Organizational Resilience:
Security, Preparedness and Continuity
Management Systems - Requirements with
Guidance for Use

ASIS SPC.1-2009
AMERICAN NATIONAL
STANDARD

Explore Resilience
and Risk
Management
Around the World

Dr. Marc Siegel
Peter Boyce (Asia)
Jose Sobron (UN)
Grant Lecky (Canada)
Johan du Ploy (Africa)
“But the real issue has to do with risk assessment. It has to do with the bloody crossroads where complex technical systems meet human psychology.” David Brooks, New York Times, “Drilling for Certainty”, May 27, 2010
Number One Lesson From Recent Disasters

• Everyone is in a supply chain:
  • The supply chain is bigger than you think.
  • Just knowing your tier one suppliers is not enough.
  • You must know your dependencies and interdependencies.
• Critical infrastructure is called “critical” for a reason.
• Risk, resilience, security and continuity management must include the supply chain, not just look internally at organizational matters.
Traditional Business Continuity Management

• Trying to address the risks of disruptive events with one hand tied behind your back by focusing on consequence management.
Traditional Security Management

• Trying to address the risks of disruptive events with one hand tied behind your back by focusing on likelihood management.
Convergence and ERM

- Security, crisis and continuity management must now fit within the overall risk management strategy of an organization.
- Risk and resilience management must support the mission of the organization.
- Organizations want to be resilient, not just security.
- The organization’s business is doing business.
- The modern security, crisis and continuity professional needs to evolve to play multiple roles at once.
Risk and Resilience Management

• A risk and resilience management standards provide:
  – A framework for managing risk;
  – Key principles and concepts, and a common language;
  – Clear direction and guidance for decision making.

• Every organization exists to provide value for its stakeholders.
  – Resilience management systems standards are used to identify and manage multiple and cross-enterprise risks.
A comprehensive management systems approach for prevention, protection, preparedness, response, mitigation, continuity, and recovery for disruptive incidents resulting in an emergency, crisis, or disaster.

Resilience and Risk Management

Security Risk Management
Emergency Management
Crisis Management
Information & Network Security
Emergency Preparedness
Critical Infrastructure Protection

Security Management
Physical Asset Protection
Disaster Management
Recovery Management
Continuity Management
Incident Response
What is Resilience?

**Resilience**: the adaptive capacity of an organization in a complex and changing environment.

Helps avoid segregating or siloing risks.
Organizational Resilience

• The ability of an organization to quickly, efficiently, and effectively adapt to a change:
  – Avoid segregating or siloing risks.
  – Avoid or prevent a disruptive incident.
  – Resist being affected by an event.
  – Return to an acceptable level of performance in an acceptable period of time after being affected by a potentially disruptive event.
  – Accommodate the unexpected.
  – Adapt, prevent and prepare for, engage with, and recover from disruptive events.
  – In some cases to become stronger as a result of the experience.
Finding Balance in Managing Risk

For organizations to cost-effectively manage risk they must develop balanced strategies to adaptively, proactively and reactively address minimization of both the likelihood and consequences of disruptive events.
A Strong Foundation for Managing Risks

Organizational Resilience

Adaptive, Proactive & Reactive Strategies

Prevention  Protection  Preparedness  Mitigation  Response  Recovery

Risk Assessment and Impact Analysis

Organizational and Supply Chain Context of Managing Risk
ASIS and ISO Standards – Built to be Business Friendly

• Aligned with the globally accepted standards:
  – ISO 9001:2000 - Quality management
  – ISO 14001:2004 - Environmental management
  – OHSAS 18001:2007 - Occupational health and safety
  – ISO 28000:2007 - Security management systems for the supply chain
  – ISO/PAS 28002:2010 – Resilience in the Supply Chain

• Supports consistent and integrated implementation and operation with related management standards.

• One suitably designed management system can satisfy the requirements of all these standards.
ISO 31000:2009 and Guide 73
ISO 31000 Changes the Perspective on Risk Management

Expanding organizational risk management competencies

Reactive mode
- Event-focused
- Post-action response
- Afterthought
- Transactional
- Protecting value

Proactive mode
- Objectives-focused
- Predictive indicators
- Foresight
- Strategic
- Creating and capturing value

Old View

New View

Defines risk as “effect of uncertainty on objectives”
Putting the Pieces in Place

- ISO 31000: Risk Management (Guidance)
- Guide 73: Risk Vocabulary (Guidance)
- Resilience Management ("Organizational" and "in the Supply Chain" Requirements)
- Maturity Model for Phased Implementation
- Risk Assessment Process (Guidance)
- Auditing Resilience Management Standards (Guidance)

Guidance documents for anticipating, assessing, preventing, protecting from, mitigating, and preparing for a disruptive event:
- Physical Asset Protection
- Security Risk Management
- Preparedness and Mitigation
- Fraud and Countermeasures

Guidance documents for responding to a disruptive event:
- Preparedness and Initial Response
- Crisis Management
- Emergency Response

Guidance documents for recovering from a disruptive event:
- Emergency Management
- Continuity Management
- Recovery Management
American National Standard
ANSI/ASIS.SPC.1-2009

Organizational Resilience:
Security, Preparedness and Continuity
Management Systems – Requirements with
Guidance for Use

ANSI/ASIS SPC.1-2009 is a practical auditable application of ISO31000:2009 Risk Management for preventing and managing disruptive incidents.

Selected by the US-DHS for the PS-Prep Program.
ISO 28002:2011

• Security management systems for the supply chain — Development of resiliency in the supply chain — Requirements with guidance for use
• Based on the ANSI/ASIS.SPC.1:2009
• Introduces supply chain resilience in organizational risk and resilience management
• Used in conjunction with ISO 28000
Supply Chain Process Approach

1. Establish Program and Apply Resources
2. Define the Supply Chain and Objectives
3. Identify Supply Chain Risks
4. Quantify and Prioritize Risks - Goals
5. Execute Risk Treatment Programs
6. Monitor Supply Chain Environment for Risks

Reassessment of risk program
Reassessment of risk sources
Reassessment of risk exposure
Continuous Risk Monitoring
Reassessment of management actions
Reassessment of supply chain
Don’t Put the Cart Before the Horse

• It’s all about resilience and agility in the organization.
• It’s about BUSINESS!
Thank You – Questions?

Dr. Marc Siegel
Commissioner, Global Standards Initiative
ASIS International
Phone: +1-858-484-9855
siegel@ASIS-Standards.net
siegel@ymail.com