ISO/PAS 22399 provides international best practice for preparedness and continuity management

Natural disasters, acts of terror, technology mishaps and environmental accidents have clearly demonstrated that no one is immune to intentional or unintentional crises. ISO/PAS 22399:2007 has been developed to address the global awareness that both the public and private sector must proactively prepare for unexpected, disruptive incidents.

by **Stefan Tangen** and **Marc Siegel**

In November 2007, ISO published a Public Available Specification which is the first internationally ratified document regarding preparedness and continuity management. ISO/PAS 22399:2007, *Societal security – Guideline for incident preparedness and operational continuity management,* is an international consensus on best practices from the five main contributions made to the ISO Workshop on Emergency Preparedness held in Florence, Italy, in April 2006. This "best of five" guideline draws its key elements and attributes from:

- NFPA 1600, *Standard on Disaster Management and Business Continuity Programs* of the US National Fire Protection Association (NFPA);

- BS 25999-1, *Business Continuity Management* Part 1: *Code of Practice* of the

British Standards Institution (BSI);

- HB 221, *Business Continuity Management*, of Standards Australia (SA);

- SI 24001:2007, *Security and continuity management systems – Requirements and guidance for use* of the Standards Institution of Israel (SII);

- the work of the Japanese Industrial Standards Committee (JISC).

ISO/PAS 22399 establishes the process, principles and terminology for incident preparedness and operational continuity management (IPOCM) within the context of societal securi-

The guideline is a tool to allow public or private organizations to consider the factors and steps necessary to prepare for an unintentionally, intentionally, and/or naturally caused incident (disruption, emergency, crisis or disaster) so that they can manage and survive the incident and take the appropriate actions to ensure the organizations' continued viability.

The guideline is a tool for public or private organizations

ment process that identifies potential impacts that threaten an organization, and it provides a framework for minimizing their effect.
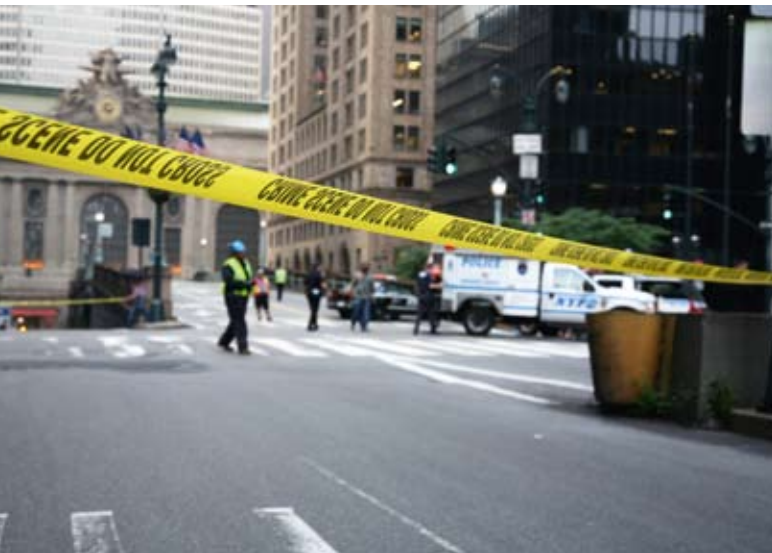
Built to be business friendly

All organizations face a certain amount of uncertainty and risk. The challenge is to determine how much risk is acceptable and how to cost-effectively manage risk while meeting the organization's strategic and operational objectives.

The ISO/PAS 22399 approach to preparedness and continuity management emphasizes business friendliness.

ISO/PAS 22399 uses classical management approaches recognized as good business practices. By building on the general concepts of Total Quality Management and the Plan-Do-Check-Act (PDCA) approach (see **Figure 1**), ISO/PAS 22399 follows the easily understood and widely applied management framework for identifying problems and their solutions.

Through a structured and systematic process, organizations can manage risk and uncertainty proactively, as well as mitigating and recovering from unavoidable disruptions. It must be recognized that by implementing appropriate preventive controls and

ty. The purpose of the 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.

Today, organizations must proactively prepare for potential incidents and disruptions in order to avoid suspension of critical operations and services. When crises occur, they need to be ready to resume operations and services as rapidly as possible. ISO/PAS 22399 describes a holistic manage-

ISO/PAS 22399 integrates preparedness and continuity into the culture and management practices of the organization to enhance its resilience. It is written with the flexibility necessary for the organization to adopt a system that supports its mission and objectives.
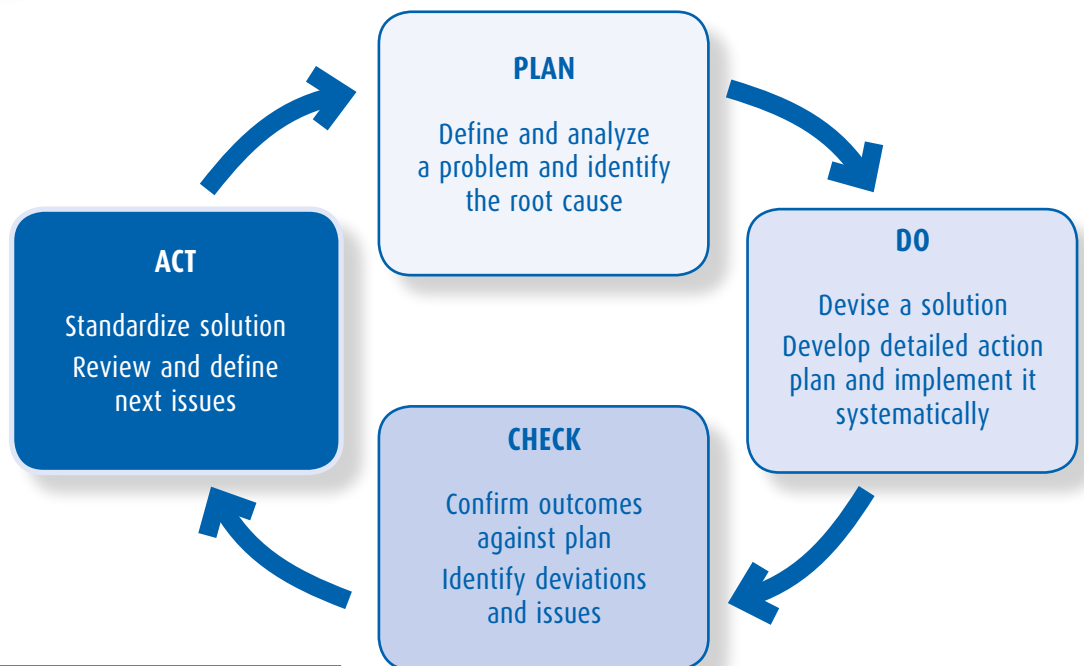
risk treatments, an organization can reduce the residual risk of a disruptive event, be it be it natural, accidental, or intentional.

However, it is not possible to completely eliminate the likelihood of a disruption. Therefore, effective security-,

CONTINUITY AND RISK

preparedness- and continuity-related risk management must address mitigation, response, operational/business continuity, and recovery in addition to prevention and deterrence.

ISO/PAS 22399 incorporates the key elements and attributes of preparedness and continuity management into a continual improvement management cycle (see **Figure 2** *overleaf*). Major attributes recognized as common elements in all five of the contributing documents include:

PLAN

Define and analyze a problem and identify the root cause

ACT

Standardize solution Review and define next issues

DO

Devise a solution Develop detailed action plan and implement it systematically

CHECK

Confirm outcomes against plan Identify deviations and issues

Figure 1 – *Plan-Do-Check-Act (PDCA).*

Plan

- Project initiation: definition and scope, resource allocation, management support

- Policy and management commitment

- Risk assessment and impact analysis

- Development of management strategies.

Do

- Development and implementation of operational and control strategies, plans, procedures and programmes, including:

  – awareness, competence and training strategies, plans and programmes

  – definition of roles and responsibilities

  – communication strategies, plans and programmes

  – allocation of human, physical and financial resources.

Check

- Performance assessment and evaluation and system maintenance.

Act

- Review and improvement.

The approach of combining key elements and attributes into a continual improvement cycle is not new. Indeed, this is one of the major improvements of ISO/PAS 22399 over some of its contributing documents. The ISO/PAS 22399 approach is aligned with the globally accepted ISO 9001:2000 (quality management), ISO 14001:2004 (environmental management) and ISO/IEC 27001:2005 (information security management) standards to support consistent and integrated implementation and operation with related management standards.

About the authors

Dr. Stefan Tangen is the Secretary of ISO technical committee ISO/TC 223, *Societal Security*, and a project manager at SIS, Swedish Standards Institute. He has previously been the Secretary of ISO/TC 184/SC 2, *Robots and Robotic Devices*, and has worked with numerous Swedish mirror committees. Before joining standardization, he worked as a senior researcher at the Royal Institute of Technology in Stockholm. Dr. Tangen holds a PhD in production engineering.

E- mail stefan.tangen@sis.se

Web www.sis.se

Dr. Marc Siegel serves as security management system consultant for ASIS International. He is an Adjunct Professor at San Diego State University, USA in the College of Business Administration and the Master's Program in Homeland Security. He initiated the concept and spearheaded the effort with the Standards Institution of Israel to develop the Israel National Standard: *Security and Continuity Management Systems – Requirements and guidance for use*. He is co-author of ISO/PAS 22399, *Societal Security – Guideline for incident preparedness and operational continuity management*.

E-mail marc_h_siegel@yahoo.com

Web www.asisonline.org

One suitably designed management system can thus satisfy the requirements of all these standards, providing the private and public sectors with a flexible, robust and cost-effective tool to assure the resilience of their organizations.

Enhancing cross-jurisdictional protection

For many years, the need for preparedness and continuity standards has been globally recognized, leading to disparate national efforts to develop relevant standards. However, since the challenges of natural disasters and intentional disruptions do not recognize borders or jurisdictional boundaries, this has led to confusion as to which standard to apply.

In April 2006, the American National Standards Institute (ANSI) and the New York University International Center for Enterprise Preparedness (NYU InterCEP) organized and hosted an ISO International Workshop Agreement meeting to address this issue.

Rather than endorse a single document, delegates from around the world endorsed the concept of using the contributions as a basis for developing an internationally recognized set of best practices for preparedness and continuity management. The recommendation was to develop a single globally recognized roadmap for preparedness and continuity management, and thereby eliminate the confusion of separate national approaches.

Thus the "best of five" concept was born. Thereafter, teams representing the different national documents, including the British Standards Institution, the Japanese Industrial Standards Committee, National Fire Protection Association/New York

ISO/PAS 22399 is aligned with globally accepted ISO management standards

Universtity, SA and Standards Institution of Israel, joined a special Task Group led by Mr. Ivar Jachwitz, of Standards Norway. Within a few months, the Task Group was able to fully agree on common principles

and develop the first draft of ISO/PAS 22399. The fast-track mechanism of an ISO Publicly Available Specification was chosen to address this pressing market need.

The document went through a review process by the member countries of ISO technical committee ISO/TC 223, *Societal security,* and a final draft was crafted and submitted for ballot. ISO/PAS 22399 received unanimous approval by the countries casting ballots, including an endorsement by all the member countries of the Task Group.

Demonstrating a spirit of international cooperation on the important issue of emergency and disaster management, in just a little over 15 months from

the conclusion of the IWA, ISO/TC 223 has achieved final agreement and approval on a uniform global vision of best practices for incident preparedness and continuity management.

The unanimous vote of approval of ISO/PAS 22399:2007 was largely due to it being considered stronger than the sum of its parts, and to the need to bring order to a fractured landscape of separate national standards.
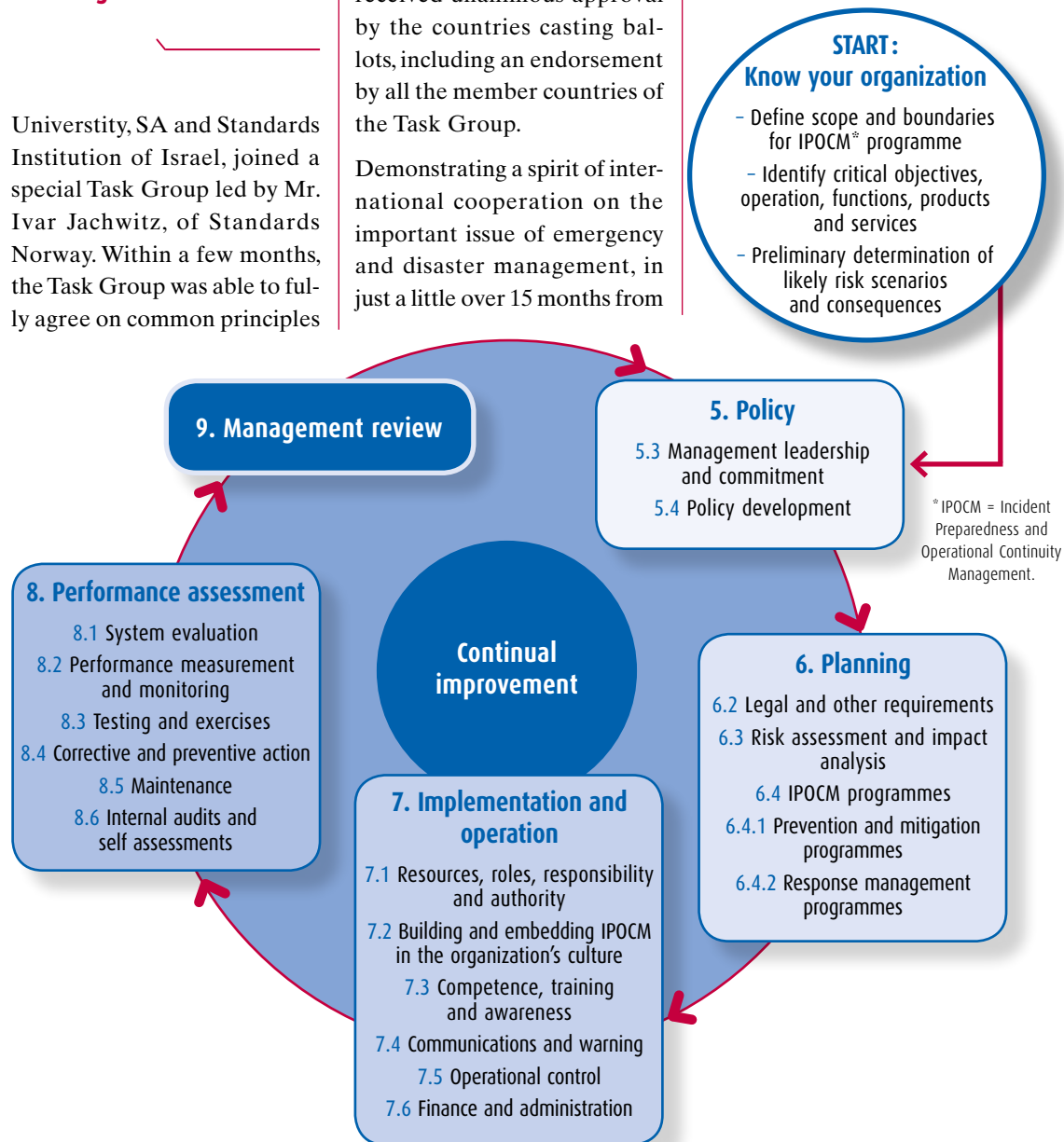

Figure 2 – *Preparedness and continuity management flow diagram.*

ISO/TC 223, *Societal security*

ISO/PAS 22399 is the first deliverable of ISO/TC 223. Reactivated by the ISO Technical Management Board in 2006, it was tasked with developing standards in the area of crisis and continuity management. SIS, Swedish Standard Institute, is responsible for the secretariat and the committee is comprised of representatives from business, industry, the first responder community, emergency and disaster managers, security professionals, government and non-governmental organizations from more than 50 countries.

The committee will address issues before, during and after a disruptive incident relevant to individual organizations, as well as cross-jurisdictional and multi-organizational interactions. It will develop the future ISO 22300 family of standards. It currently has the following work programme:

- fundamentals and vocabulary

- principles for command, control, coordination and cooperation in resolving incidents

- essential information and data requirements for command and control

- inter- and intra-organizational warning procedures

- principles and procedures for exercises and testing

- public/private partnerships.

At the 4th plenary meeting, held in The Hague, 14-16 November 2007, it was decided to initiate the ISO/PAS 22399 as a DIS (Draft International Standard), which means that the committee aims to turn the document into a full International Standard as soon as possible. The committee also decided to prepare a new work item proposal for a management system within the area of societal security.

The work of ISO/TC 223 will become increasingly important in coming years to help organizations and communities prepare for, respond to and recover from disruptive incidents that could escalate into emergencies, crises or disasters. ISO/TC 223 provides the only global forum to develop international standards, procedures and systems needed to protect human and physical assets from intentional, unintentional and naturally occurring disasters.

A level playing field of global consensus in preparedness and continuity management is key to protecting lives and helping affected communities rebound when disaster strikes, thus giving them more resilience than those which are not prepared. Global trade and the cross-border nature of the challenges require international cooperation, which is the cornerstone of the ISO process. •