ensure the integrity of records by rendering them tamperproof; securely backed-up; accessible only to authorized personnel; and protected from damage, deterioration, or loss.

The organization should consult with the appropriate legal authority within their organization to determine the appropriate period of time the documents should be retained and establish, implement, and maintain the processes to effectively do so. Records should be retained as required or limited by law, regulatory and/or contractual requirements.

A.9 Operation and Implementation

A.9.1 Operational Control

A.9.1.1 General

An organization should evaluate those of its operations that are associated with its identified significant risks, and ensure that they are conducted in a way that will enable the pursuit of opportunities, and control or reduce the likelihood and adverse consequences associated with them in order to fulfill the requirements of its ORMS policy and meet its objectives and targets. This should include all parts of its operations including subcontractor, supply chain, and maintenance activities.

As this part of the ORMS provides direction on how to take the system requirements into day-to-day operations, it requires the use of documented procedures to control situations where the absence of documented procedures could lead to deviations from the ORMS policy, objectives, and targets.

To minimize the likelihood of an undesirable or disruptive event, these procedures should include administrative, operational and technological controls. Where existing arrangements are revised or new arrangements introduced that could impact on operations and activities, the organization should consider the associated risks before their implementation.

A.9.1.2 Establishing Norms of Behavior and Codes of Ethical Conduct

The organization should establish, implement, and maintain a Code of Ethical Conduct for its employees, subcontractors, and outsource partners. The Code of Ethical Conduct should clearly communicate respect for the rights and dignity of people, as well as the prohibition of discriminatory practices, harassment, bribery, fraud, conflicts of interest, corruption, and other crimes. The Code of Ethical Conduct should ensure that all persons working on behalf of the organization understand their responsibilities to abide by legal, regulatory and contractual obligations as well as voluntary commitments.

The organization should clearly communicate and provide training on the Code of Ethical Conduct to all persons working on behalf of the organization. The organization should document and maintain records of communication, training, and sign-off acknowledgement.

A.9.2 Resources, Roles, Responsibility, and Authority

A.9.2.1 General

The successful implementation of an ORMS calls for a commitment and sense of shared purpose from all persons working for the organization or on its behalf. The roles, responsibilities, and authorities of individuals should be clearly defined to ensure implementation of the ORMS, prevent misunderstandings (particularly during an undesirable or disruptive event), and avoid missed tasks.

Top management should also ensure that appropriate resources are provided to ensure that the ORMS is established, implemented, and maintained. It is also important that the key ORMS roles and responsibilities are well-defined and communicated to all persons working for or on behalf of the organization.

Roles, responsibilities, and authorities should also be defined, documented, and communicated for coordination with external stakeholders. This should include interactions with subcontractors, supply chain, partners, suppliers, public authorities, and local communities. The organization should define and communicate the responsibilities and authorities of all persons engaged in ORMS regardless of their other roles in the organization. The resources provided by top management should enable the fulfillment of the roles and responsibilities assigned. The roles, responsibilities, and authorities should be reviewed when a change in the operational context of the organization occurs.

To demonstrate its commitment, top management should establish and communicate the organization's ORMS policy and ensure the necessary resources for the implementation of the ORMS. Therefore, top management should designate a specific management representative with defined responsibilities and authority for implementing the ORMS, who:

a) Champions the ORMS;
b) Ensures that the ORMS is established and implemented;
c) Reports on ORMS performance over time; and
d) Works with others to modify the ORMS as needed.

A.9.2.2 Personnel

The organization should retain and train personnel with the skill, knowledge, and ability to meet its contractual obligations. All persons working on the organization's behalf should be adequately compensated and provided sufficient insurance protection corresponding with their responsibilities. Personnel, competence, and training needs are an output of the context of the organization and its contractual requirements, as well as the risk assessment and definition of objectives.

Organizations should establish procedures for the welfare of persons working on their behalf, consistent with the protections provided by applicable labor and other laws including:

a) Providing personnel, a copy of any contract to which they are party to, in a language they understand;
b) Providing personnel with adequate pay and remuneration arrangements commensurate to their responsibilities and working conditions;
c) Adopting operational safety and health policies;
d) Ensuring personnel unrestricted access to their own travel documents; and
e) Preventing unlawful discrimination in employment.

The privacy and confidentiality of information about individuals should be protected. Background and operational information about individuals can be highly sensitive. It is essential that the organization establish and maintain procedures to appropriately and strictly secure the confidentiality of information both internally and externally. The organization should retain relevant documents in a secure manner for a period of time that complies with applicable laws and regulations, contractual requirements, and the organization's records policies.

At a minimum, the following information should be documented for all personnel:

a) Name, address, and contact information;
b) Contact information for immediate family and persons to notify in event of injury or death;
c) Personal identification information; and
d) Information required by legal, regulatory, contractual and other requirements.

A.9.2.3 Response Structure

It is necessary that an appropriate administrative structure be put in place to effectively deal with incident management during an undesirable or disruptive event. Clear definitions should exist for a management structure, authority for decisions, and responsibility for implementation. An organization should have an "Incident Management Team" to lead event response under the clear direction of top management or its representatives. The team should be comprised of such functions as:

a) Planning;
b) Incident response and management;
c) Human resource management;
d) Health, safety, and medical response;
e) Information management;
f) Security;
g) Legal;
h) Communications/media relations; and
i) Other critical support functions.

The Incident Management Team may be supported by as many teams as appropriate taking into account such factors as organization size and type, number of employees, location, etc. Teams should develop response plans to address various aspects of potential crises – such as damage assessment and control, communications, human resources, information technology, and administrative support. Incident response and management plans should be consistent with and included within the overall ORMS. Individuals should be recruited for membership on incident management teams based upon their skills, level of commitment, and vested interest.

The response structure should include provisions/threshold criteria to activate response plans, and identify who has the authority to do the activation. The response structure provides for:

a) A determination of the nature and extent of the undesirable or disruptive incident to establish the scope of the response required, and define actions that might be necessary based on impact and/or potential impact;
b) A response to protect people, assets, and stakeholders' interests;
c) Communication with stakeholders and authorities, as well as the media, using pre-established message templates; and
d) Coordination with initial responders, first responders, and government agencies.

In some organizations, certain divisions, departments, and activities are better situated to address specific aspects of incident response, continuity, and recovery. These organizations may use a tiered approach, establishing multiple teams to focus on specific aspects of managing the disruptive incident (e.g., communications and media response team). The teams should coordinate their activities to assure a seamless response, and be appropriate to the size and nature of the organization. The response structure should avoid vesting authority of the mobilization of a response in a single individual.

A.9.2.4 Selection, Background Screening, and Vetting of Personnel

The organization should establish a documented procedure for pre-employment background checks and vetting of individuals working on behalf of the organization. The organization should establish, document, implement, and maintain procedures that screen out personnel who do not meet minimum qualifications established for positions, and select appropriately qualified personnel based on their knowledge, skills, abilities, and other attributes. The screening and selection procedures should be consistent with legal, regulatory and contractual obligations as well as voluntary commitments. The screening and vetting process should be based on the nature of the job for which the candidate is being considered, the person's level of authority, and the area of specialization. The screening and vetting should take place before the candidate is offered a position and commences work. Candidates should sign appropriate authorizations and consents prior to performing background screening. A decision to retain the services of an individual should be based on the totality of the candidate's qualifications and the results of the background screening and vetting.

Wherever possible, the screening and vetting process should include:

a) Identity verification;
b) Personal history verification; and
c) Credentialing.

Exclusions should be documented when information is unavailable, unreliable, or unsuitable.

Identity verification should include verification of the validity of personal history and minimum age of the prospective employee. Personal history, validated by personal history searches when available, should consider (but not be limited to):

a) Home addresses;
b) Employment records;
c) Electronic media;
d) Criminal and civil record history;
e) Records of human rights violations;
f) Military service records;
g) Motor vehicle records;
h) Credit reports;
i) Sexual offender indices;
j) Government and industry sanctions lists; and
k) Industry specific licensing records.

Credentialing involves verifying the experience and qualifications that are presented by the candidate. The organization should look for unexplained gaps. Credentialing provides information on, but is not limited to:

a) Education verification;
b) Employment verification;
c) Licensure/certification/registration verification;

d) Personal references;
e) Supervisor and coworker interviews; and
f) Military history verification.

The organization should also establish clearly defined criteria for the screening and vetting of individuals based on:

a) Substance abuse;
b) Physical and mental fitness for activities;
c) Suitability to carry weapons or handle hazardous materials; and
d) Ability to operate in stressful and adverse conditions.

The privacy and confidentiality of information about individuals should be protected. Personal documents, such as passports, licenses, and original birth certificates should be returned to personnel within a reasonable timeframe.

A.9.2.5 Selection, Background Screening, and Vetting of Subcontractors

The organization should only retain the services, on a temporary or continuing basis, of competent subcontractors capable of operating in a manner consistent with this *Standard*. The organization is responsible and liable for the subcontractor's work. The organization should establish, maintain, and document clearly defined criteria for the screening and vetting of subcontractors to be used in contracting. Contractual agreements with subcontractors should be documented and retained in accordance with applicable laws and contractual obligations with the client.

Criteria for subcontracting should include the subcontractor's capacity to:

a) Meet the requirements of this *Standard*;
b) Carry out its activities in compliance with relevant laws;
c) Protect the image and reputation of the contracting body;
d) Provide adequate resources and expertise, including competent personnel, to meet operational objectives;
e) Ensure transparency, accountability, and appropriate supervision in the implementation of assigned duties;
f) Take into account the financial and economic obligations (including appropriate remuneration of their personal and insurance coverage);
g) Obtain requisite registrations, licenses, or authorizations;
h) Maintain accurate and up to date personnel and property records; and
i) Acquire, use, return, and dispose of materials in accordance with applicable laws and contractual obligations.

A.9.2.6 Resources

An organization should provide resources, capabilities, structures, and support mechanisms necessary to:

a) Achieve its risk management policy, objectives, and targets;

b) Meet the changing requirements of the organization;

c) Communicate that the ORMS matters, internally and externally; and

d) Provide for the ongoing operation and continual improvement of the ORMS to improve the organization's performance in managing risk.

Top management plays a key role by providing resources needed to implement the ORMS. The management of an organization should determine and make available appropriate resources to establish, implement, maintain, and improve the ORMS. These resources should be provided in a timely and efficient manner.

When identifying the resources needed to establish, implement, and maintain the ORMS, an organization should consider:

a) People and people-related resources (which may include):
   - i. The time necessary to perform ORMS requirements
   - ii. Security
   - iii. Transportation logistics (including parking)
   - iv. Welfare needs
   - v. Emergency expenses

b) Facilities:
   - i. Emergency Operations Centers
   - ii. Site hardening
   - iii. Lodging
   - iv. Recovery locations
   - v. Infrastructure

c) Technology:
   - i. Applications
   - ii. Technology Services Methods to manage and control documentation and records

d) Communications:
   - i. Landline, cellular, mobile, wireless, and satellite telephone
   - ii. Smart device
   - iii. Land-based radio
   - iv. HAM radio
   - v. Social media

e) Information (which may include):
   - i. Policies
   - ii. Standard operating procedures
   - iii. Work instructions
   - iv. Internal and external contact information
   - v. Financial (e.g., payroll) details
   - vi. Customer account records

vii. Supplier and stakeholder details
viii. Legal documents (e.g., contracts, insurance policies, title deeds, etc.)
ix. Other services documents (e.g., contracts and service level agreements)

f) Supplies

Resources and their allocation should be reviewed periodically, and in conjunction with the management review, to ensure their adequacy. In evaluating adequacy of resources, consideration should be given to planned changes and/or new facilities, projects, or operations.

A.9.3 Competence, Training, and Awareness

The organization should identify the awareness, knowledge, understanding, and skills needed by any person with the responsibility and authority to perform tasks on its behalf. The organization should establish training and awareness programs for internal and external stakeholders who may be affected by an undesirable or disruptive event. The organization should require that subcontractors working on its behalf are able to demonstrate that their employees have the requisite competence and/or appropriate training. Management should determine the level of experience, competence, and training necessary to ensure the capability of personnel having documented responsibility for carrying out specialized ORMS management activities. Monitoring and reassessing the level of training should be conducted on an ongoing basis to identify opportunities for improvement.

It is the organization's responsibility that all persons working on behalf of the organization are sufficiently trained, both prior to any deployment and on an ongoing basis, in the performance of their functions and to respect relevant laws, regulations and contractual obligations and voluntary commitments. Defined training objectives should be based on the risk assessment and facilitate uniformity and standardization of training requirements. Training should specifically include:

a) Respect for human rights;
b) Positive behaviors to support a common vision for the achievement of objectives; and
c) Skill sets needed to perform function and activities in routine and atypical situations.

The organization should identify and assess any differences between the competence needed to perform a risk-related task or activity and that possessed by the individual required to perform the activity. This difference can be rectified through additional education, training, or skills development program which may include the following steps:

a) Identification of competence and training needs;
b) Design and development of a training plan to address defined competence and training needs;
c) Selection of suitable methods and materials;
d) Verification of conformity with ORMS training requirements;
e) Training of target groups;
f) Documentation and monitoring of training received;
g) Evaluation of training received against defined training needs and requirements; and

h) Improvement of the training program, as needed.

Training may include general and task- and context-specific topics, preparing personnel for performance under the specific contract and in the specific environment. General topics include, but are not limited to:

a) The individual's role within the ORMS;
b) Identifying opportunities for improvement;
c) Situational awareness and assessing risk;
d) Addressing undesirable and disruptive events;
e) Human rights and respect for law;
f) Religious, gender, and cultural issues, and respect for the local community;
g) Handling complaints, including transmitting them to the appropriate authority; and
h) Measures against fraud, bribery, corruption, and other related crimes.

Examples of task and context specific topics may include:

a) Emergency response;
b) Evacuation procedures;
c) Personal protection measures;
d) Media and other stakeholder communications;
e) Tactical driving;
f) Interview techniques;
g) Land navigation;
h) Electronic communications;
i) Medical aid;
j) Casualty evacuation; or
k) Other specified and implied tasks under the terms of the contract or services offered by the organization.

The organization should use practical, scenario-driven training that will require persons trained to make decisions in situations that reflect conditions that may be faced by personnel in the performance of their activities, and will require them to react to the consequences of those decisions.

A training and awareness program may include:

a) A consultation process with staff throughout the organization concerning the implementation of the ORMS program;
b) Discussion of ORMS in the organization's newsletters, briefings, induction program, or journals (including new employee orientation);
c) Inclusion of ORMS on relevant web pages or intranets;
d) Online training modules housed in the organization's learning management system;
e) Learning from internal and external incidents through after action reports;
f) ORMS as an item at management team meetings;

g) Conferences, classroom and individualized training; and
h) First aid and other hands-on training.

All personnel should receive training to perform their individual ORMS-related responsibilities. They should receive briefs and training on the key components of the ORMS. Such training could include procedures for prevention and mitigation measures, response, documentation and accountability requirements, the handling of local community, client, and media inquiries.

Event response teams should receive education and training about their responsibilities and duties, including interactions with first responders and other internal and external stakeholders. Team members should be trained at regular intervals (at least annually). New members should be trained when they join the organization. These teams should also receive training on prevention of undesirable events. The organization should include relevant external stakeholders and resources in their competence, awareness, and training programs.

A.9.4 Communication

Arrangements should be made for communication and consultation, internally and externally, during routine and atypical conditions. Effective communication is one of the most important ingredients in preventing, managing, and reporting an undesirable or disruptive event. Proactive communications and consultation planning should be conducted with internal and external stakeholders in order to convey day-to-day, alert, disruptive event, and organizational and community response information. To provide the best communications and suitable messages for various groups, it may be appropriate to segment the audiences. In this way, messages may be tailored that can be released to specific groups such as employees, clients, the local community, or the media.

The communication and consultation procedures and processes should consider:

a) Internal communication between the various levels and activities of the organization and with supply chain partners, subcontractors, clients, and partner entities;
b) Receiving, documenting, and responding to relevant communications from external stakeholders (including local communities);
c) Proactive planning of communications with external stakeholders (including the media);
d) Preemptive communication of response and reporting plans to applicable stakeholders facilitating communication and assuring stakeholders that proper planning is in place;
e) Facilitating structured communication with emergency responders; and
f) Availability of communication channels (including redundancies) during a disruptive situation.

Operational communication plans are necessary to provide adequate control, coordination, and visibility over ongoing activities. Such plans should include a description of how relevant threat information will be shared between persons working on behalf of the organization and other internal and external stakeholders (including public authorities). Information should be exchanged in a way that can be understood at each level of performance.

The organization should implement a procedure for receiving, documenting, and responding to relevant communications from stakeholders and interested parties, both internal and external. This procedure can include a dialogue with interested parties and consideration of their relevant concerns. In some circumstances, responses to concerns of interested parties may include relevant information about the risks and impacts associated with the organization's activities and operations. These procedures should also address necessary communications with public authorities regarding emergency planning and other relevant issues.

A.9.4.1 Risk Communication

The organization should also identify and establish relationships with the community, public sector agencies, organizations, and officials responsible for intelligence, warnings, prevention, response, and recovery related to potential undesirable and disruptive events. The organization should formally plan its prevention, mitigation, and response communications strategy, taking into account the decisions made specific to relevant target groups, the appropriate messages and subjects, and the choice of means. When considering communication about hazards, threats, risks, impacts, and control procedures, organizations should take into consideration the views and information needs of all stakeholders, as well as the sensitivity of information.

The organization should establish procedures to communicate and consult with internal and external stakeholders specific to its risks, their impacts, and control procedures. These procedures should consider the specific stakeholder group, the type of information to be communicated, the type of undesirable or disruptive event and its consequences, the availability of methods of communication, and the individual circumstances of the organization. Methods for external communication can include:

a) News or press releases;
b) Media;
c) Financial reports;
d) Newsletters;
e) Websites, apps and social media;
f) Phone calls, emails, and text messages (manually delivered and/or via automated emergency notification systems);
g) Voice mails;
h) HAM radio (H = Hertz, A = Armstrong, M = Marconi); and
i) Community meetings.

The organization should conduct preplanning of communication for a disruptive event. Draft message templates, scripts, and statements can be crafted in advance for threats identified in the risk assessment, for distribution to one or more stakeholder groups identified in the risk assessment. Procedures to ensure that communications can be distributed on short notice should also be established. Communications should occur over as many platforms as necessary to ensure receipt by appropriate stakeholders.

The organization should designate and publicize the name of a primary spokesperson (with back-ups identified) who should manage/disseminate crisis communications to the media and others.

These individuals should receive training in media relations in preparation for a crisis, and on an ongoing basis. All information should be funneled through a single team to assure the consistency of messages. Top management should stress that all organization personnel should be informed quickly regarding where to refer calls from the media and that only authorized company spokespeople may speak to the media. In some situations, an appropriately trained site spokesperson may also be necessary.

A.9.4.2 Communicating Complaint and Grievance Procedures

The organization should establish and communicate to relevant stakeholders internal and external complaints and grievances procedures. The procedures should assure privacy and confidentiality and be tailored to the culture, language, education, and technology requirements of the target audience. Procedures should be established for creating a reporting mechanism for anonymous and non-anonymous complaints and grievances.

A.9.4.3 Whistleblower Policy

Whistleblowing occurs when a person working on behalf of the organization raises a concern about danger, unethical conduct, or illegality that affects others, internally or externally. Persons working on the organization's behalf may be fearful that raising the alarm will lead to retribution from their colleagues or employer. The organization should encourage persons working on its behalf to voice their concerns over malpractice and inappropriate acts against any internal or external stakeholder. A whistleblower policy will help the organization deal with a concern internally and in an appropriate manner, rather than publicly, causing potential damage to the organization and its client. A whistleblower policy can also serve as a deterrent to those who may be considering an illegal, improper, or unethical practice. A good whistleblower policy will help the organization to reduce problems and improve working conditions and operational effectiveness.

Effective whistleblower policies provide individuals with an alternative route other than their direct line management through which to raise their concerns. Therefore, organizations should establish and communicate a whistleblower policy that provides for a clear internal mechanism for anonymously reporting non-conformances and concerns about danger, unethical conduct, or illegality that affects others, internally or externally. The policy should also designate circumstances and conditions where external disclosures are acceptable and protected. Whistleblowers should receive protection for raising concerns so long as they have acted in good faith and have reasonable grounds for raising a concern.

A.9.5 Prevention and Management of Undesirable or Disruptive Events

A.9.5.1 General

The organization should establish, implement, and maintain procedures to prevent, prepare for, and respond to undesirable and disruptive events to ensure the integrity its operations and human, tangible and intangible assets.

The organization should establish, document, and implement procedures for a command and control structure to prevent, prepare for, and manage a disruptive event. This command and control structure should provide for cross-discipline and cross-functional teams with the necessary resources, authority, experience, and competence to:

a) Determine and confirm the nature and extent of a disruptive event, and trigger appropriate control measures;
b) Execute a coordinated response between different business functions and disciplines (e.g., coordination with risk management, information technology, and business continuity teams);
c) Implement plans, processes, and procedures for the activation, operation, coordination, and communication of the prevention, protection, mitigation response, and recovery measures;
d) Communicate with internal and external stakeholders -- including supply chain partners, local authorities, and the media; and
e) Evaluate the level of response with the authority to identify actions of each phase of the disruption -- including declaring the end of the situation.

It is the responsibility of the organization to develop proactive risk treatment procedures that suit its particular needs. In developing its procedures, the organization should address its needs with regard to:

a) The protection of people;
b) The protection of tangible and intangible assets;
c) The most appropriate methods for mitigation and emergency response to a disruptive event to avoid its escalation to a crisis or disaster;
d) Procedures and authority to assess and declare an emergency situation, activate plans and actions, assess damage, and make financial decisions to assure the continuity of operations;
e) Internal and external communication plans -- including notification of appropriate authorities and stakeholders;
f) The actions required to secure physical and information assets;
g) The need for a process for post-event evaluation to establish and implement corrective and preventive actions;
h) Periodic testing of the ORMS under normal and abnormal conditions;
i) The potential impact on organization’s and its supply chain’s risk treatment plans by disruption of critical infrastructure (e.g., electricity, water, communications, transportation) and other dependencies and interdependencies (e.g., information technology systems); and
j) Procedures and actions required for recovery within the organization’s recovery time objective and the resources that it requires for recovery.

The organization should continually assess, and periodically review and revise, its incident prevention, response and management procedures -- in particular, after near misses or incidents that escalated or could have escalated into an emergency or crisis situation.

The organization should document this information and update it at regular intervals or as changes occur. Incident reports should be included in management review.

A.9.5.2 Risk Functions

It is the responsibility of each organization to develop incident prevention, preparedness, mitigation response, and recovery procedures that address its needs as elucidated by the risk assessment. In developing its procedures, the organization should include consideration of:

a) Safeguarding life and assuring the safety of internal and external stakeholders is the top priority;
b) Respect for human rights and human dignity;
c) The risk assessment should be used to identify the specifics of potential disruptive events, including any precursors and warning signs;
d) Risk management should be a systematic and holistic process that builds on the formal risk assessment to identify, measure, quantify, and evaluate risks to provide the optimal solution;
e) Risk treatment options can include avoidance, elimination, reduction, spreading, transfer, and acceptance strategies:
    i. *Avoidance* and *elimination* can either evade activities that gives rise to the risk or remove the source of the risk.
    ii. *Reduction* lowers the risk or the severity of the loss.
    iii. *Spreading* distributes assets and/or the potential loss of capacity.
    iv. *Sharing* involves distributing the risk with another party or parties.
    v. *Acceptance* is an informed decision to take a particular risk.
f) Notification of appropriate authorities and stakeholders.

The organization should establish monitoring and notification procedures to recognize when specific dangers are noticeable that necessitate the need for some level of reaction to avoid, prevent, mitigate, or respond to the potential of the undesirable event. A strong program of detection and avoidance policies and procedures should support this process.

A potential disruptive incident, once recognized, should be immediately reported to the designated authorities, a member of management, or another individual tasked with the responsibility of crisis notification and management internally and with external stakeholders. Specific notification criteria should be established, documented, and adhered to.

Problem assessment (an evaluative process of decision making that will determine the nature of the issue to be addressed) and *severity assessment* (the process of determining the severity of the disruption and what any associated consequences) should be made at the outset of an undesirable event. Factors to be considered include the size of the problem, its potential for escalation, and the possible impact of the situation on the organization and its stakeholders (e.g., local community and clients).

Prevention can include proactive steps to coordinate with internal and external stakeholders. Organizational culture, operational plans, and management objectives should motivate individuals to feel personally responsible for prevention, avoidance, deterrence, and detection.

Cost-effective mitigation strategies should be employed to prevent or lessen the consequences of potential events. The various resources that would contribute to the mitigation process should be identified.

Preparedness and response plans should be developed around a realistic "worst case scenario," with the understanding that the response can be scaled appropriately to match the actual crisis. Considerations include:

a) People are the most important aspect of any preparedness and response plan;
b) Delegation and lines of authority and decision-making roles;
c) How an organization’s human resources are managed will impact the success or failure of incident management;
d) Logistical decisions made in advance will impact the success or failure of a good preparedness and response plan; and
e) Existing funding and insurance policies should be examined.

The organization should establish documented procedures that detail how the organization will manage a disruptive event and how it will recover or maintain its activities to a predetermined level, based on management-approved recovery objectives.

A.9.5.3 Design of Controls and Countermeasure

The design of risk controls and countermeasures should be derived from and consistent with the ORMS policy and risk assessment necessary to achieve the organization’s ORMS objectives and targets. It should characterize the organization’s functions, consistent with the source of risk to the organization and the achievement of objectives. The organization should design risk controls and countermeasures through the process of:

a) Determining the objectives based on the threat/opportunity, vulnerability/capability, and criticality/impact analyses in the risk assessment to clearly identify potential consequences and outcomes;

b) Determining cross-functional and cross-disciplinary interdependencies in a team effort;

c) Identifying risk controls and countermeasures needed to protect assets by reducing the likelihood of a threat successfully materializing, mitigating the consequences should the threat materialize, and planning an appropriate response;

d) Evaluating potential points of failure in the system to determine the appropriate need for redundancies and layered protection methods;

e) Evaluating the competencies required to support effective design and deployment of risk controls and countermeasures by qualified, approved, and recognized professionals;

f) Evaluating the systems criteria to develop the design specifications (drawings, schedules, and schematics) for equipment, materials, hardware, and software requirements;

g) Estimating design costs and lifecycle costs, and developing budgets based on evaluation of cost-benefit options;

h) Ensuring a process of appropriateness, acceptance, approval, responsibility, and accountability;

i) Continually monitoring to analyze, assess, measure, and evaluate the effectiveness of the risk controls and countermeasures design and design processes; and
j) Maintaining the integrity of the organization and the functions and assets to which the system is to be applied.

The risk controls and countermeasures should integrate people, procedures, and equipment for the protection of the organization's assets, its properties, facilities, and operations. The functions of risk controls and countermeasures are to prevent or deter the occurrence of an undesirable event, detect an undesirable event or adversary attack, delay adversaries from reaching their target, and provide a response to deny adversaries from reaching their target or succeeding in their objective. When designing the risk controls and countermeasures, the organization should consider layering the controls and countermeasures, including (but not limited to):

a) Environmental design;
b) Physical barriers and site hardening (which includes overhead penetrations and underground pathways);
c) Physical entry and access control;
d) Security lighting;
e) Intrusion detection;
f) Video surveillance;
g) Electronic and network controls;
h) Personnel; and
i) Administrative procedures (may include memoranda of understanding, mutual aid agreements, other external resources).

The organization should document all phases of the controls and countermeasures design process.

A.9.5.4 Incident Management Procedures and Plans

The risk treatments are reflected in documented approaches to achieve the organization's objectives and targets. Risk treatments should be coordinated or integrated with other organizational plans, strategies, and budgets.

To ensure its success, the procedures should define:

a) Responsibilities for achieving goals (who will do it and what will be done?);
b) Means and resources for achieving goals (where and how to do it?); and
c) Timeframe for achieving those goals (when will it be done?).

The procedures may be subdivided to address specific elements of the organization's operations. The organization may use several action plans as long as the key responsibilities, tactical steps, resource needs, and schedules are adequately defined in each of the documented plans.

The strategies should include – where appropriate and practical – consideration of all stages of an organization's activities related to planning, design, construction, commissioning, operation, retrofitting, production, marketing, outsourcing, and decommissioning. Strategy development may be undertaken for current activities and new activities, products, and/or services.

Prevention, preparedness, and mitigation strategies should give priority to the safe removal of people and property at risk. Additional topics include:

a) E-location, retrofitting, and provision of protective systems or equipment;
b) Information, data, document, and cyber security;
c) Establishment of threat or hazard warning and communication procedures; and
d) Redundancy or duplication of systems, essential personnel, equipment, information, operations, or materials – including those from partner organizations.

The organization should plan for incident response and recovery, taking into account the priority of activities, contractual obligations, employee and neighboring community necessities, operational continuity, and environmental remediation. Organizations have different approaches to managing crises. Regardless of the approach, there are interrelated management response steps that require pre-emptive planning and implementation in case of an undesirable or disruptive incident:

a) *Prevention*: Measures are proactively taken to avoid the occurrence of an event and to mitigate potential consequences.
b) *Response*: The initial response to a disruptive incident usually involves the protection of people and property from immediate harm. An initial reaction by management may form part of the organization's first response.
c) *Continuity*: Processes, controls, and resources are made available to ensure that the organization continues to meet its continuity and ORMS objectives.
d) *Recovery*: Processes, resources, and capabilities of the organization are re-established to meet ongoing operational requirements. This may often include the introduction of significant organizational improvements even to the extent of refocusing strategic, operational, tactical, and reputational objectives.

Strategies should be dynamic, performance-based, and modified when:

a) Outcomes of the risk assessment change;
b) Objectives and targets are modified or added;
c) Relevant legal, regulatory, or contractual requirements and voluntary commitments are introduced or changed;
d) Substantial progress in achieving the objectives and targets has been made (or has not been made); or
e) Products, services, processes, or facilities change or other issues arise.

Determining risk treatments enables the organization to evaluate a range of options. The organization may choose an appropriate response for each activity, such that it can continue to deliver activities at an acceptable level of operations and within an acceptable timeframe before, during and after an event. Options should be considered for the resumption of activity to pre-determined levels and timeframes. The most appropriate strategy or strategies should depend on a range of factors such as:

a) The results of the organization's risk assessment;
b) The costs of implementing a strategy or strategies; and

c) The consequences of inaction.

Procedures and plans might be required for the following organizational resources:

a) Staff;
b) Premises;
c) Technology;
d) Information;
e) Supplies;
f) Stakeholders; and
g) Supporting Infrastructure.

The organization should establish documented plans that detail how the organization should manage an undesirable or disruptive event and how it should recover or maintain its activities to a predetermined level, based on management-approved recovery objectives.

Each plan should define:

a) Purpose and scope;
b) Objectives and measures of success;
c) Activation criteria and procedures;
d) Implementation procedures;
e) Roles, responsibilities, and authorities;
f) Communication requirements and procedures;
g) Internal and external interdependencies and interactions;
h) Resource requirements; and
i) Information flow, documentation, and record keeping processes.

The organization should periodically (at least annually) test, review, and revise its business continuity plans—in particular, after the occurrence of the disruptive event and its associated post-event review.

A.9.5.5 Occupational Health and Safety

The organization should provide a safe and healthy working environment, recognizing the possible inherent dangers and limitations presented by the local environment. Reasonable precautions should be taken to protect all persons working on behalf of the organization – or those in their care – in high-risk or life-threatening situations.

All personnel should receive initial and recurrent training in emergency response plans, first aid and casualty care, with special emphasis on immediate response to traumatic injury following an attack or accident. Training should be conducted to an accepted standard.

A.9.5.6 Incident Monitoring, Reporting, and Investigations

The organization should establish procedures for incident reporting, documenting any incident involving persons working on its behalf that involves injury to persons, threats to tangible or intangible assets, use of force, damage to equipment or property, malevolent or criminal acts, accidents, and any other such reporting as otherwise required by organizational policies, jurisdictional law, or a client. The organization should establish procedures for an internal inquiry to determine the following:

a) Time and location of the incident;
b) Identity of any persons involved including contact details;
c) Injuries/damage sustained;
d) Circumstances leading up to the incident;
e) Any measures taken by the organization in response to the incident;
f) Causes of internal and external casualties;
g) Notification of appropriate authorities;
h) Identification of root causes; and
i) Corrective and preventive actions taken.

Upon completion of the inquiry, the organization should produce in writing an incident report including the above information, copies of which should be provide to appropriate stakeholders (e.g., clients and jurisdictional authorities).

Persons working on behalf of the organization should be aware of the responsibilities and mechanisms for incident reporting, including evidence gathering and preservation. The incident reporting program should be included in the organization's training program.

A.9.5.7 Internal and External Complaint and Grievance Procedures

The organization should establish a complaint and grievance procedure whereby any internal or external stakeholder who believes there are potential or actual nonconformance's with this *Standard*, or violations of laws, or human rights may file a grievance. The procedure should state that the organization, or persons working on its behalf, may not retaliate against anyone who files a grievance or cooperates in the investigation of a grievance.

Complaint and grievance procedures are not for merely documenting grievances; they should be designed to resolve disputes by identifying root causes, improving accountability, and driving a culture of continual improvement. Once a complaint or grievance has been verified, corrective and preventive actions should be implemented in an expedited fashion.

When developing complaint and grievance procedures, one or more individuals should be designated with the authority to coordinate the efforts to investigate and resolve any complaints that the organization receives alleging any actions that threaten human life, rights, or safety; or are not in conformance with the requirements of the *Standard*, or as required by a client. The organization should adopt and publish its grievance procedures providing for prompt and equitable resolution of complaints.

The procedures should include, but are not limited to:

a) Mechanisms for submission of the complaint or grievance;

b) Information requirements of the submitter, including submission of corroborating information;
c) Timeframes for submission, investigations, and outcomes;
d) Provisions for confidentiality and privacy;
e) Hierarchical steps for the resolution process;
f) Investigation procedures, both internal and external;
g) Maintenance requirements of files and records related to the grievance and investigation;
h) Disciplinary actions;
i) Steps for resolution of complaint or grievance, including actions to prevent a recurrence;
j) Documentation and communication of outcomes; and
k) Notification to appropriate authorities.

A.10 Performance Evaluation

A.10.1 Monitoring and Measurement

Performance evaluation involves the measurement, monitoring, and evaluation of the organization's management of risk, legal and regulatory compliance, health and safety, and human rights performance. The organization should have a systematic approach for measuring and monitoring its risk management performance on a regular basis. Metrics assure the organizations policy, objectives, and targets are achieved, as well as elucidate areas for improvement.

To measure and monitor the organization's risk management performance, a set of performance indicators should be developed to measure both the management systems and its outcomes. Measurements can be either quantitative or qualitative, and should be directly related to the risk assessment and security and resilience objectives and targets. Performance indicators can be management, operational, or economic indicators. Indicators should provide useful information to identify both successes and areas requiring correction or improvement.

The ORMS should provide procedures for defining metrics, collection of data, and analysis of data collected. Metrics should be established to monitor and measure the effectiveness of the ORMS, and identify areas for improvements to enhance performance to preemptively prevent potential undesirable and disruptive events. Knowledge gained from this information can be used to implement corrective and preventive action.

Key characteristics are those that the organization needs to consider to determine how it is managing its significant risks, achieving objectives and targets, and improving security and resilience performance.

When necessary to ensure valid results, measuring equipment should be calibrated or verified at specified intervals, or prior to use, against measurement standards traceable to international or national measurement standards. Where no such standards exist, the basis used for calibration should be recorded.

A.10.2 Evaluation of Compliance

The organization should be able to demonstrate that it has evaluated compliance with the legal, regulatory, and contractual obligations as well as voluntary commitments identified, including applicable permits or licenses.

The organization should be able to demonstrate that it has evaluated compliance with the other identified requirements to which it has subscribed.

A.10.3 Exercises and Testing

Exercising and testing scenarios should be designed using the events identified in the risk assessment. Exercising and testing can serve as an effective training tool, and can be used to validate the assumptions and conclusion of the risk assessment.

Exercising ensures that technology resources function as planned, and that persons working on the organizations behalf are adequately trained in their use and operation. Exercising can keep persons working on the organizations behalf effective in their duties, clarify their roles, and identify areas for improvement in the ORMS plans and procedures. Exercising can reveal weaknesses in the ORMS that should be corrected. A commitment to exercising lends credibility and authority to the ORMS.

The first step in exercises and testing should be the setting of goals and expectations. A critical goal is to determine whether certain prevention and response processes work and how they can be improved. The organization should use exercises and the documented results of exercises to ensure the effectiveness and readiness of the ORMS – specifically, its risk treatment plans, team readiness, and facilities – to perform and validate its risk and business management functions.

Benefits of exercising and testing include:

a) Validation of planning scope, assumptions, and strategies;
b) Examine and improve competence of persons working on behalf of the organization;
c) Capacity testing (e.g., the capacity of a call-in or call-out phone system);
d) Increase efficiency and reduce the time necessary for accomplishment of a process (e.g., using repeated drills to shorten response times); and
e) Awareness and knowledge for internal and external stakeholders about the ORMS and their roles.

The organization should design exercise scenarios to evaluate the risk treatment plans. An exercise schedule and timeline for periodically exercising the ORMS and its components should be established. Exercising and testing should be realistic, evaluate the capabilities and capacities of ORMS, and assure the protection of people and assets involved. The scope and detail of the exercises should mature based on the organization's experience, resources, and capabilities. Early tests may include checklists, simple exercises, and small components of the ORMS. Examples of increasing maturity of exercises include:

a) *Orientation*: Introductory, overview, or education session;
b) *Table Top*: Practical or simulated exercise presented in a narrative format;

c) *Functional*: Walk-through or specialized exercise simulating a scenario as realistically as possible in a controlled environment; and
d) *Full Scale*: Live or real-life exercise simulating a real-time, real-life scenario.

There are several roles that exercise participants may fill. All participants should understand their roles in the exercise. The exercise should involve all organizational participants defined by the scope of the exercise; where appropriate, external stakeholders may be included. As part of the exercise, a review should be scheduled with all participants to discuss issues and lessons learned. This information should be documented in a formal exercise report which should be reviewed by top management. Updates should be made to plans and procedures, and corrective and preventive measures expeditiously implemented.

Design of tests and exercise should be evaluated and modified as necessary. They should be dynamic, taking into account changes to the ORMS, personnel turnover, actual incidents, and results from previous exercises. Lessons learned from exercises and tests, as well as actual incidents experienced, should be built into future exercises and test planning for the ORMS.

Exercise and test results should be documented, used during debriefs, added to lessons learned, and retained as records.

A.10.4 Nonconformities, Corrective and Preventive Action

The organization should establish effective procedures to ensure that non-fulfillment of a requirement, inadequacies in planning approach, incidents, near misses, and weaknesses associated with the ORMS (its plans and procedures) are identified and communicated in a timely manner to prevent further occurrence of the situation, as well as to identify and address root causes. The procedures should enable ongoing detection, analysis, and elimination of actual and potential causes of nonconformities.

An investigation should be conducted of the root cause(s) of any identified nonconformity in order to develop a corrective action plan for immediately addressing the problem to mitigate any consequences, make changes needed to correct the situation and to restore normal operations, and take steps to prevent the problem from recurring by eliminating cause(s). The nature and timing of actions should be appropriate to the scale and nature of the nonconformity and its potential consequences.

Sometimes, a potential problem may be identified, but no actual nonconformity exists. In this case, a preventive action should be taken using a similar approach. Potential problems can be extrapolated from corrective actions for actual nonconformities, identified during the internal ORMS audit process, analysis of industry trends and events, or identified during exercise and testing. Identification of potential nonconformities can also be made part of routine responsibilities of persons aware of the importance of noting and communicating potential or actual problems.

Establishing procedures for addressing actual and potential nonconformities and for taking corrective and preventive actions on an ongoing basis helps to ensure reliability and effectiveness of the ORMS. The procedures should define responsibilities, authority, and steps to be taken in planning and carrying out corrective and preventive action. Top management should ensure that corrective and preventive actions have been implemented and that there is systematic follow-up to evaluate their effectiveness.

Corrective and preventive actions that result in changes to the ORMS should be reflected in the documentation, as well as trigger a revisit of the risk assessment related to the changes to the system to evaluate the effect on plans, procedures, and training needs. Changes should be communicated to affected stakeholders.

A.10.4.1 Corrective Action

The organization should take action to eliminate the cause of nonconformities associated with the implementation and operation of the ORMS to prevent their recurrence. The documented procedures for corrective action should define requirements for:

a) Identifying any nonconformities;

b) Determining the causes of nonconformities;

c) Evaluating the need for actions to ensure that nonconformities do not recur;

d) Determining and implementing the corrective action needed;

e) Recording the results of action taken; and

f) Reviewing the corrective action taken and the results of that action.

A.10.4.2 Preventive Action

The organization should take action to prevent potential nonconformities from occurring. Preventive actions taken should be appropriate to the potential impact of nonconformities.

The documented procedure for preventive action should define requirements for:

a) Identifying potential nonconformities and their causes;

b) Determining and implementing preventive action needed;

c) Recording results of action taken;

d) Reviewing preventive action taken;

e) Identifying changed risks and ensuring that attention is focused on significantly changed risks;

f) Ensuring that all those who need to know are informed of the non-conformity and preventive action put in place; and

g) The priority of preventive actions based on results of risk assessments.

A.10.5 Internal Audit

It is essential to conduct internal audits of the ORMS to ensure that the ORMS is achieving its objectives, that it conforms to its planned arrangements, that it has been properly implemented and maintained, and to identify opportunities for improvement. Internal audits of the ORMS should be conducted at planned intervals to determine and provide information to top management on appropriateness and effectiveness of the ORMS, as well as to provide a basis for setting objectives for continual improvement of ORMS performance.

The organization should establish an audit program (see ANSI/ASIS SPC.2-2014 for guidance) to direct the planning and conduct of audits, and identify the audits needed to meet the program objectives. The program should be based on the nature of the organization's activities, in terms of its risk assessment, the results of past audits, and other relevant factors.

An internal audit program should be based on the full scope of the ORMS; however, each audit need not cover the entire system at once. Audits may be divided into smaller parts, so long as the audit program ensures that all organizational units, activities, and system elements – and the full scope of the ORMS – are audited in the audit program within the auditing period designated by the organization.

The `results of an internal ORMS audit can be provided in the form of a report, and used to correct or prevent specific nonconformities and provide input to the conduct of the management review.

Internal audits of the ORMS can be performed by personnel from within the organization or by external persons selected by the organization, working on its behalf. In either case, the persons conducting the audit should be competent and in a position to do so impartially and objectively. In smaller organizations, auditor independence can be demonstrated by an auditor being free from responsibility for the activity being audited.

NOTE: If an organization wishes to combine audits of its ORMS with quality, safety, or environmental audits, the intent and scope of each should be clearly defined. Third-party conformity assessment, performed by a body that is independent of the organization, provides confidence to internal and external stakeholders that the requirements of this *Standard* are being met. The value of certification is the degree of public confidence and trust that is established by an impartial and competent external assessment.

A.10.6 Management Review

Management review provides top management with the opportunity to evaluate the continuing suitability, adequacy, and effectiveness of the ORMS. The management review should cover the scope of the ORMS, although not all elements of the ORMS need to be reviewed at once, and the review process may take place over a period of time. The management review will enable top management to address need for changes to key ORMS elements, including:

a) Policy;

b) Resource allocations;

c) Risk appetite and risk acceptance;

d) Objectives and targets; and

e) Security and resilience strategies.

Review of the implementation and outcomes of the ORMS by top management should be regularly scheduled and evaluated. While ongoing system review is advisable, formal review should be structured, appropriately documented, and scheduled on a suitable basis. Persons who are involved in implementing the ORMS and allocating its resources should be involved in the management review. In addition to the regularly scheduled management system reviews, the following factors can trigger a review and should otherwise be examined once a review is scheduled:

a) *Risk Assessment*: The ORMS should be reviewed every time a risk assessment is completed for the organization. The results of the risk assessment can be used to determine whether the ORMS continues to adequately address the risks facing the organization.

b) *Sector/Industry, Contractual, and Political Trends*: Significant changes in sector/industry, contractual, and political trends should initiate an ORMS review. General trends and best practices in the sector/industry and in security and resilience planning techniques can be used for benchmarking purposes.

c) *Regulatory Requirements*: New regulatory requirements may require a review of the ORMS.

d) *Event Experience*: A review should be performed following an undesirable or disruptive event, whether the prevention, mitigation, or response plans were activated or not. If the plans were activated, the review should take into account the history of the plan itself, how it worked, why it was activated, etc. If the plans were not activated, the review should examine why not, and whether this was an appropriate decision.

e) *Test and Exercise Results*: Based on test and exercise results, the ORMS should be modified as necessary.

Continual improvement and ORMS maintenance should reflect changes in the risks, activities, and operation of the organization that will affect the ORMS. The following are examples of procedures, systems, or processes that may affect the plan:

a) Policy changes;

b) Hazards and threat changes;

c) Changes to the organization and its business processes;

d) Changes in assumptions in risk assessment;

e) Personnel changes (employees and contractors) and their contact information;

f) Subcontractor and supply chain changes;

g) Process and technology changes;

h) Systems and application software changes;

i) Lessons learned from exercising and testing;

j) Lessons learned from external organizations' undesirable and disruptive events;

k) Issues discovered during actual invocation of the plan;

l) Changes to external environment (new client needs, political changes, relations with local communities, etc.); and

m) Other items noted during review of the plan and identified during the risk assessment.

A.11 Maturity Model for the Phased Implementation

Implementation of a management system standard can be a daunting task, especially for small to medium sized enterprises. All organizations face the challenge of managing their risks within the bounds of organizational objectives and available resources. Only through the full implementation, ongoing maintenance, and continual improvement of the ORMS can an organization reach its goal of achieving its objectives. Building the ORMS in a phased approach with documented baselines and achieving benchmarks of maturity provides the organization a link between objectives and its resources.

By using a maturity model for the phased implementation of the ORMS, the organization defines a series of steps designed to help it evaluate where they currently are with regard to security and resilience, and respect for human rights, to set goals for where they want to go, to benchmark where they are relative to those goals, and to plot a business-sensible path to get to full implementation of the ORMS.

Annex B

(informative)

B EXAMPLES OF INCIDENT PREVENTION, PREPAREDNESS, AND RESPONSE

It is the responsibility of each organization to develop (an) incident prevention, preparedness, and response procedure(s) that suits its own particular needs. In developing its procedure(s), the organization should include consideration of:

a) A potential disruptive incident should be identified, understood, and addressed and – in doing so – avoided or prevented. The risk assessment can be used to identify the specifics of potential disruptive incidents, including any precursors and warning signs.

    i. Risk management should be a systematic and holistic process that builds on the formal risk assessment to identify, measure, quantify, and evaluate risks to provide the optimal solution.

    ii. Risk treatment options can include avoidance, elimination, reduction, spreading, sharing, and acceptance strategies. *Avoidance* and *elimination* can either evade activities that gives rise to the risk or remove the source of the risk. *Reduction* lowers the risk or the severity of the consequences. *Spreading* distributes assets and/or the potential loss of capacity. *Sharing* the risk with another party or parties. *Acceptance* is an informed decision to take a particular risk.

b) Prevention can include proactive steps to coordinate with intelligence, law enforcement, and public agencies; establish information sharing agreements; physical protection of key assets; access controls; awareness and readiness training programs; warning and alarm systems; and practices to reduce the threat.

c) Organizational culture, operational plans, and management objectives should motivate individuals to feel personally responsible for prevention, avoidance, deterrence, and detection.

d) Deterrence and detection can make a disruptive act or activity more difficult to carry out against the organization or significantly limit, if not negate, its impact. Consideration of prevention, detection, and deterrence strategies may be:

    i. *Architectural*: Natural or manmade barriers; redesigned or relocated infrastructure.

    ii. *Operational*: Removal of hazardous materials; redesigned systems and operations; security officers' post orders; employee awareness programs; counter surveillance and counter intelligence as avoidance; relocation of systems, operations, infrastructure, and personnel.

iii. *Technological*: Alternative materials and processes, interoperable communication and information networks, intrusion detection, access control, recorded surveillance, package and baggage screening, and system controls.

e) Physical security planning includes protection of perimeter grounds, building perimeter, internal space protection, and protection of contents. Defense begins at the external perimeter.

i. *Physical security planning* is a function of deterrence, detection, delay, and response.
ii. *Physical security measures* should be designed so detection is as far from the target as possible. Delays are planned closer to the target.
iii. *Security system design* should link exterior or interior detection with assessment and response.
iv. *Physical security measures* may include crime prevention through environmental design; physical barriers and site hardening; physical entry and access controls; security lighting; intrusion detection systems and alarms; closed-circuit televisions; security personnel; and security policies and procedures.

f) Cost-effective mitigation strategies should be employed to prevent or lessen the impact of potential crises.

i. The mitigation strategy should consider immediate, interim, and long-term actions.

ii. The various resources that would contribute to the mitigation process should be identified. These resources – including essential personnel and their roles and responsibilities, facilities, technology, and equipment – should be documented in the plan and become part of "business as usual."

iii. Systems and resources should be monitored continually as part of mitigation strategies. Such monitoring can be likened to simple inventory management.

iv. The resources that will support the organization to mitigate the crisis should also be monitored continually to ensure that they will be available and able to perform as planned during the crisis. Examples of such systems and resources include, but are not limited to: emergency equipment, fire alarms and suppression systems, local resources and vendors, alternate worksites, maps and floor plans, system backup, and offsite storage.

g) The organization should establish procedures to recognize when specific dangers occur that necessitate the need for some level of response. A strong program of detection and avoidance policies and procedures will support this process.

i. Certain departments or functions are uniquely situated to observe warning signs of an imminent crisis. Personnel assigned to these departments or functions should be trained appropriately. The responsibility to report a potential crisis (including the notification mechanism) should be communicated to all employees. The general employee population may also be an excellent source of predictive information when there is a documented reporting structure and where attention is paid to what the employee reports.

h) A potential disruptive incident, once recognized, should be immediately reported to a supervisor, a member of management, or another individual tasked with the responsibility of crisis notification and management.

  i. Specific notification criteria should be established, documented, and adhered to by all employees (with the timing and sequence of notification calls clearly documented). The actual activation of a response process should require very specific qualifications being met.
  ii. Qualified personnel should have ready access to the updated, confidential listings of persons and organizations to be contacted when certain conditions or parameters of a potential crisis are met.
  iii. Notifications in a crisis situation should be timely and clear, and should use a variety of procedures and technologies – with recognition that devices used have advantages and limitations.
  iv. In some types of crises, the notification systems are themselves impacted by the disaster, either through capacity issues or infrastructure damage. Thus, it is important to have redundancies built into the notification system, and several different ways to contact the listed individuals and organizations.

i) *Problem assessment* (an evaluative process of decision making that will determine the nature of the issue to be addressed) and *severity assessment* (the process of determining the severity of the crisis and what any associated costs may be in the long run) should be made at the outset of a crisis. Factors to be considered include the size of the problem, its potential for escalation, and the possible impact of the situation.

j) The point at which a situation is declared to be an emergency or crisis should be clearly defined, documented, and fit very specific and controlled parameters. Responsibility for declaring a crisis should also be clearly defined and assigned. First and second alternates to the responsible individual should be identified. The activities that declaring a emergency or crisis will trigger include, but are not limited to:

  i. Additional call notification;
  ii. Evacuation, shelter, or relocation;
  iii. Safety protocol;
  iv. Response site and alternate site activation;
  v. Team deployment;
  vi. Personnel assignments and accessibility;
  vii. Emergency contract activation; and
  viii. Operational changes.

k) Preparedness and response plans should be developed around a "worst case scenario," with the understanding that the response can be scaled appropriately to match the actual crisis.

l) People are the most important aspect of any preparedness and response plan. How an organization's human resources are managed will impact the success or failure of incident management.

    i. A system should be devised by which all personnel can be accounted for quickly after the onset of a crisis. This system could range from a simple telephone tree to an elaborate external vendor's call-in site. Current and accurate contact information should be maintained for all personnel. Consideration should be given to engaging the company's travel services to assist in locating employees on business travel.
    ii. Arrangements should be made for notification of any next-of-kin in case of injuries or fatalities. If at all possible, notification should take place in person by a member of senior management. Appropriate training should be provided.
    iii. The organization should implement a Family Representative program in case of severe injury or fatality. The Family Representative should be someone other than the person who performed the notification. This representative should act as the primary point of contact between the family and the organization. Comprehensive training for the representative is a necessity.
    iv. Crisis counseling should be arranged as necessary. In many cases, such counseling goes beyond the qualifications and experience of an organization's employee assistance program (where available). Other reliable sources of counseling should be identified prior to a crisis situation.
    v. A crisis may have far reaching financial implications for the organization, its employees and their families, and other stakeholders; these implications should be considered an important part of a preparedness and response plan. Implications may include financial support to families of victims. Additionally, there may be tax implications that should be referenced and clarified in advance.
    vi. The payroll system should remain functional throughout the crisis.

m) Logistical decisions made in advance will impact the success or failure of a good preparedness and response plan. Among them are the following:

    i. A primary Crisis Management Center should be identified in advance. This is the initial site used by the Crisis Management Team and Response Teams for directing and overseeing crisis management activities. The site should have an uninterruptible power supply; essential computer, telecommunications, heating/ventilating/air conditioning systems; and other support systems. Additionally, emergency supplies should be identified and kept in the center.
    ii. Where a dedicated center is not possible, a designated place where the teams may direct and oversee crisis management activities should be guaranteed. Access control measures should be implemented, with the members of all teams given 24x7 access.
    iii. A secondary Crisis Management Center should also be identified in the event that the primary center is impacted by the crisis event.

   iv. The organization should consider the establishment of virtual command centers for distributed access to information as well as to reach dispersed or remote stakeholders.
   v. The organization should have alternate worksites identified for business resumption and recovery. In the absence of other company facilities being available and/or suitable, access to alternate worksites can be arranged through appropriate vendors. Planning concerning the identification and availability of alternate worksites should take place early in the preparedness and response plan process. Alternate worksites should provide adequate access to the resources required for business resumption identified in the impact analysis.
   vi. Offsite storage is a valuable mitigation strategy allowing rapid crisis response and business resumption/recovery. The off-site storage location should either be a sufficient distance from the primary facility or hardened, so that it is not likely to be similarly affected by the same event. Items to be considered for off-site storage include vital records (paper and other media) critical to the operations of the business. Procedures should be included in the plan to ensure the timely delivery of any necessary items from offsite storage to the Crisis Management Center or the alternate worksites.

n) Once the Crisis Management Team has been activated, the damage should be assessed. The damage assessment may be performed by the Crisis Management Team itself or a designated Damage Assessment Team. Responsibility should be assigned for the documentation of all incident related facts and response actions, including financial expenditures.
   i. For situations involving physical damage to company property, the Crisis Management Team or its designated Damage Assessment Team should be mobilized to the site. The team will gain entry if permission from the public safety authorities is granted, and make a preliminary assessment of the extent of damage and the likely length of time that the facility will be unusable.
   ii. Certain types of crises do not involve immediate physical damage to a company worksite or facility. These would include the business, human, information technology, and societal types of crises. In these crises, the team will likely assess the damage or impact as the crisis unfolds.
   iii. A reconstitution or reconstruction team should be created once it becomes apparent that the facility requires significant repair or the search for a replacement becomes necessary due to severe damage.

o) If appropriate, existing funding and insurance policies should be examined, and additional funding and insurance coverage should be identified and obtained.
   i. Policy parameters should be established in advance, including pre-approval by the insurance provider of any response related vendors. Where possible, the amount of funds to help ensure continuity of operations should be determined in the planning process.

ii. Any cash should be stored in an easily accessible location to assure its availability during a crisis, and some cash and credit should be available for weekend and after-hours requirements.
iii. All crisis related expenses should be recorded throughout the response and recovery periods.
iv. Insurance providers should be contacted as early as possible in the crisis period, particularly in instances of a wide-reaching crisis, where competition for such resources could be vigorous. All insurance policy and contact information should be readily available to the Crisis Management Team and backed up or stored offsite as appropriate.

p) Transportation in a time of crisis can be a challenge. Provisions should be arranged ahead of time, if possible. Areas where transportation is critical include, but are not limited to:

i. Evacuation of personnel (this may be from a demolished work-site or from a satellite facility in another region or country);
ii. Transportation to an alternate worksite;
iii. Supplies into the site or to an alternate site;
iv. Transportation of critical data to worksite; and
v. Transportation for staff with special needs.

q) Critical vendor or service provider agreements should be established as appropriate and their contact information maintained as part of the preparedness and response plan. Such information could include phone numbers, contact names, account numbers, pass-codes (appropriately protected), and other information in the event that someone unfamiliar with the process would need to make contact.

i. In some instances, it may be appropriate to request and review the preparedness and response plan, or a summary of such, of the critical vendors, in order to evaluate their ability to continue to provide necessary supplies and services in the case of a far-reaching crisis. At a minimum, the vendor or service provider roles and service level agreements should be discussed in advance of the crisis.

r) Mutual aid agreements identify resources that may be shared with or borrowed from other organizations during a crisis, as well as mutual support that may be shared with other organizations. Such agreements should be legally sound and properly documented, clearly understood by all parties involved, and representative of dependable resources as well as a commitment to cooperation. However, it must be determined if other competing mutual aid agreements are in place with this resource.

s) Strategic alliances identify delivery partners with which it has an interdependent relationship with other organizations to produce and supply products and services and share risk.

t) Once the extent of damage is known, the process recovery needs should be prioritized and a schedule for resumption determined and documented. The prioritization should take into account the fundamental criticality of the process and other factors, including relationships to other processes, critical schedules, and regulatory requirements, as identified in the impact analysis. Decisions regarding prioritization of processes should be documented and recorded, including the date, time, and justification for the decisions.

u) Once the processes to be restored have been prioritized, the resumption work can begin with processes restored according to the prioritization schedule. The resumption of these processes may occur at either the current worksite or an alternate worksite, depending on the circumstances of the crisis. Documentation should be kept of when the processes were resumed.

v) Once the critical processes have been resumed, the resumption of the remaining processes can be addressed. Where possible, decisions about the prioritization of these processes should be thoroughly documented in advance, as should the timing of actual resumption.

w) The organization should seek to bring the organization "back to normal." If it is not possible to return to the pre-crisis "normal," a "new normal" should be established. This "new normal" creates the expectation that, while there may be changes and restructuring in the workplace, the organization will phase back into productive work. Each step of the process and all decisions should be carefully documented.

    i. As a rule, it is at this point that the crisis may be officially declared "over." It is important to document this decision. Press conferences and mass media communications may be undertaken to bolster employee and client confidence.

Annex C

(informative)

C Examples of Risk Treatment Procedures That Enhance Resilience of the Organization

C.1 General

Building a resilient organization is part of any good business management strategy. In order to thrive and survive, organizations need to adapt to an ever-changing environment. To be agile and resilient in order to achieve the organization's objectives, the organization needs to leverage all the disciplines that contribute to managing risk. For organizations to cost-effectively manage risk, they must develop balanced strategies to adaptively, proactively, and reactively address maximizing opportunities and minimizing the likelihood and consequences of potential undesirable and disruptive events.

The organization should establish, implement, and maintain procedures to prevent and manage disruptive events which have the potential to harm the organization, its key stakeholders including supply chain partners, and the environment.

Procedures should be concise and accessible to those responsible for their implementation. Flow charts, diagrams, tables, and lists of action should be used rather than expansive text.

The purpose and scope of each procedure should be agreed by top management and understood by those responsible for its implementation. Dependencies and interdependencies should be identified and the relationships between procedures, including those of the emergency services and local authorities, should be stated and understood. The following sections provide more information on selected procedures. At the end of this annex are some templates for different plans.

C.2 Prevention and Mitigation Procedures

The purpose of a prevention or mitigation procedure is to define the measures to be taken by the organization to minimize the likelihood of a disruptive event or to minimize the potential for the severity of the consequences of the event.

Prevention procedures should describe how the organization will take proactive steps to protect its assets by establishing architectural, administrative, design, operational, and technological approaches to avoid, eliminate, or reduce the likelihood of risks materializing including the protection of assets from unforeseen threats and hazards.

Mitigation procedures should describe how the organization will take proactive steps to protect its assets by establishing immediate, interim, and long-term approaches to reduce the consequences of risks before they materialize including the protection of assets from unforeseen threats and hazards.

Organizations may choose to have a single procedure with sections and/or annexes dealing with different types of incidents. Alternatively, separate procedures may be written for each type of incident.

Each procedure should specify as a minimum:

a) The purpose and scope of the procedure;
b) Assets to be protected from the disruptive event;
c) Objectives and measures of success;
d) Implementation steps and the frequency with which the procedure is carried out;
e) Roles, responsibilities, and authorities;
f) Communication requirements and procedures;
g) Internal and external interdependencies and interactions;
h) Resource, competency, and training requirements; and
i) Information flow and documentation processes.

The organization should nominate a primary "owner" of each prevention and mitigation procedure and should state who is responsible for reviewing, amending, and updating the procedure. The process of reviewing, amending, updating, and distributing procedures should be controlled.

Examples of prevention and mitigation procedures include the following:

a) Eliminate the risk by complete removal of the threat or risk exposure;
b) Reduce the risk by modifying activities, processes, equipment or materials;
c) Isolation or separation of the risk from assets (human or physical);
d) Engineering controls to deter, detect, and delay a potential threat;
e) Administrative controls such as work practices or procedures that reduce risk; and
f) Protection of the asset if the risk cannot be eliminated or reduced.

C.3 Response Procedures

The purpose of a response procedure is to define the initial measures to be taken by the organization in response to a disruptive event.

Response procedures should describe how the organization will respond to one or more types of disruptive events. Organizations may choose to have a single procedure with sections and/or annexes dealing with different types of incidents. Alternatively, separate procedures may be written for each type of incident.

Some response procedures may be implemented in advance of a disruptive event; for example, in the expectation of harm from a forthcoming tropical cyclone, wildfire, or malicious attack on the organization or a supply chain partner. In such circumstances, emphasis will be given to protecting and/or removing priority assets and to communicating the risk of harm to staff and to external organizations and authorities.

Each procedure should specify as a minimum:

a) The purpose and scope of the procedure;
b) Prioritize assets to be protected during the disruptive event;
c) Prioritize activities to be maintained during the disruptive event;

d) Measures to limit the form and extent of environmental damage caused by the disruptive event;
e) Situations/conditions in which each procedure will be implemented;
f) Criteria that will determine whether the disruptive event is to be classed as an incident, accident, emergency, crisis, and/or a disaster;
g) Criteria that will indicate the end of the response phase;
h) Roles and responsibilities of individuals and groups required to implement the procedure;
i) The organizational structure to be used, including the establishment of an incident command center, and links with external agencies such as the emergency services and occupational health and safety bodies;
j) Procedures for communicating within the organization to key external stakeholders including supply chain partners, the emergency services, local authorities, and the media; and
k) Contact details of all individuals responsible for implementing the procedure and others who need to be notified that the procedure is to be, or has been, implemented.

The organization should nominate a primary "owner" of each response procedure and should state who is responsible for reviewing, amending, and updating the procedure. The process of reviewing, amending, updating, and distributing procedures should be controlled.

NOTE: Response procedures are sometimes referred to as emergency response procedures.

C.4 Continuity Procedures

The purpose of a continuity procedure is to define the measures to be taken by the organization to maintain and/or re-establish priority activities of the organization and its supply chain partners.

Continuity procedures should describe how the organization will maintain and/or re-establish critical activities in the period immediately following the response/emergency phase. Organizations may choose to have a single procedure with sections and/or annexes dealing with different types of incident. Alternatively, separate procedures may be written for each type of incident.

Each procedure should specify as a minimum:

a) The purpose and scope of the procedure;
b) Priority assets to be protected during and immediately following the disruptive event;
c) Priority activities to be maintained during and immediately following the disruptive event;
d) Activities to be restored as a priority following the disruptive event;
e) Measures to limit the form and extent of environmental damage caused by the disruptive event;
f) Situations/conditions in which each continuity procedure will be implemented;
g) Criteria that will indicate the end of the continuity phase;
h) Roles and responsibilities of individuals and groups required to implement the procedure;

i) The organizational structure to be used including links with external agencies such as emergency services and occupational health and safety bodies;
j) Procedures for communicating within the organization, to key external stakeholders including supply chain partners, the emergency services, local authorities, loss adjusters/insurance companies, and the media; and
k) Contact details of all individuals responsible for implementing the procedure and others who need to be notified that the procedure is to be implemented.

The organization should nominate a primary "owner" of each continuity procedure and should state who is responsible for reviewing, amending, and updating the procedure. The process of reviewing, amending, updating, and distributing procedures should be controlled.

NOTE: Continuity procedures may run concurrently with response and recovery procedures.

C.5 Recovery Procedures

The purpose of a recovery procedure is to define the measures to be taken by the organization to recover from a disruptive event and thus ensure it is able to meet its strategic, operational, tactical, and reputational objectives.

Recovery procedures should describe how the organization will re-establish all necessary operational and support activities, replace damaged and/or destroyed assets and information, rebuild the brand and reputation of the organization, and assist staff to recover from the event. Organizations may choose to have a single procedure with sections and/or annexes dealing with different types of incidents. Alternatively, separate procedures may be written for each type of incident.

Each procedure should specify as a minimum:

a) The purpose and scope of the procedure;
b) Operational and support activities to be re-established and/or restored, and the priority of such restoration;
c) Assets including property, equipment, information, vehicles, and stores to be repaired and/or replaced, and the priority for such repair and replacement;
d) Assistance to staff affected, either physically or psychologically, by the disruptive event;
e) Actions to be taken to rebuild the organization's brand and reputation;
f) Actions to be taken to mitigate any environmental damage;
g) Situations/conditions in which each recovery procedure will be implemented;
h) Criteria that will indicate the end of the recovery phase;
i) Roles and responsibilities of individuals and groups who will be required to implement the procedure. It may be necessary to modify the normal procurement procedures in order to rapidly restore the organization's activities and assets;
j) The organizational structure to be used, including links with external agencies such occupational health and safety bodies, and loss adjusters/insurance companies; and
k) Procedures for communicating within the organization, to key external stakeholders including supply chain partners, the emergency services, local authorities, and the media.

The organization should nominate a primary “owner” of each recovery procedure, and should state who is responsible for reviewing, amending, and updating the procedure. The process of reviewing, amending, updating, and distributing procedures should be controlled.

NOTE 1: Recovery procedures may run concurrently with continuity procedures.

NOTE 2: Recovery procedures are sometimes referred to as recovery and restoration procedures.

PREVENTION AND MITIGATION TREATMENT PLAN	
Function / Activity:	
Risk:	Risk Reference Number:

	Mitigation Procedure
The Purpose and Scope of the Procedure	
The Assets to be Protected	
Objectives and Measures of Success	
Implementation Steps and Frequency	
Roles, Responsibilities and Authorities	
Communications Requirements	
Internal and External Interdependencies and Interactions	
Resource, Competency and Training Requirements	
Informational Flow and Documentation	

Received by:	Date:	Reviewed / Approved by:	Date:

RESPONSE TREATMENT PLAN		
Function / Activity:		
Risk:	Risk Reference Number:	
	Response Procedure	Owner
The Purpose and Scope		
Priority Assets to be Protected		
Priority Activities to be Maintained		
Measures to Limit Damage		
Situation /Conditions in Which Plan Will be Implemented		
Criteria for Classifying an Event		
Criteria for Indicating the End of The Response Plan		
Roles and Responsibilities of Individuals and Groups		

RESPONSE TREATMENT PLAN			
Organization Structure to be Used, Including Incident Command & External Links			
Procedures for Communication within the Organization			
Contact Details of All Individuals			
Received by:	Date:	Reviewed / Approved by::	Date:

CONTINUITY TREATMENT PLAN		
Function / Activity:		
Risk:		Risk Reference Number:
	Continuity Procedure	Owner
The Purpose and Scope		
Priority Assets to be Protected		
Priority Activities to be Maintained		
Activities to be Restored as a Priority After an Event		
Measures to Limit the Damages Caused by the Event		
Situation /Conditions in Which Plan Will be Implemented		
Criteria for Indicating the End of The Continuity Plan		
Roles and Responsibilities of Individuals and Groups		

<table>
<tr><th colspan="6">CONTINUITY TREATMENT PLAN</th></tr>
<tr><td>Organization Structure to be Used, Including Incident Command & External Links</td><td colspan="3"></td><td colspan="2"></td></tr>
<tr><td>Procedures for Communication Within the Organization</td><td colspan="3"></td><td colspan="2"></td></tr>
<tr><td>Contact Details of All Individuals Involved</td><td colspan="3"></td><td colspan="2"></td></tr>
<tr><td colspan="2">Received by:</td><td>Date:</td><td colspan="2">Reviewed / Approved by:</td><td>Date:</td></tr>
</table>

Annex D

(informative)

D Business Impact Analysis

Elimination of all risk is not possible. The risk assessment provides a thorough analysis of the levels of risk and the treatment methods required to bring risk to a level that is as low as reasonably practical. The costs and benefits of treating a risk and the potential to exploit opportunities will affect the determination of what treatment methods will bring risk to a level that is as low as reasonably practical. Residual risks need further consideration to develop contingency plans.

A business impact analysis (BIA) provides a structured approach to gaining information about the critical activities, functions, and processes of the organization and the associated resources necessary for an organization to mitigate the impacts of undesirable and disruptive events. The BIA identifies the likely and potential impacts from undesirable and disruptive events on the organization or its processes and the criteria to be used to quantify and qualify such impacts.

The criteria to measure and assess the financial, operational, customer, regulatory and/or reputational impacts need to be defined, accepted and used consistently to establish the recovery objectives for each organizational process. The result of this analysis is to identify time sensitive processes and the requirements to recover them in an acceptable timeframe.[2] The BIA:

a) Evaluates critical activities, functions, and processes and their role in achieving organizational objectives;
b) Determines the most critical activities, functions, and processes and the resources (assets) that are needed to achieve the desired outcome;
c) Prioritizes the critical activities, functions, and processes that must be operational to maintain an acceptable level of business functionality during and immediately following an unacceptable business interruption; and
d) Determines the time frames and resource requirements to maintain critical activities, functions, and processes following a risk event to restore operations to the level required to meet organizational objectives.

The organization may conduct a BIA on critical activities, functions, and processes related to its residual risk and develop contingency plans. The purpose of the BIA should be to determine:

a) Criticality - Every critical business function is identified (with related dependencies and interdependencies) and the impact of an undesirable or disruption event determined.

[2] Source: DRI International < https://www.drii.org/certification/professionalprac.php?lang=EN >

b) Maximum Downtime - Estimate the maximum downtime that can be tolerated while still maintaining viability. Management should determine the longest period of time that a critical process can be disrupted before recovery becomes unlikely.
c) Resource Requirements - Realistic recovery efforts require a thorough evaluation of the resources required to resume critical operations and related interdependencies as quickly as possible.

Timeframes and recovery objectives should consider:

a) The maximum period of time that an organization can tolerate the loss of capability of a critical business function, process, or asset.
b) The period of time a business' activities and resources must be recovered to an acceptable capability after a disruptive event, often defined in hours or days.
c) The point in time to which products, organizational activities, or data in a known, valid or integral state, can be restored from. Often viewed as the maximum amount of loss tolerance and defined in hours or days.

The output also includes:

a) Timeframe when the organization requires 100% of operational capability;
b) Prioritization of recovery resources;
c) Content for response and recovery strategies; and
d) Reset of product/service acceptable disruption periods, as needed.

The methodology should be tailored to the decision-making needs of the organization and achievement of organizational objectives. The following three figures present a generalized approach to conducting a business impact analysis.

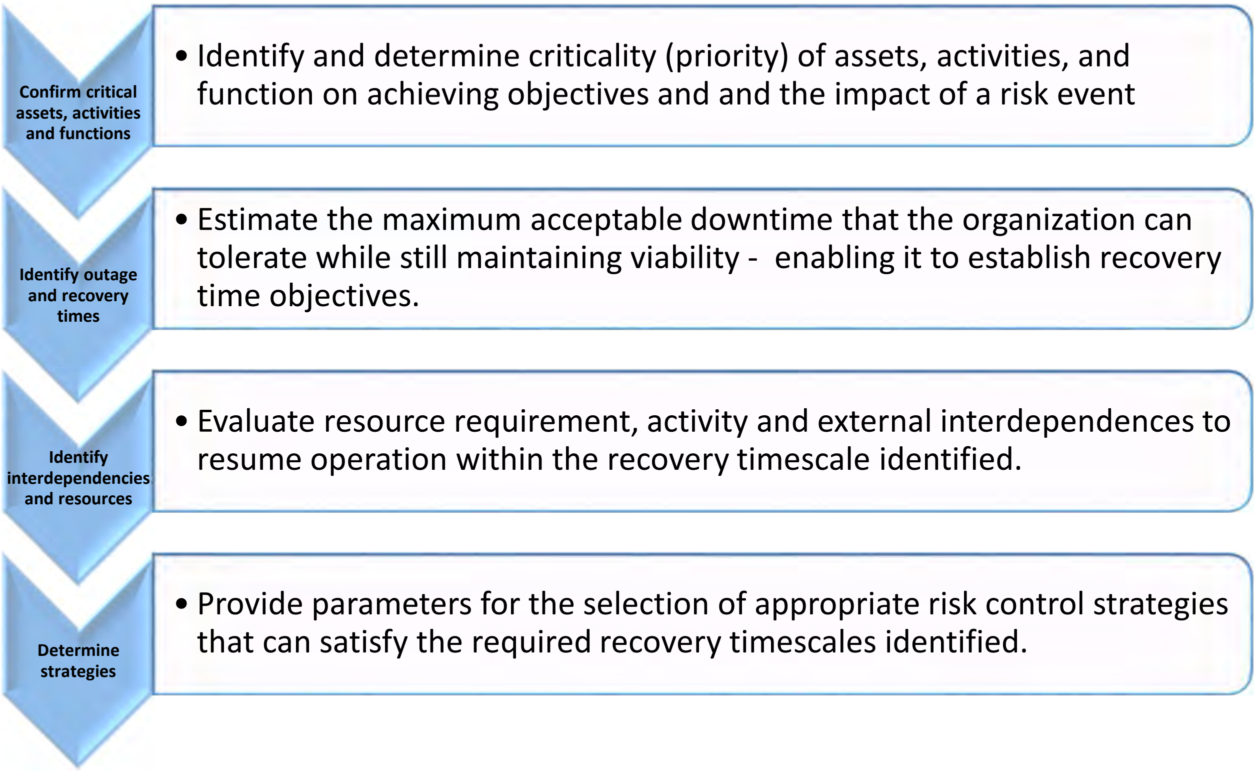
Confirm critical assets, activities and functions
• Identify and determine criticality (priority) of assets, activities, and function on achieving objectives and and the impact of a risk event
Identify outage and recovery times
• Estimate the maximum acceptable downtime that the organization can tolerate while still maintaining viability - enabling it to establish recovery time objectives.
Identify interdependencies and resources
• Evaluate resource requirement, activity and external interdependences to resume operation within the recovery timescale identified.
Determine strategies
• Provide parameters for the selection of appropriate risk control strategies that can satisfy the required recovery timescales identified.

Figure 3: Business Impact Analysis (BIA)

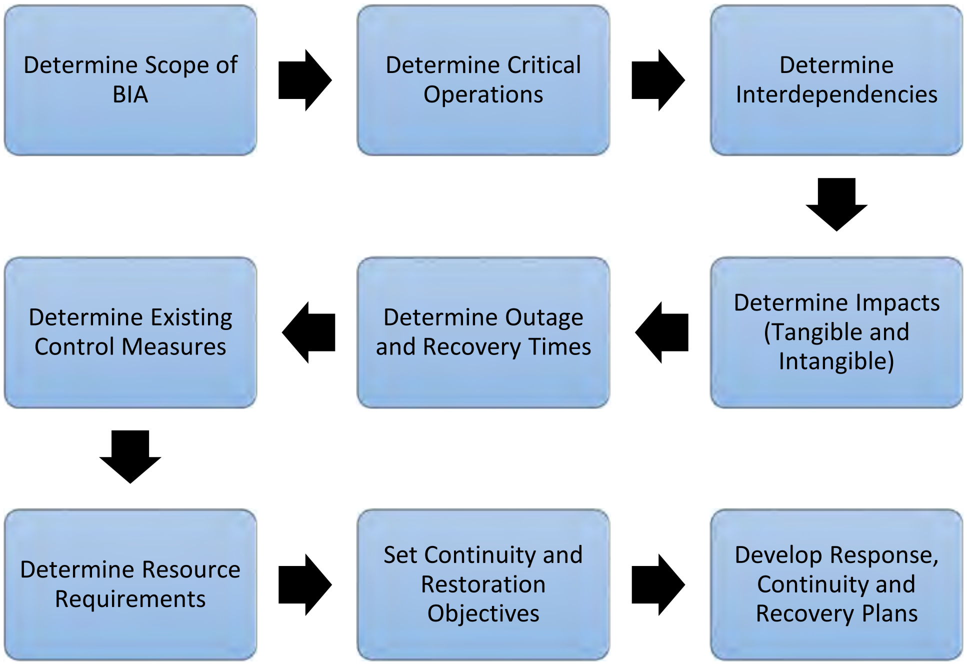
Determine Scope of BIA
Determine Critical Operations
Determine Interdependencies
Determine Impacts (Tangible and Intangible)
Determine Outage and Recovery Times
Determine Existing Control Measures
Determine Resource Requirements
Set Continuity and Restoration Objectives
Develop Response, Continuity and Recovery Plans

Figure 4: Example of BIA Methodology

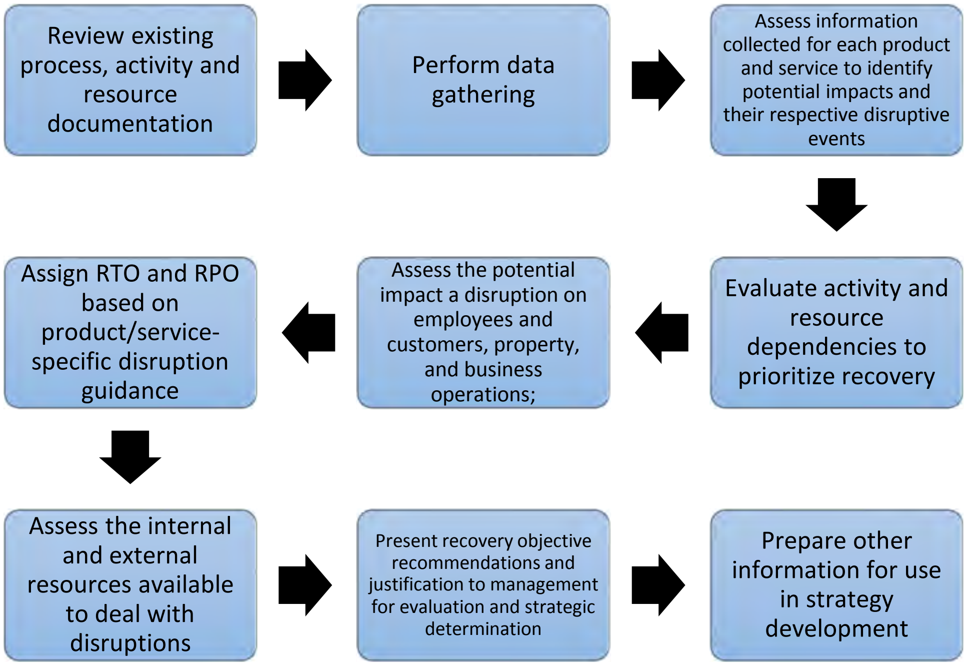
Review existing process, activity and resource documentation
Perform data gathering
Assess information collected for each product and service to identify potential impacts and their respective disruptive events
Evaluate activity and resource dependencies to prioritize recovery
Assess the potential impact a disruption on employees and customers, property, and business operations;
Assign RTO and RPO based on product/service-specific disruption guidance
Assess the internal and external resources available to deal with disruptions
Present recovery objective recommendations and justification to management for evaluation and strategic determination
Prepare other information for use in strategy development

Figure 5: Typical BIA Activities

Annex E

(informative)

E AN INTEGRATED MANAGEMENT SYSTEMS APPROACH

E.1 General

The management systems approach considers how local policies, culture, actions, or changes influence the state of the organization as a whole and its environment. The component parts of a system can best be understood in the context of relationships with each other, rather than in isolation. Therefore, a management system examines the linkages and interactions between the elements that compose the entirety of the system. The management systems approach systematically defines activities necessary to obtain desired results and establishes clear responsibility and accountability for managing key activities. This management systems standard provides requirements for establishing, implementing, operating, monitoring, reviewing, maintaining, and improving an organization's management system. An organization needs to identify and manage many activities in order to function effectively. Any activity which enables the transformation of inputs into outputs, that uses resources and is formally managed, can be considered to be a process. Often the output from one process directly forms the input to the next process.

The management systems approach for ORMS presented in this *Standard* encourages its users to emphasize the importance of:

a) Understanding an organization’s risk and business management requirements;
b) Establishing a policy and objectives to manage risks;
c) Implementing and operating controls to manage an organization’s risk and enhance resilience;
d) Monitoring and reviewing the performance and effectiveness of the ORMS, administratively and operationally; and
e) Continual improvement based on objective measurement.

This *Standard* adopts the "Plan-Do-Check-Act" (PDCA) model, which is applied to structure the security and resilience processes. Figure 6 illustrates how an ORMS takes as input the ORMS requirements and expectations of the interested parties and through the necessary actions and processes produces risk management outcomes that meet those requirements and expectations. Figure 6 also illustrates the links in the processes presented in this *Standard*.

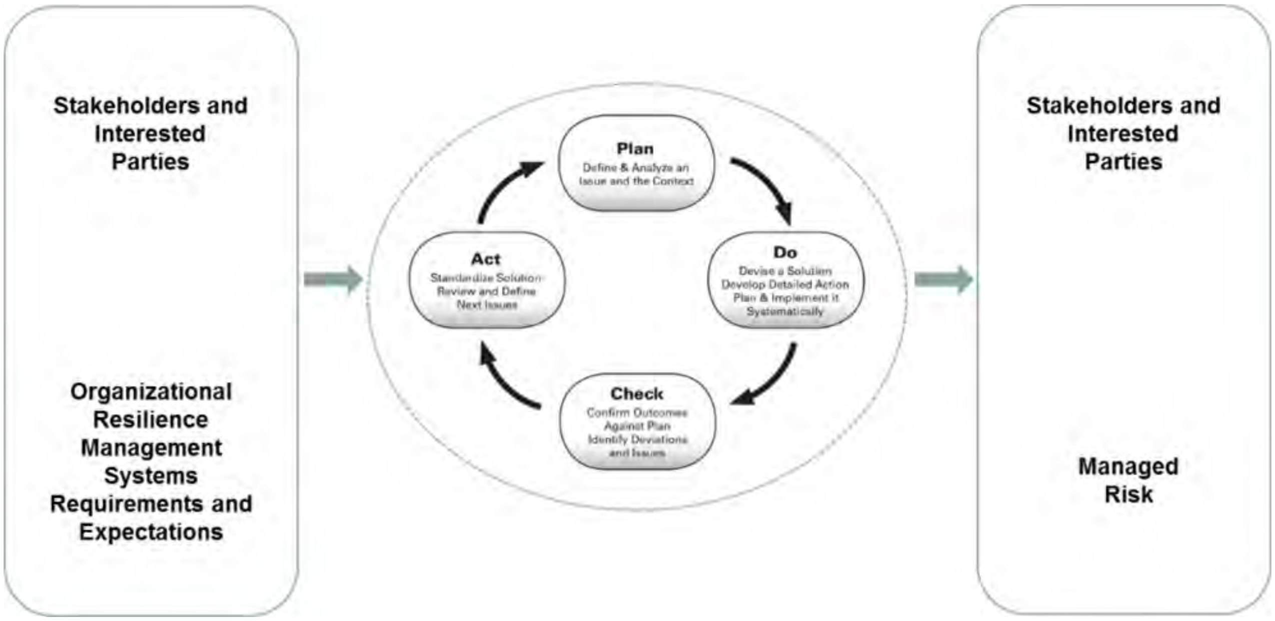
Stakeholders and Interested Parties
Organizational Resilience Management Systems Requirements and Expectations
Plan
Define & Analyze an Issue and the Context
Do
Devise a Solution Develop Detailed Action Plan & Implement it Systematically
Check
Confirm Outcomes Against Plan Identify Deviations and Issues
Act
Standardize Solution Review and Define Next Issues
Stakeholders and Interested Parties
Managed Risk

Figure 6: Plan-Do-Check-Act Model

PLAN (establish the management system)	Establish management system policy, objectives, processes, and procedures relevant to managing operations and improving risk management to deliver results in accordance with an organization's overall policies and objectives.
DO (implement and operate the management system)	Implement and operate the management system policy, controls, processes, and procedures.
CHECK (monitor and review the management system)	Assess and measure process performance against management system policy, objectives, and practical experience and report the results to management for review.
ACT (maintain and improve the management system)	Take corrective and preventive actions, based on the results of the internal management system audit and management review, to achieve continual improvement of the management system.

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

a) Set measurable objectives and targets;
b) Monitor, measure, and evaluate progress;
c) Identify, prevent or remedy problems as they occur;
d) Assess competence requirements and train persons working on the organizations behalf; and
e) Provide top management with a feedback loop to assess progress and make appropriate changes to the management system.

Furthermore, it contributes to information management within the organization, thereby improving operational efficiency.

This *Standard* is designed so that it can be integrated with quality, safety, environmental, information security, resilience, risk, security, and other management systems within an organization. A suitably designed management system can thus satisfy the requirements of all these standards. Organizations that have adopted a management systems approach (e.g., according to ANSI/ASIS PSC.1-2012, ISO 9001:2015, ISO 14001:2015, ISO/IEC 27001:2013, ISO 28000:2007, ISO 22301:2012, OHSAS 18001:2007) may be able to use their existing management system as a foundation for the ORMS as prescribed in this *Standard*. Conformance with this *Standard* can be verified by an auditing process that is compatible and consistent with the methodology of ISO/IEC 17021:2011, *Conformity assessment – Requirements for bodies providing audit and certification of management systems*.

E.2 Scope of the ORMS

This scope defines the boundaries, extent and applicability of the ORMS within the organization. It also details any exclusions from this *Standard's* requirements and the justification for the exclusions. Exclusions as well as risks, activities and functions considered outside the scope are not part of the ORMS.

The scope defines what your ORMS covers within your organization and its supply chain. The scope of the ORMS can include the whole organization, specific risk sources, and functions within the organization and its supply chain, specific divisions of the organization, or one or more functions across a group of organizations. All processes, activities and functions considered within the scope are managed by the ORMS including those of supply chain partners and subcontractors.

When defining scope, the organization should consider:

- External and internal issues that are relevant to the pursuit of the organization's objectives;
- The risk profile and risk environment;
- Legal, regulatory, and contractual obligations as well as voluntary commitments;
- The culture and maturity of the organization and relevant stakeholders;
- The resources, capabilities, and the ability to achieve intended outcomes;
- Requirements and perceptions of stakeholder;

- Commercial and financial objectives and constraints;
- The products and services of the organization; and
- The organization's pursuit of opportunities and enhancement of its resilience.

The organization should revisit its scope statement after it conducts the risk assessment to determine if the boundaries and applicability of the ORMS has been set to address the organization's and its stakeholder's needs to manage risk, to pursue opportunities and prevent harm.

The scope statement can be expanded, so in many cases, it is advisable to initially set a scope based on resource constraints as well as achievable goals and timelines. When the management framework of the ORMS is established, it can then be used to address a broader range of issues in a continual improvement fashion.

Annex F

(informative)

F QUALIFIERS TO APPLICATION

The adoption and implementation of a range of ORMS techniques in a systematic manner can contribute to optimal outcomes for all stakeholders and affected parties. However, adoption of this *Standard* will not by itself guarantee optimal security and resilience outcomes. To achieve its objectives, the ORMS should incorporate the best available practices, techniques, and technologies, where appropriate and where economically viable. The cost-effectiveness of such practices, techniques, and technologies should be taken fully into account.

This *Standard* does not establish absolute requirements for security and resilience performance beyond commitments in the organization's policy to:

a) Comply with applicable legal, regulatory, and contractual obligations as well as voluntary commitments;
b) Support prevention of undesirable and disruptive events and risk minimization; and
c) Promote continual improvement.

The main body of this *Standard* contains only those generic criteria that may be objectively audited. Guidance on supporting ORMS techniques is contained in the other annexes of this document.

This *Standard*, like other management standards, is not intended to be used to create non-tariff trade barriers or to increase or change an organization's legal obligations. Indeed, compliance with a standard does not in itself confer immunity from legal obligations. For organizations that so wish, an external or internal auditing process may verify compliance of their ORMS to this *Standard*. Verification may be by an acceptable first-, second-, or third-party mechanism. Verification does not require third-party certification.

This *Standard* does not include requirements specific to other management systems, such as those for quality, occupational health and safety, or resilience management – though its elements can be aligned or integrated with those of other management systems. It is possible for an organization to adapt its existing management system(s) to establish an ORMS that conforms to the criteria of this *Standard*. It should be understood, however, that the application of various elements of the management system might differ depending on the intended purpose and the stakeholders involved.

The level of detail and complexity of the ORMS, the extent of documentation, and the resources devoted to it will be dependent on a number of factors – such as the scope of the system; the size of an organization; and the nature of its activities, products, services, and supply chain. This may be the case in particular for small and medium-sized enterprises.

This *Standard* provides a common set of criteria for ORMS programs. Terminology used in this *Standard* emphasizes commonality of concepts, while acknowledging nuances in term usage in the various disciplines. Risk assessment is the process of risk identification, analysis, and evaluation.

Annex G

(informative)

G BIBLIOGRAPHY

G.1 ASIS International Publications[3]

ASIS International (2008), *ASIS International glossary of security terms*. [Online]. Available: <http://www.asisonline.org/Membership/Library/Security-Glossary/Pages/Security-Glossary-A.aspx> Accessed 2011, August 19.

G.2 National Standards Publications[4]

ASIS International (2014), ANSI/ASIS SPC.2-2014, *Auditing Management Systems: Risk, Resilience, Security, and Continuity—Guidance for Application.*

ASIS International (2012), ANSI/ASIS SPC.4-2012, *Maturity Model for the Phased Implementation of the Organizational Resilience Management System.*

ASIS International (2012), ANSI/ASIS SCRM.1-2014, *Supply Chain Risk Management: A Compilation of Best Practices.*

ASIS International (2015), ANSI/ASIS/RIMS RA.1-2015, *Risk Assessment.*

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

[4] These documents are available at < http://www.asisonline.org >.

Annex H

(informative)

H REFERENCES

H.1 Government Publications

[FIPS 200] Federal Information Processing Standard (FIPS) 200, Minimum Security Requirements for Federal Information and Information Systems, 2006, http://csrc.nist.gov/publications/fips/fips200/FIPS-200-final-march.pdf.

[NIST SP 800-161] Supply Chain Risk Management Practices for Federal Information Systems and Organizations, April 2016, http://dx.doi.org/10.6028/NIST.SP.800-161.

ASIS INTERNATIONAL
Advancing Security Worldwide®

1625 Prince Street
Alexandria, Virginia 22314-2882
USA
+1.703.519.6200
Fax: +1.703.519.6299
www.asisonline.org

ISBN 978-1-934904-82-4
9 781934 904824