BEYOND THE SILOS – ORGANIZATIONAL RESILIENCE

Dr. Marc Siegel
Security Management Systems Consultant
ASIS International
European Bureau
Brussels, Belgium
siegel@ASIS-Standards.net
All organizations face a certain amount of uncertainty and risk.

In order to 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...

ASIS SPC.1-2009

AMERICAN NATIONAL STANDARD

Organizational Resilience

- Provides an overall risk profile allowing the organization to better understand the relationships between risks and identify solutions to problems.

- Enables an organization to anticipate and adapt to instabilities to assure resiliency.
What is Resilience?

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

Helps avoid segregating or...
Organizational Resilience

- **Resilience** is the ability of an organization to prevent, resist being affected by an event, or the ability to return to an acceptable level of performance in an acceptable period of time after being affected by an event.

- **Resilience** is the capability of a system to maintain its functions and structure in the face of disruption.
Why Organizational Resilience?

• Helps the organization anticipate, prevent, and prepare for and respond to a disruptive incident.

• A resilient organization recognizes the synergies between prevention, preparedness (readiness), mitigation, response,
Organizational Resilience
Proactive & Reactive Strategies
What Do We Have in the Toolbox?

- Standards can address your organizational resilience needs.
What are Standards?

- Consensus-based specifications which define materials, methods, processes, services or practices.
- Provide a basis for consistent and repeatable performance.

Standards ≠ Regulations!
What is a Management System?

- **Management system** refers to what the organization does to manage its processes, or activities, so that it meets objectives it has set itself, such as:
  - satisfying supply chain requirements,
  - complying with regulations, or
  - meeting security, preparedness and continuity objectives.

- **Management system standards** provide a model to follow in setting up and operating a management system.
PDCA or APCI Model

Approach to structured problem solving focused on continual improvement:

**Plan (Assess) - Do (Protect) - Check (Confirm) - Act (Improve)**

**Plan**
- Define & Analyze a Problem and Identify the Root Cause

**Act**
- Standardize Solution
- Review and Define Next Issues

**Check**
- Confirm Outcomes Against Plan
- Identify Deviations and

**Do**
- Devise a Solution
- Develop Detailed Action Plan & Implement It Systematically
Why a Management System?

- Set of benchmarked tools and processes
- Systematically identify risks and problems
- Problem-solving and decision-making tools
- Inclusive process
- Specialized training
- Establishes operational controls/procedures
- Measurable/verifiable goals and methods for accomplishing identified objectives
- Protect reputation and brand
- Continual improvement
- Bottom line: Proactively improve
Why Management Systems Work

- Needs focused
- Goals driven
- People oriented
  - Leadership driven
  - Involves people at all levels
  - Promotes cultural change
- Emphasizes process approach
- System approach to management
- Factual basis for decision making
- Continual improvement

→ Business Advantage
The “Program” Approach

Structure, Responsibility
Training, Awareness, Operational Controls, and Communication

Planning, and Program Development

Review and Improvement

Know your Organization

Policy and Management Commitment

Checking & Corrective Action

Lists what is needed – gives pieces of the puzzle
The “Systems” Approach

The systems approach puts the pieces of the puzzle together to see the whole picture.

- Structure, Responsibility, Training, Awareness, Operational Controls, and Communication
- Planning, Risk Assessment, and Impact Analysis
- Checking & Corrective Action
- Review and Improvement
- Policy and Management Commitment
- Know your Organization
- Planning, Program Development
- Structure, Responsibility, Training, Awareness, Operational Controls, and Communication
Security/Continuity Management Standards

- The Security/Continuity Families:
  - ISO/IEC 27001 Family
    - Information Security Management
  - ISO 28000 Family
    - Supply Chain management
  - ISO 22300 Family
    - Societal Security (Security, Preparedness and Continuity Management)
  - ISO 31000 Family
    - Risk Management

All ISO Families have evolved from the original ISO 9000 Family
Meet the Family
• ISO 28000:2007
  - Specification for security management systems for the supply chain

• ISO 28001:2007
  - Security management systems for the supply chain -- Best practices for implementing supply chain security, assessments and plans -- Requirements and guidance

• ISO 28003:2007
  - Security management systems for the supply chain -- Requirements for bodies providing audit and certification of supply chain security management systems
What Does the Future Hold?

ISO 28002, 
Resilience in the Supply Chain

ISO 28005,  
Ships and marine technology - Computer applications -

ASIS SPC.1-2009

Standards Built to be

• Aligned with the globally accepted standards:
  - ISO 9001:2000 - Quality management
  - ISO 14001:2004 - Environmental management
  - OHSAS 18001:2007 - Occupational health and safety
  - ISO/IEC 27001:2005 - Information technology security
  - ISO 28000:2007 - Security management systems for the supply chain

• Supports consistent and integrated implementation and operation with related management standards
• Provides generic auditable criteria to establish, check, maintain, and improve a management system to enhance prevention, preparedness (readiness), mitigation, response, continuity and recovery from disruptive incidents.
All Hazards Risk Assessment

Focus on Protection of Critical Assets and Functions

Incident Management Regardless of Event Trigger

Management of All Hazards Risks
After Introduction/Implementation of ORMS

Operational Level

100%

Mitigate the impact of disaster

Preparedness / Prevention

Occurrence of Incident

Response

Recovery / Resumption

Shorten the period of re-establishment

Before Introduction/Implementation of ORMS

After Introduction/Implementation of ORMS

ORMS - Holistic Management Process
Builds on the PDCA Model

- **Plan**: Define & Analyze a Problem and Identify the Root Cause
- **Do**: Devise a Solution, Develop Detailed Action, Plan & Implement It Systematically
- **Check**: Confirm Outcomes Against Plan, Identify Deviations and Issues
- **Act**: Standardize Solution, Review and Define Next Issues

- Stakeholders and Interested Parties
- Organizational Resilience Management Systems Requirements and Expectations

Managed risk
Know your
Organization
Define scope and boundaries for preparedness, response, continuity and recovery management program
Identify critical objectives, operations, functions, products and services
Preliminary determination of likely risk scenarios and consequences

Management Review
Adequacy and Effectiveness
Need for Changes
Opportunities for Improvement

Policy
Management Commitment
Commitment to Protection of Critical Assets and Continuous Improvement
Commitment of Resources

Planning
Risk Assessment and Impact Analysis
Legal and Other Requirements
Objectives and Targets
Strategic Prevention, Preparedness and Response Programs (Before, During and After an Incident)

Implementation and Operation
Structure and Responsibility
Training, Awareness, Competence
Communication
Documentation
Document Control
Operational Control

Continual Improvement

Checking & Corrective Action
Monitoring and Measurement
Evaluation of compliance and system performance
Nonconformity, Corrective and Preventive Action Records

© 2009
Know your Organization

- Define scope and boundaries for preparedness, response, continuity and recovery management program
- Identify critical objectives, operations, functions, products and services
- Preliminary determination of likely risk scenarios and consequences
Know your Organization
Define scope and boundaries for preparedness, response, continuity and recovery management program
Identify critical objectives, operations, functions, products and services
Preliminary determination of likely risk scenarios and consequences

Management Review
Adequacy and Effectiveness
Need for Changes
Opportunities for Improvement

Checking & Corrective Action
Monitoring and Measurement
Evaluation of compliance and system performance
Nonconformity, Corrective and Preventive Action
Records
Internal Audits

Implementation and Operation
Structure and Responsibility
Training, Awareness, Competence
Communication
Documentation
Document Control
Operational Control

Organizational Resilience Policy
- Management Commitment
- Commitment to Protection of Critical Assets
- Commitment to Continuous Improvement
- Commitment of Resources

Planning
Risk Assessment and Impact Analysis
Requirements
Objectives and Targets
Strategic Prevention, Preparedness, and Response Programs (Before, During and After an Incident)

© 2009 Organizational Resilience Policy
- Management Commitment
- Commitment to Protection of Critical Assets
- Commitment to Continuous Improvement
- Commitment of Resources
Planning
- Risk Assessment and Impact Analysis
- Legal and Other Requirements
- OR Management Objectives and Targets
- Strategic Prevention, Preparedness, Response and Continuity Programs (Before, During and After an Incident)
- Know your Organization
  - Define scope and boundaries for preparedness, response, continuity and recovery management program
  - Identify critical objectives, operations, functions, products and services
  - Preliminary determination of likely risk scenarios and consequences
- Management Review
  - Adequacy and Effectiveness
  - Need for Changes
  - Opportunities for Improvement
- Policy
  - Management Commitment
  - Commitment to Protection of Critical Assets and Continuous Improvement
  - Commitment of Resources
- Checking & Corrective Action
  - Monitoring and Measurement
  - Evaluation of compliance and system performance
  - Nonconformity, Corrective and Preventive Actions
  - Records
  - Internal Audits
- Implementation and Operation
  - Structure and Responsibility
  - Training, Awareness, Competence
  - Communication
  - Documentation
  - Document Control
  - Operational Control

© 2009
Check your Organization
- Define scope and boundaries for preparedness, response, continuity and recovery management program
- Identify critical objectives, operations, functions, products and services
- Preliminary determination of likely risk scenarios and consequences

Policy
- Management Commitment
- Commitment to Protection of Critical Assets and Continuous Improvement
- Commitment of Resources

Planning
- Risk Assessment and Impact Analysis
- Legal and Other Requirements
- Objectives and Targets
- Strategic Prevention, Preparedness and Response Programs (Before, During and After an Incident)

Management Review
- Adequacy and Effectiveness
- Need for Changes
- Opportunities for Improvement

Checking & Corrective Action
- Performance Monitoring and Measurement
- Evaluation of compliance and system performance
- Exercises and Testing
- Nonconformity, Corrective and Preventive Action
- Control of Records
- Audits

Operational Control
- Planning
- Risk Assessment and Impact Analysis
- Legal and Other Requirements
- Objectives and Targets
- Strategic Prevention, Preparedness and Response Programs (Before, During and After an Incident)

Know your Organization
- Define scope and boundaries for preparedness, response, continuity and recovery management program
- Identify critical objectives, operations, functions, products and services
- Preliminary determination of likely risk scenarios and consequences

Policy
- Management Commitment
- Commitment to Protection of Critical Assets and Continuous Improvement
- Commitment of Resources

Planning
- Risk Assessment and Impact Analysis
- Legal and Other Requirements
- Objectives and Targets
- Strategic Prevention, Preparedness and Response Programs (Before, During and After an Incident)

Management Review
- Adequacy and Effectiveness
- Need for Changes
- Opportunities for Improvement

Checking & Corrective Action
- Performance Monitoring and Measurement
- Evaluation of compliance and system performance
- Exercises and Testing
- Nonconformity, Corrective and Preventive Action
- Control of Records
- Audits

Operational Control
- Planning
- Risk Assessment and Impact Analysis
- Legal and Other Requirements
- Objectives and Targets
- Strategic Prevention, Preparedness and Response Programs (Before, During and After an Incident)

Know your Organization
- Define scope and boundaries for preparedness, response, continuity and recovery management program
- Identify critical objectives, operations, functions, products and services
- Preliminary determination of likely risk scenarios and consequences

Policy
- Management Commitment
- Commitment to Protection of Critical Assets and Continuous Improvement
- Commitment of Resources

Planning
- Risk Assessment and Impact Analysis
- Legal and Other Requirements
- Objectives and Targets
- Strategic Prevention, Preparedness and Response Programs (Before, During and After an Incident)

Management Review
- Adequacy and Effectiveness
- Need for Changes
- Opportunities for Improvement

Checking & Corrective Action
- Performance Monitoring and Measurement
- Evaluation of compliance and system performance
- Exercises and Testing
- Nonconformity, Corrective and Preventive Action
- Control of Records
- Audits

Operational Control
- Planning
- Risk Assessment and Impact Analysis
- Legal and Other Requirements
- Objectives and Targets
- Strategic Prevention, Preparedness and Response Programs (Before, During and After an Incident)

Know your Organization
- Define scope and boundaries for preparedness, response, continuity and recovery management program
- Identify critical objectives, operations, functions, products and services
- Preliminary determination of likely risk scenarios and consequences

Policy
- Management Commitment
- Commitment to Protection of Critical Assets and Continuous Improvement
- Commitment of Resources

Planning
- Risk Assessment and Impact Analysis
- Legal and Other Requirements
- Objectives and Targets
- Strategic Prevention, Preparedness and Response Programs (Before, During and After an Incident)

Management Review
- Adequacy and Effectiveness
- Need for Changes
- Opportunities for Improvement

Checking & Corrective Action
- Performance Monitoring and Measurement
- Evaluation of compliance and system performance
- Exercises and Testing
- Nonconformity, Corrective and Preventive Action
- Control of Records
- Audits

Operational Control
- Planning
- Risk Assessment and Impact Analysis
- Legal and Other Requirements
- Objectives and Targets
- Strategic Prevention, Preparedness and Response Programs (Before, During and After an Incident)

Know your Organization
- Define scope and boundaries for preparedness, response, continuity and recovery management program
- Identify critical objectives, operations, functions, products and services
- Preliminary determination of likely risk scenarios and consequences

Policy
- Management Commitment
- Commitment to Protection of Critical Assets and Continuous Improvement
- Commitment of Resources

Planning
- Risk Assessment and Impact Analysis
- Legal and Other Requirements
- Objectives and Targets
- Strategic Prevention, Preparedness and Response Programs (Before, During and After an Incident)

Management Review
- Adequacy and Effectiveness
- Need for Changes
- Opportunities for Improvement

Checking & Corrective Action
- Performance Monitoring and Measurement
- Evaluation of compliance and system performance
- Exercises and Testing
- Nonconformity, Corrective and Preventive Action
- Control of Records
- Audits

Operational Control
- Planning
- Risk Assessment and Impact Analysis
- Legal and Other Requirements
- Objectives and Targets
- Strategic Prevention, Preparedness and Response Programs (Before, During and After an Incident)

Know your Organization
- Define scope and boundaries for preparedness, response, continuity and recovery management program
- Identify critical objectives, operations, functions, products and services
- Preliminary determination of likely risk scenarios and consequences

Policy
- Management Commitment
- Commitment to Protection of Critical Assets and Continuous Improvement
- Commitment of Resources

Planning
- Risk Assessment and Impact Analysis
- Legal and Other Requirements
- Objectives and Targets
- Strategic Prevention, Preparedness and Response Programs (Before, During and After an Incident)

Management Review
- Adequacy and Effectiveness
- Need for Changes
- Opportunities for Improvement

Checking & Corrective Action
- Performance Monitoring and Measurement
- Evaluation of compliance and system performance
- Exercises and Testing
- Nonconformity, Corrective and Preventive Action
- Control of Records
- Audits

Operational Control
- Planning
- Risk Assessment and Impact Analysis
- Legal and Other Requirements
- Objectives and Targets
- Strategic Prevention, Preparedness and Response Programs (Before, During and After an Incident)

Know your Organization
- Define scope and boundaries for preparedness, response, continuity and recovery management program
- Identify critical objectives, operations, functions, products and services
- Preliminary determination of likely risk scenarios and consequences

Policy
- Management Commitment
- Commitment to Protection of Critical Assets and Continuous Improvement
- Commitment of Resources

Planning
- Risk Assessment and Impact Analysis
- Legal and Other Requirements
- Objectives and Targets
- Strategic Prevention, Preparedness and Response Programs (Before, During and After an Incident)

Management Review
- Adequacy and Effectiveness
- Need for Changes
- Opportunities for Improvement

Checking & Corrective Action
- Performance Monitoring and Measurement
- Evaluation of compliance and system performance
- Exercises and Testing
- Nonconformity, Corrective and Preventive Action
- Control of Records
- Audits

Operational Control
- Planning
- Risk Assessment and Impact Analysis
- Legal and Other Requirements
- Objectives and Targets
- Strategic Prevention, Preparedness and Response Programs (Before, During and After an Incident)
Know your Organization
Define scope and boundaries for preparedness, response, continuity and recovery

Management Review
- Adequacy and Effectiveness
- Need for Changes
- Opportunities for Improvement

Policy
Management Commitment
Commitment to Protection of Critical Assets and Continuous Improvement
Commitment of Resources

Continual Improvement

Planning
Risk Assessment and Impact Analysis
Legal and Other Requirements
Objectives and Targets
Strategic Prevention, Preparedness and Response Programs (Before, During and After an Incident)

Implementation and Operation
Structure and Responsibility
Training, Awareness, Competence
Communication
Documentation
Document Control
Operational Control

Checking & Corrective Action
Monitoring and Measurement
Evaluation of compliance and system performance
Nonconformity, Corrective and Preventive Actions
Records
Internal Audits

Adequacy and Effectiveness
Need for Changes
Opportunities for Improvement

© 2009
Keep in mind – An ORMS

- Is a **dynamic management** system
  - THAT’S WHAT MAKES IT WORK!!
  - Organization must use the tools, not just have them.
- Is more than compliance - includes safety, energy, water etc. and non-regulated impacts
- **Supports mission!**
- Takes time - it is a process, not an event
Standards
Auditing

• **Audit:** systematic, independent and documented process for obtaining audit evidence and evaluating it objectively to determine the extent to which audit criteria are fulfilled.

  - Internal audits, sometimes called first-party audits, are conducted by, or on behalf of, the organization itself for management review and other internal purposes, and may form the basis for an organization’s declaration of conformity.

  - External audits include those generally termed second- and third-party audits.

    • **Second-party audits** are conducted by parties having an interest in the organization, such as
Accreditation and Certification (Registration) Bodies

**Accreditation Bodies**
An organization (usually a national standards body associated with ISO) that checks certification bodies and, provided their certification assessment processes pass muster, accredits them i.e. grants them the authority to issue recognized certificates.

**ISO/IEC 17011:2004**
Conformity assessment -- General requirements for accreditation bodies accrediting conformity assessment bodies

**ISO/IEC 17040:2005**
Conformity assessment -- General requirements for peer assessment of conformity assessment bodies and accreditation bodies

**Certification (Registration) Bodies**
An independent external body that issues written assurance (the certificate) that it has audited a management system and verified that it conforms to the requirements specified in the standard.

**ISO 28003:2007**
Security management systems for the supply chain -- Requirements for bodies providing audit and certification of supply chain security management systems

**ISO/IEC 17021:2006**
Conformity assessment -- Requirements for bodies providing audit and certification of management systems

**Certified Lead Auditor**
**ISO 19011:2002**
Guidelines for quality and/or environmental management systems auditing

**Organization**
Implements standard - may seek formal recognition (certification) by a specialized third party body.

**ISO 28000:2007**
Specification for security management systems for the supply chain

© 2009
Thank You

Dr. Marc Siegel
Security Management System Consultant
ASIS International
Phone: +1-858-484-9855
siegel@ASIS-Standards.net
siegel@ymail.com