# Management Systems for Security in the Supply Chain

**Dr. Marc Siegel**
Security Management Systems Consultant
ASIS International
European Bureau
Brussels, Belgium
siegel@ASIS-Standards.net

**Supplier – Manufacturer – Distributor – Retailer – Logistics**



**Security and resilience in the supply chain are key components of today's global marketplace**

# 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 preparedness and continuity objectives.

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

- **The Plan – Do – Check – Act (PDCA) cycle** is the operating principle of ISO's management system standards.

# PDCA or APCI Model
*Approach to structured problem solving*

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

**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
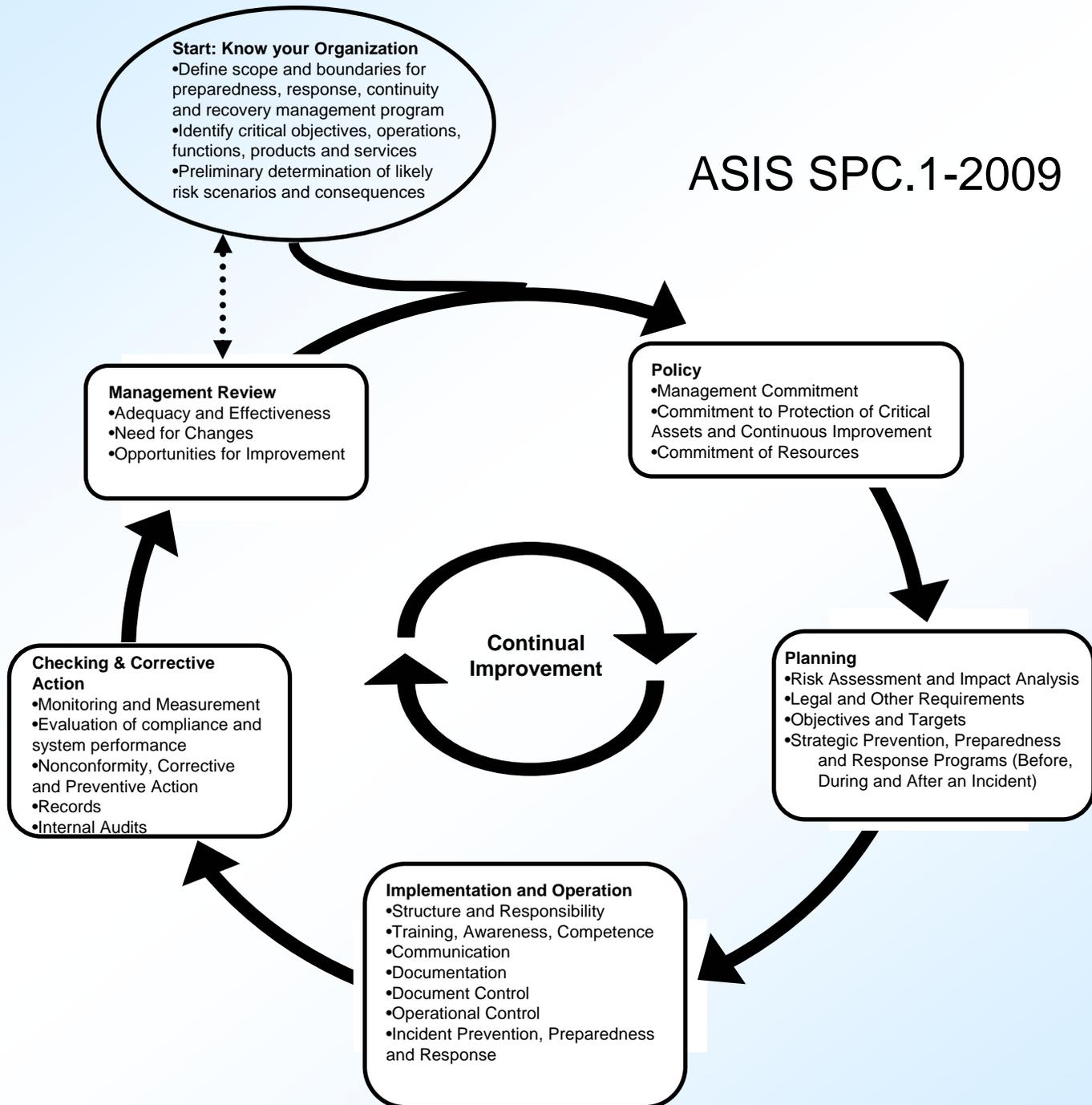- Review and Define Next Issues

© 2008

# ISO 28000 Series of Standards

- **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 28002:xxxx**
  - Resilience in the Supply Chain

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

- **ISO 28004:2007**
  - Security management systems for the supply chain -- Guidelines for the implementation of ISO 28000
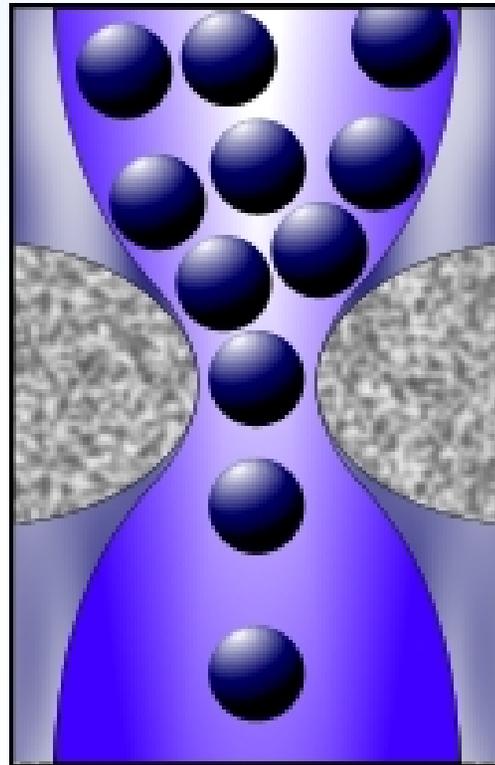
# Risk Management

- Establishes risk management as proactive means of protecting the organization

  - Pragmatic and business-centric approach to risk management

  - Promotes risk management as a central component of effective management

  - Key decision making and commitment of resources is based on a process of effective risk assessment

# Including Organizational Resilience

- Complementary perspectives with varying weights of focus:
  - Focus bulk of efforts on the avoidance or reduction of risks prior to a disruptive event
  - Emphasize management of a crisis as event unfolds.
  - Focus on preparing for and responding to the impacts and consequences of a disruptive event.

- In determining a strategy for the spectrum of options for management of risks before, during and after a disruptive event, business constrains and realities usually determine where an organization will focus its efforts.

© 2008

**Start: 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

ASIS SPC.1-2009

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

**Management Review**
•Adequacy and Effectiveness
•Need for Changes
•Opportunities for Improvement

**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)

**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
•Incident Prevention, Preparedness and Response

**Lead Auditors Needed**



**Demand for implementation and certification is currently outpacing the availability of lead auditors**

# Globalization of Supply Chains

**Disruption of the Supply Chain a Rising Threat**

- Just-in-time manufacturing
- Outsourcing
- Global sourcing
- Specialized factories
- Centralized distribution
- Supply consolidation
- Reduction of the supplier base
- Volatility of demand
- Lack control procedures

# So What Could Happen?

- Human trafficking
- Contraband smuggling
- Theft
- Cyber-crime
- Internal sabotage
- Industrial sabotage
- Terrorism
- Counterfeiting
- Insurgency
- Bio-terrorism
- Wholesale and retail supply loss
- Organized crime
- WMD in containers
- Political disruptions
- $$$ Damages

# What are the Consequences of an Incident?

- Damage to tangibles:
  - Human and physical assets – property, products, infrastructure, personnel and the environment

- Damage to intangibles:
  - Non-physical assets - reputation, market position, goodwill

- The harm to the organization may include;
  - Injury or serious harm to persons and property
  - Business integrity
  - Reputation
  - Clients property
  - Standing in industry community
  - Regulatory issues