INTERNATIONAL STANDARD

ISO 22320

First edition
2011-11-01

Societal security — Emergency management — Requirements for incident response

Sécurité sociétale — Gestion des urgences — Exigences relatives aux réponses aux incidents

Reference number
ISO 22320:2011(E)

COPYRIGHT PROTECTED DOCUMENT

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.

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 22320 was prepared by Technical Committee ISO/TC 223, *Societal security*.

Introduction

In recent years there have been many disasters, terrorist attacks and other major incidents which have shown the importance of effective incident response in order to save lives, mitigate harm and damage, and to ensure a base level of continuity of essential societal functions. Such functions include health and rescue services, water and food supply, and electricity and fuel delivery. While in the past the focus of incident response has been national, regional or within single organizations, today and for the future there is a need for a multinational and multi-organizational approach. This is a result of worldwide governmental, non-governmental, commercial and industrial relationships and dependencies.

This International Standard enables public and private incident response organizations to improve their capabilities in handling all types of emergencies (for example, crisis, disruptions and disasters). The multiple functions of incident response are shared between organizations and agencies, with the private sector and the government having different levels of responsibility. Thus there is a need to guide all involved parties in how to prepare and implement effective incident responses. This International Standard will, based on minimum requirements, enable organizations involved to operate with joint optimum efficiency.

Effective incident response needs structured command and control, and coordination and cooperation, in order to establish coordination and cooperation, carry out command processes and facilitate information flow amongst the involved organizations, agencies and other parties.

Cross-organization, -region or -border assistance during incident response is expected to be appropriate to the needs of the affected population and also to be culturally acceptable. Therefore community participation in the development and implementation of incident response measures is essential. Involved organizations require the ability to share a common approach across geographical and organizational boundaries.

Information requirements, as well as requirements pertaining to the information management process and structure, may enable industry to develop technical solutions which will provide maximal interoperability according to information and communication exchange needs during incident response.

An effective incident preparedness and operational continuity management programme can be implemented using ISO/PAS 22399, and by conducting regular multi-organizational exercises.

This International Standard can be used alone or together with the other standards developed by ISO/TC 223.

Societal security — Emergency management — Requirements for incident response

1 Scope

This International Standard specifies minimum requirements for effective incident response and provides the basics for command and control, operational information, coordination and cooperation within an incident response organization. It includes command and control organizational structures and procedures, decision support, traceability, information management, and interoperability.

It establishes requirements for operational information for incident response which specifies processes, systems of work, data capture and management in order to produce timely, relevant and accurate information. It supports the process of command and control as well as coordination and cooperation, internally within the organization and externally with other involved parties, and specifies requirements for coordination and cooperation between organizations.

This International Standard is applicable to any organization (private, public, governmental or non-profit) involved in preparing or responding to incidents at the international, national, regional or local levels, including organizations

a) responsible for, and participating in, incident prevention and resilience preparations,

b) offering guidance and direction in incident response,

c) developing regulations and plans for command and control,

d) developing multi-agency/multi-organizational coordination and cooperation for incident response,

e) developing information and communication systems for incident response,

f) researching in the field of incident response, information and communication and data interoperability models,

g) researching in the field of human factors in incident response,

h) responsible for communication and interaction with the public.

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 22300, *Societal security — Vocabulary*[1)]

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO 22300 and the following apply.

1) To be published.

3.1
command and control
activities of target-orientated decision-making, assessing the situation, planning, implementing decisions and controlling the effects of implementation on the incident

NOTE This process is continuously repeated.

3.2
command and control system
system that supports effective emergency management of all available assets in a preparation, incident-response, continuity and/or recovery process

3.3
cooperation
process of working or acting together for common interests and values based on agreement

NOTE The organizations agree by contract or by other arrangements to contribute with their resources to the incident response but keep independence concerning their internal hierarchical structure.

3.4
coordination
way in which different organizations (public or private) or parts of the same organization work or act together in order to achieve a common objective

NOTE 1 Coordination integrates the individual response activities of involved parties (including public or private organizations and government) to achieve synergy to the extent that the incident response has a unified objective and to coordinate activities through transparent information sharing regarding their respective incident-response activities.

NOTE 2 All organizations are involved in the process to agree on a common incident-response objective and accept to implement the strategies by this consensus decision-making process.

3.5
emergency management
overall approach preventing emergencies and managing those that occur

NOTE In general, emergency management utilizes a risk-management approach to prevention, preparedness, response and recovery before, during and after potentially destabilizing and/or disruptive events.

3.6
incident command
part of an organized incident response structure

NOTE Incident command is the process that is conducted within the command structures that evolve during the management of an incident.

3.7
incident preparedness
activities taken in order to prepare incident response

3.8
incident response
actions taken in order to stop the causes of an imminent hazard and/or mitigate the consequences of potentially destabilizing or disruptive events, and to recover to a normal situation

NOTE Incident response is part of the emergency management process.

3.9
information
data that are processed, organized and correlated to produce meaning

3.10
operational information
information that has been contextualized and analysed to provide an understanding of the situation and its possible evolution

3.11
organization
group of people and facilities with an arrangement of responsibilities, authorities and relationships

EXAMPLES Company, corporation, firm, enterprise, institution, charity, sole trader, association, agency or parts or combination thereof.

NOTE 1 The arrangement is generally orderly.

NOTE 2 An organization can be public or private.

NOTE 3 This definition is valid for the purposes of quality management system standards. The term “organization” is defined differently in ISO/IEC Guide 2.

[ISO 9000:2005, definition 3.3.1]

NOTE 4 An organization can be either a standing group or a temporary one established ad-hoc to perform a specific and limited task.

4 Requirements for command and control

4.1 General

In general, command and control includes the following tasks:

a) establishing and updating goals and objectives for the incident response;

b) determining roles, responsibilities and relationships;

c) establishing rules, constraints and schedules;

d) ensuring legal compliance and liability protection;

e) monitoring, assessing and reporting on the situation and progress;

f) recording key decisions and assumptions;

g) managing resources;

h) dissemination of information;

i) taking and communicating decisions;

j) follow-up of decisions taken.

When multiple organizations, or different parts of one organization, are involved in the incident response

— consensus should be sought on overall mission objectives among involved organizations,

— structures and processes should permit operational decisions to be taken at the lowest possible level, and coordination and support offered from the highest necessary level,

— authority and resources shall be appropriate to this mission, and

— organizations shall encourage community participation in the development and implementation of incident response measures.

4.2 Command and control system

4.2.1 General

The objective of a command and control system is to enable organizations to carry out efficient incident responses, independently as well as jointly, with all other involved parties, in order to support all measures to save lives and limit adverse effects.

For the purpose of incident response the organization shall implement a command and control system which complies with relevant legislation and regulations as well as with the requirements of this International Standard.

Along with the setting up of a command and control system, the organization shall, as quickly as possible, determine the following lines of command both within the organization and with other organizations, actors and involved parties (e.g. designation of an incident commander):

a) a common understanding of the mission's purpose;

b) a common operational picture;

c) relations to other organizations that are not within the line of command;

d) appointment of persons with appropriate delegated authority to be accountable for leadership.

All of the above issues shall be taken into account during planning and exercises.

The command and control system shall be

— scalable for different incident types and involved organizations,

— adaptable to any type of incident,

— able to integrate different incident response organizations and involved parties, and

— flexible to the evolution of the incident and the outcome of incident responses.

To fulfil these tasks a command and control system shall include

— a command and control structure,

— a command and control process, and

— the resources necessary to implement the command structure and process.

The organizational structure, and the processes of the command and control system, shall be documented.

NOTE The number of persons, roles and responsibilities involved in the command and control organization may differ, depending on the scale of the incident.

4.2.2 Roles and responsibilities

One role within the organization, i.e. the incident commander, shall be identified as having the overall responsibility for command and control within that organization. This role shall have responsibility for

— initiating, coordinating and taking responsibility for all measures of incident response,

— setting up an organization,

— considering the activation, escalation and termination processes, and

— identifying and meeting legal and other obligations.

The command and control structure shall be organized in such a way that the incident commander can delegate authority.

4.2.3 Command and control structure

The command and control structure shall be divided into different levels (e.g. tactical, operational, strategic and normative levels) where different types of decisions are taken within different timescales. An example is given in Table A.1.

4.2.4 Levels of incident response

Corresponding to the predefined strategic and tactical command structure, the organization shall categorize a scale of incident severity levels. This is in order to implement, as soon as reasonably practicable, the appropriate level of command and control. An example is given in Table A.2.

4.2.5 Command and control process

The organization shall establish a command and control process which is ongoing and includes the following activities:

— observation;

— information gathering, processing and sharing;

— assessment of the situation, including forecast;

— planning;

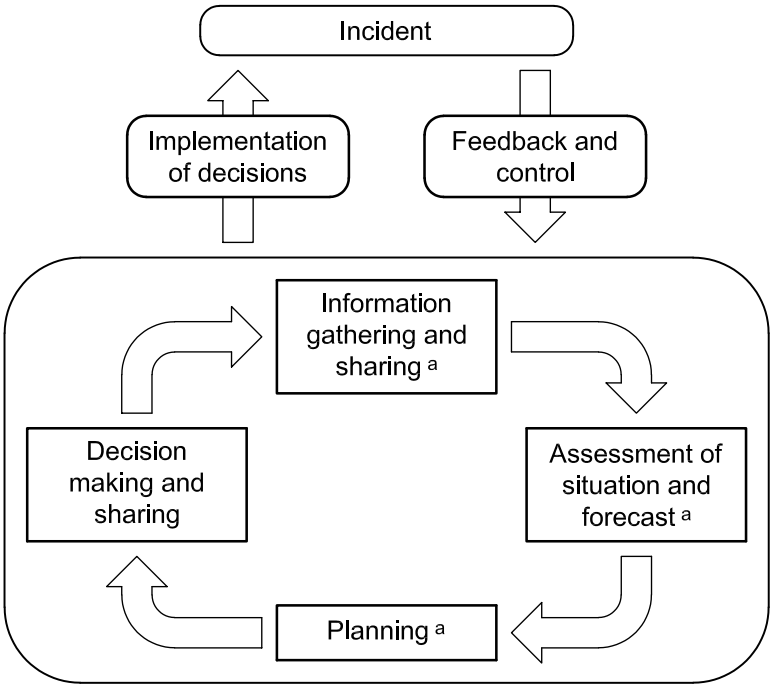
— decision-making and the communication of the decisions taken;

— implementation of decisions;

— feedback gathering and control measures.

The command and control process shall not be limited to the actions of the incident commander but shall also be applicable to all persons involved in the incident command team, at all levels of responsibility.

An example of a command and control process for an incident involving organization(s) under a single hierarchy command is given in Figure 1.



a With limited need for coordination with partners outside the organization.

Figure 1 — Example of command and control process in single hierarchical organization with limited coordination needs

NOTE The principles of command and control, coordination and cooperation apply to all organizations, whether they have a single or multiple hierarchical structure. In multiple hierarchical command and control structures the principles of coordination and cooperation are of enhanced relevance.

Within the command and control process, the key roles and responsibilities should be appropriate to the scale of the incident and should include at least the following functions:

a) personnel, administration and finance;

b) situational awareness and forecast;

c) operation (planning, decision-making, recording and implementation);

d) logistics;

e) media and press;

f) communications and transmission;

g) liaison (e.g. between responding organizations and NGOs);

h) alerting and contact (i.e. providing information to the public);

i) safety (e.g. health and safety of on-site personnel).

4.2.6 Decision-making

Decision-making should be as clear and transparent as possible. The decision-making should be communicated within the organization and to other involved organizations, as well as to the public, where appropriate.

4.2.7 Command and control resources

The organization shall establish appropriate locations and facilities for decision-making and the use of equipment, as well as a process to ensure that resources are available and functional according to need. This may involve the establishment of a control centre.

A command post from which the command and control functions are carried out may be either mobile or stationary. If appropriate, subcommand posts may be established either on-site or off-site.

4.3 Human factors

It is essential to consider the human role in incident response so that organizations can operate and meet the mission objectives without failure due to human limitations. Incident response activities shall be performed in a culturally acceptable way and appropriate to the needs of the affected population.

The organization shall consider the following human factors and shall take appropriate actions, e.g.

— workload distribution,

— health and safety,

— rotation of personnel,

— the design of human–machine–system interfaces.

When specifying and designing command and control structures, processes and equipment (especially for multi-organizational or cross-border use), account shall be taken of user differences such as competency levels, cultural backgrounds, language skills and operating protocols.

All actors involved shall be able to maintain an understanding of where they fit into the overall operational structure and shall have the appropriate competencies to handle the assets under their control through training and exercises.

When designing human–system interfaces, the actor's abilities, characteristics, limitations, skills, and task needs shall be primary considerations. Where electronic and/or mechanical systems are a part of a command and control structure, the human operator should be the highest authority in the human–machine–system, unless otherwise prohibited.

Suitable measures shall be taken to deal with spiritual, emotional and psychological stress experienced by any actors.

5 Requirements for operational information

5.1 General

Operational information is required during incident response in order to effectively manage incident response activities. It assists in building situational awareness, organizing resources and controlling activities. Operational information results from the processing of information (see Figure 2) concerning the incident, its location and incident response activities. Operational information can be generated dynamically by the incident or given as static information related to the location, i.e. buildings, infrastructure, population.

NOTE Operational information provides the basis for assessment of the situation and facilitates the accomplishment of the mission. The production, integration and dissemination of operational information (as described in 4.2) is an essential element in command and control.

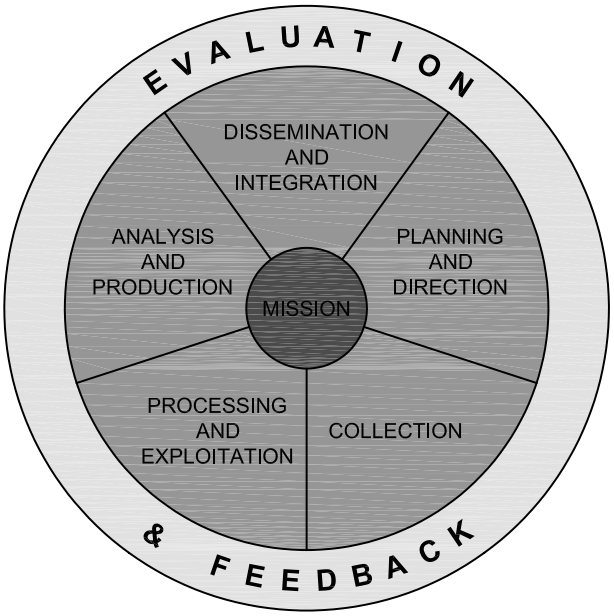


Figure 2 — Process of providing operational information

5.2 Operational information process

5.2.1 General

The organization shall establish an ongoing process for providing operational information, including the following activities:

a) planning and direction;

b) collection;

c) processing and exploitation;

d) analysis and production;

e) dissemination and integration;

f) evaluation and feedback.

NOTE These activities can take place simultaneously.

5.2.2 Planning and direction

Operational information shall be planned and prepared as part of the command and control process (see 4.2.5).

The following activities shall be included:

a) provisions of direction and mission objectives for the conduct of response operations;

b) specification of key questions for efficient decision-making;

c) planning of information collection with guidelines for collection methods and outcomes;

d) planning of information storage, exploitation, access rights and restrictions (database design, data formats, communication means, etc.);

e) identification of the information needs of involved parties;

f) identification of time constraints on the information required;

g) determination of dissemination requirements and protocols (technical and non-technical);

h) planning of human resources for the processing of operational information;

i) planning of information-processing equipment and its operational management.

5.2.3 Collection

Collection includes those activities related to the acquisition of operational information, e.g. to determine the direction, scheduling, and control of specific information sources.

The following activities shall be included:

a) identification of accessible information sources;

b) acquisition of information;

c) recording and logging of the information obtained, including the identification of sources and time.

5.2.4 Processing and exploitation

During processing and exploitation, collected data is converted into formats that can be readily used by decision-makers at all levels and other users with operational information needs.

The following activities shall be included:

a) adaption of the information into a relevant format(s) for effective dissemination;

b) initial evaluation of the information (the rating of its validity and reliability of its source), an example of which is given in Table A.3;

c) elimination of useless, irrelevant or incorrect information;

d) indication of the level of dissemination (including classification level);

e) evaluation of the credibility of the information, an example of which is given in Table A.4.

5.2.5 Analysis and production

During analysis and production, all available processed information is integrated, evaluated, analysed, and interpreted to create operational information. The outputs shall satisfy the incident commander's priority requirements or request for information.

The following activities shall be included:

a) revision of information;

b) prioritization and categorization of the information;

c) collation, assembly and synthesizing of the information;

d) risk identification and risk analysis;

e) inference of likely outcomes, deduction of trends;

f) production of proposals, recommendations, reports and other information-processing outputs.

5.2.6 Dissemination and integration

During dissemination and integration, operational information is delivered based on its categorization and used by decision-makers and other users. Dissemination is facilitated by a variety of means. The means are

determined by the needs of the users, the implications and criticality of the operational information, and the available transmission means.

The following activities shall be carried out:

— dissemination in accordance with specified dissemination requirements (technical and/or non-technical), which protocols should be established, documented and accessible by all operational information users;

— integration of the operational information into the user's operational picture.

5.2.7 Evaluation and feedback

During evaluation and feedback the organization shall make an assessment at all levels to see how well the activities involved with providing of operational information are being performed. Based on these evaluations, and any resulting feedback, corrective actions should be initiated, as required, to improve the process.

5.3 Operational information process criteria

The organization shall ensure within the operational information processes that the following criteria are considered:

— quality;

— perspective;

— synchronization;

— integrity;

— coordination and cooperation;

— prioritization;

— prediction;

— agility;

— collaboration;

— fusion.

NOTE See Annex B for further explanations and requirements.

6 Requirements for cooperation and coordination

6.1 General

In order to achieve effective incident response based on common interest and values, necessary cooperation agreements shall be established as a part of the incident preparedness where appropriate. This cooperation should be based on identified risks and consequences of possible incident scenarios for the organization.

For example, cooperation is needed between

— states, federal states or public authorities concerning mutual assistance in large scale disasters with their public services,

— governments on different levels with non-governmental organizations to provide incident response resources (e.g. agreements with radio stations for broadcasting warning and information, general agreements with non-governmental organizations),

— governments with private industry for incident response support activities (e.g. food, shelter, health services, transportation, communications),

— government with private industry to provide a certain level of disaster resilience, if not required by law (e.g. delivery of medicaments, vaccine, emergency power supply capacity, drinking water distribution), and

— within private industry, to provide mutual assistance to ensure continuation of production and delivery of incident-response-relevant products.

6.2 Cooperation

The organization shall

— assess the need for cooperation with other organizations, actors and involved parties to prepare effective incident response,

— establish cooperation agreements based on the assessment,

— enable integration of the cooperation partners into the command and control process by exchanging experts where appropriate, and

— test, evaluate and revise cooperation agreements at intervals specified by the organization.

6.3 Coordination

6.3.1 General

The organization shall assess the need of coordination with the relevant actors and parties and establish essential and necessary cooperation as a part of the incident preparedness. This coordination should be based on identified risks and consequences of possible incident scenarios for the organization. Coordination should result in humane, neutral and impartial incident relief.

The organization shall implement active working relationships with the relevant actors and parties in order to

— share information,

— contribute to the planning and decision-making process,

— implement the emergency's management decisions, and

— repeat the process as long as needed.

There shall be an exchange of experts where appropriate.

Figure 3 shows the multiple hierarchical command and control process with increased relevance of coordination.

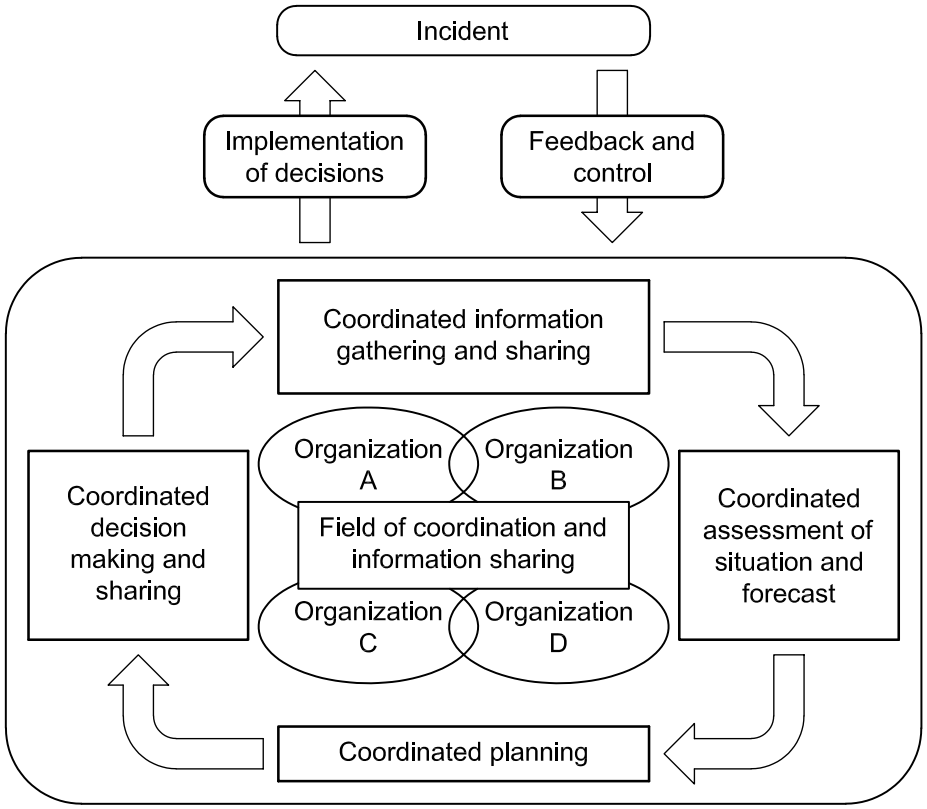


Figure 3 — Circular chart for multiple hierarchical command and control process with enhanced relevance of coordination

6.3.2 Coordination process

The organization shall establish a multi-hierarchical command and control process to achieve the best possible coordination among the involved organizations. This process shall respect existing cooperation agreements.

The involved organizations shall evaluate and, as considered appropriate and feasible, enable other organizations to participate in their decision-making for decisions that can affect them.

All organizations shall inform other organizations about decisions taken that can affect them.

The multi-hierarchical command and control process shall include the following.

a) **Early field coordination**

The first responders in the field shall implement an early field coordination based on available human capacity and experience. The initial incident response can be critical for saving lives/infrastructure and protection of people from being exposed to additional danger. This early field coordination shall later be replaced by planned and sustained coordination set up by command and control.

b) **Participation**

All organizations involved in coordination shall participate in deciding policies, procedures, strategies and plans which will affect them. The coordinators shall act in such a way that the confidence of the other actors is maintained.

c) **Equity**

Coordination shall ensure fairness in operations and shall respect the competencies and equal opportunities of all involved actors.

6.3.3 Coordination objectives

The organization shall ensure and prioritize objectives to achieve effective sustained coordination at all operational levels.

The organization shall assess the following coordination objectives with regard to the actual incident response activity, and shall evaluate their applicability:

a) establishment of a command and control structure;

b) identification of common and transparent decision-making procedures;

c) implementation of an information sharing and situational awareness policy;

d) implementation of a communication flow plan and communication guidelines;

e) division of operational tasks;

f) preparation and implementation of a logistic support network;

g) setting of boundaries (geographical and areas of responsibility) between the different organizations;

h) implementation of a special resources management;

i) interoperability of communication, geographic and information management network;

j) identification of critical needs;

k) continuity of the coordination process, taking account of staff turnover.

6.4 Information sharing

Information sharing is the basis for coordination and cooperation, and needs to be based on trust between the involved organizations. The success of joint multi-organizational or multinational incident response depends on timely and accurate information and effective operational information sharing.

The most timely and accurate operational information is the result of the unified integration of interagency and multinational operational information. This unified integration surpasses any single organization's effort.

For all information that needs to be shared, organizations shall establish the means to enable information sharing appropriate to the actual incident and the organizations involved.

The organization shall assess information-sharing needs as follows.

a) **Information-sharing environment**

   Creation of an operational information-sharing environment (composed of a common operating picture, an enhanced situational awareness).

b) **Unity of effort**

   Personnel of each organization need to view the situation from interagency or multinational viewpoint, as well as from their own perspectives.

c) **Adjustments to resolve significant differences**

   Differences in doctrine and procedures among the various organizations taking part in incident response may occur. A key to effective interagency or multinational operational information is readiness, beginning with the highest levels of command, to make the adjustments required to resolve significant differences.

d) **Information-processing planning**

   The need to determine the operational information that may be shared with other organizations early in the planning process and how it should be shared.

e) **Complementary incident response operations**

The need to share operational information about complementary operational activities of cooperating organizations.

f) **Language or symbology**

The need to set up a common language or symbology.

6.5 Human factors

When specifying and designing organizational structures, systems and equipment (especially for multi-agency, cross-border use), account shall be taken of differences such as competency levels, cultural backgrounds, operating protocols and languages.

NOTE It is usual in these situations to assume the lowest level of training.

Annex A
(informative)

Examples

A.1 Command and control structure

The requirements for command and control structure are specified in 4.2.3.

Table A.1 — Example of how to divide command and control structure into different levels

Command band	Command level	Description	Support
Strategic	Normative	State and national/federal government levels which operate according to the demands of the incident to either monitor, support or to intervene	Administrative (e.g. transport, waste management, education department, social services, financial support services)
	Command of strategic operations, policy and objectives	Heads of jurisdictions, e.g. the executive mayor, and chiefs of individual response agencies, the final operational decision-makers	
Tactical	Incident command, control, coordination cooperation	Incident command level of each participating organization	
	Task level control of operations	Control and support operation on the ground (crews and sectors/divisions, and at equivalent levels in support functions)	
NOTE 1 The objective of the strategic and tactical components is to be able to make comprehensive and effective decisions in a timely manner taking into account all necessary aspects under the time-critical regime of the incident, as shown exemplarily in Table A.1.			
NOTE 2 The objective of the administrative component on a strategic level is to bring administrative departments and institutions not directly involved in the strategic incident response “into the loop”, to enable them to assist in the return to normal conditions as quickly as possible.			

A.2 Levels of incident response

The requirements for levels of incident response are specified in 4.2.4.

Table A.2 — Example of how to categorize incident levels specified by resources deployed

Incident level	Description of incident level	Command level
Level 1	Event can be dealt with by resources deployed on the initial predetermined response.	Tactical: task level perhaps monitored and supported by tactical coordination
Level 2	Event can be dealt with by resources deployed solely by the affected organization.	Tactical command and coordination
Level 3	Event can be dealt with by resources deployed by the affected organization, supported by mutual aid assistance from neighbouring organizations under normal arrangements.	Strategic command and coordination of operations within the jurisdictions
Level 4	Event can be dealt with by resources deployed by the affected organization, supported by mutual assistance from organizations anywhere within the affected geographical jurisdiction. This assistance may be obtained through the use of a local governmental coordination centre.	Strategic command within and across the jurisdictions Probably monitored by grand strategic
Level 5	Covers the management of any incoming aid to help the organization respond to an event and will be facilitated by the affected government, using the existing protocols of bilateral treaties and international organizations.	Strategic command within and across the jurisdictions, sometimes requiring the support and even intervention of grand strategic

A.3 Processing and exploitation

The requirements for processing and exploitation are specified in 5.2.4.

The scales presented in the examples given by Table A.3 and Table A.4 are not progressive degrees of accuracy; they only help to formalize the credibility of information received. The letters and numerals are independent of each other and give an overall evaluation of the information. For example, a source known to be unreliable (E) might provide accurate information which is confirmed by other sources and therefore given the rating of E1. Additionally, a report evaluated as F6 may be totally accurate and should not be arbitrarily rejected.

Table A.3 — Example of how to rate reliability of sources

Rating	Description
A	**Completely reliable** — a tried and tested source which can be depended upon with confidence. These are extremely rare.
B	**Usually reliable** — a source which has been successful in the past but for which there is still some element of doubt in a particular case. Used for those of known integrity such as UN agencies, military imagery, some major NGOs, etc.
C	**Fairly reliable** — a source which has occasionally been used in the past and upon which some degree of confidence can be based. Could be applied to some press sources and NGOs.
D	**Not usually reliable** — a source which has been used in the past but has proved more often than not to be unreliable. Could be applied to some press sources and NGOs.
E	**Unreliable** — a source which has been used in the past and has proved unworthy of any confidence.
F	**Reliability cannot be judged** — a source which has not been used in the past.

Table A.4 — Example of how to rate credibility of information

Rating	Description
1	**Confirmed by other sources** — applicable when a source different from that originally reporting a piece of already existing information confirms that information.
2	**Probably true** — indicates confirmation of essential parts of information reported by another source. Aerial imagery is usually included in this category.
3	**Possibly true** — investigation of a reported fact or action has revealed no further information; however, the information is compatible with previous actions or background information available.
4	**Doubtful** — an item of information that tends to conflict with previously reported and validated information.
5	**Improbable** — an item of information that positively contradicts previously reported and validated information.
6	**Truth cannot be judged** — any freshly reported item of information that cannot be compared with any other category's source. It is used when ratings 1 to 5 cannot be applied. It is preferable to use a rating of 6 rather than an inaccurate 1 to 5 rating.

Annex B
(normative)

Operational information process criteria

B.1 General

This annex gives explanations and requirements further to those specified in 5.3.

B.2 Quality

The quality of outputs is paramount to the success of response operations and the incident commander's success in taking the right decisions. To achieve the highest standards of quality, operational information shall have the following characteristics.

a) **Anticipatory**

Operational information anticipates the needs of the incident commander to provide a foundation for operational planning and decision-making. Anticipating needs requires staff to identify and fully understand the command current and potential mission objectives, and the relevant aspects of the operational environment.

b) **Timely**

Operational information is available when required by the incident commander. Timely operational information enables the incident commander to anticipate events in the operational area. This, in turn, enables the incident commander to time operations for maximum effectiveness and to avoid being taken unawares.

c) **Accurate**

Operational information is correct, conveys an appreciation for facts and the situation as it actually exists, and provides the best possible estimate of the situation based on sound evaluation of all the information available. The accuracy of operational information outputs may be enhanced by placing proportionally greater emphasis on information reported by the most reliable sources. Source reliability should be evaluated through a feedback process.

d) **Usable**

Operational information is tailored to the specific needs of the incident commander, and is provided in forms suitable for immediate comprehension. The incident commander shall be able to quickly apply operational information to the task at hand. Providing useful operational information requires the producers to understand the circumstances under which their outputs are used.

e) **Complete**

Operational information answers the incident commander's questions as fully as possible. It also tells the incident commander what remains unknown.

f) **Relevant**

Operational information is relevant to the planning and execution of the operation at hand. It aids the incident commander in the accomplishment of the mission objective. Operational information contributes to the incident commander's understanding of the situation, but does not burden the incident commander with operational information that is of minimal or no importance to the current mission.

NOTE 1 Incident commanders communicate objectives and strategy to the operational information staff. Requirements are updated and refined as the situation evolves.

g) **Objective**

Operational information is unbiased, undistorted and free of prejudicial judgments.

h) **Available**

Operational information is readily accessible to the incident commander. Availability is a function of not only timeliness and usability, but also appropriate security classification, interoperability and connectivity.

NOTE 2 Operational information is kept at the lowest level of classification possible with the least restrictive releasability caveats, thereby maximizing accessibility.

B.3 Perspective

Operational information provides a comprehensive understanding of the situation faced. It is essential to recognize challenges to allow clear formulation of relevant and attainable objectives and strategy, determining, planning, and conducting operations that will help the successful conduct of response operations.

B.4 Synchronization

Operational information shall be synchronized with response activities and plans in order to provide answers to requirements in time to influence the decision they are intended to support. Operational information planning and direction, collection, processing and exploitation, analysis and production, and dissemination shall be accomplished with sufficient lead time to permit the integration of the output in decision-making and execution.

To avoid “late” operational information, a common error in attempting to synchronize operational information with operations and plans, sufficient lead time for operational information production to support decision-making should be allowed.

B.5 Integrity

Integrity requires adherence to facts and truthfulness in the way those facts are interpreted and presented. The methodology, production, and use of operational information shall not be directed or manipulated to conform to a desired result, institutional position, preconceptions of a situation or predetermined objective, operation, or method of operation.

B.6 Coordination and cooperation

Coordination and cooperation leads to common interests to achieve desired mission objectives. This unity of effort is essential to an effective operational information process, reducing unnecessary redundancy and duplication in operational information collection and production.

B.7 Prioritization

Prioritization of collection and analysis efforts are vital aspects of planning. Prioritization offers a mechanism for addressing requirements and effectively managing risk by identifying the most important tasks and applying available resources against those tasks.

Operational information consumers (e.g. incident commanders or decision-makers) should drive the prioritization effort by identifying the operational information needs and the relative importance of those needs.

B.8 Prediction

Operational information also provides a forecast of possible evolution. If there are inadequate or uncertain elements of information upon which to base forecasts, the operational information staff shall ensure that the incident commander is aware of this shortcoming.

B.9 Agility

The key to achieving agility is advance preparation and organization for all contingencies. Maintaining responsiveness under such circumstances requires considerable awareness and foresight. Therefore, structures, methodologies, databases and products for operational information should be sufficiently agile and flexible to meet changing situations, needs, priorities and opportunities.

B.10 Collaboration

By its nature, operational information is imperfect (i.e. everything cannot be known, analysis is vulnerable to deception, and information is open to alternative interpretations). The best way to avoid these obstacles and achieve a higher degree of fidelity is to consult with, and solicit the opinions of, other analysts and experts, particularly in external organizations.

B.11 Fusion

Fusion is the process of collecting and examining information from all available sources and operational information disciplines to derive as complete an assessment as possible of the situation.

Bibliography

[1] ISO/IEC Guide 2, *Standardization and related activities — General vocabulary*

[2] ISO 9000:2005, *Quality management systems — Fundamentals and vocabulary*

[3] ISO 9241 (all parts), *Ergonomic requirements for office work with visual display terminals (VDTs)*

[4] ISO 11064 (all parts), *Ergonomic design of control centres*

[5] ISO/PAS 22399:2007, *Societal security — Guideline for incident preparedness and operational continuity management*

[6] ISO Guide 73:2009, *Risk management — Vocabulary*

[7] International Red Cross Society and Red Crescent Society, *Introduction to the guidelines for the domestic facilitation and regulation of international disaster relief and initial recovery assistance*[2)]

2) Issued by the International Federation of Red Cross and Red Crescent Societies, P.O. Box 372, CH-1211 Geneva 19, Switzerland; available at http://www.ifrc.org/what/disasters/idrl/resources/guidelines.asp.

ICS 03.100.01

Price based on 21 pages