PUBLICLY AVAILABLE SPECIFICATION

ISO/PAS 22399

First edition
2007-12-01

Societal security — Guideline for incident preparedness and operational continuity management

Sécurité sociétale — Lignes directrices pour être préparé à un incident et gestion de continuité opérationnelle

Reference number
ISO 22399:2007(E)

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Published in Switzerland

Contents

Page

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

International Standards are drafted in accordance with the rules given in the ISO/IEC Directives, Part 2.

The main task of technical committees is to prepare International Standards. Draft International Standards adopted by the technical committees are circulated to the member bodies for voting. Publication as an International Standard requires approval by at least 75 % of the member bodies casting a vote.

In other circumstances, particularly when there is an urgent market requirement for such documents, a technical committee may decide to publish other types of normative document:

— an ISO Publicly Available Specification (ISO/PAS) represents an agreement between technical experts in an ISO working group and is accepted for publication if it is approved by more than 50 % of the members of the parent committee casting a vote;

— an ISO Technical Specification (ISO/TS) represents an agreement between the members of a technical committee and is accepted for publication if it is approved by 2/3 of the members of the committee casting a vote.

An ISO/PAS or ISO/TS is reviewed after three years in order to decide whether it will be confirmed for a further three years, revised to become an International Standard, or withdrawn. If the ISO/PAS or ISO/TS is confirmed, it is reviewed again after a further three years, at which time it must either be transformed into an International Standard or be withdrawn.

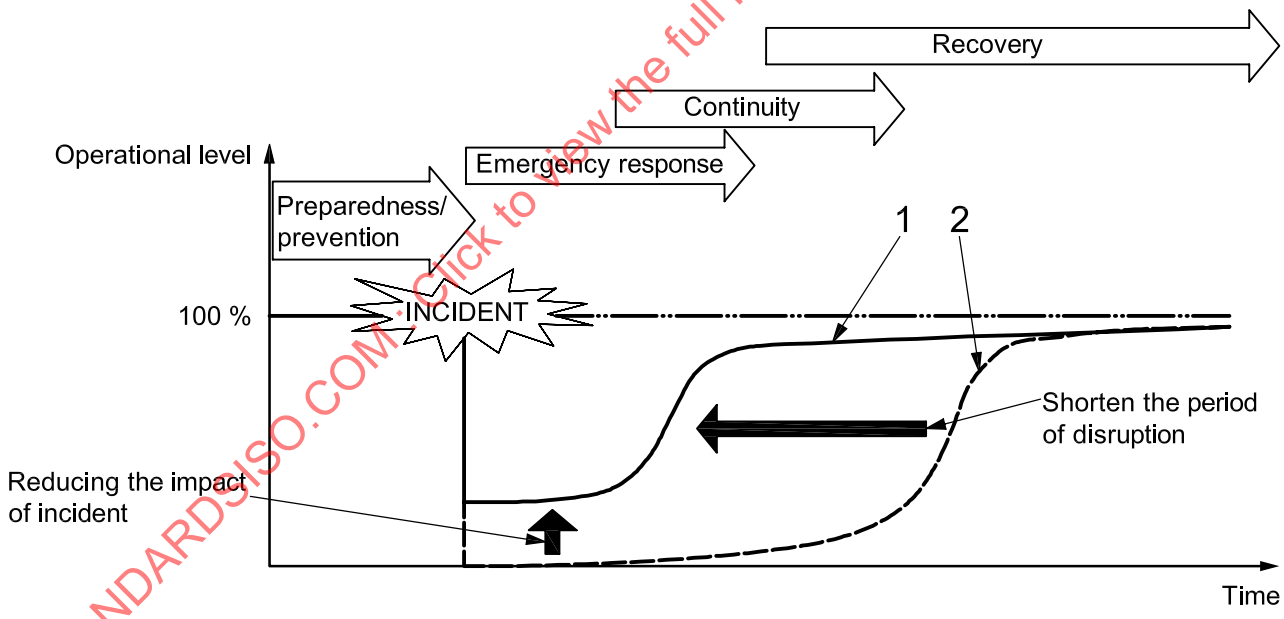
Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights.

ISO/PAS 22399 was prepared by Technical Committee ISO/TC 223, *Societal security*. It includes parts of *NFPA 1600:2004*, *BS 25999-1:2006*, *HB 221:2004*, *INS 24001:2007* and the compiled work of the *Japanese Industrial Standards Committee*.

Introduction

This incident preparedness and operational continuity guideline establishes the process, principles and terminology of incident preparedness and operational (business) continuity management (IPOCM) within the context of societal security. The purpose of this guideline is to provide a basis for understanding, developing and implementing incident preparedness and operational continuity within an organization and to provide confidence in organization-to-community, business-to-business and organization-to-customer/client dealings. The guideline is a tool to allow public or private organizations to consider the factors and steps necessary to prepare for an unintentionally, intentionally, or naturally caused incident (disruption, emergency, crisis or disaster) so that it can manage and survive the incident and take the appropriate actions to help ensure the organization's continued viability. It also enables the organization to measure its IPOCM capability in a consistent and recognized manner. This guideline provides a generic framework applicable to all types and sizes of organizations enabling consideration of diverse geographical, cultural, economic, national, political and social conditions.

Interested parties and stakeholders require that organizations proactively prepare for potential incidents and disruptions in order to avoid suspension of critical operations and services, or if operations and services are disrupted, that they resume operations and services as rapidly as required by those who depend on them, as shown in Figure 1. IPOCM is a holistic management process that identifies potential impacts that threaten an organization and provides a framework for minimizing their effect.



Key

1 after introduction implementation of IPOCM

2 before introduction implementation of IPOCM

Figure 1 — Concept of incident preparedness and IPOCM

This Publicly Available Specification provides a comprehensive set of controls based on IPOCM best practice and covers the whole IPOCM lifecycle. It is intended for use by anyone with responsibility for public or private sector organization operations, from directors and executives through all levels of the organization; from those with a single site to those with a global presence; from small and medium enterprises (SMEs) to organizations employing thousands of people. It is therefore applicable to anybody who holds responsibility for any

operation, and thus the continuity of that operation. For purposes of this guide, operational continuity is the more general term for business continuity and is used to emphasize relevance to all types of organizations in the public and private sectors.

This guideline details integrated planning and management processes that proactively help organizations to

— understand the environment within which the organization operates, the existence of constraints, and threats to the organization that could result in a significant disruption;

— quantify the impact of a disruption on critical operational (business) functions and processes;

— determine the parts of the operations and business that are critical to its short- and long-term success;

— identify the infrastructure and resources required to enable the organization to continue to operate at a minimum acceptable level;

— document the key resources, infrastructure, tasks and responsibilities, required to support these critical operational functions in the event of a disruption;

— establish processes that ensure the information remains current and relevant to the changing risk and operational environments;

— ensure that relevant employees, customers, suppliers and other stakeholders are aware of the preparedness and continuity arrangements and, where appropriate, have confidence in their application;

— implement solutions accordingly and provide for their continual improvement.

It is important to recognize that effective IPOCM requires a fundamental cultural change within the organization including an acceptance of uncertainty and imperfection. All levels of an organization need to appreciate that risk is inherent in every decision and activity, and that a proportion of this risk has the potential to create disruption. People at all levels of an organization, therefore, need to consider how they will manage such disruptions to their activities.

This IPOCM guideline enables a public or private sector organization to assess and manage risk with the goal of assuring organizational resilience and long-term performance. It does not prescribe any particular model for application. There are various recognized models and methodologies which weave incident preparedness and operational continuity decision-making into the fabric of an organization's overall operational and business practices, making the organization more efficient, more competitive, and better able to meet important challenges. This guideline provides a set of problem identification and problem-solving tools that can be implemented by any organization in many different ways, depending on its activities and needs. By incorporating a dynamic systematic risk-based process into incident and continuity management, organizations can make informed decisions tailored to their resources. The model chosen should instill an organizational culture that drives continual improvement.

Typically, management models include several common elements: policy, planning, implementation and operation, performance assessment, improvement and management review. This Publicly Available Specification provides guidance on addressing these common elements when developing and implementing a management model that addresses the specific needs of the organization and its place in the community.

Whichever management model or methodology is chosen, the full set of IPOCM actions should be adopted. IPOCM is directly linked to organizational governance and establishes good management practice. IPOCM establishes a strategic and operational framework to implement, proactively, an organization's resilience to disruption, interruption, or loss in supplying its products and services. It should not be a purely reactive measure taken after an incident has occurred. IPOCM requires planning across many facets of an organization; therefore its resilience depends equally on its management and operational staff, as well as technology, and requires a holistic approach to be taken in establishing the IPOCM model or methodology.

The adoption and implementation of a range of IPOCM techniques in a systematic manner can contribute to optimal outcomes for all interested and affected parties. However, adoption of this guideline will not itself guarantee optimal preparedness and continuity outcomes. In order to achieve preparedness and continuity objectives, the incident preparedness and operational continuity program 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.

IPOCM requires the coordination and collaboration of many different entities in the public and private sectors (such as government and public authorities at various levels, business and industry, non-governmental organizations and individual citizens). Each of these entities has its own focus, unique missions and responsibilities, varied resources and capabilities, and operating principles and procedures. It should be recognized that the key IPOCM program elements relate to and interact with the functions and interests of different entities that may be involved in an incident. Therefore, the key program areas should be considered within the context of all the entities impacted and their relationship to the IPOCM program.

An organization's response to risks, which aims at minimizing their impacts and reducing social loss, should be promoted and recognized as its social responsibility. When a disruptive incident occurs, an organization should understand that cooperation with other organizations in allocating human and physical resources is essential for its own operational continuity because resources required for emergency response and restoration may be scarce or not optimally distributed. An organization should make an active contribution to community through a cooperative effort with citizens, local governments, etc. by participating in supportive activities to rescue human lives and to offer supplies. It is also necessary for an organization to collaborate and cooperate with the first responder community and its stakeholders and partners in human and physical aspects.

An organization may chose to limit the scope of their implementation of the guideline elements by restricting its application to specific products, services or one or more geographic locations. Any such limitation in scope should be documented.

It should be noted that this guideline does not establish absolute requirements for incident preparedness and operational continuity performance beyond commitments, in the policy statement, to comply with applicable legal requirements and with other requirements to which the organization subscribes, proactive risk and incident/disruption prevention, and to continual improvement. This guideline has adopted a system for continual improvement, but it is not intended to be used as third-party certification/registration criteria.

Societal security — Guideline for incident preparedness and operational continuity management

1 Scope

This guideline provides general guidance for an organization — private, governmental, and non-governmental organizations — to develop its own specific performance criteria for incident preparedness and operational continuity, and design an appropriate management system. It provides a basis for understanding, developing and implementing continuity of operations and services within an organization and to provide confidence in business, community, customer, first responder and organizational interactions. It also enables the organization to measure its resilience in a consistent and recognized manner.

This guideline is applicable to all sizes of public or private organizations engaged in providing products, processes, or services that wishes to:

— understand the overall context within which the organization operates;

— identify critical objectives;

— understand barriers, risks, and disruptions that may impede critical objectives;

— evaluate residual risk and risk tolerance to understand outcomes of controls and mitigation strategies;

— plan how an organization can continue to achieve its objectives should a disruptive incident occur;

— develop incident and emergency response, continuity response and recovery response procedures;

— define roles and responsibilities, and resources to respond to an incident;

— meet compliance with applicable legal, regulatory, and other requirements;

— provide mutual and community assistance;

— interface with first responders and the media;

— promote a cultural change within the organization that recognizes that risk is inherent in every decision and activity, and must be effectively managed.

This guideline presents the general principles and elements for incident preparedness and operational continuity of an organization. The extent of the application will depend on factors such as the policy of the organization, the nature of its activities, products and services, and the location where and the conditions under which it functions.

The scope of this guideline, however, excludes specific emergency response activities following an incident, such as disaster relief and social infrastructure recovery that are primarily to be performed by the public sector in accordance with relevant legislation. It is important, however, that coordination with these activities be maintained and documented.

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/IEC Guide 73:2002, *Risk management — Vocabulary — Guidelines for use in standards*

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

3.2
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]

3.3
crisis
any incident(s), human-caused or natural, that require(s) urgent attention and action to protect life, property, or environment

3.4
disaster
event that causes great damage or loss

3.5
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.

3.6
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.

3.7
exercising
evaluating IPOCM 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 IPOCM 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 operational continuity procedures, but is more likely to involve the simulation of an operational continuity incident, announced or unannounced, in which participants role-play in order to assess what issues might arise, prior to a real invocation.

3.8
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]

3.9
hazard
possible source of danger, or conditions physical or operational, that have a capacity to produce a particular type of adverse effects

3.10
impact
evaluated consequence of a particular outcome

3.11
impact analysis
process of analyzing all operational functions and the effect that an operational interruption might have upon them

3.12
incident
event that might be, or could lead to, an operational interruption, disruption, loss, emergency or crisis

3.13
incident 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

3.14
incident preparedness
activities, programs, and systems developed and implemented prior to an incident that may be used to support and enhance mitigation of, response to, and recovery from disruptions, disasters, or emergencies

3.15
incident preparedness and operational continuity management
IPOCM
systematic and coordinated activities and practices through which an organization optimally manages its risks, and the associated potential threats and impacts there from

3.16
IPOCM policy
overall intentions and direction of an organization, related to its incident preparedness and operational continuity, as formally expressed by top management

3.17
mitigation
limitation of any negative consequence of a particular incident

3.18
mutual aid agreement
pre-arranged agreement developed between two or more entities to render assistance to the parties of the agreement

3.19
operational continuity
OC
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.

3.20
operational continuity management
OCM
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 Operational continuity management also involves the management of recovery or continuity in the event of an incident, as well as management of the overall program through training, rehearsals, and reviews, to ensure the operational continuity plan stays current and up-to-date.

3.21
operational continuity 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

3.22
operational continuity management team
group of individuals functionally responsible for directing the development and execution of the operational continuity plan, declaring an emergency/crisis situation and providing direction during the recovery process, both pre-and post-disruptive incident

NOTE The operational continuity management team may include individuals from the organizations as well as immediate and first responders, stakeholders, and other interested parties.

3.23
operational continuity plan
OCP
documented collection of procedures and information that is developed, compiled and maintained in readiness for use in an incident

3.24
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

3.25
operational continuity team
group of individuals responsible for developing, executing, rehearsing, and maintaining the operational continuity plan, including the processes and procedures

3.26
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.

3.27
prevention
measures that enable an organization to avoid, preclude, or limit the impact of a disruption

3.28
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]

3.29
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

3.30
residual risk
risk remaining after risk treatment

3.31
resilience
ability of an organization to resist being affected by an event

3.32
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.

3.33
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]

3.34
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]

3.35
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.

3.36
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]

3.37
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]

3.38
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]

3.39
risk reduction
actions taken to lessen the probability, negative consequences, or both, associated with a risk

[ISO/IEC Guide 73]

3.40
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]

3.41
risk tolerance
total amount of risk that an organization is prepared to accept, tolerate, or be exposed to at any point in time

3.42
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]

3.43
simulation exercise
test performed under conditions as close as practicable to real world conditions

3.44
source
item or activity having a potential for a consequence

NOTE In the context of safety, source is a hazard.

[ISO/IEC Guide 73]

3.45
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.

3.46
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

3.47
testing
activity in which some part(s) of the operational continuity plan(s) is/are followed to ensure that the plan(s) contain(s) the appropriate information and produces the desired result

3.48
threat
potential cause of an unwanted incident, which may result in harm to individuals, a system or organization, the environment or the community

3.49
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

4 General

The incident preparedness and operational continuity management approach and the ongoing process of continual improvement are shown in Figure 2. IPOCM is an organizing framework that should be continually monitored and periodically reviewed to provide effective direction for an organization's incident preparedness and operational continuity management in response to changing internal and external factors. All levels in the organization should accept responsibility for working to achieve incident preparedness and operational continuity improvements, as applicable. IPOCM considerations can be integrated into all the organization's operational and business decisions.

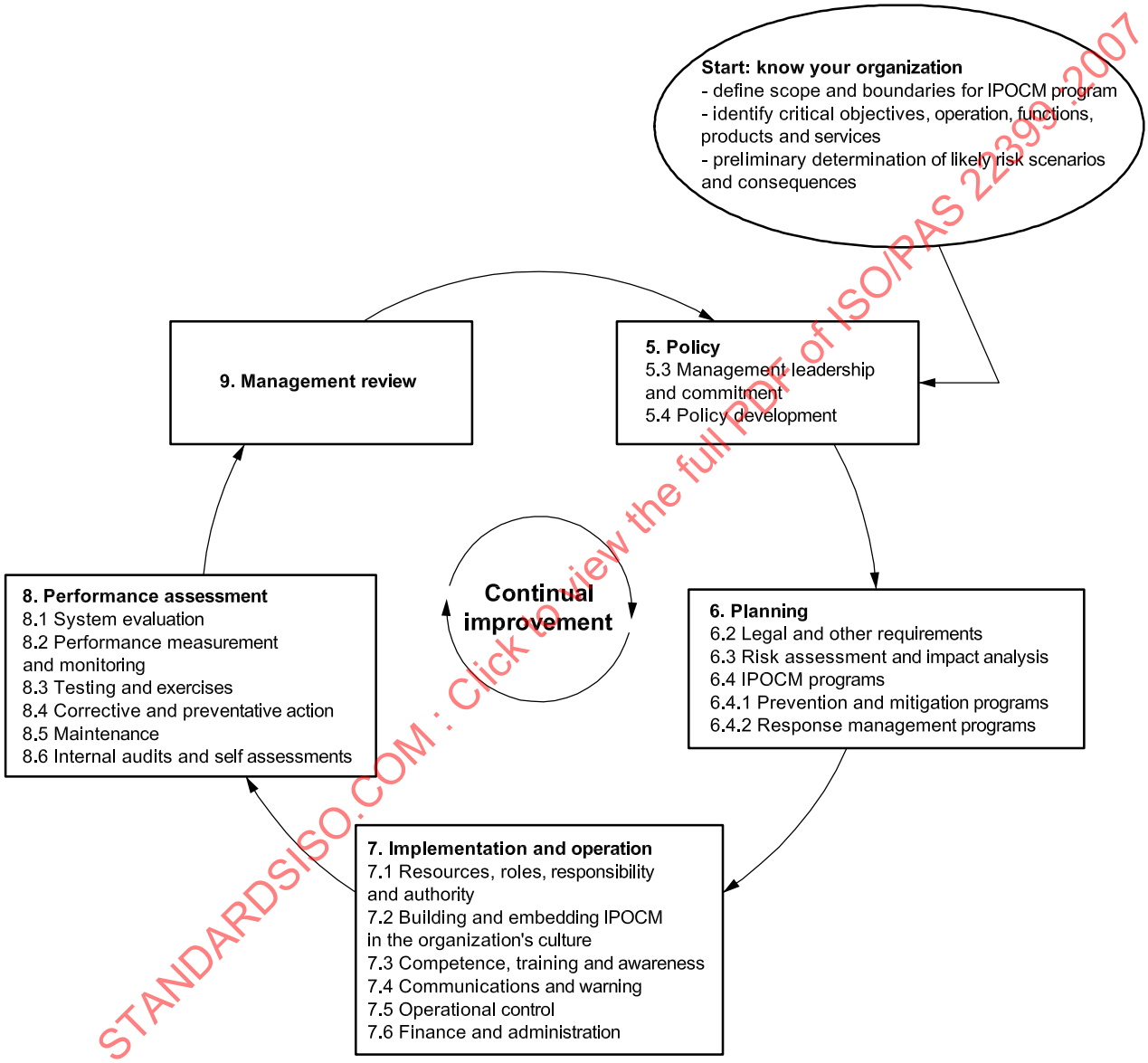


Figure 2 — Incident preparedness and operational continuity flow diagram

5 Policy

5.1 Establishing the program

The purpose of establishing an incident preparedness/operational continuity program is to ensure that all risk management and continuity activities are conducted and implemented in an agreed and controlled manner within the organization, thereby achieving a capability that meets the changing operational needs and is appropriate to the size, complexity and nature of the organization. It establishes a clearly defined framework for the ongoing management of the operational continuity capability.

The set-up activities, which usually take the form of a project, incorporate the end-to-end designing, building, implementing, and initial testing and exercising of the operational continuity capability. Early integration of IPOCM techniques and procedures in the organizational or business process design, planning, operations, training, and financial and economic policies and procedures should be considered. The ongoing maintenance and management activities include ensuring that operational continuity is embedded within the organization, is regularly tested and updated, and is considered whenever there is a significant change (e.g. environment, personnel, process or technology). IPOCM should also ensure the protection of stakeholders from possible adverse impact due to the disruption of the organization's operations and functions.

In summary, the management program represents the set-up, organization and ongoing management of the operational continuity capability.

5.2 Defining program scope

The organization should establish, document, implement, maintain, evaluate and continually improve its incident preparedness and operational continuity programs.

The organization should determine its critical operational objectives and activities as identified in strategies, business plans, policy and mission statements, risk management plans, and management tools such as SWOT analysis (Strengths, Weakness, Opportunities and Threats) and balanced scorecard. Operational critical processes should be identified and documented. This will allow the organization to focus the resources required to operate the organization's critical activities and functions within the context of the economic constraints of the organization.

The organization should establish a justification for the IPOCM program to determine the advantages of adopting an organization-wide approach. This may be based on:

— historical risk events within the organization;

— current and emerging risk exposures;

— operational disruption trends and prior incidents;

— cost increases and revenue losses arising from potential disruptions;

— risk financing costs;

— liabilities;

— social responsibilities;

— success and failure of other IPOCM projects and programs.

The organization should define and document the scope of its IPOCM system. An organization has the freedom and flexibility to define its boundaries, and may choose to implement this guideline with respect to the entire organization or to specific operating units or activities of the organization. It should consider, however, relationships with other organizations (partner entities) and stakeholders that contribute to or influence the organization's operations, including influences due to the outsourcing of processes/activities and the supply

chain. The scope should be directly related to the critical activities, functions, products, and services of the organization, defining the parameters for risk assessment and program development based on their criticality and the potential likelihood and consequences of an incident.

5.3 Management leadership and commitment

To be effective, an IPOCM program should be an integrated management process driven from the top of the organization, endorsed and promoted by the principal managers and executives. It should be managed at both the operational and organizational levels.

A number of professional incident preparedness and OCM practitioners and staff from other management disciplines and departments may be required to support and manage the IPOCM program. The quantity of resources required will be dependent upon the size and diversity of the organization.

5.4 Policy development

The organization should develop an IPOCM policy. Initially, this may be at a high level with further refinement and enhancement as the capability is developed. The policy should be regularly reviewed and updated in line with operational needs.

The IPOCM policy should provide the organization with documented principles to which it will aspire and against which its IPOCM capability should be measured.

The policy process of an organization should be composed of the following elements:

— top management should decide to develop an IPOCM program and communicate the decision throughout the organization;

— top management should establish a basic IPOCM policy;

— top management should communicate IPOCM activities of the organization to appropriate internal and external stakeholders;

— top management should ensure the availability of resources, such as budget and personnel necessary to perform activities in line with the basic IPOCM policy;

— top management should participate in a process of IPOCM program development.

5.5 Policy review

An organization should establish regular review of the IPOCM policy, considering the following, including but not limited to:

— results of IPOCM system review;

— changes in physical environment;

— changes in risk profile;

— changes in key personnel, operations, services, processes, products, suppliers, distributors, sourcing and outsourcing arrangements, and market forces;

— mergers and acquisitions;

— significant changes in the legislative and regulatory environment.

The IPOCM policy review should be integrated as part of the organization-wide business and operational planning process approved by top management. An organization-wide IPOCM policy should be cascaded down to each functional IPOCM policy.

5.6 Organizational structure for implementation

Policy and strategy for the program is developed and implemented by the project team. Determine the need for formal or informal project management structures based on:

— requirements for continuing top management visibility and involvement;

— skills requirements;

— resource, budget, and financing requirements for the project;

— specialist knowledge of the organization;

— areas of organization involved in the project.

An organization may appoint an IPOCM program coordinator who should have responsibility for establishing the IPOCM program. The IPOCM program coordinator should be responsible for coordinating incident preparedness and operational continuity projects, managing incident preparedness and operational continuity organizational structure, obtaining support from top management, developing and implementing the IPOCM program, providing training, and regularly reviewing the incident preparedness and operational continuity program among others. Responsibility and authority of top management should be defined in order to make it clear where ultimate responsibility lies in the organization.

A cross-functional IPOCM program committee may be formed. Its members should be composed of those involved in the major functions relating to the IPOCM program in order to enable it to address various organization-wide issues.

6 Planning

6.1 General

The organization should establish, implement, and maintain procedures to perform threat and hazard identification; risk, vulnerability, and criticality assessments; and impact analysis. This phase sets the parameters for the strategy and planning stages that will enable the organization to minimize the likelihood of a disruption and continue to meet its objectives during a disruption by performing at an acceptable level of operation. An understanding of the organization comes from identifying and evaluating potential risks and threats of disruptions to the organization as well as determining the duration of a disruption that is tolerable to its stakeholders. It is an essential pre-requisite for the following steps in this stage that the organization should understand its products and services, and how these are delivered by activities within the organization. Process mapping and other management tools may assist an organization to document this understanding of their critical operations.

6.2 Legal and other requirements

The organization should establish and maintain procedures to identify and evaluate the applicable legal, regulatory, and other requirements to which the organization subscribes that are related to the threats and risks that are applicable to its facilities, activities, products, services, contractors, and supply chain. The organization should keep this information up-to-date, and communicate relevant information on legal and other requirements to its employees and other relevant third parties including contractors.

The IPOCM system should commit to comply with applicable legislation and regulations, conform to directives and policies, and consider industry good practices concerning IPOCM activities, products, or services.

6.3 Risk assessment and impact analysis

There are various methodologies for risk assessment and impact analysis which will determine the order of the analysis steps adopted.

6.4 Hazard, risk, and threat identification

Hazard, risk, and threat identification should include, but not be limited to:

— naturally occurring hazards that can occur without the influence of people and have potential for direct or indirect impact on the organization's operations, people, property and/or environment (geological, meteorological and biological hazards);

— human and technology caused events (accidental and intentional);

— business-related events (positive and negative).

Risk identification should be an ongoing activity. The organization should find out sources and potentials to cause damage and identify risks. The organization should consult with appropriate authorities and other public services to identify potential risks to the organization and the stakeholders.

6.5 Risk assessment

The organization may use a formal and documented evaluation process to identify its risks and threats, the likelihood of their occurrence, and the vulnerability and criticality of people, property, the environment, and the organization itself to those threats. An organization should quantitatively or qualitatively estimate likelihood or probability of the identified potential risks and significance of impacts of the potential risks when they are realized. These estimation results should be used as input to risk evaluation to prioritize the potential risks.

An organization should assess potential risks on the basis of reasonable criteria by giving due consideration to all potential risks to its operations that it recognizes. The organization should consider various elements such as human lives, assets, compensation, profit, credit and natural environment. An organization should 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.

The organization should keep information related to its threat, risk and criticality assessments up-to-date and confidential, as is appropriate. Threat, risk and criticality assessments should be re-evaluated within the context of changes within the organization or made to the organization's operating environment, procedures, functions, and services.

6.6 Impact analysis

An organization should analyze impacts of disruptions to its operations and identify critical business operations that are given high priority for restoration, in order to set up recovery time objectives (RTO), see Annex A.

The organization should conduct an impact analysis to determine the potential for detrimental impacts of a disruption on operations including, but not limited to, the following:

— health and safety of persons in the affected area at the time of the incident (injury and death);

— health and safety of personnel responding to the incident;

— continuity of operations;

— property, facilities, and infrastructure;

— delivery of services;

— the environment;

— welfare of stakeholders;

— economic and financial impacts (including cost–benefit analysis);

— regulatory and contractual obligations;

— reputation of or confidence in the organization.

Among products and services provided by the supply chain, an organization should identify which are essential for support of the critical operations and take necessary precautions.

Organizations are dependent on an increasingly complex and interdependent service infrastructure comprising electricity, water, gas, transport and communications. Almost every organization is dependent on an effective working infrastructure, and hence, on the continuity of utility services. The corollary to this is that organizations are particularly vulnerable to disruption, from a continuity perspective, when a utility or critical infrastructure fails, therefore the organization should evaluate the impact on service disruptions on its critical operations.

The organization should consider the amount of time, cost, and resources required to restore critical functionality and clear backlogs resulting from the disruption including workarounds and continuity arrangements with other organizations.

6.7 Incident preparedness and operational continuity management programs

6.7.1 General

The IPOCM program should be measurable where practicable and consistent with the IPOCM policy and emphasize a commitment to incident and disruption prevention, compliance with applicable legal requirements and with other requirements to which the organization subscribes and continual improvement.

The organization should establish, implement, and maintain programs for achieving its objectives and targets at all relevant functions and levels of the organization, including:

— a means and timeframe by which they will be achieved;

— designation of responsibility for achieving the objectives and targets.

IPOCM programs, whether deterrent or responsive in nature, should be aligned and integrated with each other such that there are no conflicts of functionality, response, resource requirements or timings. Review plans as an integrated suite ensuring information flows and actions are logical, consistent and collaborative and resource allocations and usage are efficient, effective, and achievable. An organization may appoint a member of top management as the overall IPOCM program manager or coordinator.

6.7.2 Prevention and mitigation programs

The prevention and mitigation program should be based on the results of a threat and hazard identification and risk assessment. In case of an incident, the program should minimize the effects, plan to respond and achieve prompt recovery.

The program should consider removing, eliminating, or mitigating the threats and hazards through methodological and technological options, and the experience of other entities while taking into account financial, operational and business requirements as well as the views of partner organizations, and stakeholders.

The prevention and mitigation program should consider benefits and costs. These should include, but not be limited to, technological solutions, estimates of the effects of IPOCM efforts, the nature and costs of ongoing efforts, costs in relationship to the strategy's impact on non-IPOCM efforts, and the return on investment for organizations.

The prevention and mitigation program 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 mitigation plan should establish interim and long-term actions to eliminate hazards that impact the entity or to reduce the impact of those hazards, risks, and threats that cannot be eliminated. The organization should evaluate these actions to determine if these prevention and mitigation measures have themselves introduced new risks. Therefore, it is necessary to examine and assess risks associated with the prevention and mitigation solutions when developing the mitigation plan, as well as consider the consequences of any risk transfer strategies.

6.7.3 Response management programs

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

— 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;

— Continuity response: Processes, controls and resources are made available to ensure that the organization continues to meet its critical operational objectives;

— 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.

All response plans have common elements, including:

— the functional roles and responsibilities of internal and external agencies, organizations, departments, and individuals should be identified;

— lines of authority for those agencies, organizations, departments, and individuals should be established or identified;

— the competencies required should be specified;

— minimum resource requirements should be identified and locations secured.

The organization should also consider the range and nature of external interdependencies. The organization should identify contact details (business and after hours); stakeholder expectations (agreed minimum service levels, mandatory requirements, etc.); alternate functional relationships (e.g. locations for deliveries, changed frequency of interactions, etc.); and alternate sources for contract requirements. Consideration needs to be given to relationships with customers, suppliers, strategic partners, contractors, regulators, and competitors.

It should be recognized that depending on the severity and impact of the incident an organization, at the top management level, may make the decision to do nothing. In this case, top management may determine the risk to be acceptable and within the organization's risk tolerance. However, this should be done explicitly and documented. In some circumstances, the impact of a risk might be outside the organization's normal risk tolerance, but, due to the low likelihood of the risk occurring and/or the uneconomic cost of control, top management may accept the risk.

6.7.4 Emergency response management program

The principal purpose of the emergency response management program is the preservation of life and property, see Annex B. It should identify the criteria or triggers for managing the incident and implementing the emergency response. Incident management should be a process that can be rapidly triggered and should be activated whenever a likely incident starts to become apparent so that:

— no time is lost;

— decisions are made on what needs to be done;

— early steps are taken to contain and control events.

Organizations have a direct responsibility to safeguard the welfare of employees, contractors, visitors/customers where any incident poses a direct risk to life, livelihood and welfare. Special attention should be paid to any of the above groups with disabilities or other specific needs (e.g. pregnancy, temporary disability due to injury). Planning to meet these requirements in advance can reduce risk, enhance response times and reassure those affected. Due to the time sensitive nature of emergency response, scenarios should be considered based on the risk assessment. Furthermore, organizations should establish a system for risk communication with stakeholders as well as a socially responsible system for mutual assistance with other organizations and stakeholders.

In order to ensure top management is immediately notified that an incident has occurred, an organization should define multiple levels of severity and specify who should be notified and contacted for each level of severity. The organization should define and communicate what should be reported including what happens, where it happens, how serious it is, why it happens, how quickly it may be restored, and whether external assistance needs to be called in.

Plans should be tailored for the intended level of response and include:

— the role of the team within the organization's response structure (strategic/tactical/operational);

— a clearly defined process for providing team leaders with the information needed to inform their decision as to whether to invoke or mobilize a response team;

— a location/room/space for the team to meet should be pre-identified. This area will be the focal point for the organization's response. An alternate meeting point should also be nominated in case access to the primary location is denied.

The emergency response management program should outline human welfare strategies that include emergency response procedures and defined teams with clear roles and responsibilities for coordinating human welfare needs within the organization. Plans should be prepared including provisions for roles and responsibilities of teams with appropriate training to undertake such activities and functions.

To be effective, emergency response and management plans need to be pre-prepared and championed at the highest levels of the organization. They should have top management buy-in, job descriptions for all roles and personnel involved, and a budget. In larger organizations, they may also have an identified program manager or coordinator and development team responsible for strategic program development.

Resources for the emergency response and management plans should be specifically identified. A resource should be available in a timely manner and should have the capability to do its intended function. Restriction on the use of the resource should be taken into account, and application of the resource should not incur more liability than would failure to use the resource. The cost of the resource should not outweigh the benefit.

6.7.5 Continuity management program

Continuity plans are developed and documented in a comprehensive and simple manner that allows the organization to respond flexibly to a wide variety of potentially disruptive incident scenarios, see Annex C.

An organization may determine that each operational unit has specialized OCM plans that will be enacted, and that the organization will have an overarching OCM plan to manage the activities of each operational unit and to coordinate assets required for restoration and recovery activities.

The OCM plan is the toolbox that the incident management team can call upon and invoke/activate, based on the needs of the response to the incident. It helps to provide, through a set of logical sections, the information that would be required to maintain the organization at a time of a disruptive incident. The main objective of an OCM plan is to enable an organization to maintain what is critical in the event of a major interruption affecting its normal operations as usual. The OCM plan is developed in response to the anticipated consequences of incidents and is based on the risk assessment (highlighting the main areas of risk that require management) and the impact analysis (which would have identified the specific activities that are critical to the organization and the urgency in which they have to be recovered). The OCM plan describes and details the critical objectives, procedures, activities and contact information to be followed in the event of a disruptive incident affecting the ability of an organization, in whole or in part, to function at the agreed acceptable level in order to stabilize the critical operational functions and activities prior to medium- to long-term recovery.

The components and contents of OCM plans vary from organization to organization and have a different level of detail based on the scale, environment, culture and technical complexity of the industry and associated solutions, risk profile and environment in which it operates. Large organizations might require separate documents for each of their critical operation areas/functions, whereas smaller organizations might be able to cover what is critical to them within a single document.

The organization should identify equipment, supplies, and supply chain interactions that support its critical activities and develop strategies to secure operations and the supply chain. OCM plan strategies seek to improve the organization's resilience to a disruptive incident by ensuring that critical activities continue at an acceptable minimum level and to agreed timeframes stipulated within the risk and impact analysis. The ultimate aim is to re-establish operations within agreed timeframes, whilst maintaining the functions required to maintain operations and services, and to fulfill the key deliverables and obligations.

6.7.6 Recovery management program

The principle purpose of the recovery management plan is the staged return to a level of normal pre-incident activity while considering improved capabilities and performance. The organization should plan incident/disruption recovery taking into account contractual obligations, core activities, employee and neighboring community necessities, operational continuity, risk reduction, environmental remediation, and process improvement.

The recovery management plan should set specific recovery targets and procedures for implementing relevant activities. After reviewing information on the extent of the damage and its operational impact collected by emergency response and continuity teams, top management should select measures to be taken and specify recovery milestones, time and level of resource allocation. Based on the prioritization of operations predetermined in impact analysis, an organization should prioritize the actual measures, comprehensively considering the extent of damage on equipment, actual availability of personnel and prospective progress of restoration. In accordance with this priority, the organization should establish a plan for allocation of resources such as personnel and supplies.

The recovery plan should identify top management, decision makers, and other appropriate parties that will consider:

— progress and time table for restoration of operations;

— to what extent operations can be restored;

— total or partial suspension of some operations;

— when to resume all operations;

— additional resource investment required;

— improvement of processes, physical infrastructures, and operations;

— competitor and partner threats and opportunities;

— pre-emptive planning based on lessons learned.

7 Implementation and operation

7.1 Resources, roles, responsibility and authority

The organization should determine and provide resources and any necessary partnership arrangements essential to the implementation and control of the IPOCM system and to continually improve its effectiveness. Resources include human resources performing work affecting the IPOCM system and specialized skills, infrastructure, technology and financial resources, and information and intelligence. Personnel should be competent on the basis of appropriate education, training, skills, and experience.

Roles, responsibilities, and authorities should be defined, documented, and communicated in order to facilitate effective IPOCM.

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

— ensuring that IPOCM system elements and processes are established, implemented and maintained;

— assessing, reviewing and reporting to the top management about achieving the performance of the IPOCM system as a basis for its improvement;

— ensuring the promotion of awareness of the IPOCM system elements throughout the organization.

The organization should establish 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 IPOCM system.

The resource management objectives established should consider, but not be limited to, the following:

— personnel, equipment, training, facilities, funding, expert knowledge, materials, and the timeframes within which they will be needed from organization's resources and from any partner entities;

— quantity, response time, capability, limitations, cost, and liability connected with using the involved resources.

7.2 Building and embedding IPOCM in the organization's culture

Building, promoting and embedding an IPOCM culture within an organization ensures that it becomes part of the organization's core values and corporate governance, see Annex D. Effectively established, it instills confidence with stakeholders in the ability of the organization to cope with major disruptions.

To be successful IPOCM should be “owned” by everyone within an organization. All management levels, top and middle, play an essential role in the initial charting of critical activities and processes, so gaining their support at an early stage is vital. All staff should be convinced that IPOCM is a serious issue for the organization and that they have an important role to play in maintaining the delivery of products and services to their clients and customers. It is essential that awareness and training programs be established as part of the overall introduction of IPOCM.

Raising awareness with all the organization's staff is important to ensure that they are aware that IPOCM is being introduced and why. They will need to be convinced that this is a lasting initiative that has the support of the leadership of the organization. They need to have confidence that their jobs will be protected whilst any disruptive incident is being contained. It is also critical that individuals named in the IPOCM plans know what actions they are required to take when plans are invoked.

New recruits to an organization should be made aware of the IPOCM policy and their part in any plans. This can be done by incorporating IPOCM material into staff induction programs.

Awareness of the overall IPOCM program should be maintained. Methods may include internal newspapers, emails, the organization's intranet, team meetings and communications from top management. These might highlight examples where the organization successfully managed an incident or near-miss and praising those involved. The organization may also draw upon lessons identified from external failures.

7.3 Competence, training and awareness

The organization should ensure that any persons performing tasks for it or on its behalf that have the potential to prevent, cause, respond, mitigate or be affected 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 should assess training needs and should develop and implement a training and educational curriculum to support the IPOCM program. The training and education curriculum should comply with all applicable regulatory requirements. The objective of the training should be to create awareness and enhance the skills required to develop, implement, maintain and execute the IPOCM program. The frequency and scope of training should be identified.

The organization should establish, implement and maintain procedures to ensure persons working for it or on its behalf are aware of:

— the importance of conformity with the IPOCM policy and procedures, and with the elements of the IPOCM system;

— the significant threats and risks and related actual or potential impacts, associated with their work and the benefits of improved personal performance;

— their roles and responsibilities in achieving objectives and goals of the IPOCM program;

— the procedures for incident/disruption deterrence, mitigation, response and recovery;

— the potential consequences of departure from specified procedures.

7.4 Communications and warning

With regard to its threats and risks and IPOCM system, the organization should establish, implement and maintain procedures to disseminate and respond to requests for pre-incident, incident/disruption, and post-incident information. This should include procedures to provide information to internal and external audiences, including the media, and deal with their inquiries considering the requirements for routine and emergency states, for:

— internal communication between the various levels and functions of the organization and with partner entities;

— receiving, documenting and responding to relevant communication from external interested parties;

— adapting and integrating any national or regional risk or threat advisory system or equivalent into planning and actual operational use;

— alerting people potentially impacted by an actual or impending IPOCM incident;

— facilitating structured communication with emergency responders;

— assuring availability of the communication means with emphasis on a crisis situation and disruption;

— assuring the interoperability of multiple responding organizations and personnel;

— recording of vital information about the incident, actions taken and decisions made;

— the need for a central contact facility or communications hub.

The organization should decide, based on life safety as the first priority and in consultation with stakeholders, whether to communicate externally about its significant risks and threats, both before and after an incident, and should document its decision. If the decision is to communicate, the organization should establish and implement methods for this external communication, alerts, and warnings. The data communicated should preserve the integrity of sensitive information and make only non-sensitive information publicly available as is appropriate to coordinate IPOCM.

Prior to an incident the organization should develop communications strategy based on:

— who needs information;

— what and when information is needed or required;

— what organizational constraints or restrictions exist;

— who has the authority to approve and disseminate communications;

— how to interface with the media and how to conduct rumor control.

The organization may develop communications for release before an incident including proactive action guidelines and awareness of the IPOCM program. The strategy should also define the means by which different types of communications will be promulgated to each of the stakeholders.

The IPOCM communications system should be regularly tested.

7.5 Operational control

The organization should establish and implement a system of documented operational procedures and controls consistent with IPOCM policy, threats, risk and criticality assessment, impact analysis and organizational objectives. The organization should plan these operations, including maintenance, in order to ensure that they are carried out under specified conditions by:

— establishing, implementing and maintaining documented internal procedures;

— stipulating operating criteria in the internal procedures;

— establishing implementing and maintaining procedures related to the identified significant risks, threats and hazards to the organization and communicating applicable procedures and requirements to the supply chain, including contractors.

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.

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

The organization should establish procedures to create and maintain an IPOCM documentation system necessary to ensure the effective planning, operation and control of processes that relate to its IPOCM system.

7.6 Finance and administration

The organization should develop financial and administrative procedures to support the IPOCM program before, during, and after an incident. Procedures should be established to ensure that fiscal decisions can be expedited and should be in accordance with established authority levels and accounting principles. The procedures should include, but not be limited to, the following:

— establishing and defining responsibilities for the program;

— finance authority, including its reporting relationships to the program coordinator(s);

— program procurement procedures;

— payroll;

— accounting systems to track and document costs.

8 Performance assessment

8.1 System evaluation

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

Consistent with its commitment to compliance, the organization should establish, implement and maintain procedures for periodically evaluating compliance with applicable legal requirements, industry best practices, and conformance with its own policy and objectives.

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

8.2 Performance measurement and monitoring

Proactive monitoring should be used to check conformity and effectiveness of the IPOCM program, while reactive monitoring should be used to investigate, analyze, and record system failures, events and disruptions, including near-misses.

The organization should establish and maintain procedures to monitor and measure performance on a regular basis. These procedures should provide for:

— both qualitative and quantitative measures, appropriate to the needs of the organization;

— monitoring of the extent to which the organization's IPOCM objectives are being met;

— proactive measure of performance that monitor conformity with IPOCM program, operational criteria and applicable legislations and regulatory requirements;

— reactive measures for performance to monitor events and disruptions, including near-misses, and other evidence of deficient IPOCM performance;

— recording of data and results of monitoring and measurement sufficient to facilitate subsequent corrective and preventative action analysis.

8.3 Testing and exercises

An exercise program should be consistent with the objectives of the organization and the regulatory regimes to which it is subject. Exercises may include tests which anticipate a predetermined outcome, tabletops, simulations, and full operational exercises. Exercises should be based on realistic scenarios that are carefully planned and agreed with stakeholders, so that there is minimum risk of disruption to operational processes. Every exercise should have clearly defined aims and objectives and a post-exercise report that contains recommendations. This report should be formalized and used to improve IPOCM arrangements in a timely manner.

Exercises enable:

— verification that the IPOCM program incorporates the organizational critical activities and their dependencies and priorities;

— orientation and testing of those charged with the responsibility for the IPOCM program with their roles and responsibilities;

— continuous improvement of the IPOCM program;

— testing of the technical, logistical, administrative, procedural and other operational systems of the IPOCM plans;

— testing of IPOCM organization and infrastructure (including command centers and work areas);

— technology and telecommunications resource recovery, availability and relocation of staff;

— recording of data and results of testing and exercises sufficient to facilitate subsequent corrective and preventative action analysis.

Testing requirements should include, but not be limited to:

— staff plans;

— incident management plans;

— communication plans;

— recovery of critical activities;

— site plans;

— data back-up and recovery, and physical and computer security;

— requirements imposed by law.

8.4 Corrective and preventive action

The organization should establish, implement and maintain corrective procedures for dealing with actual and potential program shortfalls and for taking corrective action and preventive action. The procedures should define criteria for:

— identifying and correcting program shortfalls and taking actions to mitigate their impacts;

— investigating program shortfalls, determining their causes and taking actions in order to avoid their recurrence;

— evaluating the need for actions to prevent program shortfalls and implementing appropriate actions designed to avoid their occurrence;

— recording the results of corrective actions and preventive actions taken;

— reviewing the effectiveness of corrective actions and preventive actions taken.

Actions taken should be appropriate to the magnitude of the problems and the risk and their potential impacts encountered. The organization should ensure that any necessary changes are made to IPOCM system documentation.

8.5 Maintenance

A clearly defined and documented IPOCM maintenance program should be established. This program should ensure that any changes (internal or external) that impact the organization are reviewed in relation to IPOCM. It should also identify any new critical activities that need to be included in the IPOCM maintenance program.

The IPOCM maintenance program should periodically:

— review and challenge any assumptions made in the impact analysis;

— distribute updated, amended or changed IPOCM policy, strategies, solutions, processes and plans to key personnel under a formal change (version) control process.

The outcomes from the IPOCM maintenance process should include:

— documented evidence of the proactive management and governance of the organization's IPOCM program;

— verification that effective change (version) control processes or procedures are in place;

— verification that key people who are to implement the IPOCM strategy and plans remain in place;

— identification and documentation of the IPOCM maintenance schedule;

— verification of the monitoring and control of the IPOCM risks faced by the organization.

8.6 Internal audits and self assessment

The organization should ensure that internal audits and self-assessment of the IPOCM system are conducted at planned intervals to determine whether the IPOCM system conforms to planned arrangements for IPOCM and that the IPOCM program has been properly implemented and is maintained. The self-assessment should take into consideration the importance of the resilience of operations concerned and the results of previous audits.

Audit and self-assessment procedures should be established, implemented and maintained that address responsibilities and requirements for planning and conducting audits, reporting results and retaining associated records, determination of audit criteria, scope, frequency and methods, and provide information on the results of audits to management.

Selection of auditors and conduct of audits should ensure objectivity and the impartiality of the audit process.

Self-assessment of the organization's IPOCM program should incorporate verification that:

— the critical activities and their dependencies have been identified and included in the organization's IPOCM strategy;

— the organization's IPOCM policy, strategies, framework and plans continue to accurately reflect its priorities and requirements;

— the organization's IPOCM competence and its IPOCM capability are effective and fit-for-purpose and will permit management, command, control and coordination of a IPOCM incident;

— the organization's IPOCM solutions are effective, up-to-date and fit-for-purpose, and appropriate to the level of risk faced by the organization;

— the organization's IPOCM maintenance and exercising program have been effectively implemented;

— IPOCM strategies and plans incorporate lessons learned from exercises, as contained in a post-exercise report, and amendments arising from the maintenance program;

— change control processes are in place and operate effectively.

Self assessment should be conducted against the organization's objectives. It should also take into account relevant industry standards and good practice.

9 Management review

Top management should review the organization's IPOCM system, at planned intervals, to ensure its continuing suitability, adequacy and effectiveness. Reviews should include assessing opportunities for improvement and the need for changes to the IPOCM system, including the IPOCM policy and IPOCM objectives. Records of the management reviews should be retained.

Input to management reviews should include, but not be limited to:

— results of internal audits and evaluations of compliance with legal requirements and with other requirements to which the organization subscribes;

— communication(s) from external interested parties, including complaints;

— incident preparedness and operational continuity performance of the organization;

— extent to which organizational objectives have been met;

— status of corrective and preventive actions;

— follow-up actions from previous management reviews;

— changing threats and hazards, circumstances, including developments in legal and other requirements related to its risks, threats and hazards;

— recommendations for improvement.

The outputs from management reviews should include any decisions and actions related to possible changes to IPOCM policy, objectives, targets and other elements of the IPOCM system, consistent with the commitment to continual improvement.

Annex A
(informative)

Impact analysis procedure

A.1 General

When performing an impact analysis for the disruption of operations, an organization should categorize disruptions by extent in the following way:

a) Impact due to an incident limited to the organization's premises;

b) Impact due to an incident is spread into neighboring areas of the organization;

c) Impacts due to an incident in wide areas and where damage is spread through local citizens, other organizations in the community, community infrastructure, and supply chain.

A.2 Impact analysis procedure

Depending on the urgency and nature of critical operations affected by an incident, an organization should make an overall decision about operational impacts and restoration measures, including but not limited to the following interactive steps:

a) Estimation of acceptable downtime and treatment for a disruptive incident: Estimation of maximum tolerable period of disruption by considering the possible reaction of all stakeholders especially those to whom the delivery of products and services would be disrupted. Quantifiable costs and intangible impacts should both be assessed. The organization should evaluate impacts of the high-priority risks determined in the risk evaluation and assessment on its organizational management, and estimate how long operations can be suspended;

b) Determination of critical operations: The organization should identify critical operations that are given high priority for continuation when risks are realized. An organization should quantitatively evaluate impacts of suspension of the critical operations on its organizational management as these may increase over time;

c) Anticipation of damage on the critical operations: The organization should anticipate degree of damage on the critical operations by considering impacts on various elements such as facilities, equipment, personnel, raw materials, transport, packaging and customers. The organization should primarily consider the high-priority risks when anticipating damage. The organization, however, should note suspension of its functions, when anticipating damage, so that it can apply the damage anticipation results to other potential risks and unexpected risks;

d) Setting up recovery time objectives (RTO): Based on the impact analysis results, relationship with stakeholders and social mission, an organization should set up RTOs to restore the critical operations while considering maximum tolerable period of disruption of the critical operations. If the RTO is stipulated in contracts, special laws or ordinances, an organization should abide by such requirements when setting up its own RTO. In the event of wide-area disaster such as natural disaster, an organization should understand that cooperation with other organizations in allocating locally-available human and physical resources is essential for its own operational restoration because resources required for response or restoration may be scarce or not optimally distributed. Estimating progress of community recovery activities, the organization should set up its RTO in a way not to hinder rescue of human lives and local emergency operations, but to enable an organization to perform assistance activities in collaboration and cooperation with community's recovery activities;