SLOVENSKI STANDARD
SIST-TS CEN/TS 17091:2018

01-december-2018

Krizno vodenje - Navodilo za razvoj strateške zmogljivosti

Crisis management - Guidance for developing a strategic capability

Krisenmanagement - Strategische Lösung

Gestion de crise - Recommandations pour le développement d'une capacité stratégique

Ta slovenski standard je istoveten z: **CEN/TS 17091:2018**

ICS:

03.100.01	Organizacija in vodenje podjetja na splošno	Company organization and management in general

SIST-TS CEN/TS 17091:2018 en,fr,de

iTeh STANDARD PREVIEW
(standards.iteh.ai)

TECHNICAL SPECIFICATION

SPÉCIFICATION TECHNIQUE

TECHNISCHE SPEZIFIKATION

CEN/TS 17091

October 2018

ICS 03.100.01

English Version

Crisis management - Guidance for developing a strategic capability

Gestion de crise - Recommandations pour le développement d'une capacité stratégique

Krisenmanagement - Strategische Lösung

This Technical Specification (CEN/TS) was approved by CEN on 20 May 2018 for provisional application.

The period of validity of this CEN/TS is limited initially to three years. After two years the members of CEN will be requested to submit their comments, particularly on the question whether the CEN/TS can be converted into a European Standard.

CEN members are required to announce the existence of this CEN/TS in the same way as for an EN and to make the CEN/TS available promptly at national level in an appropriate form. It is permissible to keep conflicting national standards in force (in parallel to the CEN/TS) until the final decision about the possible conversion of the CEN/TS into an EN is reached.

CEN members are the national standards bodies of Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, Former Yugoslav Republic of Macedonia, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and United Kingdom.

EUROPEAN COMMITTEE FOR STANDARDIZATION
COMITÉ EUROPÉEN DE NORMALISATION
EUROPÄISCHES KOMITEE FÜR NORMUNG

CEN-CENELEC Management Centre: Rue de la Science 23, B-1040 Brussels

Ref. No. CEN/TS 17091:2018 E

CEN/TS 17091:2018 (E)

Contents   Page

2

iTeh STANDARD PREVIEW
(standards.iteh.ai)

CEN/TS 17091:2018 (E)

European foreword

This document (CEN/TS 17091:2018) has been prepared by Technical Committee CEN/TC 391 "Societal and Citizen Security", the secretariat of which is held by NEN.

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

According to the CEN/CENELEC Internal Regulations, the national standards organisations of the following countries are bound to announce this Technical Specification: Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, Former Yugoslav Republic of Macedonia, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Serbia, Slovakia, Slovenia, Spain, Sweden, Switzerland, Turkey and the United Kingdom.

Introduction

Crises are the most serious challenge facing any organization. A crisis is an inherently abnormal, unstable and complex situation that represents a threat to the strategic objectives, reputation and, ultimately, the existence of an organization.

Crises present organizations with complex and difficult challenges that may have profound and far-reaching consequences. These consequences can be very damaging, especially where it is perceived that the organization failed to prepare for, manage or recover from a crisis. There is a risk of significant damage to reputation, and possibly of the collapse of the business and its operations. In short, crises are of potentially existential significance to an organization.

This technical specification sets out the principles and good practice for the provision of a crisis management response, delivered by strategic decision makers of any organization of any size in the public or private sector. The intention of this technical specification is to aid the design and ongoing development of an organization's crisis management capability.

In a general sense, a capability is a demonstrable ability to perform a function, under specified conditions, to defined levels. Capability is bounded by assumptions and expectations, and an organization should be able to ensure its capability within those parameters. In this technical specification, a crisis management capability should include the following aspects:

— physical (e.g. equipment, facilities and logistics);

— intellectual (e.g. doctrine, concepts and procedures);

— structural (e.g. organization, relationships and linkages); and

— human (e.g. selection, training and education).

This technical specification has close links with other disciplines such as organizational resilience, information security, emergency management, incident management, risk management, business continuity management, and security. Recognizing that crisis management varies from organization to organization and sector to sector, this technical specification provides the principles behind crisis management and the development of the necessary capabilities that are applicable to any size of organization.

The ability to manage crises is one aspect of a more resilient organization - where resilience is the ability of the organization to endure and continue through all manner of disruptive challenges, and to adapt as required to a changing operating environment. Resilience requires effective crisis management, which needs to be understood, developed, applied and validated in the context of the range of other relevant disciplines that include, amongst others, risk management, business continuity management, security management and crisis communication.

The ability to manage crises cannot simply be deferred until an organization is hit by a crisis. An organization should take every opportunity to practice their crisis response protocols in order to ensure the most effective transition to crisis management status in the event that an actual crisis situation is triggered. It requires a forward-looking, systematic approach that creates a structure and processes, trains people to work within them, and is evaluated and developed in a continuous, purposeful and rigorous way. The development of a crisis management capability needs to be a regular activity that is proportionate to an organization's size and capacity.

1 Scope

This document provides guidance on good practice for crisis management to help the strategic decision makers of an organization to plan, implement, establish, operate, monitor, review, maintain and continually improve a crisis management capability. It is intended for any organization regardless of location, size, type, industry, structure, or sector. While it is important to be aware of human and cultural factors as they can cause stress when working as individuals and as part of groups, it is not the purpose of this document to examine aspects of these areas in detail.

This document provides guidance for:

— understanding the context and challenges of crisis management;

— developing an organization's crisis management capability through preparedness (see 5.5);

— recognizing the complexities facing a crisis team in action;

— communicating successfully during a crisis; and

— reviewing and learning.

NOTE 1   For further information on organizational resilience, see ISO 22316.

This technical specification is intended for management with strategic responsibilities for the delivery of a crisis management capability. It is for those who operate under the direction and within policy of top management in:

— implementing the crisis plans and structures; and

— maintaining and assuring the procedures associated with the capability.

It is not intended for emergency and incident response - these require the application of operational procedures whereas crisis management relies on an adaptive, agile, and flexible strategic response (see 4.3).

It does not cover interoperability or command and control or business continuity management systems.

NOTE 2   For more information on interoperability and command and control, see ISO 22320. For more information on business continuity management systems, please see EN ISO 22301.

2 Normative references

There are no normative references in this document.

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

ISO and IEC maintain terminological databases for use in standardization at the following addresses:

• IEC Electropedia: available at http://www.electropedia.org/

• ISO Online browsing platform: available at http://www.iso.org/obp

3.1
crisis
unprecedented or extraordinary event or situation that threatens an organization and requires a strategic, adaptive, and timely response in order to preserve its viability and integrity

Note 1 to entry: The event might include a high degree of uncertainty.

Note 2 to entry: The event might exceed the response capacity or capability of the organization.

Note 3 to entry: There is no adequate or appropriate plan to deal with the event such that a flexible and dynamic approach is needed.

3.2
crisis management team
CMT
group of individuals functionally responsible for the direction and implementation of the organization's crisis management capabilities

Note 1 to entry: The crisis management team can include individuals from the organization as well as immediate and first responders, stakeholders, and other interested parties.

3.3
monitoring
determining of the status of a system, a process or an activity

Note 1 to entry: To determine the status there may be a need to check, supervise or critically observe.

[SOURCE: Annex SL of ISO/IEC Directives, Part 1: Consolidated ISO Supplement – Procedures specific to ISO]

Note 2 to entry: Monitoring in a flexible way, changes that might occur in the near future and will require a response. It includes forward looking for symptoms of change, updating the situation picture as the situation evolves, and identifying emerging opportunities or threats that demand a crisis response from the organization.

3.4
crisis management plan
document specifying which procedures and associated resources should be applied by whom and where to a particular type of crisis

[SOURCE: ISO 24518:2015]

3.5
business continuity
capability of the organization to continue delivery of products or services at acceptable predefined levels following a disruptive incident

[SOURCE: ISO 22301]

3.6
business continuity management
holistic management process that identifies potential threats to an organization and the impacts to business operations those threats, if realized, might cause, and which provides a framework for building organizational resilience with the capability of an effective response that safeguards the interests of its key stakeholders, reputation, brand and value-creating activities

[SOURCE: ISO 22301]

CEN/TS 17091:2018 (E)

3.7
media communications management
pro-active engagement with the media to ensure that accurate information is provided

Note 1 to entry: Coverage in the media, including social media, is monitored to improve situational awareness.

Note 2 to entry: An important aspect of effective media communications management action is providing accurate counterbalancing information where the organization's reputation is being damaged.

3.8
crisis management
development and application of the process, systems, and organizational capability to deal with crises

3.9
incident
adverse event that might be, or could lead to, a disruption, loss, emergency or crisis

3.10
interested party (preferred term)
stakeholder (admitted term)
person or organization that can affect, be affected by, or perceive themselves to be affected by a decision or activity

[SOURCE: Annex SL of ISO/IEC Directives, Part 1: Consolidated ISO Supplement – Procedures specific to ISO]

3.11
risk management
coordinated activities to direct and control an organization with regard to risk

[SOURCE: ISO Guide 73]

3.12
situation report
summary, either verbal or written, produced by an officer or body, outlining the current state and potential development of an incident or crisis and the response to it

[SOURCE: BS 65000]

3.13
situational awareness
state of individual and/or collective knowledge relating to past and current events, their implications and potential future development

Note 1 to entry: "Knowledge" can include human aspects including perceptions and sentiments.

3.14
top management
person or group of people who directs and controls an organization at the highest level

[SOURCE: Annex SL of ISO/IEC Directives, Part 1: Consolidated ISO Supplement – Procedures specific to ISO]

4   Crisis management: Core concepts and principles

4.1 Understanding crises and how best to manage them

The definition of crisis (see 3.1) captures the essence of crises, notably their extraordinary nature and strategic implications for an organization. An organization might have established processes for managing routine disruptions. However, crises can be dynamic and unpredictable, and become difficult to manage. These crises challenge organizations, their people, functions and processes, and require a dedicated and dynamic management and response.

Crisis management is the developed capability of an organization to prepare for, anticipate, respond to and recover from crises. This capability is not normally part of routine organizational management, and should be consciously and deliberately built and sustained through capital, resource and time investment throughout the organization.

Understanding the conceptual and practical relationship between incidents and crises is important, and Table 1 summarizes the key distinctions.

Table 1 — Distinctions between incidents and crises

Characteristics	Incidents	Crises
Predictability	Incidents are generally foreseeable and amenable to pre-planned response measures, although their specific timing, nature and spread of implications are variable and therefore unpredictable in detail.	Crises are unique, rare, unforeseen or poorly managed events, or combinations of such events, that can create exceptional challenges for an organization and are not well served by prescriptive, pre-planned responses.
Onset	Incidents can be no-notice or short notice disruptive events, or they can emerge through a gradual failure or loss of control of some type. Recognizing the warning signs of potential, actual or impending problems is a critical element of incident management.	Crises can be sudden onset or no-notice, or emerge from an incident that has not been contained or has escalated with immediate strategic implications, or arise when latent problems within an organization are exposed, with profound reputational consequences.
Urgency and pressure	Incident response usually spans a short time frame of activity and is resolved before exposure to longer-term or permanent significant impacts on the organization.	Crises have a sense of urgency and might require the response to run over longer periods of time to ensure that impacts are minimized.

CEN/TS 17091:2018 (E)

Characteristics	Incidents	Crises
Impacts	Incidents are adverse events that are reasonably well understood and are therefore amenable to a predefined response. Their impacts are potentially widespread. Minimal to minor impact, but manageable impact for interested parties/stakeholders, that will not lead to unmanageable collateral damage.	Due to their strategic nature, crises can disrupt or affect the entire organization, and transcend organizational, geographical and sectoral boundaries. Because crises tend to be complex and inherently uncertain, e.g. because a decision needs to be made with incomplete, ambiguous information, the spread of impacts is difficult to assess and appreciate. Impact, especially when not managed properly, to stakeholders/interested parties that will lead to damage for those involved.
Media scrutiny	Effective incident management attracts little, but positive, media attention where adverse events are intercepted, impacts rapidly mitigated and business-as-usual quickly restored. However, this is not always the case and negative media attention, even when the incident response is effective and within agreed parameters, has the potential to escalate an incident into a crisis.	Crises are events that cause significant public and media interest, with the potential to negatively affect an organization's reputation. Coverage in the media and on social networks might be inaccurate in damaging ways, with the potential to rapidly and unnecessarily escalate a crisis.
Manageability through established plans and procedures	Incidents can be resolved by applying appropriate, predefined procedures, available adequate resources, and plans to intercept adverse events, mitigate their impacts and recover to normal operations.	Crises, through a combination of their novelty, inherent uncertainty and potential scale and duration of impact, are rarely resolvable through the application of predefined procedures and plans. They demand a flexible, creative, strategic and sustained response that is rooted in the values of the organization and sound crisis management structures and planning.

4.2 The potential origins of crises

It is important for people at all levels of an organization to recognize the warning signs and understand that crises can be initiated in a number of different ways, summarized in the following three groups.

1) Extreme disruptive incidents that have immediately obvious strategic implications. These can arise, for example, from serious acts of malice, misconduct or negligence, or a failure (perceived or actual) to deliver products or services that meet the expected standards of quality or safety.

2) Those stemming from poorly-managed incidents and business fluctuations that are allowed to escalate to the point at which they create a crisis.

3) The emergence of latent problems with serious consequences for trust in an organization's brand and reputation. Such problems can "incubate" over time, typically as a result of:

10