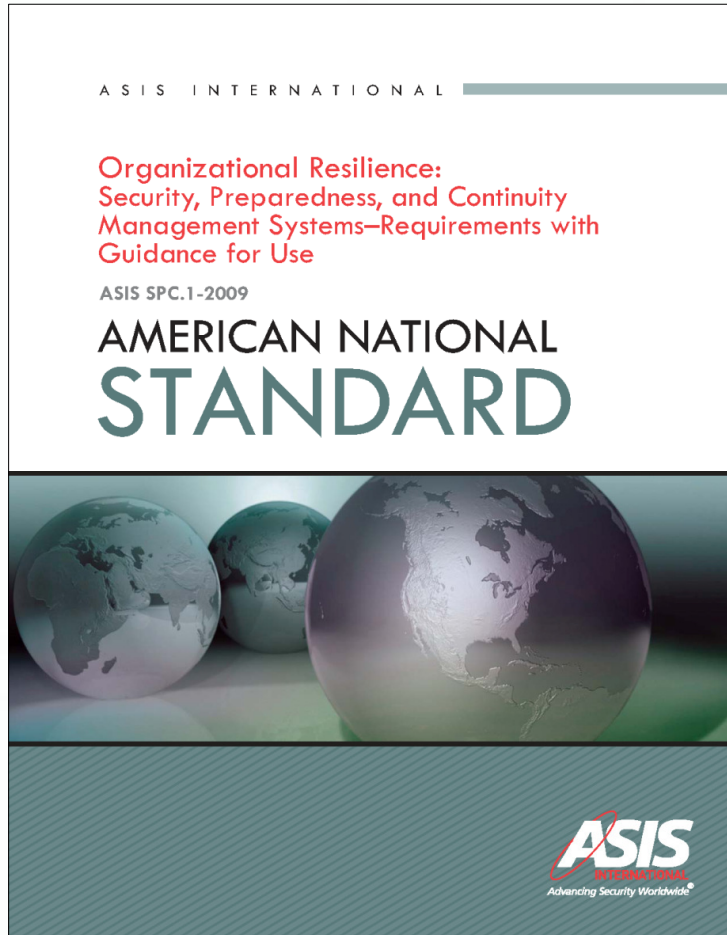


Making Your Organization Resilient



Dr. Marc Siegel

ASIS International
European Bureau
Brussels, Belgium

An International Effort

- Written collaboratively by teams in Australia, the Netherlands and the US.
- Adopted as National Standard in the Netherlands and Denmark
- Accepted by Technical Committee in Italy
- Draft in Technical Committee in Australia
- Providing the basis for ISO 28002: Resilience in the Supply Chain
- Danish version submitted as New Work Item Proposal (NWIP) in ISO/TC 223.
- Selected for US-DHS PS-Prep Program

A comprehensive management systems approach for prevention, protection, preparedness, response, mitigation, continuity, and recovery for disruptive incidents resulting in an emergency, crisis, or disaster.



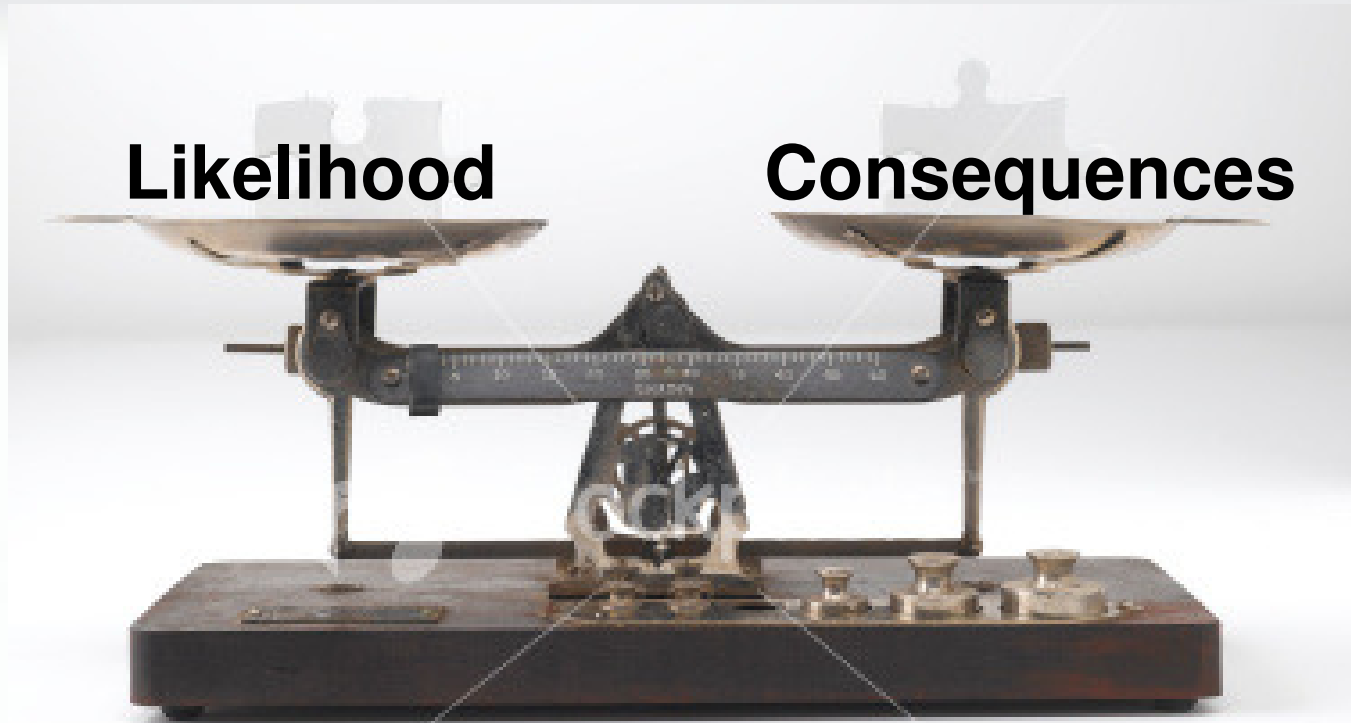
Resilience Management is Everybody's Business

- Managing risks is not just the responsibility of management.
- For a resilience management program to be effective it must be implemented by every person in the organisation.
- Managing risk and resilience must become an integral part of the organisational culture.
- The risk makers and risk takers must be the risk managers.
- The organization must take ownership – implementation of a management system is by and for the organization.

A Cultural Change



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.

ANSI/ASIS SPC.1-2009 is a Practical Application of the ISO31000:2009 Risk Management

ASIS INTERNATIONAL

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

ASIS SPC.1-2009

AMERICAN NATIONAL
STANDARD



ASIS
INTERNATIONAL
Advancing Security Worldwide®

INTERNATIONAL
STANDARD

ISO/FDIS
31000

**Risk management — Principles and
guidelines**

Management du risque — Principes et lignes directrices



Reference number
ISO/FDIS 31000:2009(E)

© ISO 2009

What is Resilience?

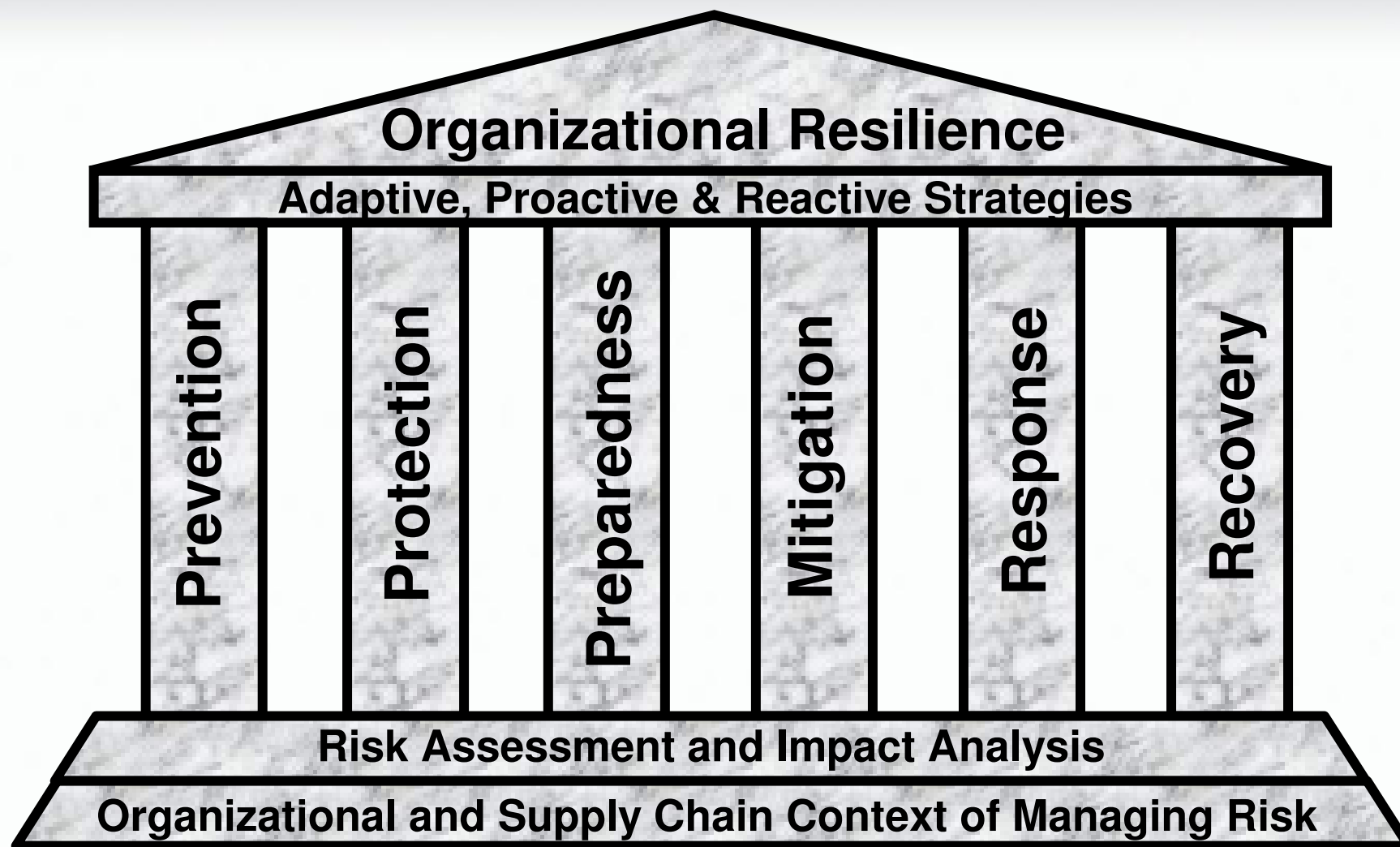
Achieve core objectives
in the face of adversity.

Reduce the size and
frequency of crises, as
well as improve the
ability and speed to
manage crises
effectively.

Avoid stove piping or
siloeing risks.



A Strong Foundation for Managing Risks



Why an Integrated Approach ?

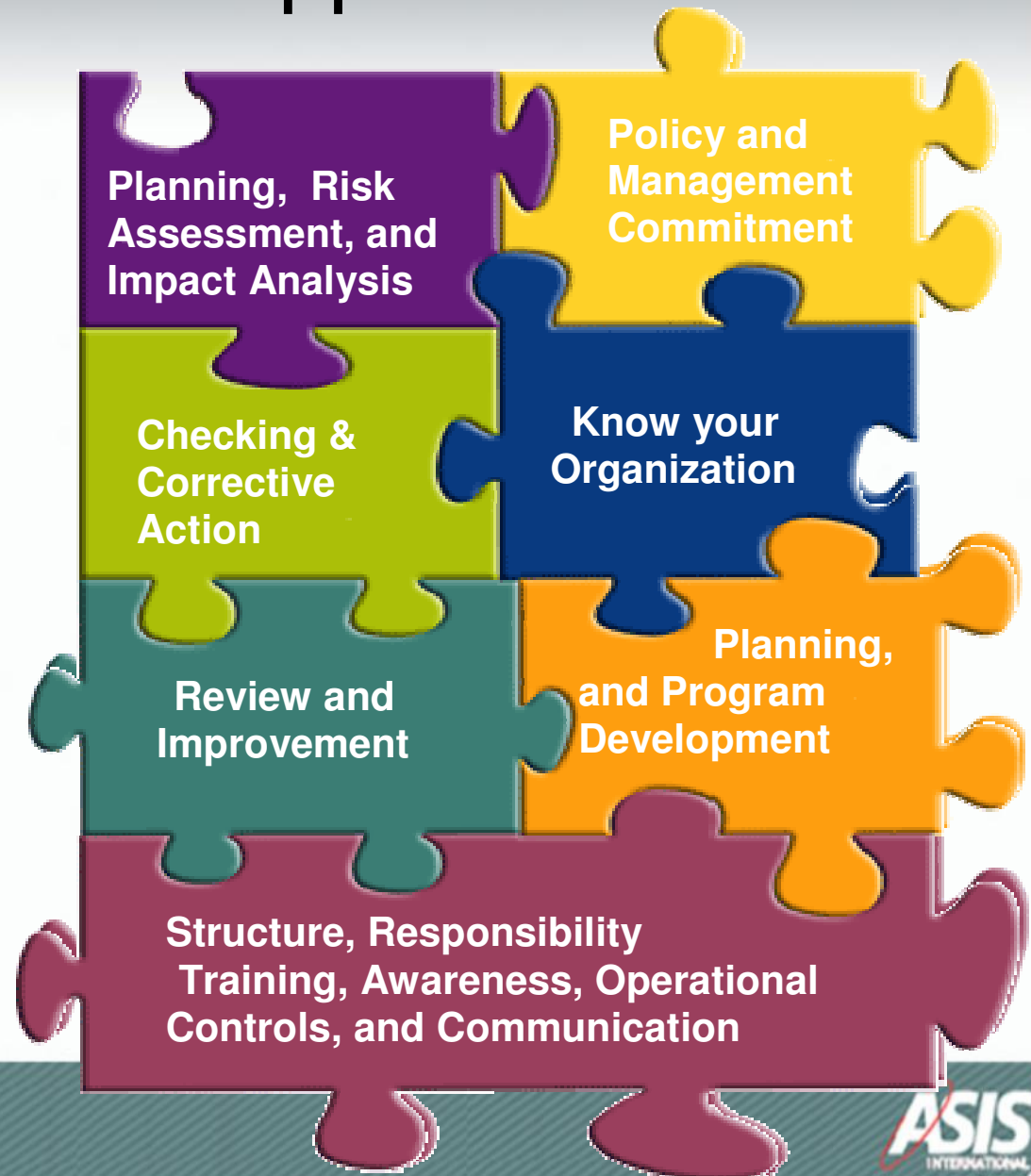
- Helps avoid segregating or siloing risks.
- Provides an overall risk profile allowing the organization to better understand the relationships between risks and identify solutions to problems.
- Leverages the perspectives, knowledge and capabilities of divisions and individuals within an organization.
- Because of the relatively low probability and yet potentially high consequence nature of many natural, intentional, or unintentional threats and hazards, an integrated approach allows an organization to establish priorities that address its individual needs for managing operational risks within an economically sound context.

What is a “Systems Approach”?

- A process of estimating how local policies, actions, or changes influence the state of the whole and its environment.
- Component parts of a system can best be understood in the context of relationships with each other, rather than in isolation.
- Examines the linkages and interactions between the elements that compose the entirety of the system.
- Views "problems" as parts of an overall system, rather than reacting to immediate events and potentially contributing to further development of the problem.

The "Systems" Approach

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



ISO Management Systems Standards



Identify risks, set priorities and establish dynamic programs and plans to cost effectively improve performance

Generic framework for organizations of all sizes and types – private, public, faith-based or not-for-profit organizations.

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/IEC 27001:2005 - Information technology security
 - ISO 28000:2007 - Security management systems for the supply chain
 - ISO 31000:2009 – Risk Management
- Supports consistent and integrated implementation and operation with related management standards.
- One suitably designed management system can satisfy the requirements of all these standards.

PDCA or APCI Model

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

Do

Devise a Solution
Develop Detailed Action Plan & Implement It Systematically

Check

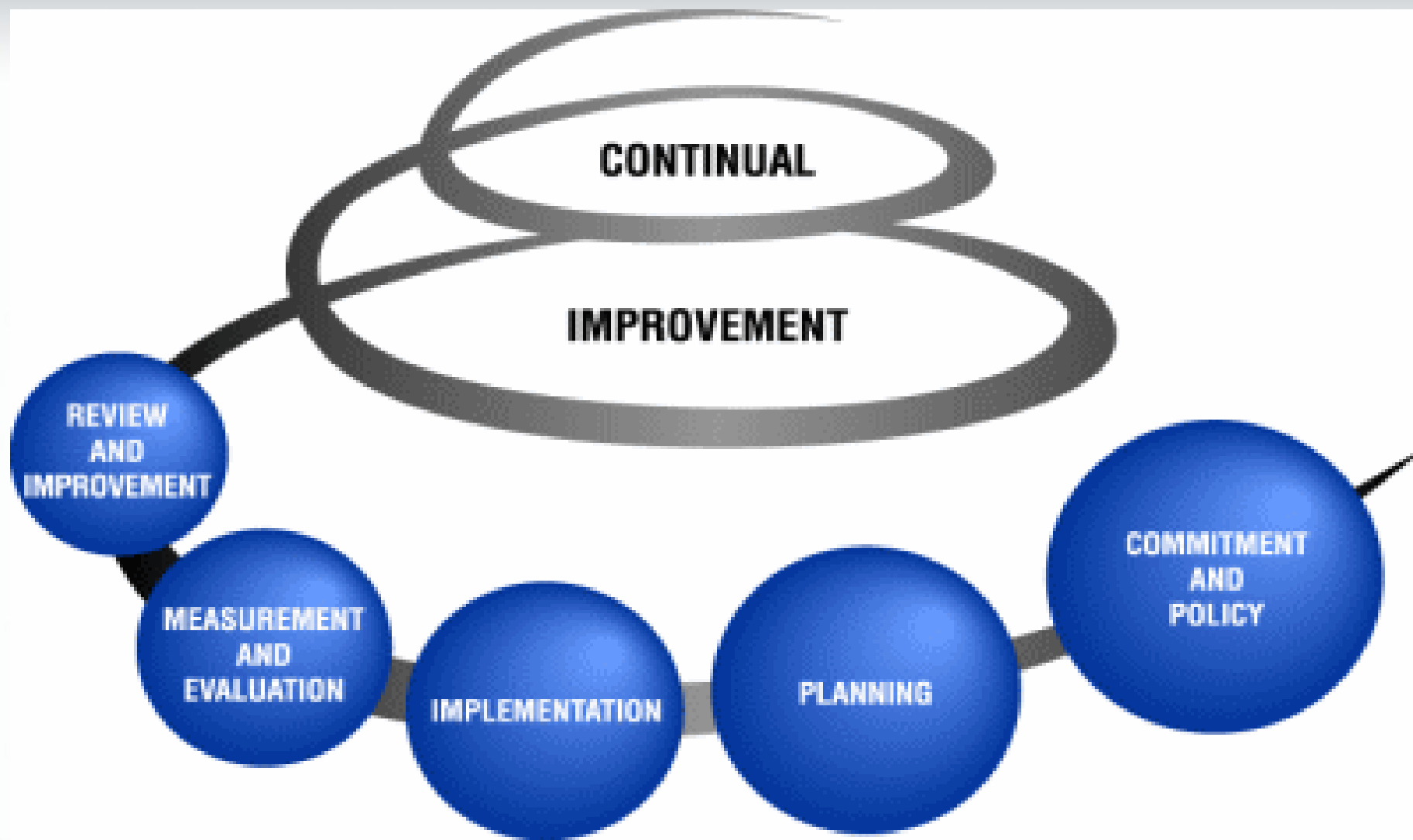
Confirm Outcomes Against Plan
Identify Deviations and Issues

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**



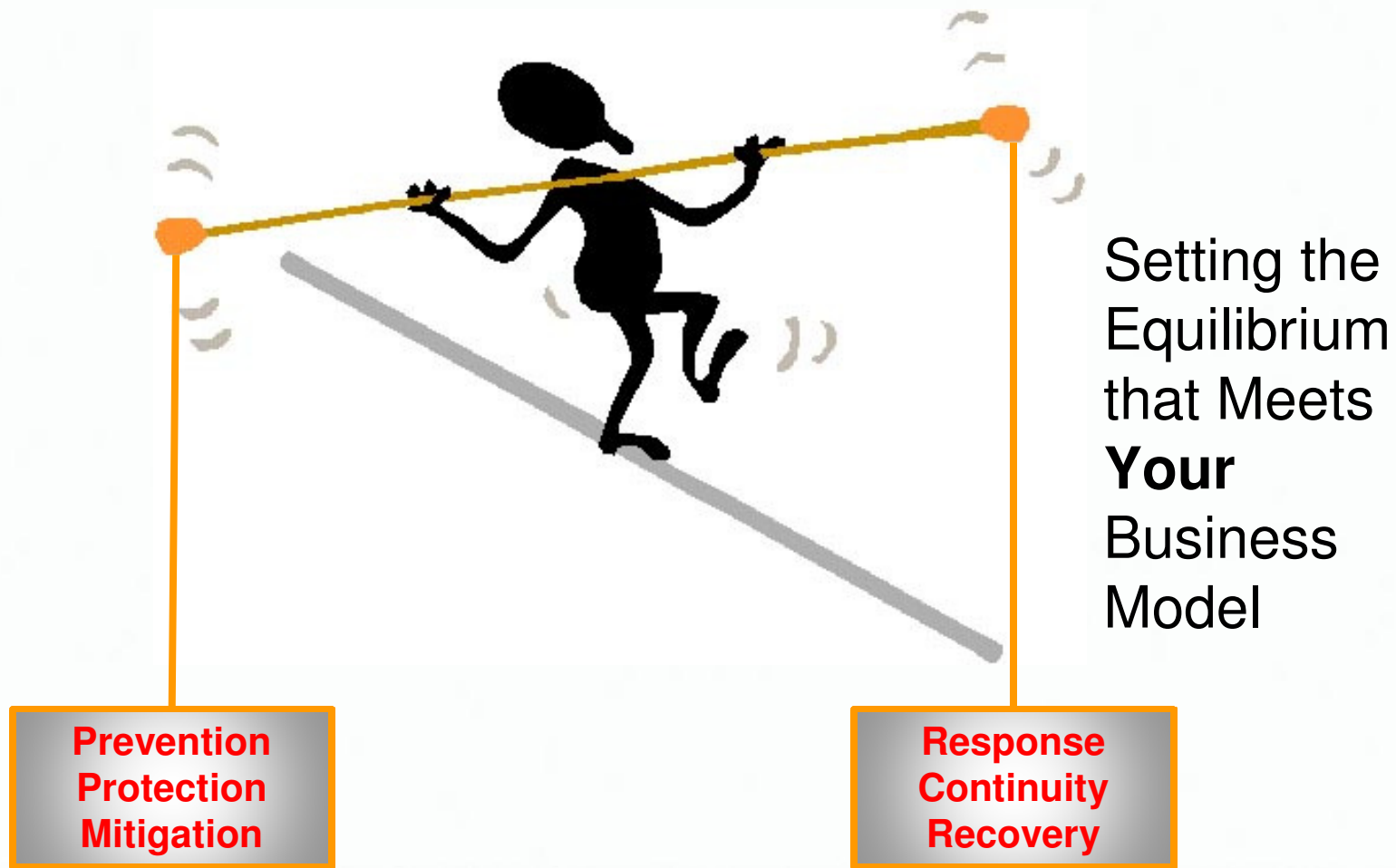
Continual Improvement – Not Linear

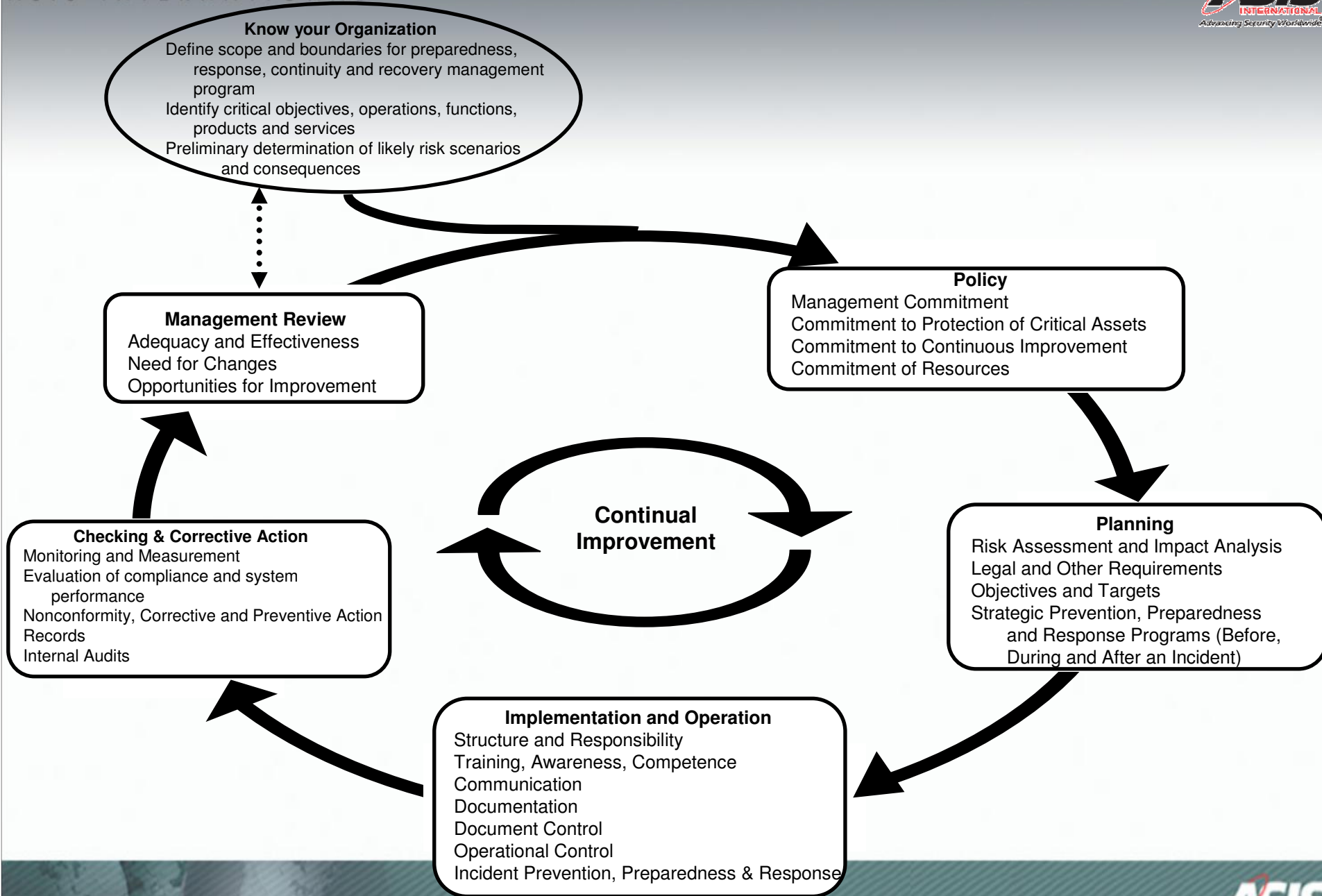


Maturity Model for Phased Implementation

ANSI/ASIS.SPC.1:2009

Let's You Set the Appropriate Balance





Know your Organization

- Establish the context
- 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
 Commitment
 Protection of Critical Assets
 Commitment to Continuous Improvement
 Efficient Use 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)

Continual Improvement

Implementation and Operation

Structure and Responsibility
 Training, Awareness, Competence
 Communication
 Documentation
 Document Control
 Operational Control
 Incident Prevention, Preparedness & Response

Checking & Corrective Action

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

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

Organizational Resilience Policy

- Management Commitment
- Commitment to Protection of Critical Assets
- Commitment to Continuous Improvement

Improvement of Resources

- 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
 Incident Prevention, Preparedness & Response

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
 Commitment to Continuous Improvement
 Commitment of Resources

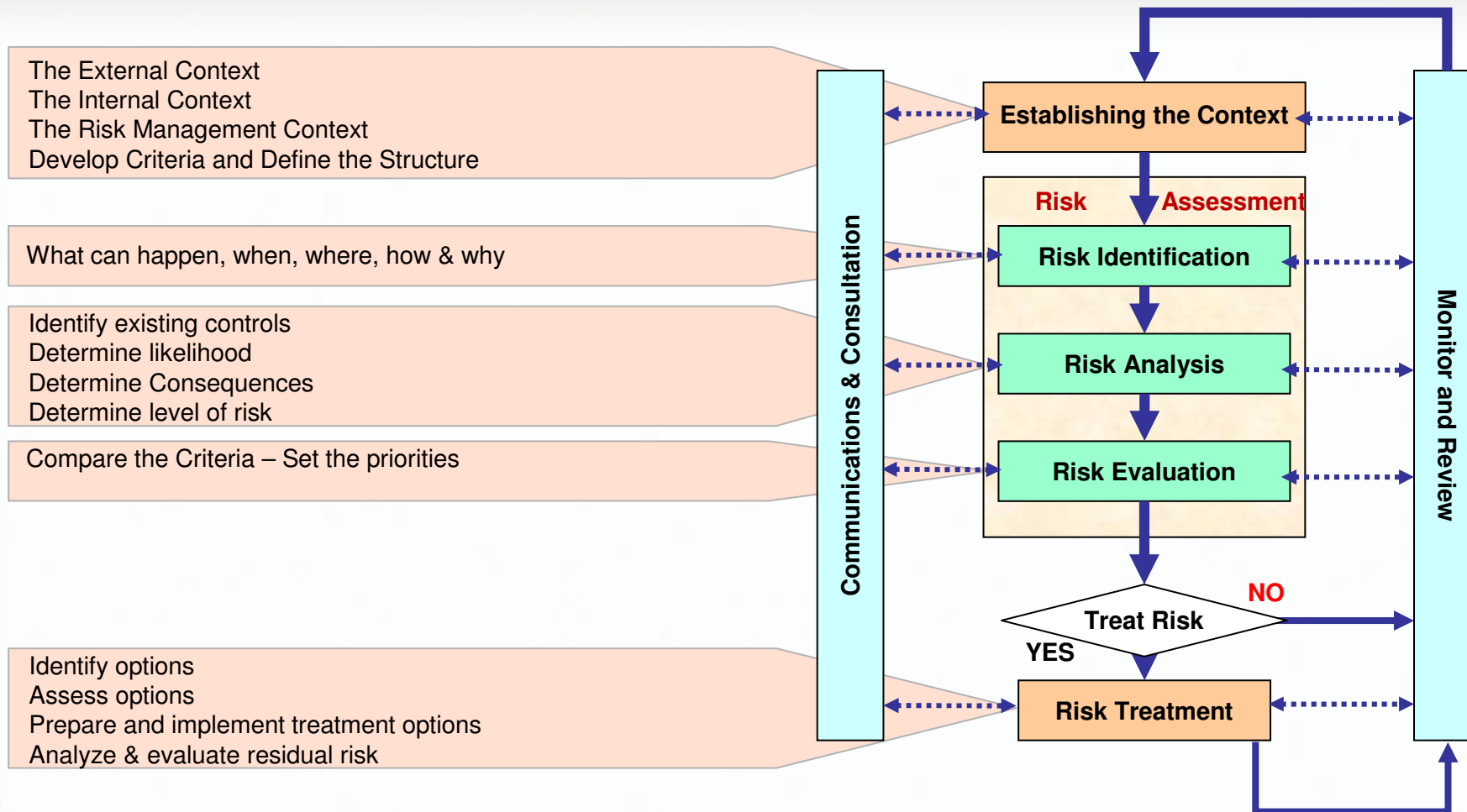
Checking & Corrective Action
 Monitoring and Measurement
 Evaluation of compliance and system performance
 Nonconformity, Corrective and Preventive Action Records
 Internal Audits

Planning

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

Str
 Tra
 Co
 Doc
 Docu
 Operational Control
 Incident Prevention, Preparedness & Response

ISO 31000:2009 Risk Management



Source: ISO 28002, Author: Peter Boyce

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
Continuous Improvement

Implementation and Operation
Structure, Authority and Responsibility
Competence, Training, and Awareness
Communication
Documentation
Document and Data Control
Operational Control
Incident Prevention, Protection, Preparedness, Mitigation, Response and Recovery

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

Planning
Risk Assessment and Impact Analysis
Identify Requirements and Targets
Incident 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

Management Review
Adequacy and Effectiveness

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

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

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)

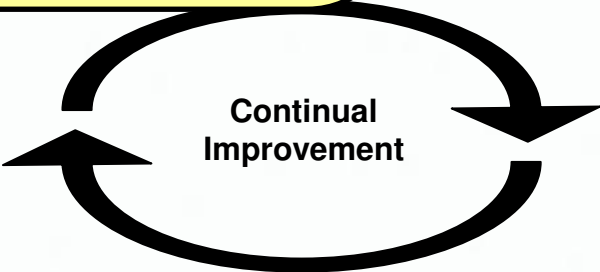
Operation
Incident Prevention, Preparedness & Response

Know your Organization
Define scope and boundaries for preparedness,
response, continuity and recovery management

Management Review
Adequacy and Effectiveness
Need for Changes
Opportunities for Improvement

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
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

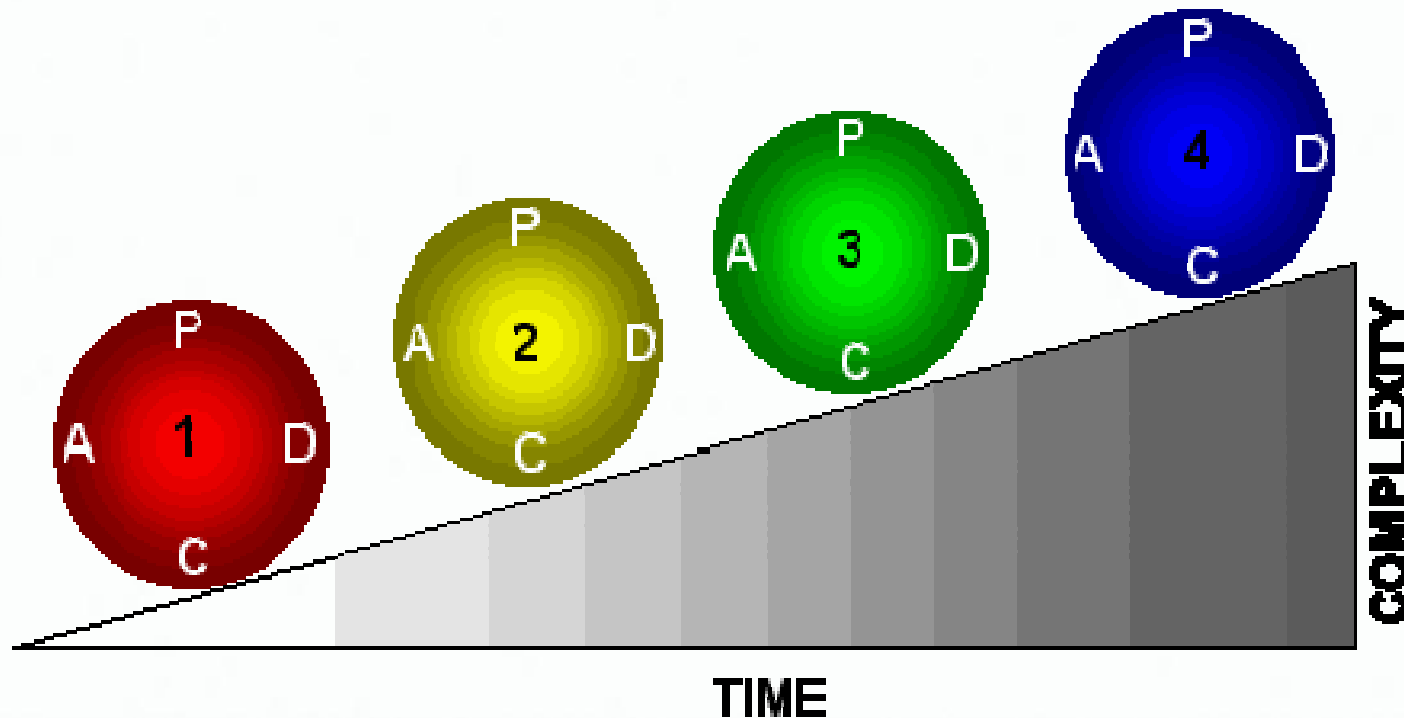
Implementation and Operation
Structure and Responsibility
Training, Awareness, Competence
Communication
Documentation
Document Control
Operational Control
Incident Prevention, Preparedness & Response

Triggers for a Review

- Factors that can trigger a review and/or should be examined in a scheduled review:
 - **Risk Assessment:** Conduct review every time a risk assessment is completed for the organization.
 - **Sector/Industry Trends:** Major sector/industry initiatives should initiate a review.
 - **Regulatory Requirements:** New regulatory requirements may require a review.
 - **Event Experience:** A review should be performed following a response to an event, whether the ORM plan was activated or not.
 - **Test/Exercise Results:** Based on test/exercise results, the ORM plan should be modified as necessary.

The Continual Improvement Process

- As each full PDCA cycle comes to completion, a new and slightly more complex issue can be addressed.



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
- Requires security people to get out of their box
- ORMS requires commitment - its not a part-time job!

Thank You

Dr. Marc Siegel

Commissioner, Global Standards Initiative

ASIS International

Phone: +1-858-484-9855

Email: siegel@ASIS-Standards.net

siegel@gmail.com

