Re-Emphasizing Risk Management

by George Huff

November 9, 2011

Risk Management and Supply Chain Security

- ISO 28000's Risk-Based Approach to Management Systems
  - ISO Format adopted from ISO 14001:2004 Environmental Performance, but
  - Organizations with Process Approach (e.g. ISO 9001:2000) may be able to use their existing Management Systems; and
  - Uses "Plan-Do-Act-Check" Methodology.

- Resiliency Disciplines: Incident Management, Business Continuity, Facility & Risk Management, Social Resilience, Supply Chain, Logistics & Transportation

- Incident Management, Business Continuity/ Organizational Resilience Management Systems
  - Understand the Organization – Risk Assessment & BIA
  - Develop the BCM Strategy – Secure the Supply Chain

Next steps: Steering committees are to deliver and set the SCSMS/ IMS/BCMS/ORMS frameworks and policies, and meet regularly to review and update threats to the organization's critical processes and mitigation.

ISO 28000: 2007
Security Management Systems for Supply Chain

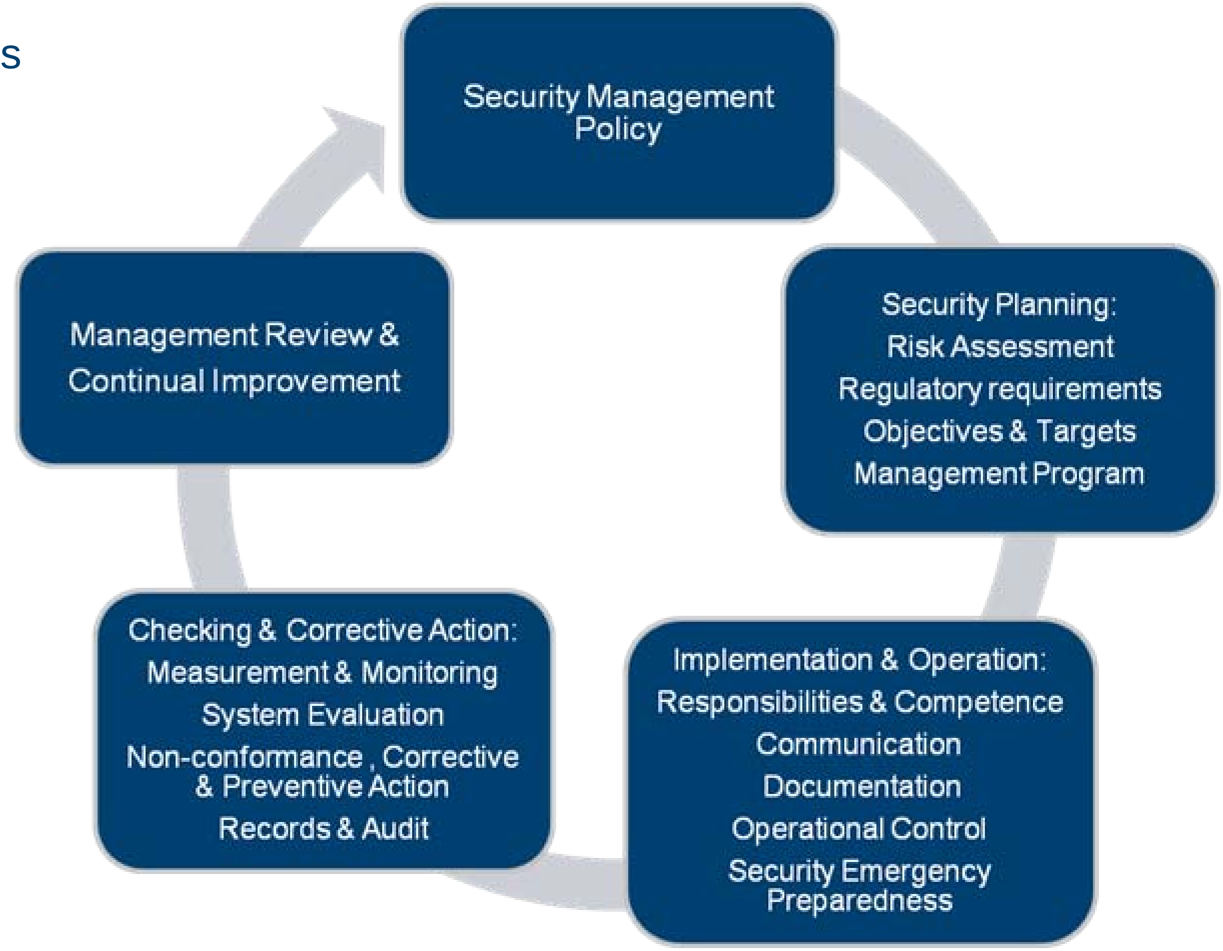
What it Does: Provides requirements and guidance for organizations in international supply chains to:

- 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 (see, World Customs Organization (WCO) SAFE Framework of Standards to Secure and Facilitate global trade), and conformity to national supply chain security codes & programs
- Applies to both exporters and importers
- Applies to airports, seaports and terminals, as well as organizations that move product by air, sea, rail or road
- Applied to logistics, transportation, and service companies, as well as manufacturers, shippers, wholesalers and distributors.

Next steps: Organizations are to assure conformance to SM policy, demonstrate conformance to others, seek registration/certification by Accredited third party CB, or make a self-declaration of conformance.

Security Management System Lifecycle

- SM Elements
- Continual Improvement



Security Management Policy

Security Planning:
Risk Assessment
Regulatory requirements
Objectives & Targets
Management Program

Implementation & Operation:
Responsibilities & Competence
Communication
Documentation
Operational Control
Security Emergency Preparedness

Checking & Corrective Action:
Measurement & Monitoring
System Evaluation
Non-conformance , Corrective & Preventive Action
Records & Audit

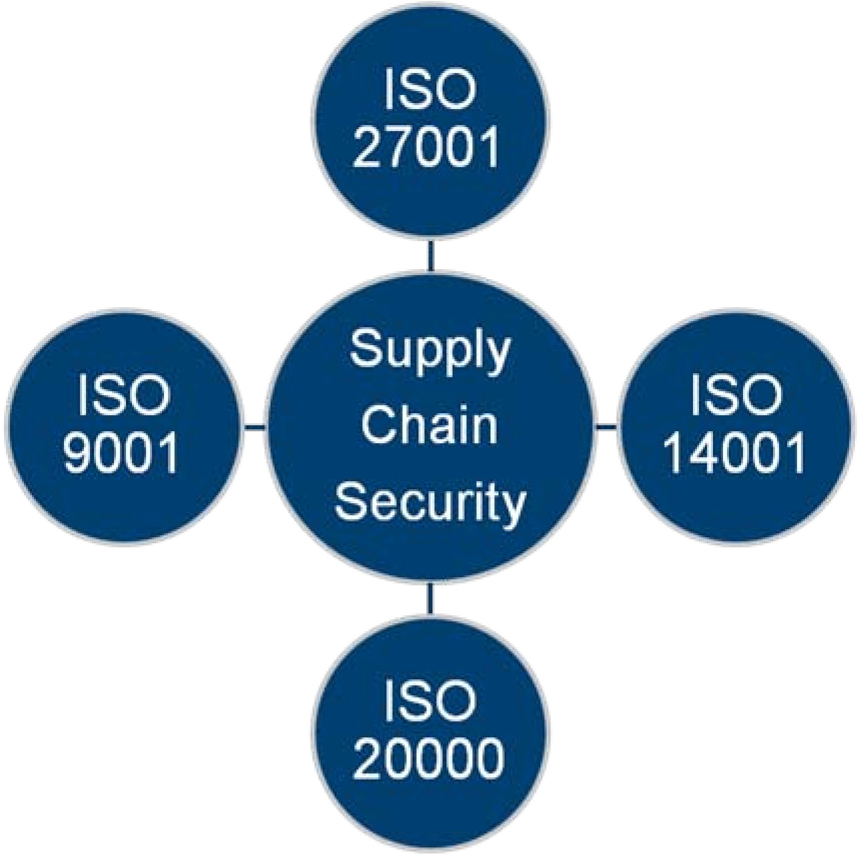
Management Review & Continual Improvement

Next steps: Lifecycle of Continual Improvement of the Elements of Security Management.

Supply Chain Security Management Systems

- SCSMS is used to manage & control security risks and improve security performance

- ISO 28000 is tied to other standards:
    - ISO 27001: Information Security
    - ISO 14001: Environmental Performance
    - ISO 20000: IT Service Management
    - ISO 9001: Quality Management Systems



Next steps: Correspondence of Elements Between ISO 28000 and Related Management Systems.

ISO 28003 – Requirements for Bodies Providing Audit and Certification of Supply Chain Security Management Systems

- Certification of Supply Chain Security Management Systems is a Third Party Conformity Assessment activity.
    - Requirements for CBs include Annexes on Auditor Time, Education, Work & Audit Experience, and Training Duration, and Criteria for Auditing Organizations with Multiple Sites
- ANSI-ASQ National Accreditation Board (ANAB) has received one application for ISO 28000 from a certification body
- ANAB has received several other inquires from certification bodies.

Next steps: Organizations that Choose Third Party Certification can further Demonstrate that They are Contributing Significantly to Supply Chain Security.

Cross-Mapping of IM/BC/OR Standards: Understanding the Organization

NFPA 1600	BS 25999-2 (2007) BS 25999-1 (2006)	ASIS SPC-1
5.4 Risk Assessment §§ 5.4.1 - - 5.4.4	4.4.1 BIA §§ 4.1.1.1 - - 4.1.1.2 4.1.2 Risk Assessment §§ 4.1.2.1 - - 4.1.2.2	4.3 Planning: Identify Hazards & Threats
5.5 Business Impact Analysis §§ 5.5.1 - - 5.5.6	6.2 Business Impact Analysis (BIA) §§ 6.2.1 - - 6.2.3	§ 4.3.1 Risk Assessment & Impact Analysis

Next steps: Voluntary Private Sector Preparedness and Accreditation Standards are Risk-Based & Designed to Understand the Organization.

Cross-Mapping of IM/BC/OR Standards: Determining the Strategy (Risk Treatment)

NFPA 1600	BS 25999-2 (2007) BS 25999-1 (2006)	ASIS SPC-1
5.6 Prevention §§ 5.6.1 - - 5.6.4 5.7 Mitigation §§ 5.7.1 - - 5.7.3	4.2 Determining BC Strategy	4.3.3 Planning: Identify Hazards & Threats
6.1 Resource Management §§ 6.1.1 - - 6.1.7	6.4 Determining Continuity Requirements	4.3.3 Planning: Identify Hazards & Threats

Next steps: Voluntary Private Sector Preparedness and Accreditation Standards are Risk-Based & Designed to Determine the Strategy.

Determining the IM/BC/OR Strategy – Examples of Supply Chain Strategy Activities

- Inventory of the extended enterprise and points of integration with other entities, identifying:

    1. Where critical services and products originate,
    2. Single points of failure in the service/supply chain, and
    3. Where single- and source suppliers are located.

- Determine how critical products are sourced and shipped from overseas locations.

- Many core items and critical outputs will not be available because most supply chains operate in a “just-in-time” model. Therefore, identify core items and critical inputs and identify critical inputs as “vulnerable,” i.e., potentially not available, or “non-vulnerable,” i.e., likely to be available.

- Where critical supplies are dependent upon specialist supplies, the organizations should identify the key suppliers and single sources of supply. Therefore, identify essential customers and suppliers, including prioritization of critical partners relationships and documentation of which customers should receive priority service

Next steps: Voluntary Private Section Preparedness and Accreditation Standards Are Risk-Based & Designed to Determine the Strategy.

The Assessment Cycle – Stages 1 and 2

- Stage 1: Conformance with Specification
  - Review of the SCSMS/IM/BC/OR documentation
  - High-level evaluation of the readiness for the stage 2 assessment
  - Review of the understanding of the requirements of the standard, and the proposed scope of stage 2 assessment
  - Review and confirmation of the resources needed for stage 2 assessment
  - Plan outlining stage 2 assessment
  - Confirmation that management review and audit/self assessments are being planned and performed

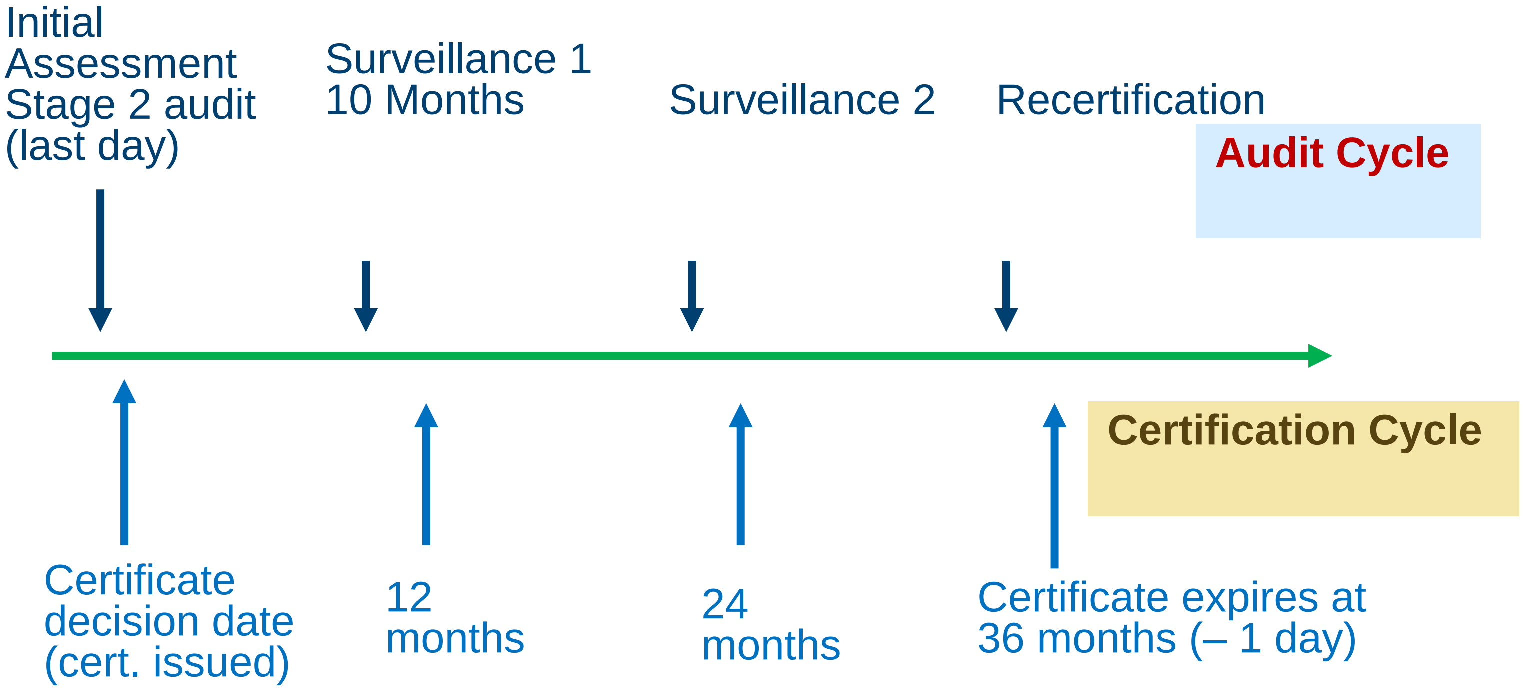
Next steps: Any areas deemed not in compliance will be raised as non-conformities and must be cleared and approved by the lead auditor, prior to moving to stage 2 assessment

The Assessment Cycle

- Stage 2: Evaluation of Implementation
  - Evaluates the implementation of the SCSMS
  - Uses a “process audit” approach, assessing all processes within the scope and all linked processes to ensure effectiveness and consistency
  - Conducts interviews with stakeholders, gathering objective evidence (procedures, reports and test results)
  - Evaluates the findings against the standard
  - Identifies any areas not in compliance and/or effective which must be cleared by the lead auditor prior to being recommended for certification.

The Assessment Cycle – 3 Year Process

- **Audit Cycle -v- Certification Cycle**



Initial Assessment Stage 2 audit (last day)

Surveillance 1
10 Months

Surveillance 2

Recertification

Audit Cycle

Certification Cycle

Certificate decision date (cert. issued)

12 months

24 months

Certificate expires at
36 months (– 1 day)

Next steps: Important Benefits to Private Sector Preparedness in the United States of America.

End of Presentation