



**All Hazards Risk Management
Systems *Draft* Best Practices
Standard:
Requirements with Guidance for Use**

***A practical management systems approach to security,
preparedness, response, business/operational
continuity and recovery for disruptive incidents
resulting in an emergency, crisis, or disaster***

This draft standard has been placed on the ASIS Guideline Web page to provide for a public review and comment period. This public review and comment period will run for 60 days from August 17 until October 16, 2007. To submit comments, one must complete the comment form that can be found at ASIS Guideline Web page. Should you have questions, please email guidelines@asisonline.org.

ASIS International (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, or reliance on this document. In issuing 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 circumstance.

This Guideline is not intended to be, and shall not be construed as, a mandatory standard of care. It does not purport to establish, nor does it establish, any industry standard or standard of due care. This Guideline has been developed by consensus, by a not-for-profit, voluntary membership organization and, as such, does not have the force of regulations or guidelines issued by governmental agencies.

This guideline does not purport to address, nor could it address, all possible remedies or methodologies. Compliance with this guideline does not necessarily prove due care, nor does non-compliance with, or disregard of, this guideline necessarily prove negligence. Security is situational. The efficacy of any security program is driven by a range of situational parameters. Practitioners must be knowledgeable about the industry and federal, state, or local laws (including case law) applicable to the jurisdiction(s) in which they practice and to the particular situation.

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

Copyright 2007 by ASIS International

ISBN X-XXXXXX-XX-X

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

10 9 8 7 6 5 4 3 2 1

Contents	Page
Foreword	iv
0 Introduction	v
0.1 Summary	v
0.2 All hazards approach	v
0.3 General	vi
0.4 Process approach	vii
0.5 Compatibility with other management systems	ix
0.6 Qualifications	x
0.7 Terminology conventions	xi
1 Scope	1
2 Normative references	1
3 Terms and definitions	2
4 All hazards risk management system requirements	13
4.1 General requirements	13
4.1.1 Scope of all hazards management system	13
4.2 All hazards risk management policy	14
4.2.1 Policy statement	14
4.2.2 Management commitment	14
4.3 Planning	15
4.3.1 Risk assessment and impact analysis	15
4.3.2 Legal and other requirements	15
4.3.3 Objectives, targets and program(s)	15
4.4 Implementation	16
4.4.1 Resources, roles, responsibility and authority	16
4.4.2 Competence, training and awareness	17
4.4.3 Communication and warning	17
4.4.4 Documentation	18
4.4.5 Control of documents	18
4.4.6 Operational control	19
4.4.7 Incident preparedness and response	19
4.5 Checking	20
4.5.1 Monitoring and measurement	20
4.5.2 Evaluation of compliance and system performance	20
4.5.2.1 Evaluation of compliance	20
4.5.2.2 Exercises and testing	21
4.5.3 Nonconformity, corrective action and preventive action	21
4.5.4 Control of records	21
4.5.5 Internal audits	22
4.6 Management review	22
4.6.1 General	22
4.6.2 Review input	22
4.6.3 Review output	23
4.6.4 Maintenance	23
4.6.5 Continual improvement	23
Annex A (informative) Guidance on the use of the standard	24
Annex B (informative) Correspondence between ISO 9001:2000, ISO 14001:2004, ISO 27001:2005 and the ASIS International Standard of Best Practices	40
Bibliography	43

Foreword

ASIS International (ASIS) is the preeminent organization for security professionals, with more than 35,000 members worldwide. Founded in 1955, ASIS is dedicated to increasing the effectiveness and productivity of security professionals by developing educational programs and materials that address broad security interests. ASIS also advocates the role and value of the security management profession to business, the media, government entities, and the public. By providing members and the security community with access to a full range of programs and services, ASIS leads the way for advanced and improved security performance.

The work of preparing ASIS Standards is carried out through the ASIS International Standards and Guidelines Commission committees. Each member interested in a subject for which a technical committee has been established has the right to be represented on that committee.

The Guidelines Program of ASIS International has received a Designation award under the Support Anti-terrorism by Fostering Effective Technology Act of 2002 (the SAFETY Act) from the U.S. Department of Homeland Security. Specifically, the SAFETY Act designation limits ASIS' liability for acts arising out of the use of the guidelines in connection with an act of terrorism and precludes claims of third party damages against organizations using the guidelines as a means to prevent or limit the scope of terrorist acts.

The ASIS International *All Hazards Risk Management Systems Best Practices Standard* incorporates the guidance provided in the ASIS International *Business Continuity Guideline: A Practical Approach for Emergency Preparedness, Crisis Management, and Disaster Recovery, 2005*. For additional information, the *Business Continuity Guideline* should be consulted. This best practices standard provides generic auditable criteria and informative guidance on prevention, preparedness (readiness), mitigation, response and recovery from disruptive incidents with a potential to escalate into an emergency, crisis or disaster.

ASIS International Commission on Standards and Guidelines Members

F. Mark Geraci , CPP™, Chair Senior Director, Corporate Security Bristol-Myers Squibb Co.	
Steven K. Bucklin President/CEO Glenbrook Security Services Inc.	Daniel H. Kropp , CPP™, Vice Chair Director, Physical Security Towers Perrin
John C. Cholewa III , CPP™ Director – Corporate Security Embarq Corporation	Robert W. Jones Chief Compliance Officer and Director of Corporate Security Praxair Inc.
Cynthia P. Conlon , CPP™ President Conlon Consulting Corporation	Michael E. Knoke , CPP™ Director Express Scripts, Inc.
Michael A. Crane , CPP™ Executive VP and General Counsel IPC International	Dr. Marc H. Siegel Director Security and Environmental Management Systems International (SEMSI) and Adjunct Professor San Diego State University

0 Introduction

0.1 Summary

This *Standard of Best Practices* (referred to as the “*Standard*”) has applicability in the private, not-for-profit and public sector environments. It is a tool to allow organizations to consider the factors and steps necessary to prepare for and respond to a disruptive incident (emergency, crisis or disaster) so that it can manage and survive the event and take all appropriate actions to help ensure the organization’s continued viability. The body of this document provides generic auditable criteria to establish, check, maintain and improve a management system to enhance prevention, preparedness (readiness), mitigation, response and recovery from disruptive incidents. Annexes provide informative guidance on system planning, implementation, testing, maintenance and improvement.

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) providing top management driven vision and leadership for strategies to protect assets and assure the resilience of the organization;
- b) identifying and evaluating assets, services and functions to determine the parts of the operations and business that are critical to its short and long term success;
- c) identifying potential hazards and threats, and assessing risks and impacts;
- d) mitigating the impact of a wide variety of hazards, including natural disasters, technology and environmental accidents, terrorism and extreme crime, and weapons of mass destruction;
- e) understanding the roles and responsibilities needed to protect assets and further resilience;
- f) managing necessary incident/emergency preparedness and response resources;
- g) developing mutual aid agreements;
- h) developing and maintaining incident/emergency preparedness and response plans, and associated operational procedures;
- i) developing and conducting training and exercises to support and evaluate incident/emergency preparedness and response plans and operational procedures;
- j) developing and conducting training programs for security guards to implement emergency preparedness and response plans and operations procedures;
- k) ensuring that relevant employees, customers, suppliers and other stakeholders are aware of the incident/emergency preparedness and response arrangements and, where appropriate, have confidence in their application;
- l) developing internal and external communications procedures including response to requests for information from the media or the public;
- m) establishing metrics for measuring and demonstrating success;
- n) documenting the key resources, infrastructure, tasks and responsibilities, required to support critical operational functions; and
- o) establishing processes that ensure the information remains current and relevant to the changing risk and operational environments.

The generic criteria of this *Standard* provides a framework for any organization in the private, not-for-profit and public sectors to tailor its application and implementation to address the organization’s particular needs and special circumstances.

0.2 All hazards approach

Applying this high-level management *Standard* affords protection from and response to risks of unintentionally, intentionally, and naturally caused emergencies, crises and disasters that disrupt and have consequences on organizational and societal functions. It uses an all-hazards perspective covering the phases of emergency and crisis management before, during, and after a disruptive incident. Its generic criteria are applicable to all types and sizes of organizations and accommodate diverse geographical, cultural, and social conditions.

An all hazards approach emphasizes resilience and protection of critical assets, human, environmental and physical. It assumes an inclusive view of protection from risk (referred to as “security”) assuring consequence management regardless of the trigger of a disruptive event. This voluntary *Standard* provides a common set of cross-disciplinary criteria for prevention, preparedness, mitigation, disaster management, emergency management, environmental management and business/operational continuity programs.

The all hazards approach avoids segregating or “siloeing” risks and provides an overall risk profile allowing the organization to better understand the relationships between risks and identify solutions to problems. It leverages the perspectives, knowledge and capabilities of divisions and individuals within an organization. Because of the relatively low probability and yet potentially high consequence nature of many natural, intentional, or unintentional threats and hazards that an organization may face, an all hazards approach allows an organization to establish priorities that address its individual needs for risk management within an economically sound context.

0.3 General

The recent wave of natural disasters, environmental accidents, technology mishaps and man-made crises have demonstrated that incidents can and will happen, impacting the public and private sectors alike. The challenge goes beyond the mere emergency response plan or disaster management activities that were previously employed. Organizations now must engage in a comprehensive and systematic process of prevention, preparedness, mitigation, response, continuity and recovery. It is no longer enough to draft a response plan that anticipates naturally, accidentally, or intentionally caused disaster or emergency scenarios. Today’s threats require the creation of an on-going, dynamic and interactive process that serves to assure the continuation of an organization’s core activities before, during, and most importantly, after a major crisis event.

This *Standard* provides organizations of all sizes and types with the elements needed to achieve and demonstrate proactive risk reduction and security performance related to their physical facilities, services, activities, products, supply chains, and operational (business) continuity. They do so within the context of:

- a) increasing security risks and threats;
- b) more stringent legislation and regulation;
- c) more competitive business realities;
- d) increasing interdependencies in society (on an organizational, functional, or jurisdictional level);
- e) heightened awareness of the need for adequate emergency response and remediation planning;
- f) concerns of interested and affected parties; and,
- g) the need to assure operational continuity and resilience.

A disruptive incident not properly managed can rapidly escalate into an emergency, crisis or even a disaster. Preparing for an incident before it occurs can minimize its impact. In addition to potentially resulting in significant physical or environmental damage, injury or loss of life an unmanaged disruptive incident can taint an organization’s image, reputation or brand. This *Standard* provides a framework for organizations to successfully management a disruptive incident by developing a strategy and action plan to safeguard its interests and those of its stakeholders.

Proactive planning and preparation for potential incidents and disruptions will diminish both the impact and length of the disruption. The holistic management process can help avoid and minimize the suspension of critical services and operations, thereby allowing return to normal services and operations as rapidly as possible.

It is simply good business for an organization to protect its physical 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 and shareholders 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 crisis prevention, mitigation and management. This will ensure that all concerned understand who makes decisions, how the decisions are implemented, and what the roles and responsibilities of participants are. Personnel used for crisis management should be assigned to perform these roles as part of their normal duties 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. The vast majority of the national critical infrastructure is owned and operated by private sector organizations and it is these organizations that serve a critical function to society that this document is particularly relevant.

This *Standard* enables an organization to:

- a) develop a preparedness and response/continuity/recovery policy;
- b) establish objectives, procedures, and processes to achieve the policy commitments;
- c) assure competency, awareness and training;
- d) set metrics to measure performance and 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.

The overall aim of this *Standard* is to support prevention and/or mitigation of risks and threats, and recovery from such risks and threats, in balance with socio-economic needs, and to improve continuity and resilience. It describes the criteria for an organization's all hazards risk management system that can be used for auditing the organization's conformity with the management system as specified in this document. All hazards risk management encompasses a full range of issues, including those with strategic and competitive implications. Demonstration of successful implementation of this *Standard* can be used by an organization to assure interested and affected parties that an appropriate all hazards risk management system is in place.

0.4 Process approach

The management systems approach encourages organizations to analyze organizational and stakeholder requirements, define the processes that contribute to the achievement of performance that is acceptable to the organization and its stakeholders, and keep these processes under control. A management system can provide the framework for continual improvement to increase the probability of enhancing security, preparedness, response, continuity and resilience. It provides confidence to the organization and its customers that the organization is able to provide a safe and secure environment that fulfills organizational and stakeholder requirements.

This *Standard* adopts a process approach for establishing, implementing, operating, monitoring, reviewing, maintaining and improving an organization's all hazards risk management system. An organization needs to identify and manage many activities in order to function effectively. Any activity using resources and managed in order to enable the transformation of inputs into outputs can be considered to be a process. Often the output from one process directly forms the input to the next process.

The application of a system of processes within an organization, together with the identification and interactions of these processes, and their management, can be referred to as a "process approach". The process approach for all hazards risk management presented in this *Standard* encourages its users to emphasize the importance of:

- a) understanding an organization's risk, security, preparedness, response, continuity and recovery requirements and the need to establish a policy and objectives for their management;

- b) implementing and operating controls to manage an organization's risks in the context of the organization's overall operational and business risks;
- c) monitoring and reviewing the performance and effectiveness of the all hazards risk management system; and
- d) continual improvement based on objective measurement.

This *Standard* adopts the "Plan-Do-Check-Act" (PDCA) model, which is applied to structure the all hazards risk management system processes. The PDCA model is sometimes referred to as the APCI (Assess-Protect-Confirm-Improve) Model. Figure 1 illustrates how an all hazards risk management system takes as input the all hazards risk management 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 1 also illustrates the links in the processes presented in Section 4.

This *Standard* provides an organization with the assurance that its all hazards risk management performance not only meets, but will also continue to meet, its legal and policy requirements. It provides an organization with the elements of an effective and structured management system that can be integrated with other management requirements and help organizations achieve security, preparedness, response, continuity and recovery objectives, as well as economic goals. A formal approach of a structured management system can contribute directly to the business capability and credibility of the organization.

This *Standard* is designed so that it can be integrated with quality, safety, environmental and other management systems within an organization. Organizations that have adopted a process approach to management systems (e.g. according to ISO 9001:2000, ISO 14001:2004 and/or ISO/IEC 27001:2005) may be able to use their existing management system as a foundation for an all hazards risk management system as prescribed in this *Standard*.

Compliance with this security, incident preparedness and continuity management *Standard* can be verified by an auditing process that is compatible and consistent with the methodology of 9001:2000, ISO 14001:2004 and/or ISO/IEC 27001:2005, and the PDCA Model . This *Standard* provides a robust model for implementing the principles governing risk assessment, system design and implementation, all hazards risk management and reassessment.

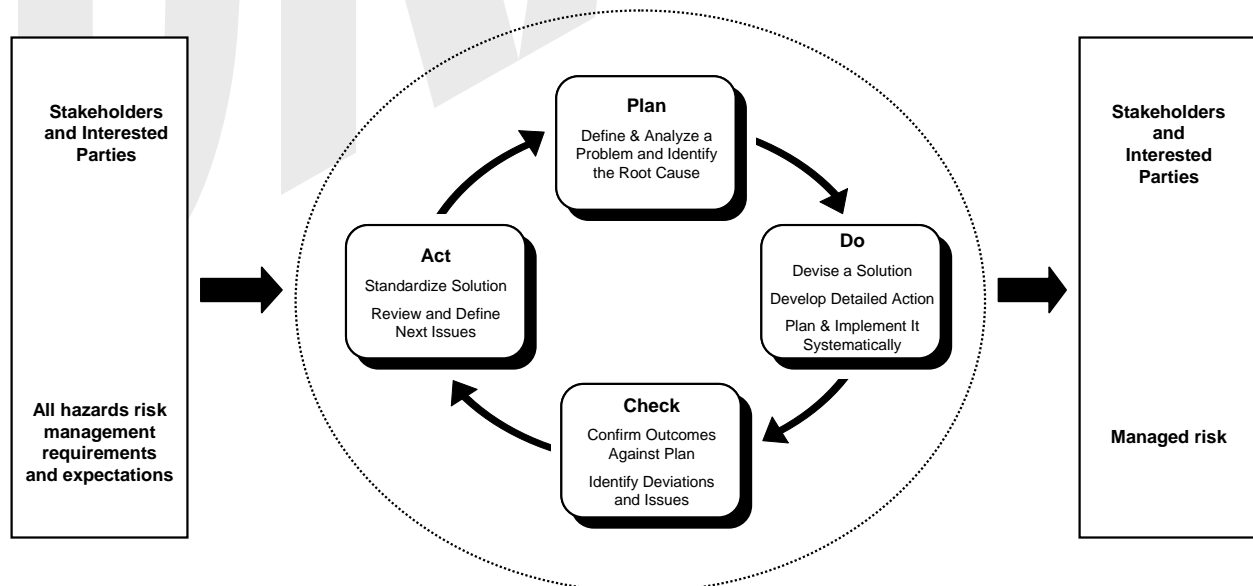


Figure 1: Plan-Do-Check-Act Model

<p>Plan (establish the management system)</p>	<p>Establish management system policy, objectives, processes and procedures relevant to managing risk and improving security, incident preparedness, response, continuity and recovery and to deliver results in accordance with an organization’s overall policies and objectives.</p>
<p>Do (implement and operate the management system)</p>	<p>Implement and operate the management system policy, controls, processes and procedures.</p>
<p>Check (monitor and review the management system)</p>	<p>Assess and, where applicable, measure process performance against management system policy, objectives and practical experience and report the results to management for review.</p>
<p>Act (maintain and improve the management system)</p>	<p>Take corrective and preventive actions, based on the results of the internal management system audit and management review or other relevant information, to achieve continual improvement of the management system.</p>

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 repair problems as they occur;
- d) train personnel; 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.

0.5 Compatibility with other management systems

This *Standard* is aligned with ISO 9001:2000, ISO 14001:2004 and ISO/IEC 27001:2005 in order to support consistent and integrated implementation and operation with related management standards. One suitably designed management system can thus satisfy the requirements of all these standards.

For example, this *Standard* may be applied in parallel to or integrated with ISO 14001:2004 *Environmental management systems – Requirements with guidance for use*. The all hazards consequence management approach contains all the elements required for implementation of the ISO 14001:2004. In order to conduct a parallel or integrated application, the risk assessment and impact analysis should include consideration of:

- environmental aspects: elements of an organization’s activities or products or services that can interact with the environment. A significant environmental aspect has or can have a significant environmental impact.
- environmental impact: any change to the environment, whether adverse or beneficial, wholly or partially resulting from an organization’s environmental aspects.

Reduction, removal and management of an organization’s hazardous materials will provide proactive benefits from both the environmental and security perspectives by providing protection from and response to risks of unintentionally, intentionally, and naturally caused events.

0.6 Qualifications

The adoption and implementation of a range of security, incident preparedness and continuity management 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, preparedness and response outcomes. In order to achieve its objectives, the all hazards risk management system should encourage organizations to consider implementation of 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, preparedness, response, continuity or recovery performance beyond commitments, in the organization's policy to:

- a) compliance with applicable legal requirements and with other requirements to which the organizations subscribes,
- b) critical risk prevention and minimization, and;
- c) continual improvement.

The main body of this *Standard* contains only those criteria that may be objectively audited. Guidance on supporting all hazards risk management techniques is contained in the 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 all hazards risk management system to this *Standard*. Verification may be by an acceptable first-, second-, or third-party organization. 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 financial risk 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) in order to establish an all hazards risk management system 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 all hazards risk management system, 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 and services. This may be the case in particular for small and medium-sized enterprises.

0.7 Terminology conventions

The terminology conventions in Table 2 are in accordance with ISO/IEC – Directives Part 2: *Rules for the structure and drafting on International Standards, Annex H, Verbal forms for the expression of provisions*, 2004.

Table 1 — Verbal forms for the expression of provisions

Verbal form	Usage (ISO/IEC – Directives Part 2: <i>Rules for the structure and drafting on International Standards</i>)
shall	Auditable requirements of a document – “used to indicate requirements strictly to be followed in order to conform to the document and from which no deviation is permitted.”
should	Recommendations – “used to indicate that among several possibilities one is recommended as particularly suitable, without mentioning or excluding others, or that a certain course of action is preferred but not necessarily required, or that (in the negative form) a certain possibility or course of action is deprecated but not prohibited.”
may	Permission – “used to indicate a course of action permissible within the limits of the document.”
can	Possibility and capability – “used for statements of possibility and capability, whether material, physical or causal.”

Items presented in lists shall not be construed to be exhaustive, unless otherwise stated. Nor shall the order of the list be viewed as specifying a sequence or priority, unless so stated. The generic nature of this *Standard* allows for organization to include additional items as well as designation a sequence or priority based on the specific operating conditions and circumstances of the organization.

All Hazards Risk Management Systems - Requirements with Guidance for Use

1 Scope

This Standard of Best Practices specifies requirements for an all hazards risk management system to enable an organization to develop and implement a policy, objectives and programs taking into account legal requirements and other requirements to which the organization subscribes and information about significant hazards and threats that might impact its, and its stakeholders, critical assets, physical, environmental and human. It applies to risks and/or their impacts that the organization identifies as those it can control and those which it can influence or reduce their impact. 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 all hazards risk management system;
- b) assure itself of its conformity with its stated all hazards risk management policy;
- 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 all hazards risk management system by an external organization.

All the requirements in this *Standard* are intended to be incorporated into any type of organization's all hazards risk management system. It provides all the elements required to integrate management, technology, facilitates, processes and people into the security culture and all hazards risk management system of an organization. The extent of the application will depend on factors such as the risk tolerance 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, applicable to all types of organizations (or parts thereof) regardless of size and nature of operation. It provides guidance for organizations to develop their own specific performance criteria enabling the organization to tailor design and implement an all hazards risk management system appropriate to its needs and that of its stakeholders.

This Standard also provides, in Annex A, informative guidance on its use.

2 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO Guide 73:2002, *Risk management – Vocabulary – Guidelines for use in standards*

For parallel or integrated application of a quality management system:

ISO 9001:2000, *Quality management systems — Requirements*

For parallel or integrated application of an environmental management system:

ISO 14001:2004, *Environmental management systems – Requirements with guidance for use*

For parallel or integrated application of an information security management system:

ISO/IEC 27001:2005, *Information technology — Security techniques — Information security management systems — Requirements*

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC Guide 73 and the following definitions apply.

3.1

all hazards risk management

systematic and coordinated activities and practices through which an organization optimally manages its risks, and the associated potential threats and impacts there from

3.2

all hazards risk management program

ongoing management and governance process supported by top management and resourced to ensure that the necessary steps are taken to identify the impact of potential losses, maintain viable recovery strategies and plans, and ensure continuity of functions/products/services through exercising, rehearsal, testing, training, maintenance and assurance

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

asset

anything that has value to the organization

[ISO/IEC 13335-1:2004]

3.5

auditor

person with competence to conduct an audit

[ISO 9001:2000]

3.6

continual improvement

recurring process of enhancing the all hazards risk management system in order to achieve improvements in overall all hazards risk management performance consistent with the organization's all hazards risk management policy

NOTE: The process need not take place in all areas of activity simultaneously

3.7

corrective action

action to eliminate the cause of a detected nonconformity

[ISO 14001:2004]

3.8

critical activity

any function or process that is essential for the organization to deliver its products and/or services

[ISO/PAS 22399:2007]

3.9

criticality assessment

a process designed to systematically identify and evaluate an organization's assets based on the importance of its mission or function, the group of people at risk, or the significance of a disruption on the continuity of the organization

3.10

consequence

outcome of an event

NOTE 1: There can be more than one consequence from one event.

NOTE 2: Consequences can range from positive to negative.

NOTE 3: Consequences can be expressed qualitatively or quantitatively.

[ISO/IEC Guide 73]

3.11

crisis

any incident(s), human-caused or natural, resulting in an unstable condition involving an impending abrupt or significant change that requires urgent attention and action to protect life, property, or the environment

3.12

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

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.

3.13

crisis management team

group of individuals functionally responsible for directing the development and execution of the response and operational continuity plan, declaring an 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.

3.14

damaging potential

harmful potential of an event, whether anticipated or unanticipated, that would impact on the ability of the organization to function effectively, cause critical harm to infrastructure, result in significant human or property losses to the organization or its stakeholders, or cause adverse effects to the reputation or integrity of the organization

3.15

disaster

event that causes great damage or loss

[ISO/PAS 22399:2007]

3.16

disruption

incident, whether anticipated (e.g., hurricane) or unanticipated (e.g., a blackout or earthquake) which disrupts the normal course of operations at an organization location

NOTE: A disruption can be caused by either positive or negative factors that will disrupt normal operations.

[ISO/PAS 22399:2007]

3.17

document

information and supporting medium

NOTE: The medium can be paper, magnetic, electronic or optical computer disc, photography or master sample, or a combination thereof

[ISO 9000:2000]

3.18

emergency

sudden, urgent, usually unexpected occurrence or event requiring immediate action

NOTE: An emergency is usually a disruptive event or condition that can often be anticipated or prepared for but seldom exactly foreseen.

[ISO/PAS 22399:2007]

3.19

exercising

evaluating all hazards risk 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 all hazards risk 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 an 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.

3.20

evacuation

organized, phased, and supervised dispersal of people from dangerous or potentially dangerous areas

[ASIS International Business Continuity Guideline: 2004]

3.21

event

occurrence of a particular set of circumstances

NOTE 1: The event can be certain or uncertain.

NOTE 2: The event can be a single occurrence or a series of occurrences.

NOTE 3: The probability associated with the event can be estimated for a given period of time.

[ISO/IEC Guide 73]

3.22

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

3.23

hazard

possible source of danger, or conditions physical or operational, that have a capacity to produce a particular type of adverse effects

[ISO/PAS 22399:2007]

3.24

impact

evaluated consequence of a particular outcome

[ISO/PAS 22399:2007]

3.25

impact analysis

process of analyzing all operational functions and the effect that an operational interruption might have upon them

[ISO/PAS 22399:2007]

3.26

incident

event that might be, or could lead to, an operational interruption, disruption or loss, and which if not managed can escalate into an emergency, crisis or disaster

3.27

incident 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

[ISO/PAS 22399:2007]

3.28

integrity

the property of safeguarding the accuracy and completeness of assets

[ISO/IEC 13335-1:2004]

3.29

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

3.30

management plan

clearly defined and documented plan of action for use at the time of an incident or disruption, typically covering the key personnel, resources, services and actions needed to implement the incident management process

3.31

mitigation

limitation of any negative consequence of a particular incident

[ISO/PAS 22399:2007]

3.32

mutual aid agreement

pre-arranged agreement developed between two or more entities to render assistance to the parties of the agreement

[ISO/PAS 22399:2007]

3.33

nonconformity

non-fulfillment of a requirement

[ISO 9000:2000]

3.34

objective

overall goal, consistent with the policy that an organization sets itself to achieve

[ISO 14001:2004]

3.35

operational continuity

strategic and tactical capability, pre-approved by management, of an organization to plan for and respond to conditions, situations and events in order to continue operations at an acceptable predefined level

NOTE: Operational continuity is the more general term for business continuity. It applies not only to for-profit companies, but organizations of all natures, such as non-governmental, public interest, and governmental organizations.

[ISO/PAS 22399:2007]

3.36

operational continuity strategy

approach by an organization that will ensure its recovery and continuity in the face of a disruptive event, crisis or other major outage

[ISO/PAS 22399:2007]

3.37

organization

group of people and facilities with an arrangement of responsibilities, authorities and relationships

NOTE: An organization can be a government or public entity, company, corporation, firm, enterprise, institution, charity, sole trade or association, or parts or combinations thereof.

[ISO/PAS 22399:2007]

3.38

policy

overall intentions and direction of an organization, related to its incident preparedness and operational continuity, as formally expressed by top management

3.39

prevention

measures that enable an organization to avoid, preclude, or limit the impact of a disruption

[ISO/PAS 22399:2007]

3.40

preventive action

action to eliminate the cause of a potential nonconformity

[ISO 14001:2004]

3.41

prevention of hazards and threats

process, practices, techniques, materials, products, services or resources used to avoid, reduce or control hazards and threats and their associated risks of any type in order to reduce their potential impact

3.42

probability

extent to which an event is likely to occur

NOTE 1: ISO 3534-1:1993, Definition 1.1 gives the mathematical definition of probability as “a real number in the scale of 0 to 1 attached to a random event. It can be related to a long-run relative frequency of occurrence or to a degree of belief that an event will occur. For a high degree of belief, the probability is near 1.”

NOTE 2: Frequency rather than probability may be used to describe risk.

NOTE 3: Degrees of belief about probability can be chosen as classes or ranks, such as

- rare/unlikely/moderate/likely/almost certain, or
- incredible/improbable/remote/occasional/probable/frequent.

[ISO/IEC Guide 73]

3.43

procedure

specified way to carry out an activity

NOTE: Procedures can be documented or not

[ISO 9000:2000]

3.44

record

document stating results achieved or providing evidence of activities performed

[ISO 9000:2000]

3.45

recovery time objective (RTO)

time goal for the restoration and recovery of functions or resources based on the acceptable down time in case of a disruption of operations

[ISO/PAS 22399:2007]

3.46

residual risk

risk remaining after risk treatment

[ISO/PAS 22399:2007]

3.47

resilience

ability of an organization to resist being affected by an event

[ISO/PAS 22399:2007]

3.48

response plan

documented collection of procedures and information that is developed, compiled and maintained in readiness for use in an incident

3.49

response program

plan, processes, and resources to perform the activities and services necessary to preserve and protect life, property, operations, and critical assets

NOTE: Response steps generally include incident recognition, notification, assessment, declaration, plan execution, communications, and resources management

[ISO/PAS 22399:2007]

3.50

response team

group of individuals responsible for developing, executing, rehearsing, and maintaining the response plan, including the processes and procedures

3.51

risk

combination of the probability of an event and its consequences

NOTE 1: The term “risk” is generally used only when there is at least the possibility of negative consequences.

NOTE 2: In some situations, risk arises from the possibility of deviation from the expected outcome or event.

[ISO/IEC Guide 73]

3.52

risk acceptance

decision to accept risk

NOTE 1: The verb “to accept” is chosen to convey the idea that acceptance has its basic dictionary meaning.

NOTE 2: Risk acceptance depends on the risk criteria.

[ISO/IEC Guide 73]

3.53

risk assessment

overall process of risk identification, analysis and evaluation

NOTE: Risk assessment involves the process of identifying internal and external threats and vulnerabilities, identifying the likelihood of an event arising from such threats or vulnerabilities, defining critical functions necessary to continue the organization’s operations, defining the controls in place necessary to reduce exposure, and evaluating the cost of such controls

[ISO/PAS 22399:2007]

3.54

risk communication

exchange or sharing of information about risk between the decision-maker and other stakeholders

NOTE: The information can relate to the existence, nature, form, probability, severity, acceptability, treatment or other aspects of risk.

[ISO/IEC Guide 73]

3.55

risk criteria

terms of reference by which the significance of risk is assessed

NOTE: Risk criteria can include associated cost and benefits, legal and statutory requirements, socio-economic and environmental aspects, the concerns of stakeholders, priorities and other inputs to the assessment.

[ISO/IEC Guide 73]

3.56

risk management

coordinated activities to direct and control an organization with regard to risk

NOTE: Risk management generally includes risk assessment, risk treatment, risk acceptance and risk communication.

[ISO/IEC Guide 73]

3.57

risk reduction

actions taken to lessen the probability, negative consequences, or both, associated with a risk.

[ISO/IEC Guide 73]

3.58

risk tolerance

total amount of risk that an organization is prepared to accept, tolerate, or be exposed to at any point in time

[ISO/PAS 22399:2007]

3.59

risk transfer

sharing with another party the burden of loss or benefit or gain, for a risk

NOTE 1: Legal or statutory requirements can limit, prohibit or mandate the transfer of certain risk.

NOTE 2: Risk transfer can be carried out through insurance or other agreements.

NOTE 3: Risk transfer can create new risks or modify existing risks.

NOTE 4: Relocation of the source is not risk transfer.

[ISO/IEC Guide 73]

3.60

risk treatment

process of selection and implementation of measures to modify risk

NOTE 1: The term "risk treatment" is sometimes used for the measures themselves.

NOTE 2: Risk treatment measures can include avoiding, optimizing, transferring or retaining risk.

[ISO/IEC Guide 73]

3.61

security

protection from risks of unintentionally, intentionally, and naturally caused crises and disasters that disrupt and have consequences on the operation, critical assets, and continuity of the organization and its stakeholders

3.62

security aspects

those characteristics, elements or properties which reduce the risk of unintentionally, intentionally, and naturally caused crises and disasters that disrupt and have consequences on the products and services, operation, critical assets, and continuity of the organization and its stakeholders.

3.63

simulation exercise

test performed under conditions as close as practicable to real world conditions

[ISO/PAS 22399:2007]

3.64

source

item or activity having a potential for a consequence

NOTE: in the context of safety, source is a hazard

[ISO/IEC Guide 73]

3.65

stakeholder (interested party)

person or group having an interest in the performance or success of an organization

NOTE: The term includes persons and groups with an interest in an organization, its activities and its achievements, e.g. customers, partners, employees, shareholders, owners, the local community, first responders, government and regulators.

[ISO/PAS 22399:2007]

3.66

supply chain

the linked set of resources and processes that begins with the sourcing of raw material and extends through the delivery of products or services to the end user across the modes of transport. The supply chain may include suppliers, vendors, manufacturing facilities, logistics providers, internal distribution centers, distributors, wholesalers and other entities that lead to the end user.

3.67

tabletop exercise

test method that presents a limited simulation of a disruption, emergency or crisis scenario in a narrative format in which participants review and discuss, not perform, the policy, methods, procedures, coordination, and resource assignments associated with plan activation

[ASIS International Business Continuity Guideline: 2004]

3.68

target

detailed performance requirement applicable to the organization, or parts thereof, that arises from the objectives and that needs to be set and met in order to achieve those objectives

[ISO 14001:2004]

3.69

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]

3.70

threat

potential cause of an unwanted incident, which may result in harm to individuals, a system or organization, the environment or the community

[ISO/PAS 22399:2007]

3.71

top management

directors 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

[ISO/PAS 22399:2007]

3.72

vulnerability

susceptibility to physical, operational, economic, business, legal, litigious, or other damage

3.73

vulnerability assessment

the process of identifying and quantifying vulnerabilities

4 All hazards risk management system requirements

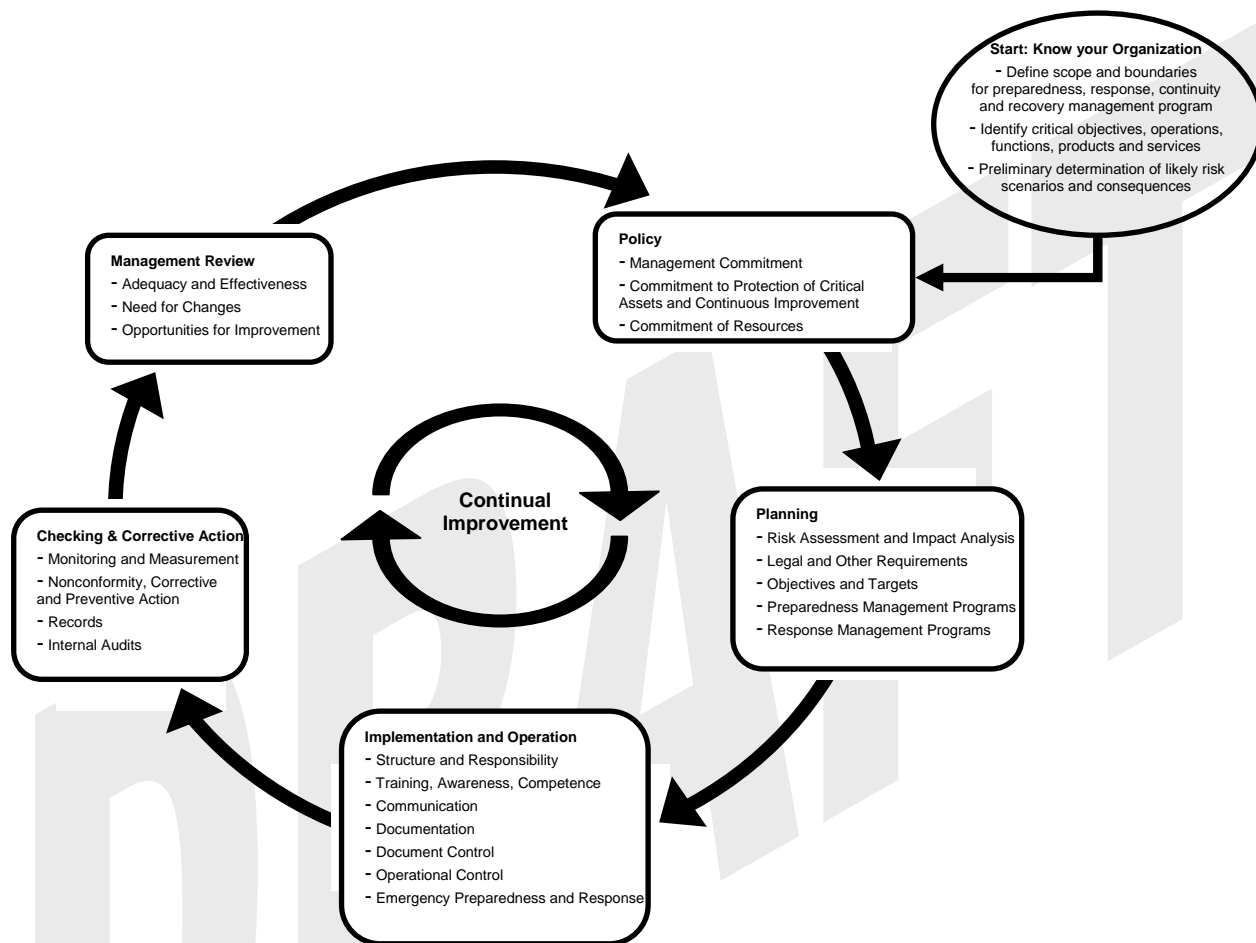


Figure 2 — All hazards risk management system flow diagram

4.1 General Requirements

The organization shall establish, document, implement, maintain and continually improve an all hazards risk management system in accordance with the requirements of this *Standard* and determine how it will fulfil these requirements.

4.1.1 Scope of all hazards management system

The organization shall define and document the scope of its all hazards risk management system.

In defining the scope, the organization shall:

- a) establish the requirements for all hazards risk management considering the organization's mission, goals, internal and external obligations (including those related to stakeholders) and legal responsibilities;
- b) consider critical operational objectives, assets, functions, services and products;

- c) determine risk scenarios that could adversely affect the critical operations and functions of the organization within the context of their potential impact; and
- d) define the scope in terms of the all hazards management system in terms of and appropriate to the size, nature and complexity of the organization.

The organization shall define the scope consistent with protecting the integrity of the organization and its relationships with stakeholders including interactions with key suppliers, outsourcing partners and other stakeholders in the organization's supply chain.

4.2 All hazards risk management policy

Top management shall define, document and provide resources for the organization's all hazard risk management policy reflecting a commitment to the protection of human, environmental and physical assets.

4.2.1 Policy statement

The policy statement of an organization shall ensure that within the defined scope of the all hazards risk management system it:

- a) is appropriate to the nature and scale of potential threats, hazards, risks and impacts (consequences) on the organization's activities, functions, products and services including stakeholders and the environment;
- b) includes a commitment to continual improvement and risk prevention, reduction and mitigation;
- c) includes a commitment to comply with applicable legal requirements and with other requirements to which the organization subscribes;
- d) includes a commitment to life safety as the first priority;
- e) provides a framework for setting and reviewing all hazards risk management objectives and targets;
- f) is documented, implemented and maintained;
- g) makes reference to limitations and exclusions;
- h) determines and documents the acceptable level of risk in relation to the scope of the management system;
- i) is communicated to all persons working for or on behalf of the organization;
- j) is available to relevant stakeholders. (Note: an organization may choose to make public a non-confidential version of its policy not including sensitive security related information.) ; and
- k) is reviewed at planned intervals and when significant changes occur.

4.2.2 Management commitment

Management shall provide evidence of its commitment to the establishment, implementation, operation, monitoring, review, maintenance and improvement of the all hazards risk management system by:

- a) establishing an all hazards risk management system policy;
- b) ensuring that all hazards risk management system objectives and plans are established;
- c) establishing roles, responsibilities and competencies for all hazards risk management;
- d) appoint one or more persons to be responsible for the all hazards risk management system with the appropriate authority and competencies to be accountable for the implementation and maintenance of the management system;
- e) communicating to the organization the importance of meeting all hazards risk management objectives and conforming to all hazards risk management system policy, its responsibilities under the law and the need for continual improvement;
- f) providing sufficient resources to establish, implement, operate, monitor, review, maintain and improve the all hazards risk management system;
- g) deciding the criteria for accepting risks and the acceptable levels of risk;

- h) ensuring that internal all hazards risk management system audits are conducted; and
- i) conducting management reviews of the all hazards risk management system.

4.3 Planning

4.3.1 Risk assessment and impact analysis

The organization shall establish, implement and maintain a formal and documented evaluation process:

- a) to identify the organization's critical activities, functions, services, products, stakeholder relationships and the potential impact related to a disruptive incident;
- b) to identify intentional, unintentional and naturally causes hazards and threats that have a potential for direct or indirect impact on the organization's operations, functions, human and physical assets, the environment and its stakeholders;
- c) to systematically analyze risk, vulnerability, criticality and impacts (consequences); and,
- d) to determine those risks that have a significant impact on activities, functions, services, products, stakeholder relationships and the environment (i.e. significant risks and impacts).

The organization shall:

- a) document and keep this information up to date and confidential, as is appropriate;
- b) re-evaluate risk and impacts within the context of changes within the organization or made to the organization's operating environment, procedures, functions and services;
- c) determine recovery time objectives and priorities;
- d) consider the cost-benefit related to the risk assessment and impact analysis; and,
- e) ensure that the significant risks and impacts are taken into account in establishing, implementing and operating the all hazards risk management system.

4.3.2 Legal and other requirements

The organization shall establish and maintain (a) procedure(s):

- a) to identify and have access to applicable legal, regulatory and other requirements to which the organization subscribes related to the organization's hazards, threats and risks that are related to its facilities, activities, functions, products, services, supply chain, the environment and stakeholders.
- b) to determine how these requirements apply to its hazards, threats, risks and their potential impacts.

The organization shall document this information and keep it up to date.

The organization shall ensure that applicable legal, regulatory and other requirements to which the organization subscribes are considered in developing, implementing and maintaining its all hazards risk management system.

4.3.3 Objectives, targets and program(s)

The organization shall establish and maintain documented objectives and targets to avoid, prevent, deter, mitigate, respond and recover from disruptive incidents at relevant functions and levels within the organization.

The objectives and targets shall be measurable where practicable and consistent with the all hazards risk management policy, including the commitments to:

- a) risk prevention, reduction and mitigation,

- b) compliance with legal and other requirements, and
- c) continual improvement.

When establishing and reviewing its objectives and targets an organization shall consider the legal, regulatory and other requirements, its significant risks and impacts, its technological options and its financial, operational and business requirements, and the views of stakeholders and other interested parties.

The organization shall establish and maintain (a) program(s) for achieving its objectives and targets. It shall include:

- a) designation of responsibility and resources for achieving objectives and targets at relevant functions and levels of the organization;
- b) consideration of its activities, functions, contractual obligations, stakeholders' needs, mutual aid agreements and environment;
- c) the means and time-frame by which they are to be achieved.

The organization shall establish and maintain (a) program(s) for:

- a) prevention and deterrence - avoid, eliminate, deter or prevent the likelihood of a disruptive incident and its consequences, including removal of human or physical assets at risk;
- b) mitigation - lessen and minimize the impact of a disruptive incident;
- c) emergency response - the initial response to a disruptive incident involving the protection of people and property from immediate harm. An initial reaction by management may form part of the organization's first response;
- d) continuity response - processes, controls and resources are made available to ensure that the organization continues to meet its critical operational objectives; and,
- e) recovery response - processes, resources and capabilities of the organization are re-established to meet ongoing operational requirements.

The organization should evaluate these strategies to determine if these measures have themselves introduced new risks.

4.4 Implementation and operation

4.4.1 Resources, roles, responsibility and authority

Management shall ensure the availability of resources essential for the implementation and control of the all hazards risk management system. Resources include human resources and specialized skills, internal infrastructure, technology, information, intelligence and financial resources.

Roles, responsibilities and authorities shall be defined, documented and communicated in order to facilitate effective all hazards risk management.

The organization's top management shall appoint (a) specific management representative(s) who, irrespective of other responsibilities, shall have defined roles, responsibilities and authority for:

- a) ensuring that an all hazards risk management system is established, communicated, implemented and maintained in accordance with the requirements of this *Standard*; and
- b) reporting on the performance of the all hazards risk management system to top management for review and as the basis for improvement.

The organization shall establish:

- a) an all hazards risk management team with appropriate authority to oversee incident preparedness, response and recovery;

- b) logistical capabilities and procedures to locate, acquire, store, distribute, maintain, test, and account for services, personnel, resources, materials, and facilities produced or donated to support the all hazards risk management system;
- c) resource management objectives for response times, personnel, equipment, training, facilities, funding, insurance, liability control, expert knowledge, materials, and the time frames within which they will be needed from organization's resources and from any partner entities; and,
- d) procedures for stakeholder assistance, communications, and mutual aid.

The organization shall develop financial and administrative procedures to support the all hazards risk management program before, during, and after an incident. Procedures shall be:

- a) established to ensure that fiscal decisions can be expedited; and
- b) in accordance with established authority levels and accounting principles.

4.4.2 Competence, training and awareness

The organization shall ensure that any person(s) performing tasks for it or on its behalf that have the potential to prevent, cause, respond, mitigate or be effected by significant hazards, risks, threats and their corresponding impacts identified by the organization are competent on the basis of appropriate education, training, or experience and retain associated records.

The organization shall identify training needs associated with its hazards, threats and risks and its all hazards risk management system. It shall provide training or take other action to meet these needs and retain associated records.

The organization shall establish, implement and maintain (a) procedure(s) to ensure persons working for it or on its behalf are aware of:

- a) the importance of conformity with the all hazards risk management policy and procedures and with the requirements of the all hazards risk management system;
- b) the significant hazards, threats and risks, and related actual or potential impacts, associated with their work and the benefits of improved personal performance;
- c) their roles and responsibilities in achieving conformity with the requirements of the all hazards risk management system;
- d) the procedures for incident prevention, deterrence, mitigation, self-protection, evacuation, response and recovery; and,
- e) the potential consequences of departure from specified procedures.

The organization shall build, promote and embed an all hazards risk management culture within the organization that:

- a) ensures that it becomes part of the organization's core values organization governance; and
- b) makes all appropriate stakeholder aware of the all hazards risk management policy and their part in any plans.

4.4.3 Communication and warning

With regard to its hazards, threats and risk and all hazards risk management system, the organization shall establish, implement and maintain (a) procedure(s) for:

- a) internal communication between the various levels and functions of the organization and with partner entities;
- b) receiving, documenting and responding to relevant communication from external interested parties;

- c) adapting and integrating any national or regional risk or threat advisory system or equivalent into planning and actual operational use;
- d) alerting people potentially impacted by an actual or impending disruptive incident;
- e) facilitating structured communication with emergency responders;
- f) assuring availability of the communication means with emphasis on a crisis situation and disruption;
- g) assuring the interoperability of multiple responding organizations and personnel;
- h) recording of vital information about the incident, actions taken and decisions made;
- i) the need for a central contact facility or communications hub.

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

The all hazards risk management communications systems should be regularly tested.

4.4.4 Documentation

The all hazards risk management system documentation shall include:

- a) the all hazards risk management policy, objectives and targets;
- b) description of the scope of the all hazards risk management system;
- c) description of the main elements of the all hazards risk management system and their interaction and reference to related documents;
- d) documents, including records, required by this *Standard*; and
- e) documents, including records, determined by the organization to be necessary to ensure the effective planning, operation and control of processes that relate to its significant risks.

4.4.5 Control of documents

Documents required by the all hazards risk management system and by this *Standard* shall be controlled. Records are a special type of document and shall be controlled in accordance with the requirements given in 4.5.4.

The organization shall establish, implement and maintain (a) procedure(s) to:

- a) approve documents for adequacy prior to issue;
- b) review and update as necessary and re-approve documents;
- c) ensure that changes and the current revision status of documents are identified;
- d) ensure that relevant versions of applicable documents are available at points of use;
- e) establish document retention and archival parameters;
- f) ensure that documents and archival documents, data and information remain legible and readily identifiable;
- g) ensure that documents of external origin determined by the organization to be necessary for the planning and operation of the all hazards risk management system are identified and their distribution controlled;
- h) prevent the unintended use of obsolete documents and to apply suitable identification to them if they are retained for any purpose;
- i) ensure the integrity of the documents by rendering them tamperproof, securely backed-up, accessible only to authorized personnel and protected from damage, deterioration or loss.

4.4.6 Operational control

The organization shall identify and plan those operations that are associated with the identified significant risks and consistent with its all hazards risk management policy, risk assessment and impact analysis, objectives and targets, in order to ensure that they are carried out under specified conditions, by:

- a) establishing, implementing and maintaining (a) documented procedure(s) to control situations where their absence could lead to deviation from the all hazards risk management policy, objectives and targets; and stipulating the operating criteria in the procedures;
- b) establishing, implementing and maintaining procedures related to the identified hazards, threats and risks to the activities, functions, products and services of the organization and communicating applicable procedures and requirements to suppliers, including contractors.

The operational control procedures shall address reliability and resiliency, the safety and health of people, and the protection of property and the environment impacted by a disruptive incident.

4.4.7 Incident preparedness and response

The organization shall establish, implement and maintain (a) procedure(s) to identify potential disruptive incidents that can have (an) impact(s) on the organization, its activities, functions, services and stakeholders, and the environment, and how it will respond to them.

The organization shall prepare for and respond to actual disruptive incidents and prevent or mitigate associated adverse consequences.

When establishing, implementing and maintaining (a) procedure(s) to prepare for and respond to a disruptive incident the priority for action(s) shall be in order of:

- a) life safety,
- b) protect assets,
- c) prevent further escalation of the disruptive incident,
- d) reduce the length of the disruption to operations,
- e) restore critical operational continuity,
- f) recover normal operations (including evaluating improvements) and
- g) protect image and reputation (including media coverage and stakeholder relationships).

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

- a) the nature of onsite hazards (e.g. flammable and toxic materials, storage tanks and compressed gases) and measures to be taken in the event of a disruptive incident or accidental releases;
- b) the most likely type and scale of disruptive incident;
- c) the most appropriate method(s) for mitigation and emergency response to a disruptive incident to avoid escalation to a crisis or disaster;
- d) command and control procedures and structure including (an) emergency operations center(s) and/or (an) alternate worksite(s);
- e) procedures and authority to declare an emergency situation, initiate emergency procedures, activate plans and actions, assess damage and make financial decisions;
- f) internal and external communication plans including notification of appropriate authorities and stakeholders;
- g) procedures to provide appropriate medical attention;
- h) the action(s) required to minimize human, physical and environmental damage;
- i) the action(s) required to secure vital information and information systems;
- j) mitigation and response action(s) to be taken for different types of disruptive incident(s) or emergency situation(s);

- k) the need for (a) process(es) for post-accident evaluation to establish and implement corrective and preventive actions;
- l) periodic testing of incident and emergency response procedure(s);
- m) training of incident and emergency response personnel;
- n) a list of key personnel and aid agencies, including contact details (e.g. fire department, emergency medical services, law enforcement, hazardous material clean-up services);
- o) evacuation routes and assembly points including lists of personnel and contact details;
- p) the potential for (a) disruptive incident or emergency situation(s) affecting critical infrastructure (e.g. electricity, water, communications, transportation);
- q) the possibility of mutual assistance to and from neighboring organizations; and
- r) procedure(s) and action(s) required to recover each critical activity within the organization's recovery time objective and the resources that it requires for recovery.

The organization shall periodically review and, where necessary, revise its incident preparedness and response procedures, in particular, after the occurrence of accidents or incidents that can escalate into an emergency, crisis or disaster.

The organization shall ensure that any person(s) performing or affected by incident preparedness and response measures for it or on its behalf are competent on the basis of appropriate education, training, or experience and retain associated records.

The organization shall document this information and keep it up to date.

4.5 Checking

The organization shall evaluate all hazards risk management plans, procedures, and capabilities through periodic reviews, testing, post-incident reports, lessons learned, performance evaluations, and exercises. Significant changes in these factors should be reflected immediately in the procedures.

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

4.5.1 Monitoring and measurement

The organization shall establish, implement and maintain (a) procedure(s) to monitor and measure, on a regular basis, the key characteristics of its operations that can have a significant impact. The procedure(s) shall include the documenting of information to monitor performance, applicable operational controls and conformity with the organization's all hazards risk management objectives and targets.

The organization shall ensure that calibrated or verified monitoring and measurement equipment is used and maintained and shall retain associated records.

4.5.2 Evaluation of compliance and system performance

4.5.2.1 Evaluation of compliance

Consistent with its commitment to compliance, the organization shall establish, implement and maintain (a) procedure(s) for periodically evaluating compliance with applicable legal and regulatory requirements.

The organization shall evaluate compliance with other requirements to which it subscribes including industry best practices. The organization may wish to combine this evaluation with the evaluation of legal compliance referred to above or to establish (a) separate procedure(s).

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

4.5.2.2 Exercises and testing

The organization shall test and evaluate the appropriateness and efficacy of its all hazards risk management system, its programs, processes and procedures.

The organization shall validate its all hazards risk management system using exercises and testing that:

- a) is consistent with the with the scope of the all hazards risk management system and objectives of the organization;
- b) is based on realistic scenarios that are well planned with clearly defined aims and objectives;
- c) minimize the risk of disruption of operations and the potential to cause risk to operations and assets;
- d) produce a formalized post-exercise report that contains outcomes, recommendations and arrangements to implement improvements in a timely fashion;
- e) reviewed within the context of promoting continual improvement; and
- f) conducted at regular time intervals established by top management and when significant changes occur within the organization and the environment it operates in.

4.5.3 Nonconformity, corrective action and preventive action

The organization shall establish, implement and maintain (a) procedure(s) for dealing with actual and potential nonconformity(ies) and for taking corrective action and preventive action. The procedure(s) shall define requirements for:

- a) identifying and correcting nonconformity(ies) and taking action(s) to mitigate their impacts;
- b) investigating nonconformity(ies), determining their cause(s) and taking actions in order to avoid their recurrence;
- c) evaluating the need for action(s) to prevent nonconformity(ies) and implementing appropriate actions designed to avoid their occurrence;
- d) recording the results of corrective action(s) and preventive action(s) taken; and
- e) reviewing the effectiveness of corrective action(s) and preventive action(s) taken.

Actions taken shall be appropriate to the impact of the potential problems, and conducted in an expedited fashion.

The organization shall identify changed risks and identify preventive action requirements focusing attention on significantly changed risks.

The priority of preventive actions shall be determined based on the results of the risk assessment and impact analysis.

NOTE: Action to prevent nonconformities is often more cost-effective than corrective action.

The organization shall make any necessary changes to the all hazards risk management system documentation.

4.5.4 Control of records

The organization shall establish and maintain records as necessary to demonstrate conformity to the requirements of its all hazards risk management system and of this *Standard* and the results achieved.

The organization shall establish, implement and maintain (a) procedure(s) to protect the integrity of records including access to, identification, storage, protection, retrieval, retention and disposal of records.

Records shall be and remain legible, identifiable and traceable.

4.5.5 Internal audits

The organization shall conduct internal all hazards risk management system audits at planned intervals to determine whether the control objectives, controls, processes and procedures of its all hazards risk management system:

- a) conform to the requirements of this *Standard* and relevant legislation or regulations;
- b) conform to the identified all risk management requirements;
- c) are effectively implemented and maintained; and
- d) perform as expected.

An audit program shall be planned, taking into consideration the status and importance of the processes and areas to be audited, as well as the results of previous audits. The audit criteria, scope, frequency and methods shall be defined. The selection of auditors and conduct of audits shall ensure objectivity and impartiality of the audit process. Auditors shall not audit their own work.

The responsibilities and requirements for planning and conducting audits, and for reporting results and maintaining records (see 4.5.4) shall be defined in a documented procedure.

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.

4.6 Management review

4.6.1 General

Management shall review the organization's all hazards risk management system at planned intervals to ensure its continuing suitability, adequacy and effectiveness. This review shall include assessing opportunities for improvement and the need for changes to the all hazards risk management system, including the its all hazards risk management system policy and objectives. The results of the reviews shall be clearly documented and records shall be maintained (see 4.5.4).

4.6.2 Review input

The input to a management review shall include:

- a) results of all hazards risk management system audits and reviews;
- b) feedback from interested parties;
- c) techniques, products or procedures, which could be used in the organization to improve the all hazards risk management system performance and effectiveness;
- d) status of preventive and corrective actions;
- e) vulnerabilities or threats not adequately addressed in the previous risk assessment;
- f) results from effectiveness measurements;
- g) follow-up actions from previous management reviews;
- h) any changes that could affect the all hazards risk management system; and
- i) recommendations for improvement.

4.6.3 Review output

The output from the management review shall include any decisions and actions related to the following:

- a) improvement of the effectiveness of the all hazards risk management system;
- b) update of the risk assessment, impact analysis and incident preparedness and response plans;
- c) modification of procedures and controls that effect risks, as necessary, to respond to internal or external events that may impact on the all hazards risk management system, including changes to:
 - i. business and operational requirements;
 - ii. risk reduction and security requirements;
 - iii. operational conditions processes effecting the existing operational requirements;
 - iv. regulatory or legal requirements;
 - v. contractual obligations; and
 - vi. levels of risk and/or criteria for accepting risks.
- d) resource needs; and
- e) improvement to how the effectiveness of controls is being measured.

4.6.4 Maintenance

Top management shall establish defined and documented all hazards risk management system maintenance program to ensure that any internal or external changes that impact the organization are reviewed in relation to the all hazards risk management system. It shall identify any new critical activities that need to be included in the all hazards risk management system maintenance program.

4.6.5 Continual improvement

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

Annex A (informative)

Guidance on the use of the standard

NOTE: The additional text given in this annex is strictly informative and is intended to prevent misinterpretation of the requirements contained in Section 4 of this *Standard*. While this information addresses and is consistent with the requirements of Section 4, it is not intended to add to, subtract from, or in any way modify these requirements.

A.1 General requirements

The implementation of an all hazards risk management system specified by this *Standard* is intended to result in 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 all hazards risk management system 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 economic and other circumstances. Improvements in its all hazards risk management system are intended to result in further improvements in security, preparedness, response, continuity and recovery performance and the organization's resilience. This *Standard* requires an organization to:

- a) establish an appropriate all hazards risk management policy;
- b) identify the hazards, threats related to the organization's past, existing or planned activities, functions, products and services to determine the risk, consequences and impacts of significance;
- c) identify applicable legal requirements and other requirements to which the organization subscribes;
- d) identify priorities and set appropriate all hazards risk management objectives and targets;
- e) establish a structure and (a) program (s) to implement the policy and achieve objectives and meet targets;
- f) facilitate planning, control, monitoring, preventive and corrective action, auditing and review activities to ensure both that the policy is complied with and that the all hazards risk management system remains appropriate; and
- g) be capable of adapting to changing circumstances.

An organization with no existing all hazards risk management system should, initially, establish its current position with regard to its critical assets and potential risk scenarios by means of a review. The aim of this review should be to consider all the organization's hazards and threats and their associated risks and impacts to critical assets as a basis for establishing the all hazards risk management system.

The review should cover four key areas:

- a) identification of risks, including those associated with normal operating conditions, abnormal conditions including start-up and shut-down, and emergency situations and accidents;
- b) identification of applicable legal requirements and other requirements to which the organization subscribes;
- c) examination of existing risk management practices and procedures, including those associated with procurement and contracting activities; and
- d) evaluation of previous emergency situations and accidents.

In all cases, consideration should be given to normal and abnormal operations and functions within the organization, its relationships with relevant stakeholders and to potential disruptive and emergency conditions. Tools and methods for undertaking a review might include checklists, conducting interviews, direct inspection and measurement, 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 all hazards risk management system.

Scoping is intended to clarify the boundaries of the organization to which the all hazards risk management system 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 all hazards risk management system. In setting the scope, the credibility of the all hazards risk management system will depend upon the choice of organizational boundaries. Where a part of an organization is excluded from the scope of its all hazards risk management system, the organization should be able to explain 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.

A.2 All hazards risk management policy

The all hazards risk management policy is the driver for implementing and improving an organization's all hazards risk management system so that it can maintain and potentially improve its security, preparedness, response, continuity and recovery performance. This policy should therefore reflect the commitment of top management to:

- a) comply with applicable legal requirements and other requirements,
- b) prevention preparedness and mitigation of disruptive incidents
- c) continual improvement.

The all hazards risk management policy forms the basis upon which the organization sets its objectives and targets. The all hazards risk management policy should be sufficiently clear to be capable of being understood by internal and external interested parties 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 within the defined scope of the all hazards risk management system.

The all hazards risk management policy should be communicated to all persons who work for, or on behalf of, the organization, including contractors working at an organization's facility. Communication to contractors can be in alternative forms to the policy statement itself such as rules, directives and procedures and may therefore only include pertinent sections of the policy. The organization's all hazards risk management policy should be defined and documented by its top management within the context of the all hazards risk management policy of any broader corporate body of which it is a part and with the endorsement of that body.

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 all hazards risk management system. This will insure that management and staff at all levels within the organization understand that the all hazards risk management system is a critical top management priority. It is equally essential that top management engage a "top down" approach to the all hazards risk management system so that management at all levels of the organization understand accountability for effective and efficient plan maintenance as part of the overall governance priorities.

An All Hazards Risk Management Planning Team with responsibility for all hazards risk management system development that includes senior leaders from all major organizational functions and support groups should be appointed to ensure wide-spread acceptance of the all hazards risk management system.

NOTE: Top management may consist of a person or group of people who direct and control an organization at the highest level.

A.3 Planning

A.3.1 Risk assessment and impact analysis

Section 4.3.1 is intended to provide a process for an organization to identify hazards, treats, risks and impacts to determine those that are significant and which should be addressed as a priority by the organization's all hazards risk management system.

An organization should conduct a comprehensive risk assessment and impact analysis within the scope of its all hazards risk management system, taking into account the inputs and outputs (both intended and unintended) associated with its current and relevant past activities, products and services, planned or new developments, or new or modified activities, functions, products and services, as well as relations with stakeholders and interactions with the environment and critical infrastructure. This process should consider normal and abnormal operating conditions, shut-down and start-up conditions, as well as reasonably foreseeable disruptive and emergency situations.

Critical activities, functions, obligations and processes should be identified and documented. They could include purchasing, manufacturing, supply chain, sales, distribution, accounts receivable, accounts payable, payroll, information technology, and research and development. Once the critical processes and functions are identified, an analysis of each can be made using the evaluation criteria. Organizations may select categories of activities, products and services to identify their criticality, risks and impacts.

There are many approaches and methodologies to risk assessment and impact analysis which will determine the order of the analysis steps adopted. Regardless of the methodology, the organization should have a formal and documented evaluation process threat and hazard identification; and risk, vulnerability, criticality, consequence and impact analysis.

The risk assessment and impact analysis should:

- a) give consideration to risks related to the organization's activities, functions, products and services and their potential for direct or indirect impact on the organization's operations, people, property, assets, compensation, image and reputation, profit, credit and/or environment;
- b) use a documented quantitative or qualitative methodology to estimate likelihood or probability of the identified potential risks and significance of their impacts if they are realized;
- c) be based on reasonable criteria by giving due consideration to all potential risks it recognizes to its operations;
- d) consider its dependencies on others and others dependencies on the organization;
- e) consider risks associated with stakeholders, contractors, suppliers and other affected parties;
- f) 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; and
- g) evaluate risks and impacts it can control and influence. (However, in all circumstances 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, societal 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 impacts on surroundings.

Since an organization might have many risks and impacts, 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 and impacts. However, the method used should provide consistent results and include the establishment and application of evaluation criteria, such as those related to criticality of each

organizational activity and function, legal issues and the concerns of internal and external stakeholders. An organization should analyze impacts of disruptions to its operations and identify critical operations that are given high priority for restoration, in order to set up recovery time objectives.

When assessing impacts the organizations should consider:

- a) Human cost: physical and psychological harm to employees, customers, suppliers, and other stakeholders.
- b) Financial cost: equipment and property replacement, downtime, overtime pay, stock devaluation, lost sales/business, lawsuits, regulatory fines/penalties, etc.
- c) Corporate image cost: reputation, standing in the community, negative press, loss of customers, etc.

Maximum allowable outage time and recovery time objects should be based on:

- a) how long process can be nonfunctional before impacts become unacceptable,
- b) how soon process should be restored (shortest allowable outage restored first),
- c) different recovery time objectives according to time of year (year-end, tax filing, etc.),
- d) identify and document alternate procedures to a process (mutual aid agreements, manual workarounds or processes, blueprints, notification/calling trees, etc.),
- e) evaluation of costs of alternate procedures versus waiting for system to be restored.

When developing information relating to its significant risks and impacts, 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 all hazards risk management system.

The process of identification and evaluation of risks and impacts 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.

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

A.3.2 Legal and other requirements

The organization needs to identify the legal requirements that are applicable to activities and functions. These may include:

- a) national and international legal requirements;
- b) state/provincial/departmental legal requirements;
- c) local governmental legal requirements.

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

- a) agreements with public authorities;
- b) agreements with customers;
- c) non-regulatory guidelines;
- d) voluntary principles or codes of practice;
- e) voluntary labeling or product stewardship commitments;
- f) requirements of trade associations;
- g) agreements with community groups or non-governmental organizations;
- h) public commitments of the organization or its parent organization; and/or
- i) corporate/company requirements.

The determination of how legal and other requirements apply to an organization's risk assessment is usually accomplished in the process of identifying these requirements. It may not be necessary, therefore, to have a separate or additional procedure in order to make this determination.

A.3.3 Objectives, targets and program(s)

The objectives and targets should be specific and measurable wherever practicable. They should cover short-and long-term issues.

Objectives, targets and program(s) should be based on the risk assessment and impact analysis.

When considering its technological options, an organization should consider the use of best available techniques where economically viable, cost-effective and judged appropriate.

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

The creation and use of one or more programs is important to the successful implementation of an all hazards risk management system. Each program should describe how the organization's objectives and targets will be achieved, including timescales, necessary resources and personnel responsible for implementing the program(s). This (these) program(s) may be subdivided to address specific elements of the organization's operations.

The program should include, where appropriate and practical, consideration all stages of an organizations activities and functions related to planning, design, construction, commissioning, operation, retrofitting, production, marketing, waste disposal and decommissioning. Program development may be undertaken for both current and new activities, products and/or services.

Prevention, preparedness and mitigation programs should consider removal of people and property at risk; relocation, retrofitting, and provision of protective systems or equipment; information, data, document, and cyber security; establishment of threat or hazard warning and communication procedures; and redundancy or duplication of essential personnel, critical systems, equipment, information, operations, or materials, including those from partner agencies.

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

- a) Emergency 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;
- b) Continuity response: Processes, controls and resources are made available to ensure that the organization continues to meet its critical operational objectives;
- c) Recovery response: Processes, resources and capabilities of the organization are re-established to meet ongoing operational requirements. This will often include the introduction of significant organizational improvements even to the extent of refocusing strategic or operational objectives).

A.4 Implementation and operation

A.4.1 Resources, roles, responsibility and authority

The successful implementation of an all hazards risk management system calls for a commitment from all persons working for the organization or on its behalf. Roles and responsibilities therefore should not be seen as confined to the risk management function, but can also cover other areas of an organization, such as operational management or staff functions other than risk management, security, preparedness, continuity and response.

This commitment should begin at the highest levels of management. Accordingly, top management should establish the organization's all hazards risk management policy and ensure that the all hazards risk management system is implemented. As part of this commitment, the top management should designate (a) specific management representative(s) with defined responsibility and authority for implementing the all hazards risk management system. In large or complex organizations there may be more than one designated representative. In small or medium-sized enterprises, these responsibilities may be undertaken by one individual.

It is necessary that an appropriate administrative structure be put in place to effectively deal with crisis management during a disruptive incident. Clear definitions must exist for a management structure, authority for decisions, and responsibility for implementation. An organization should have a Crisis Management Team to lead incident/event response. The team should be comprised of such functions as human resources, information technology, facilities, security, legal, communications/media relations, manufacturing, warehousing, and other business critical support functions, with all under the clear direction of senior management or its representatives.

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

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

A.4.2 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. This *Standard* states that:

- a) the importance of conformity with the all hazards risk management policy and procedures and with the requirements of the all hazards risk management system;
- b) the significant hazards, threats and risks, and related actual or potential impacts, associated with their work and the benefits of improved personal performance;
- c) their roles and responsibilities in achieving conformity with the requirements of the all hazards risk management system;
- d) the procedures for incident prevention, deterrence, mitigation, self-protection, evacuation, response and recovery; and,
- e) the potential consequences of departure from specified procedures.

Awareness and education programs should be established for internal and external stakeholders potentially impacted by a disruptive incident.

Awareness, knowledge, understanding and competence may be obtained or improved through training, education or work experience.

The organization should require that contractors 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, especially those carrying out specialized all hazards risk management functions.

All personnel should be trained to perform their individual responsibilities in case of a disruptive incident or crisis. They should also be briefed on the key components of the all hazards risk management system, as well as the response plans that affect them directly. Such training could include procedures for evacuation, shelter-in-place, check-in processes to account for employees, arrangements at alternate worksites, and the handling of media inquiries by the company.

The Crisis Management and Response Teams should be educated about their responsibilities and duties. Check lists of critical actions and information to be gathered are valuable tools in the education and response processes. Teams should be trained regular intervals (at least annually) and new members should be trained when they join. These teams should also be trained with respect to prevention of incidents that may escalate into crises.

It is recommended that any external resources that may be involved in a response – such as Fire, Police, Public Health, and third party vendors – should be familiar with relevant parts of the response plans.

A.4.3 Communication and warning

Internal communication is important to ensure the effective implementation of the all hazards risk management systems. Methods of internal communication may include regular work group meetings, newsletters, bulletin boards, and intranet sites.

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

The organization may wish to plan its communication taking into account the decisions made on relevant target groups, the appropriate messages and subjects and the choice of means. When considering external communication about hazards, threats, risks, impacts and control procedures, organizations should take into consideration the views and information needs of all stakeholders. If the organization decides to communicate externally on its hazards, threats, risks, impacts and control procedures, the organization should establish a procedure to do so. This procedure could change depending on several factors including the type of information to be communicated, the target group and the individual circumstances of the organization. Methods for external communication can include annual reports, newsletters, websites, warnings and community meetings.

Effective communication is one of the most important ingredients in crisis management. Internal and external stakeholders should be identified in order to convey alerts, warnings, crisis and organizational response information. In order to provide the best communications and suitable messages for various groups, it may be appropriate to segment the audiences. In this way, messages tailored specifically for a group can be released.

Preplanning for communications is critical. Draft message templates, scripts, and statements can be crafted in advance for threats identified in the risk assessment. Procedures to ensure that communications can be distributed at short notice should also be established, particularly when using resources such as Intranet and Internet sites and toll-free hotlines.

The organization should designate a single primary spokesperson, with back-ups identified, who will manage/disseminate crisis communications to the media and others. This individual should be trained in media relations prior to a crisis. All information should be funneled through a single source to assure that the messages being delivered are consistent. It should be stressed that personnel should be informed quickly regarding where to refer calls from the media and that only authorized company spokespeople are authorized to speak to the media. In some situations, an appropriately trained site spokesperson may also be necessary.

A.4.4 Documentation

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

The extent of the all hazards risk management system documentation can differ from one organization to another due to:

- a) the size and type of organization and its activities, products or services;
- b) the complexity of processes and their interactions; and
- c) the competence of personnel.

Examples of documents include:

- a) statements of policy, objectives and targets;
- b) information on significant risks and impacts;
- c) procedures;
- d) process information;
- e) organizational charts;
- f) internal and external standards;
- g) site response, mitigation, emergency and crisis plans; and
- h) records.

Any decision to document (a) procedure(s) should be based on issues such as:

- a) the consequences, including those to human and physical assets and the environment, of not doing so;
- b) the need to demonstrate compliance with legal and with other requirements to which the organization subscribes;
- c) the need to ensure that the activity is undertaken consistently;
- d) the advantages of doing so, which can include:
 - i. easier implementation through communication and training;
 - ii. easier maintenance and revision;
 - iii. less risk of ambiguity and deviations;
 - iv. demonstrability and visibility;
- e) the requirements of this *Standard*.

Documents originally created for purposes other than the all hazards risk management system may be used as part of this system and, if so used, will need to be referenced in the system.

A.4.5 Control of documents

The intent of 4.4.5 is to ensure that organizations create and maintain documents in a manner sufficient to implement the all hazards risk management system. However, the primary focus of organizations should be on the effective implementation of the all hazards risk management system and on security, preparedness, response, continuity and recovery performance and not on a complex document control system.

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

A.4.6 Operational control

An organization should evaluate those of its operations that are associated with its identified significant aspects and ensure that they are conducted in a way that will control or reduce the adverse impacts associated with them in order to fulfill the requirements of its all hazards risk management policy and meet its objectives and targets. This should include all parts of its operations including maintenance activities.

As this part of the all hazards risk management system provides direction on how to take the system requirements into day-to-day operations and requires the use of (a) documented procedure(s) to control situations where the absence of documented procedures could lead to deviations from the all hazards risk management policy and the objectives and targets.

To minimize the likelihood of a disruptive incident, these procedures should include controls for the design, installation, operation, refurbishment, and modification of risk related items of equipment, instrumentation, etc., as appropriate. Where existing arrangements are revised or new arrangements introduced, that could impact on operations and activities, the organization should consider the associated minimization of threats and risks before their implementation.

A.4.7 Incident preparedness and response

It is the responsibility of each organization to develop (an) incident 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.
- b) 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.
- c) 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.
- d) 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.
- e) 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, whether 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.
- f) 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.
- g) 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.

- h) 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.
- i) 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.
- j) 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 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.
 - v. Offsite storage is a valuable mitigation strategy allowing rapid crisis response and business resumption/recovery. The off-site storage location should be a sufficient distance from the primary facility so that it is not likely to be similarly affected by the same event. Items to be considered for off-site storage include critical and vital records (paper and other media) critical to the operations of the business. Procedures should be included in the plan to ensure the timely deliver of any necessary items from offsite storage to the Crisis Management Center or the alternate worksites.

- k) 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.
- l) 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.
- m) 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;
 - v. Transportation for staff with special needs.
- n) 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.
- o) 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.
- p) 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.

- q) 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.
- r) 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.
- s) 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.

A.5 Checking

A.5.1 Monitoring and measurement

Data collected from monitoring and measurement can be analyzed to identify patterns and obtain information. Knowledge gained from this information can be used to implement corrective and preventive action. Metrics should be established to measure success of the all hazards risk management system.

Key characteristics are those that the organization needs to consider to determine how it is managing its significant risks and impacts, achieving objectives and targets, and improving security, preparedness, response, continuity and recovery 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.5.2 Evaluation of compliance and system performance

A.5.2.1 Evaluation of compliance

The organization should be able to demonstrate that it has evaluated compliance with the legal requirements identified including applicable permits or licenses.

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

A.5.2.2 Exercises and testing

Testing scenarios should be designed using the events identified in the risk assessment and impact analysis.

Testing can keep response teams and employees effective in their duties, clarify their roles, and reveal weaknesses in the all hazards risk management system that should be corrected. A commitment to testing lends credibility and authority to the all hazards risk management system.

The first step in testing should be the setting of goals and expectations. A critical goal is to determine whether a certain crisis response process works and how it can be improved. Other examples of goals include:

- a) capacity testing (e.g. the capacity of a call-in or call-out phone system);
- b) reduce the time necessary for accomplishment of a process (e.g. using repeated drills to shorten response times); and
- c) bring awareness and knowledge to the general employee population about the all hazards risk management system.

Lessons learned from previous tests, as well as actual incidents experienced, should be built into the testing cycle for the all hazards risk management system.

The responsibility for testing the all hazards risk management system should be assigned. Larger organizations may consider establishing a Test Team. Where appropriate, the expertise of external resources (consultants, local emergency organizations, etc.) can be leveraged.

A test schedule and timeline as to how often the plan and its components will be tested should be established.

The scope of testing should be planned to develop over time. Tests should start out relatively simple, becoming increasingly complex as the test process evolves. Early tests may include checklists, simple exercises, and small components of the all hazards risk management system. As the test schedules evolve, tests should become increasingly complex, up to a full-scale activation of the entire all hazards risk management system, including external participation by public safety and emergency responders.

There are several roles that test participants can fill. All participants should understand their roles in the exercise, and the exercise should involve all participants. Various groups from the organization itself, as well as from the public sector, can participate in the tests. As part of the exercise, participants should be allowed to interact and discuss issues and lessons.

After completion, the exercises and tests should be critically evaluated. The evaluation should include, among other things, an assessment of how well the goals and objectives of the test were achieved, the effectiveness of participation, and whether the all hazards risk management system itself will function as anticipated in the case of a real crisis. Future testing, as well as the all hazards risk management system itself, should then be modified as necessary based on the test results.

Design of tests should be evaluated and modified as necessary. They should be dynamic, taking into account changes to the all hazards risk management system, personnel turnover, actual incidents, and results from previous exercises.

Exercise and test results should be documenting.

A.5.4 Nonconformity, corrective action and preventive action

Depending on the nature of the nonconformity, in establishing procedures to deal with these requirements, organizations may be able to accomplish them with a minimum of formal planning, or it may be a more complex and long-term activity. Any documentation should be appropriate to the level of action.

A.5.5 Control of records

Management system records can include, among others:

- a) complaint records;
- b) training records;

- c) process monitoring records;
- d) inspection, maintenance and calibration records;
- e) pertinent contractor and supplier records;
- f) incident reports;
- g) records of incident and emergency preparedness tests;
- h) audit results;
- i) management review results;
- j) external communications decision;
- k) records of applicable legal requirements;
- l) records of significant risk and impacts;
- m) records of management systems meetings;
- n) security, preparedness, response, continuity and recovery performance information;
- o) legal compliance records;
- p) communications with stakeholders and interested parties.

Proper account should be taken of confidential information.

Organizations 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.

NOTE Records are not the sole source of evidence to demonstrate conformity to this *Standard*.

A.5.6 Internal Audit

Internal audits of an all hazards risk management system 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 1: If an organization wishes to combine audits of its all hazards risk management system with security, safety or environmental audits, the intent and scope of each should be clearly defined.

A.6 Management review

The management review should cover the scope of the all hazards risk management system, although not all elements of the all hazards risk management system need to be reviewed at once and the review process may take place over a period of time.

The all hazards risk management system should be regularly reviewed and evaluated. Reviews should occur according to a pre-determined schedule, and documentation of the review should be maintained as necessary. The following factors can trigger a review and should otherwise be examined once a review is scheduled:

- a) Risk assessment and impact analysis: The all hazards risk management system should be reviewed every time a risk assessment is completed for the organization. The results of the risk assessment and impact analysis can be used to determine whether the all hazards risk management system continues to adequately address the risks facing the organization.
- b) Sector/industry trends: Major sector/industry initiatives should initiate an all hazards risk management system review. General trends in the sector/industry and in business/operational continuity planning techniques can be used for benchmarking purposes.
- c) Regulatory requirements: New regulatory requirements may require a review of the all hazards risk management system.
- d) Event experience: A review should be performed following a response to disruptive incident, whether the response plan was activated or not. If the plan was activated, the review should take

into account the history of the plan itself, how it worked, why it was activated, etc. If the plan was not activated, the review should examine why and whether this was an appropriate decision.

- e) Test and exercise results: Based on test and exercise results, the all hazards risk management system should be modified as necessary.

Continual improvement and all hazards risk management system maintenance should reflect changes in the risks, activities, functions and operation of the organization that will affect the all hazards risk management system. 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 and impact analysis;
- e) personnel changes (employees and contractors);
- f) supplier and supply chain changes;
- g) process and technology changes;
- h) systems and application software changes;
- i) critical lessons learned from testing;
- j) issues discovered during actual implementation of the plan in a crisis;
- k) changes to external environment (new businesses in area, new roads or changes to existing traffic patterns, etc.); and
- l) other items noted during review of the plan and identified during the risk assessment and impact analysis.

**Annex B
(informative)**

Correspondence between ISO 9001:2000, ISO 14001:2004, ISO 27001:2005 and the ASIS International Standard of Best Practices

Table B.1 — Correspondence between ISO 9001:2000, ISO 14001:2004, ISO 27001:2005 and the ASIS International Standard of Best Practices

ASIS International All Hazards Risk Management Standard	ISO 9001:2000	ISO 14001:2004	ISO 27001:2005
0 Introduction 0.1 Summary 0.2 All hazards approach 0.3 General 0.4 Process approach 0.5 Compatibility with other management systems 0.6 Qualifications 0.7 Terminology conventions	0 Introduction 0.1 General 0.2 Process approach 0.3 Relationship with ISO 9004 0.4 Compatibility with other management systems	Introduction	0 Introduction 0.1 General 0.2 Process approach 0.3 Compatibility with other management systems
1 Scope	1 Scope 1.1 General 1.2 Application		1 Scope 1.1 General 1.2 Application
2 Normative references	2 Normative reference	2 Normative reference	2 Normative references
3 Terms and definitions	3 Terms and definitions	3 Terms and definitions	3 Terms and definitions
4 All hazards risk management system 4.1 General requirements 4.1.1 Scope of the all hazards risk management system 4.2 All hazards risk management policy 4.2.1 Policy statement 4.2.2 Management commitment	4 Quality management system 4.1 General requirements 5 Management responsibility 5.1 Management commitment 5.2 Customer focus 5.3 Quality policy 5.4 Planning 5.5 Responsibility, authority and communication	4 Environmental management system requirements 4.1 General requirements 4.2 Environmental policy	4 Information security management system 4.1 General requirements 4.2 Establishing and managing the ISMS 4.2.1 Establish the ISMS 4.2.2 Implement and operate the ISMS 4.2.3 Monitor and review the ISMS 4.2.4 Maintain and improve the ISMS 5 Management responsibility 5.1 Management commitment

<p>4.3 Planning</p> <p>4.3.1 Risk assessment and impact analysis</p> <p>4.3.2 Legal and other requirements</p> <p>4.3.3 Objectives, targets and program(s)</p>	<p>7 Product realization</p> <p>7.1 Planning of product realization</p> <p>7.2 Customer-related processes</p> <p>7.2.1 Determination of requirements related to the product</p> <p>7.2.2 Review of requirements related to the product</p>	<p>4.3 Planning</p> <p>4.3.1 Environmental aspects</p> <p>4.3.2 Legal and other requirements</p> <p>4.3.3 Objectives, targets and program(s)</p>	<p>4.2 Establishing and managing the ISMS</p> <p>4.2.1 Establish the ISMS</p> <p>4.2.2 Implement and operate the ISMS</p>
<p>4.4 Implementation and operation</p> <p>4.4.1 Resources, roles, responsibility and authority</p> <p>4.4.2 Competence, training and awareness</p> <p>4.4.3 Communication and warning</p> <p>4.4.4 Documentation</p> <p>4.4.5 Control of documents</p> <p>4.4.6 Operational control</p> <p>4.4.7 Incident preparedness and response</p>	<p>6 Resource management</p> <p>6.1 Provision of resources</p> <p>6.2 Human resources</p> <p>6.2.2 Competence, awareness and training</p> <p>6.3 Infrastructure</p> <p>6.4 Work environment</p> <p>7.2.3 Customer communication</p> <p>4.2 Documentation requirements</p> <p>4.2.1 General</p> <p>4.2.2 Quality manual</p> <p>4.2.3 Control of documents</p> <p>7.3 Design and development</p> <p>7.4 Purchasing</p> <p>7.5 Product and service provision</p>	<p>4.4 Implementation and operation</p> <p>4.4.1 Resources, roles, responsibility and authority</p> <p>4.4.2 Competence, training, and awareness</p> <p>4.4.3 Communication and warning</p> <p>4.4.4 Documentation</p> <p>4.4.5 Control of documents</p> <p>4.4.6 Operational control</p> <p>4.4.7 Emergency preparedness and response</p>	<p>5.2 Resource management</p> <p>5.2.1 Provision of resources</p> <p>5.2.2 Training, awareness and competence</p> <p>4.3 Documentation requirements</p> <p>4.3.1 General</p> <p>4.3.2 Control of documents</p>
<p>4.5 Checking</p> <p>4.5.1 Monitoring and measuring</p> <p>4.5.2 Evaluation of compliance and system performance</p> <p>4.5.2.1 Evaluation of compliance</p> <p>4.5.2.2 Exercises and testing</p> <p>4.5.3 Nonconformity, corrective action and preventive action</p> <p>4.5.4 Control of records</p> <p>4.5.5 Internal audits</p>	<p>7.6 Control of monitoring and measuring devices</p> <p>8.2.3 Monitoring and measurement of processes</p> <p>8.2.4 Monitoring and measurement of product</p> <p>8.3 Control of nonconforming product</p> <p>8.5.3 Corrective actions</p> <p>8.5.3 Preventive actions</p> <p>4.2.4 Control of records</p> <p>8.2.2 Internal Audit</p> <p>8.4 Analysis of data</p>	<p>4.5 Checking</p> <p>4.5.1 Monitoring and measurement</p> <p>4.5.2 Evaluation of compliance</p> <p>4.5.3 Nonconformity, corrective action and preventive action</p> <p>4.5.4 Control of records</p> <p>4.5.5 Internal audits</p>	<p>4.2.3 Monitor and review the ISMS</p> <p>8.2 Corrective action</p> <p>8.3 Preventive action</p> <p>4.3.3 Control of records</p> <p>6 Internal ISMS audits</p>

<p>4.6 Management review</p> <p>4.6.2 General</p> <p>4.6.2 Review of Input</p> <p>4.6.3 Review of output</p> <p>4.6.4 Maintenance</p> <p>4.6.5 Continual improvement</p>	<p>5.6 Management review</p> <p>5.6.1 General</p> <p>5.6.2 Review input</p> <p>5.6.3 Review output</p> <p>8.5 Improvement</p> <p>8.5.1 Continual improvement</p>	<p>4.6 Management review</p>	<p>7 Management review of the ISMS</p> <p>7.1 General</p> <p>7.2 Review input</p> <p>7.3 Review output</p> <p>4.2.4 Maintain and improve</p> <p>8 ISMS improvement</p> <p>8.1 Continual improvement the ISMS</p>
<p>Annex A Control objectives and controls</p> <p>Annex B Correspondence between ISO 9001:2000, ISO 14001:2004, ISO 27001:2005 and the ASIS International Standard of Best Practices</p>	<p>Annex A Correspondence between ISO 9001:2000 and ISO 14001:1996</p>	<p>Annex A Guidance on the use of this International Standard</p> <p>Annex B Correspondence between ISO 14001:2004 and ISO 9001:2000</p>	<p>Annex A Control objectives and controls</p> <p>Annex B OECD principles and this International Standard</p> <p>Annex C Correspondence between ISO 9001:2000, ISO 14001:2004 and this International Standard</p>

Bibliography

ASIS publications

Business Continuity Guideline: A Practical Approach for Emergency Preparedness, Crisis Management, and Disaster Recovery, 2005

ISO standards publications

- [1] ISO 9001:2000, *Quality management systems — Requirements*
- [2] ISO 14001:2004, *Environmental management systems — Requirements with guidance for use*
- [3] ISO/IEC TR 18044:2004, *Information technology — Security techniques — Information security incident management*
- [4] ISO 19011:2002, *Guidelines for quality and/or environmental management systems auditing*
- [5] ISO/IEC 27001:2005, *Information technology — Security techniques — Information security management systems — Requirements*
- [6] ISO/PAS 22399:2007 *Societal Security – Guidelines for incident preparedness and operational continuity management*
- [7] ISO/IEC Guide 73:2002, *Risk management — Vocabulary — Guidelines for use in standards*