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)

PDF disclaimer

This PDF file may contain embedded typefaces. In accordance with Adobe's licensing policy, this file may be printed or viewed but shall not be edited unless the typefaces which are embedded are licensed to and installed on the computer performing the editing. In downloading this file, parties accept therein the responsibility of not infringing Adobe's licensing policy. The ISO Central Secretariat accepts no liability in this area.

Adobe is a trademark of Adobe Systems Incorporated.

Details of the software products used to create this PDF file can be found in the General Info relative to the file; the PDF-creation parameters were optimized for printing. Every care has been taken to ensure that the file is suitable for use by ISO member bodies. In the unlikely event that a problem relating to it is found, please inform the Central Secretariat at the address given below.

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.

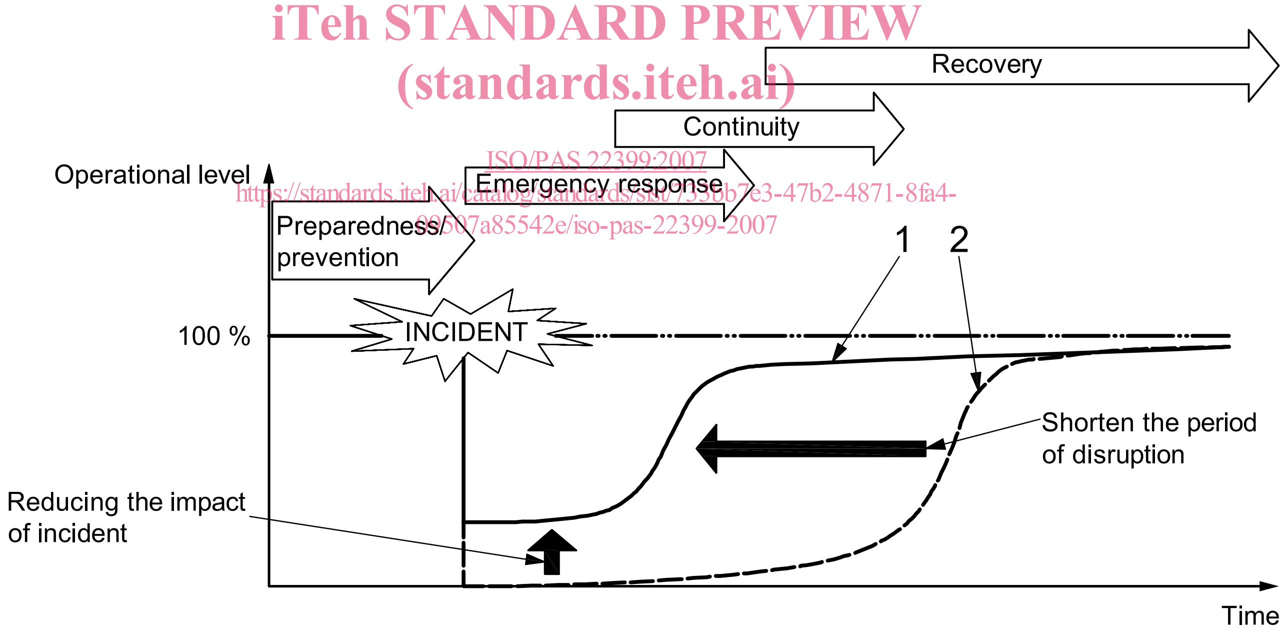
Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights.

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]