Using a Standards-Based Management-System Approach to Increasing Resilience
"The world is becoming turbulent faster than organizations are becoming resilient."

Gary Hamel
Harvard Business Review
“A resilient organization is one that is able to achieve its core objectives in the face of adversity.”
The Role of Management Systems in Increasing Resilience

The implementation of management systems encourages risk management across the organization.
The Value of Management Systems

Management systems standards return a bottom-line financial value larger than any investment or time incurred.

Adopters of management system standards have higher rates of survival than non-adopters.

Adopters of management system standards have higher sales than non-adopters.

Small businesses achieve proportionally more benefits than larger organizations.

Harvard Business School, 2008

©2013 Business Continuity Services, Inc.
The Value of Management Systems

Management systems are those activities used to **anticipate, prevent, and resolve known problems.**”

- Flexibility
- Discipline
- Consistency

Harvard Business School, 2008
SAY WHAT YOU DO
Do What You Say
PROVE IT!
Types of Management Systems

- ISO 14001: Environmental, Health & Safety
- OHSAS 18001: Occupational Health & Safety
- ISO 27001: Information Security
- ISO 28000: Supply Chain Security
- ISO 22301: Business Continuity
- ISO 20000: IT Service Management
- ISO 9001: Quality
Integration of Management Systems

Different management systems can be integrated into a single, joint system.

The integration is expected to facilitate synergies in using supporting processes that may be common to them thus eliminating waste and increasing efficiency.
Lifecycle Process of Continual Improvement

- Policy
- Planning
- Management Review
- Implementation & Operation
- Checking & Corrective Action

Continual Improvement
ISO Guide 83: A System for MS Standards

1. Scope
2. Normative References
3. Terms & Definitions
4. Context of the Organization
5. Leadership
6. Planning
7. Support
8. Operation*  *contains bulk of the requirements
9. Performance evaluation
10. Improvement
Key Components of Management Systems

Key components of all management systems include the following:

- A policy;
- People with defined responsibilities;
- Management processes relating to;
  - Policy;
  - Planning;
  - Implementation & operation;
  - Performance assessment;
  - Management review; and
  - Improvement;
- A set of documentation providing auditable evidence; and
- Topic specific processes relating to the subject.
Why do Management Systems Matter?

Businesses operating in the 21st century face many significant challenges, including:

- Profitability
- Competitiveness
- Globalization
- Speed of change
- Adaptability
- Growth
- Technology

Increasing number of risks and threats to the organization

Balancing these and other business requirements can be a difficult and daunting process. That's where management systems can help, by unlocking the potential in your organization.
What management systems does your organization already have in place?
Resilience Framework

- Business Continuity Management
- Crisis Management & Communications
- Technical Infrastructure
- Emergency Management
- Facility Management
- Legal Compliance & Audit
- Organizational Behavior
- Risk Management & Insurance
- Social Resilience
- Supply Chain, Logistics Transportation Mgmt.
Management Systems & Resilience

- Business Continuity Management: ISO 22301
- Crisis Management & Communications: PAS200:2011
- Emergency Management: ISO 22320
- Facility Management: ISO 14001
- Legal, Compliance & Audit
- Organizational Resilience: ISO 22323 / ASIS SPC.1
- Risk Management & Insurance: ISO 31000
- Social Resilience:
- Technology Infrastructure: ISO 27001 & 27031
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 for an effective response that safeguards the interests of its key stakeholders, reputation, brand and value-creating activities.
Published June 2012 - Developed from BS 25999-2:2007

Scope of the standard

Applicable to all types and sizes of organizations that wish to:

• Establish, implement, maintain, & improve a BCMS;
• Assure conformance with stated BCM policy;
• Demonstrate conformance to others;
• Seek certification/registration of its BCMS by an accredited third party certification body; or
• Make a self-determination and self-declaration of conformance with this International Standard.
This International Standard provides guidance to ISO 22301 for setting up and managing an effective business continuity management system (BCMS)
Crisis Management System: PAS: 2011

Aimed primarily at top managers with strategic responsibilities who have a role in shaping, directing, and developing the crisis management capability of their organization. It will give them the means to:

- Identify and understand the issues and challenges of crisis management from a strategic perspective
- Evaluate their implications for their organization; and
- Take practical steps to improve their organization’s crisis management capability.
Crisis Management System: PAS: 2011

Horizon Scanning

Issues Management

Situational Awareness
Overall approach to preventing emergencies and managing those that occur with a focus on international, national, regional, or local incidents

- Specifies minimum requirements for effective incident response
  - Utilizes the “command and control” process
  - Decision support
  - Traceability
  - Information management
  - Interoperability

Emergency Management: ISO 22320

Published November 2011

©2012 ICOR ALL RIGHTS RESERVED
“The organization shall establish and maintain (a) procedure(s) to identify the environmental aspects of its activities, products, or services that it can control and over which it can be expected to have an influence, in order to determine those which have or can have significant impacts on the environment.”
Environmental **aspects** are those elements of an organization’s activities, products, services or physical resources which *may* have potentially beneficial or harmful effects on the environment. These may include

- discharges and emissions,
- raw materials and energy use,
- waste recycling,
- noise,
- dust, and
- visual pollution.

An environmental **impact** is the change that takes place from the occurrence of any given aspect.

The relationship between the two is causal: an impact is the pollution that would result if an environmental aspect were not properly managed or controlled.
Environmental Health & Safety: ISO 14001

Environmental Aspects to Consider

Requirements
- Customers
- Legislation
- Policy
- Insurance
- Permits

Technical
- Process
- Storage
- Transfer
- Transport
- Utilities

Environmental
- Air
- Water
- Waste
- Soil & Groundwater
- Energy Consumption

Level
- Site/Plant
- Department
- Installation / Equipment
- Subcontractor / Supplier

©2012 ICOR ALL RIGHTS RESERVED
Every organization is required to comply with any legal requirements, any internal or external compliance issues, and be prepared for both internal and external audits in order to demonstrate continual improvement.
Emphasizes *resilience*, the *adaptive capacity* of an organization in a complex and changing environment, as well as protection of critical assets.

- Applying this standard *positions an organization to more readily prepare for and respond to all manner of intentional, unintentional, and/or naturally-caused disruptive events* – which if unmanaged could escalate into an emergency, crisis, or disaster.
- It covers *all phases of incident management* before, during, and after a disruptive event.
ISO 31000: Risk Management Standard
ISO 31000: Risk Management

Published November 2009

Establishes a number of principles that need to be satisfied to make risk management effective

These principles can be used to manage risk in all areas of the organization

- Information security
- Facility operations
- Supply chain
- Management processes
Drivers of Risk Management

**Externally Driven**

- Financial Risks
  - Accounting Standards
  - Interest Rates
  - Foreign Exchange
  - Funds and Credit
- Infrastructure Risks
  - Communications
  - Transport Links
  - Supply Chain
  - Terrorism
  - Natural Disasters
  - Pandemic

**Internally Driven**

- Internal Control
- Fraud
- Historical Liabilities
- Investments
- Capex Decisions
- Liquidity and Cashflow
- Recruitment
- People Skills
- Health and Safety
- Premises
- IT Systems

**ISO 31000**

Financial Risks
Infrastructure Risks
Marketplace Risks
Reputational Risks
As a discipline, Social and Personal Resilience focuses more on the resiliency of the individual as a singular entity or one in a small group or community.

“Resilience” is ‘the individual ability to resist, mitigate, and recover from assaults on one’s physiological and psychological integrity.’

It looks at those characteristics and traits that help a person, group, or community develop their own resiliency or ability to cope with stress and/or crisis.
Supply Chain Continuity & Security Management

PD 25222: 2011 – Supply Chain Continuity
ISO 28000: Security Management Systems for the Supply Chain
Guidance on supply chain continuity as it relates to the overall business continuity management system.

Requires supply chain “mapping” to analyze impacts of a supply chain disruption.

Includes an in-depth supply chain analysis for operational dependencies and interdependencies.
Supply Chain Security Management: ISO 28000

Security Management Systems for the Supply Chain (October 2007)

Provides requirements and guidance for organizations in international supply chains to

- Develop and implement supply chain security processes
- Establish and document a minimum level of security with a supply chain or segment of a supply chain
- Assist in meeting the applicable authorized economic operator (AEO) criteria set forth in the World Customs Organization Framework of Standards and conforming to national supply chain security programs
Protect People, Products, & Property

- Applies to any organization that is part of a local, national, or international supply chain
- Applies to both exporters and importers
- Applies to airports, seaports and terminals as well as to organizations that move product by air, sea, rail, or road
- Applies to logistics, transportation, and service companies as well to manufacturers, shippers, wholesalers, and distributors.
Use your SCSMS to manage & control security risks and to improve security performance.

ISO 28000 is tied to other standards.
Information & Communication Technology Infrastructure

ISO 27001: Information Security Management System
ISO 27031: Information & Communication Technology Readiness for Business Continuity
ISO 27001 is the international certifiable standard for organizations demonstrating the control to establish, implementing and maintain an organization’s Information Security Management System. In a nutshell, the organization

- Defines the information security policy,
- Sets the scope for the ISMS,
- Performs a risk assessment for that same scope,
- Makes a decision on how the risk forthcoming from this assessment is going to be managed,
- Selecting controls and objectives to be implemented.

And finally,

- The controls need to be implemented. Once the organization has completed this phase it can formally apply for certification.
ISO 27031: ICT for Business Continuity

Information & Communication Technology Readiness (ICT) for Business Continuity (IRBC)

Formerly BS 25777, Published March 2011

- Provides a framework of methods and processes to identify and specify all aspects for improving an organization’s ICT readiness to ensure business continuity
- Enables an organization to measure performance parameters that correlate to its IRBC in a consistent and recognized manner
- Scope = all events and incidents that could have an impact on ICT infrastructure & systems
For more information contact:

Jim Nelson
Chairperson, ICOR
jnelson@theICOR.org
President, BCS
Jim@BusinessContinuitySvcs.com
1.866.765.8321 North America
+1630.705.0910 International