Societal Security Management System Standards

Dr. Marc Siegel
Security Management System Consultant
ASIS International

ISO/TC 223: *Societal Security*

Ever since the term "Societal Security" was first used by Barry Buzan in the book *People, States and Fear: National Security Problem in International Relations* (1991), its exact meaning has been widely debated. ISO – International Organization for Standardization – Technical Committee *ISO/TC 223: Societal Security* integrates a range of interconnected disciplines including: asset protection (human, physical, environmental, financial, and intangible), security, risk management, preparedness, crisis management, emergency management, business continuity management, recovery management and disaster management. Therefore, Societal Security standardization addresses the challenges an organization, group of organizations, or society may face before, during and after a disruptive event.

International standardization in the area of Societal Security is aimed at achieving individual, multi-organizational and societal sustainability and resilience through improved management, information sharing and interoperability. This can be achieved by coordinated planning for the technical, human, organizational, and functional aspects of prevention, preparedness, response, continuity and recovery to and from disruptive events. ISO/TC 223 uses an all-hazards approach covering all necessary activities in the key phases of management of a disruptive event. This perspective improves the capacity of public and private organizations and stakeholders to prepare for and respond to a wide range of threats and hazards (natural, technological, and human – both unintentional and intentional)

An Integrated Approach to the Management of Risk

All organizations face a certain amount of uncertainty and risk. In order assure sustainability of operations and maintain resilience, competitiveness and performance, organizations must have a system to manage their risks. The challenge is to determine how much risk and uncertainty is acceptable and how to cost effectively manage the risk and uncertainty while meeting the organization's strategic and operational objectives. Given the finite resources of organizations, it is imperative that they have business-friendly tools to address any array of threats, hazards and risks they may face. Standards will be playing an ever increasing role in the management of operational risks organizations face.

An integrated approach can help avoid segregating or siloing risks and provides an overall risk profile allowing the organization to better understand the relationships between risks and identify solutions to problems. It leverages the perspectives, knowledge and capabilities of divisions and individuals within an organization. Because of the relatively low probability and yet potentially high consequence nature of many natural, intentional, or unintentional threats and hazards that an organization may face, an integrated approach allows an organization to establish priorities that address its individual needs for managing operational risks within an economically sound context.

By bringing together the disciplines of security, risk management, preparedness, crisis management, emergency management, business continuity management, recovery

management, and disaster management, Societal Security recognizes that public and private organizations have differing economic drivers for managing disruptive events. Some organizations will focus the bulk of their efforts on the avoidance or reduction of risks prior to a disruptive event, others will emphasize the management of a crisis as the event unfolds, while others will focus of preparing for and responding to the impacts and consequences of a disruptive event. These are complementary rather than mutually exclusive perspectives. However, in determining a strategy for the spectrum of options for the management of risks before, during and after a disruptive event, business constrains and realities usually determine where an organization will focus its efforts.

Building a Family of Societal Security Management System Standards

Various disciplines, practitioners and organizations focus different weight on the management of risk related to assuring continued sustainability and resiliency in light of a disruptive event, regardless of the cause. One size does not fit all; therefore, it is important that private and public organizations make appropriate choices that fit their respective business needs. The organization needs to determine which disciplinary perspective, or perspectives, it will adopt in developing a strategy for managing risks and consequences of disruptive events.

In order to create a business friendly family of standards and minimize the financial burden on organizations seeking to enhance sustainability and resilience performance, an umbrella management system standard is required to develop a strategic approach to managing a disruptive event. This high-level standard will establish the management system framework that can be used regardless if the organization wishes to emphasize security, risk management, preparedness, crisis management, emergency management, business continuity management, recovery management and/or disaster management.

The generic criteria of a high-level Societal Security standard provides a framework for any organization, regardless of size or type, to tailor its application and implementation to address the organization's particular needs and special circumstances. The high-level Societal Security standard can be aligned with other ISO management system standards in order to support consistent and integrated implementation and operation with the related management standards. One suitably designed management system can thus satisfy the requirements of all these standards. ISO published *ISO Guide 72:2001 - Guidelines for the justification and development of management system standards* in order support consistent and integrated implementation and operation with related management standards. Clearly Guide 72 is the starting point for development of any management system standard.

One generic management system framework for security, preparedness and continuity (SPC) management, applicable to all the abovementioned discipline perspectives, serves as the high level Societal Security management system standard. This is complemented by other management systems standards developed using an identical management system structure and approach. Organizations can then develop and implement a strategy appropriate to their business realities. They can decide whether to pursue a broad spectrum view of the high level standard or focus the weight of their strategic approach on managing risks before a disruptive event and/or addressing the impacts and consequences of disruptive events. Obviously for a robust strategy an organization should consider the range of risk control options of the different disciplines.

Figure One illustrates how the various disciplines and perspectives can be accommodated by constructing a family of standards addressing the spectrum of operational risk control strategies.

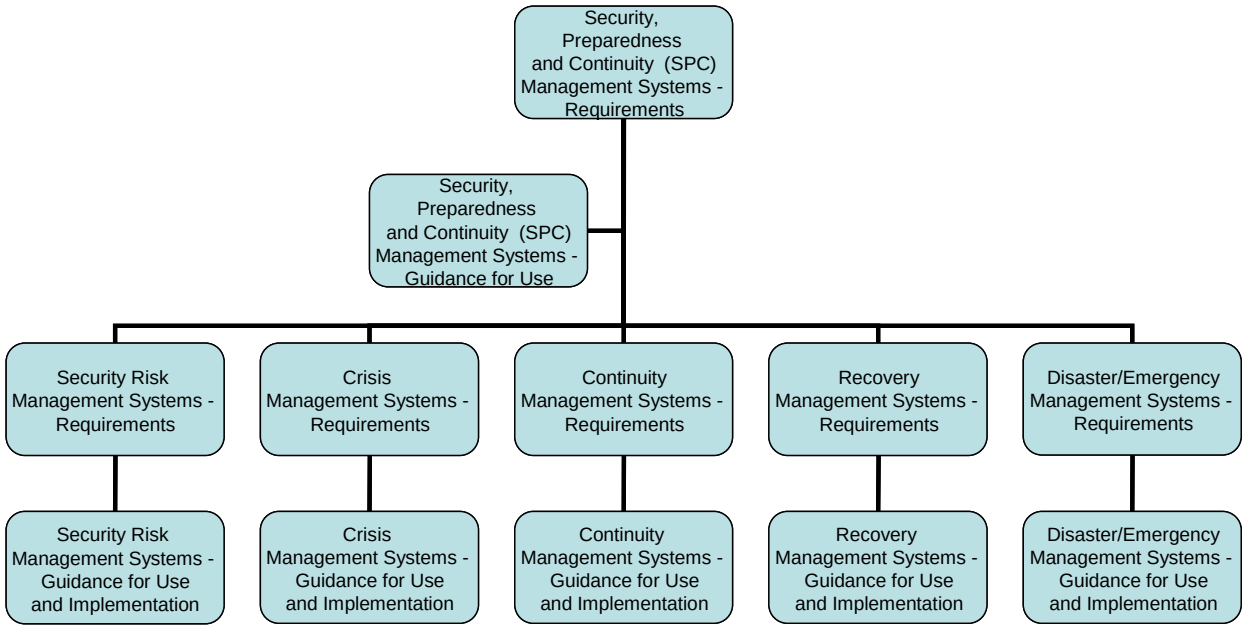

Figure One: Societal Security Discipline Family of Standards

An array of national standards writing initiatives have generated national standards (ratified and/or draft standards in the pipeline) addressing the various approaches illustrated in Figure One. Examples include:

High Level - Security, Preparedness and Continuity Management System Standards (drafts)

- ASIS International: Organizational Resilience: Security, Preparedness, and Continuity Management Systems Standard
- Australia: Organizational Resilience: Security, Preparedness, and Continuity Management Systems Standard
- Netherlands: Security, Preparedness, and Continuity Management Systems Standard

Security Management System Standards

- Australia: HB 167:2006 Security Risk Management
- Israel: IS 24001: 2007 Security and Continuity Management System Standard
- ISO 28000:2007 Specification for security management systems for the supply chain

Continuity Management System Standards

- ISO/PAS 22399:2007 Societal Security: Guidelines for Incident Preparedness and Operational Continuity Management
- Australia: HB 221:2004 Business Continuity Management
- Australia: HB 292:2006 A Practitioners Guide to Business Continuity Management
- Canada: CSA Z1600:2008 Standard on Emergency Management and Business Continuity Programs
- Singapore: Singapore Standard For Business Continuity Management (BCM) - 2008 revision of TR19-2005 Technical Reference for Business Continuity Management (BCM)
- United Kingdom: BS 25999-2:2007 Business continuity management. Specification
- United Kingdom: BS 25999-1:2006 Code of Practice for Business Continuity Management

Disaster/Emergency Management

- South Africa: SABS 0264-1:2002 Disaster Management, Part 1
- South Africa: SABS 0264-2:2002 Disaster Management, Part 2
- South Africa: SABS 0264-3:2002 Disaster Management, Part 3
- United States: NFPA 1600:2007 Standard on Disaster/Emergency Management and Business Continuity Programs (not a management system)

The three high level standards above use the Plan-Do-Check-Act model and ISO Guide 72. Therefore, they are aligned with ISO 9001:2000, ISO 14001:2004, ISO/IEC 27001:2005 and ISO 28000:2008 in order to support consistent and integrated implementation and operation with related management standards. Thus one suitably designed management system can thus satisfy the requirements of all these standards.

Expanding the Family of Societal Security Management System Related Standards

"Generic management system standards" provide criteria for an organization's management system establishing a number of critical core elements to support how it manages its processes, functions or activities. They are referred to as "generic" because they are applicable to any public or private organization, large or small, whatever its function, products, or services. Complementing these management system standards are families of standards providing implementation guidance and guides for conformity assessment.

Similar to the families of standards that have been under development for decades for the other ISO management system standards, ISO/TC 223 will develop management system guidelines standards, both generic and sector-specific intended to assist organizations in implementing and/or enhancing its management system. These standards will provide additional guidance to the elements of a management system requirements standard, or stand-alone guidance with no equivalence to a management system requirements standard.

Complementary standards can provide specific implementation guidance. For example, small and medium size enterprises (SMEs) would benefit from guidelines for a staged implementation of the management system standard (similar to a maturity model approach). Industry specific guidelines provide implementation guidance for industry sectors, both public and private. Asset specific guidelines provide guidance for the protection of human, physical, environmental and intangible assets on an individual and multi-organizational level. Standards can also elucidate the process and implementation of the management system standards providing guidance on conducting specific requirements of the standard (e.g. risk assessment, communications, exercises); auditing principles and conformity assessments; indicators for performance assessment, etc. Developing the family of standards is a long-term commitment of standards development efforts. The starting point is the high level management systems standards setting the foundation for the family's evolution.

Figure Two presents a few examples of possible standards in the Societal Security family of management system standards. This figure also shows how the family of SPC standards will relate to other standards development efforts in ISO, in particular the work of ISO/TMB Working Group on Risk Management who are in the final stages of develop the ISO 31000 Risk Management standard and the revision of ISO/IEC Guide 73 Risk Vocabulary.

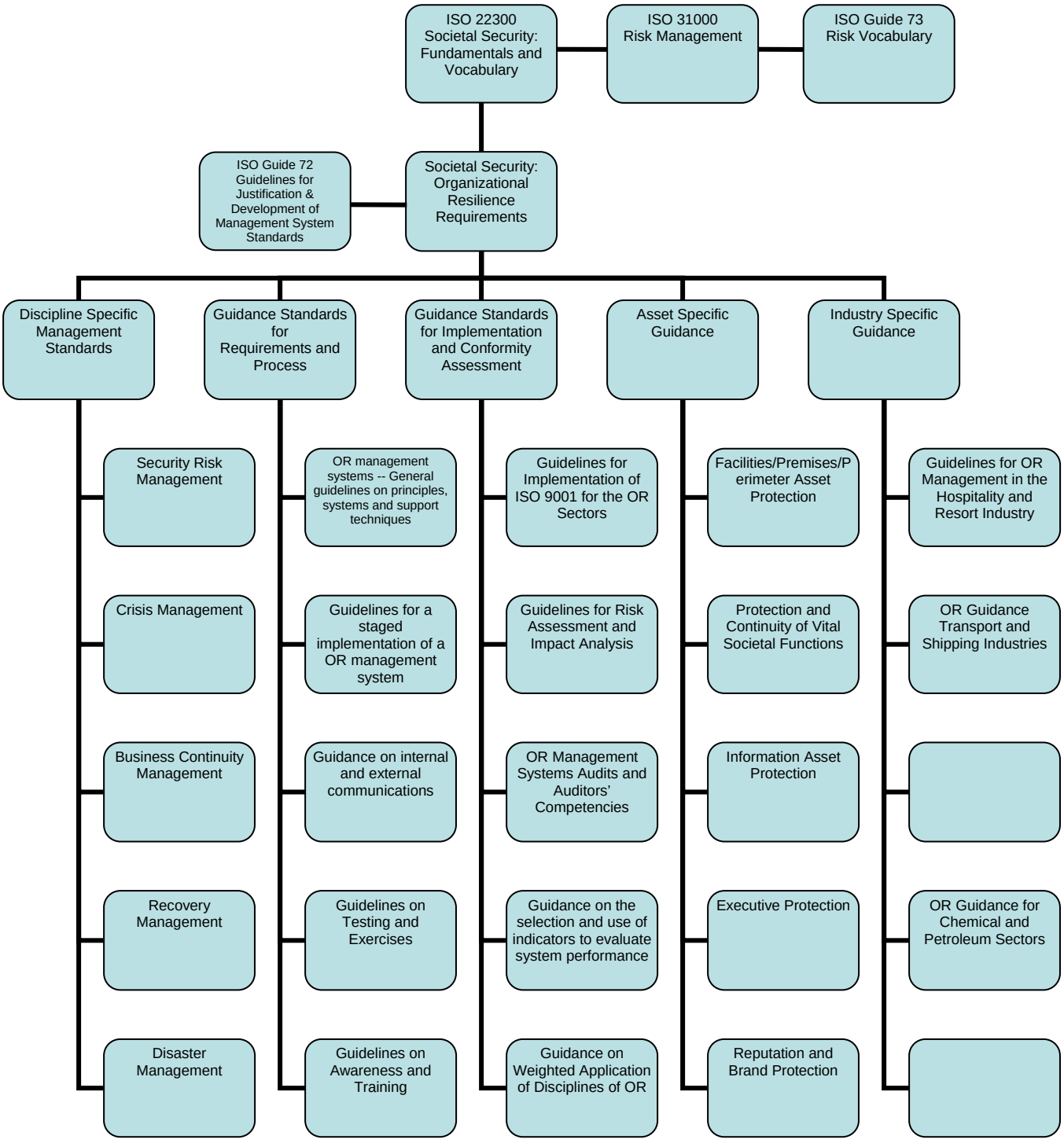

Figure Two: Societal Security Extended Family of Standards

Prepared by Dr. Marc Siegel

ASIS International has active standards development efforts underway in ASIS International chapters on five continents. Standards development efforts for the standards listed in Figure Two include:

- Guideline on Exercising and Testing – ISO/TC 223 WG1
- Guidelines for Security Management in the Hotel and Resort Sectors - South Africa
- Facilities Physical Security Management – United States
- Auditing Management Systems for Security, Preparedness and Continuity Management with Guidance for Application – The Netherlands and United States
- Business Continuity Management – United States
- Guidance on SPC Internal and External Communications – ASIS global
- Guidelines for Implementation of ISO 9001 for Security Sectors – ASIS global
- SPC Guidance for Hospitals and Medical Services – Hong Kong
- Guidelines for Risk Assessment and Impact Analysis – Australia and United States
- Chief Security Officer - United States

Where appropriate, ASIS International will submit the standards developed by the national teams to ISO technical committees as New Work Item Proposals (NWIP) for consideration for internationalization. This enables ASIS International to promote the ISO vision of consistent standards development approach globally and thereby avoid trade barriers.

ASIS International is the largest organization for security professionals, with more than 36,000 members in 204 Chapters worldwide. ASIS International is recognized as an international organization and serves as a Type A Liaison in ISO/TC223: Societal Security. The Global Standards Initiative coordinates ASIS's worldwide standards activities promoting a message of business-friendly international cooperation in standards development.