STANDARDS AND GUIDELINES

BEYOND THE SILOS – ORGANIZATIONAL RESILIENCE

Dr. Marc Siegel
Commissioner, Global Standards Initiative
ASIS International
European Bureau
Brussels, Belgium
siegel@ASIS-Standards.net

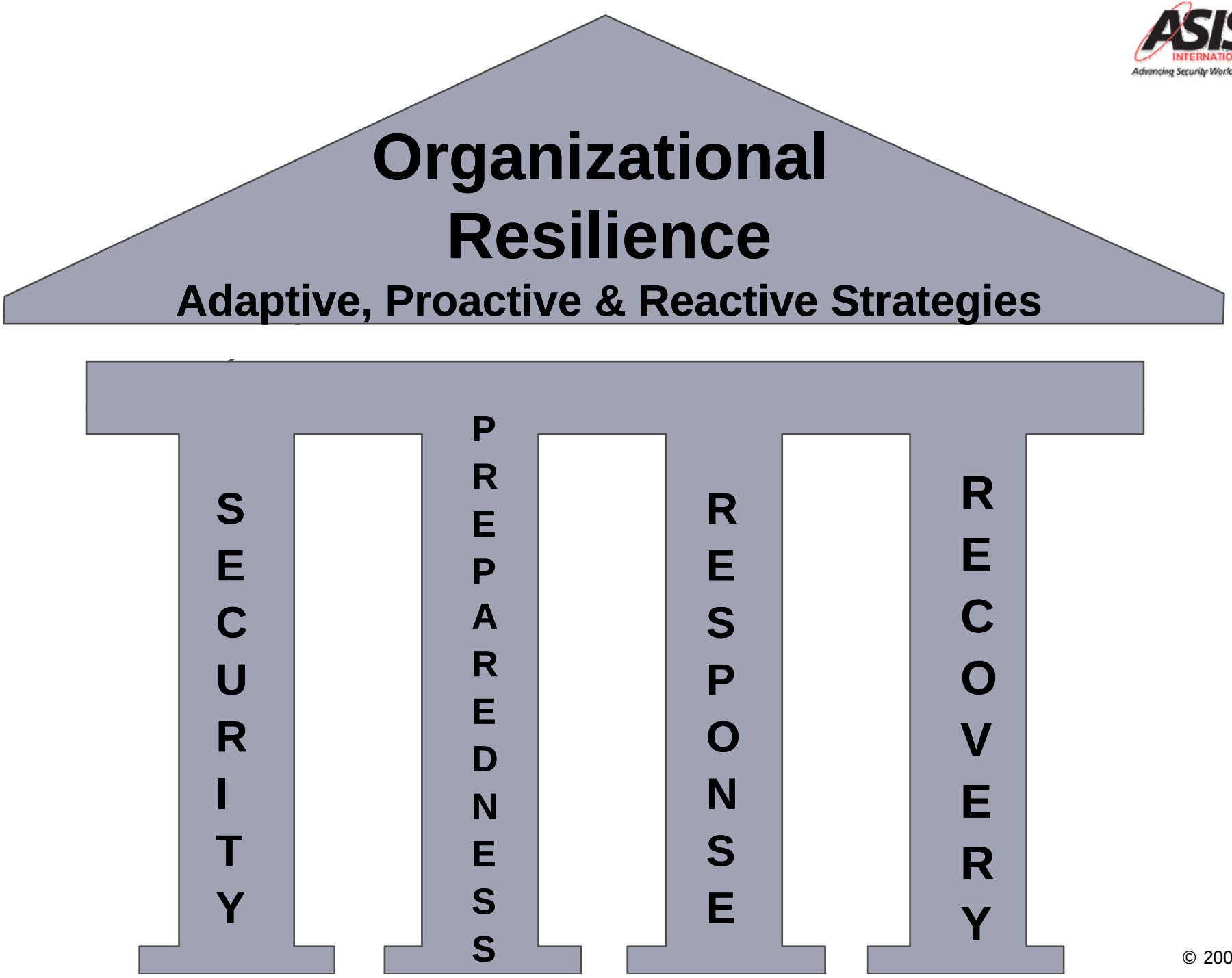
Why an Integrated Approach ?

- 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 Resilience?

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

Helps avoid segregating or siloing risks.


Organizational Resilience
Adaptive, Proactive & Reactive Strategies
SECURITY
PREPAREDNESS
RESPONSE
RECOVERY

What Do We Have in the Toolbox?

- Management System Standards can address your organizational resilience needs.

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.

ISO Management System Standards

- Specify requirements for a generic management system.
  - Provides a framework for a holistic, strategic approach
- Do not dictate how the requirements should be met by a particular organization.
  - Leaves flexibility for scope and implementation
  - Does not dictate specific performance requirements
- "Generic" therefore means:
  - Applicable to any size or type of organization
  - Adaptable to different business cultures and different national cultures.
- All ISO management system standards are developed using a similar approach to assure a high degree of compatibility.

Management Systems

- "**Management system**" refers to what the organization does to manage its processes, functions or activities, so that its products or services meet the objectives it has set itself.
  - Set of interrelated elements used to establish and achieve an organization's policy and objectives.
  - Includes policies, organizational structure, responsibilities, planning activities, resources, practices, procedures and processes.
  - A methodology to assess performance against the objectives and targets.
  - A review process to ensure problems are corrected and opportunities for improvement are recognized and implemented .
  - Allows an organization to create and manage its processes and activities to meet its business objectives.

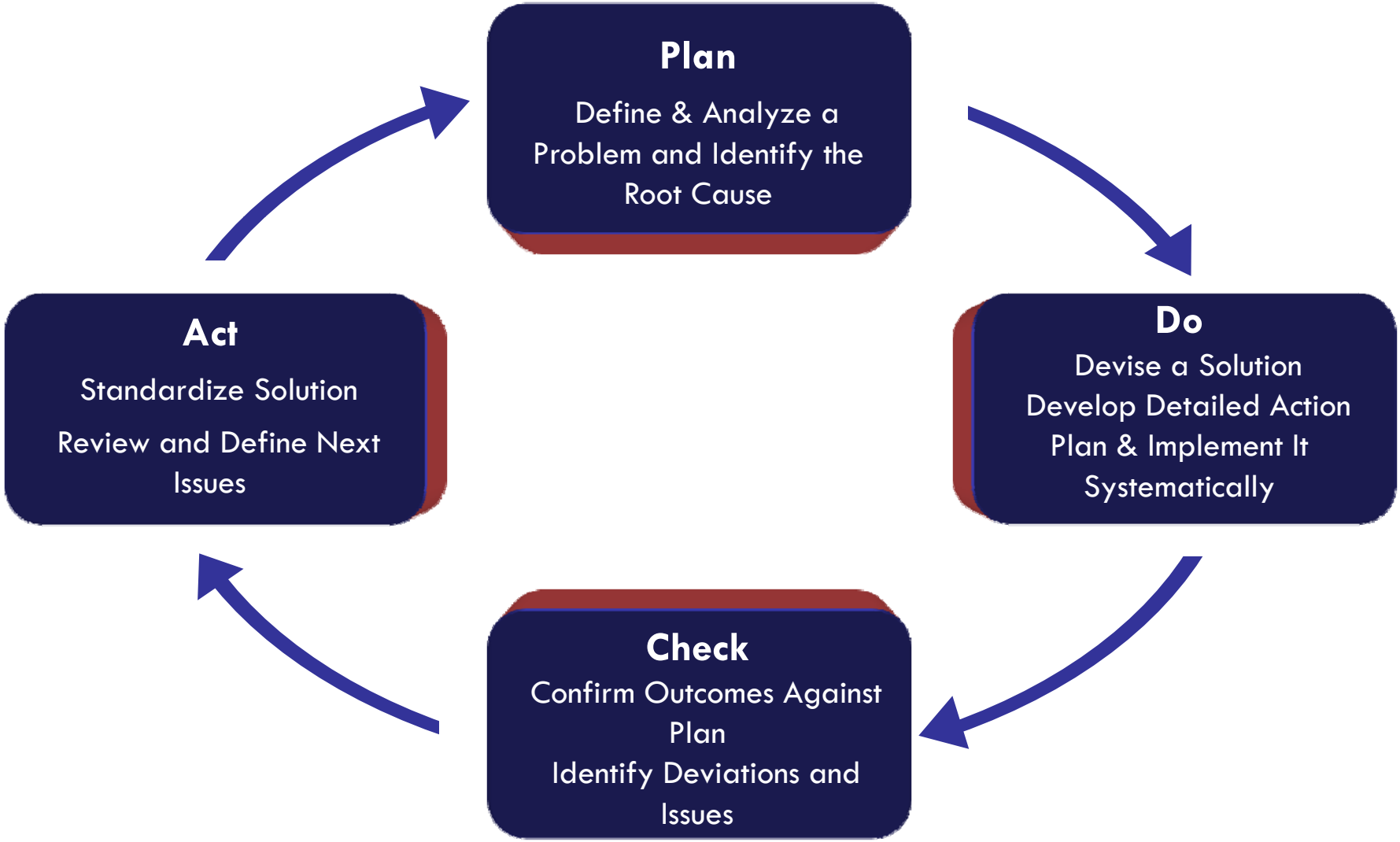
- Management system standards provide a model to follow in setting up and operating a management system.

- 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 focused on continual improvement:

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



ASIS INTERNATIONAL

ASIS SPC.1-2009

Advancing Security Worldwide

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®

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

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
- Supports consistent and integrated implementation and operation with related management standards.
- One suitably designed management system can satisfy the requirements of all these standards.

ASIS SPC.1-2009

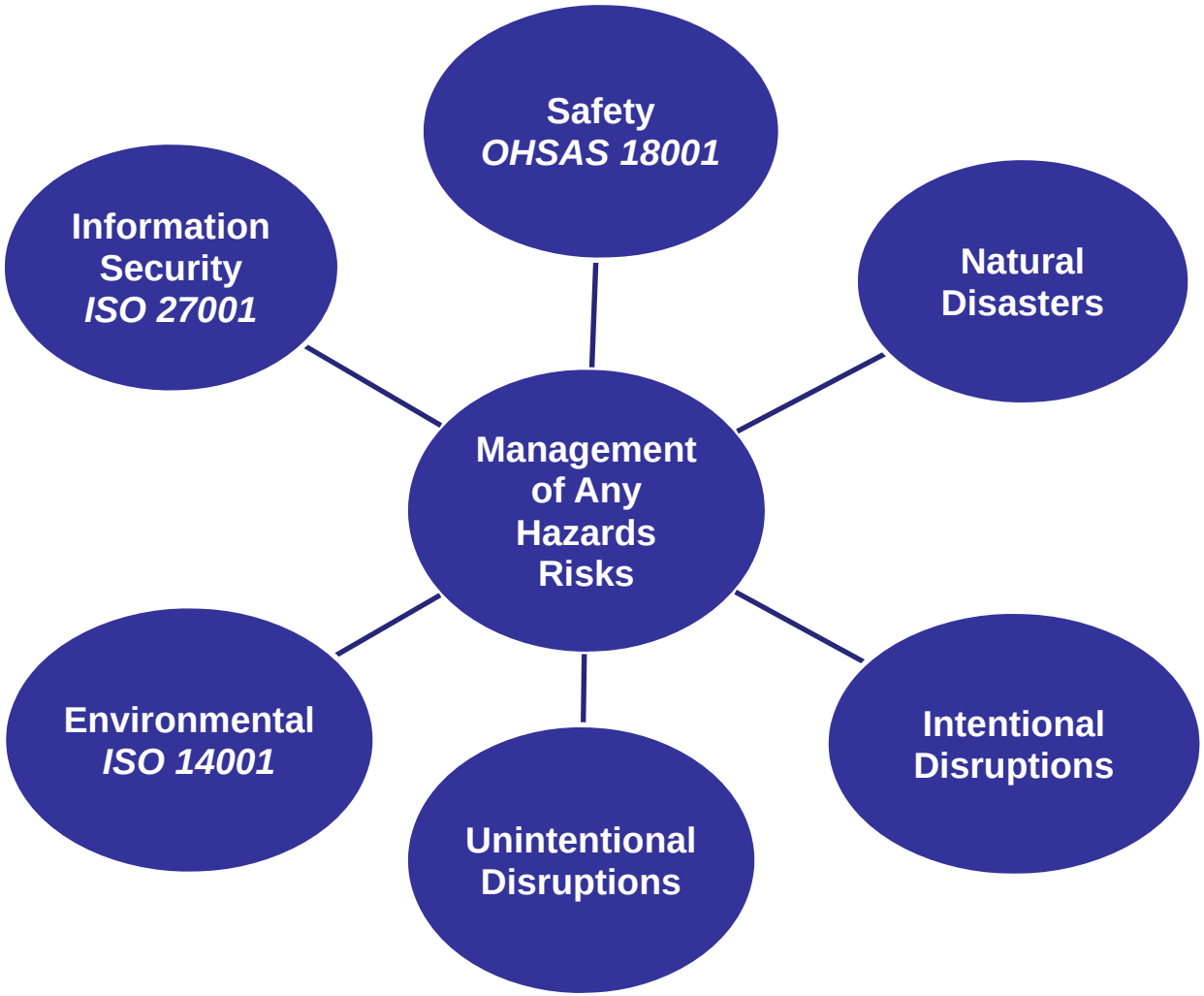
- Provides generic auditable criteria to establish, check, maintain, and improve a management system to enhance prevention, preparedness (readiness), mitigation, response, continuity and recovery from disruptive incidents.

- Flexible, robust and cost effective tool to assure resilience.

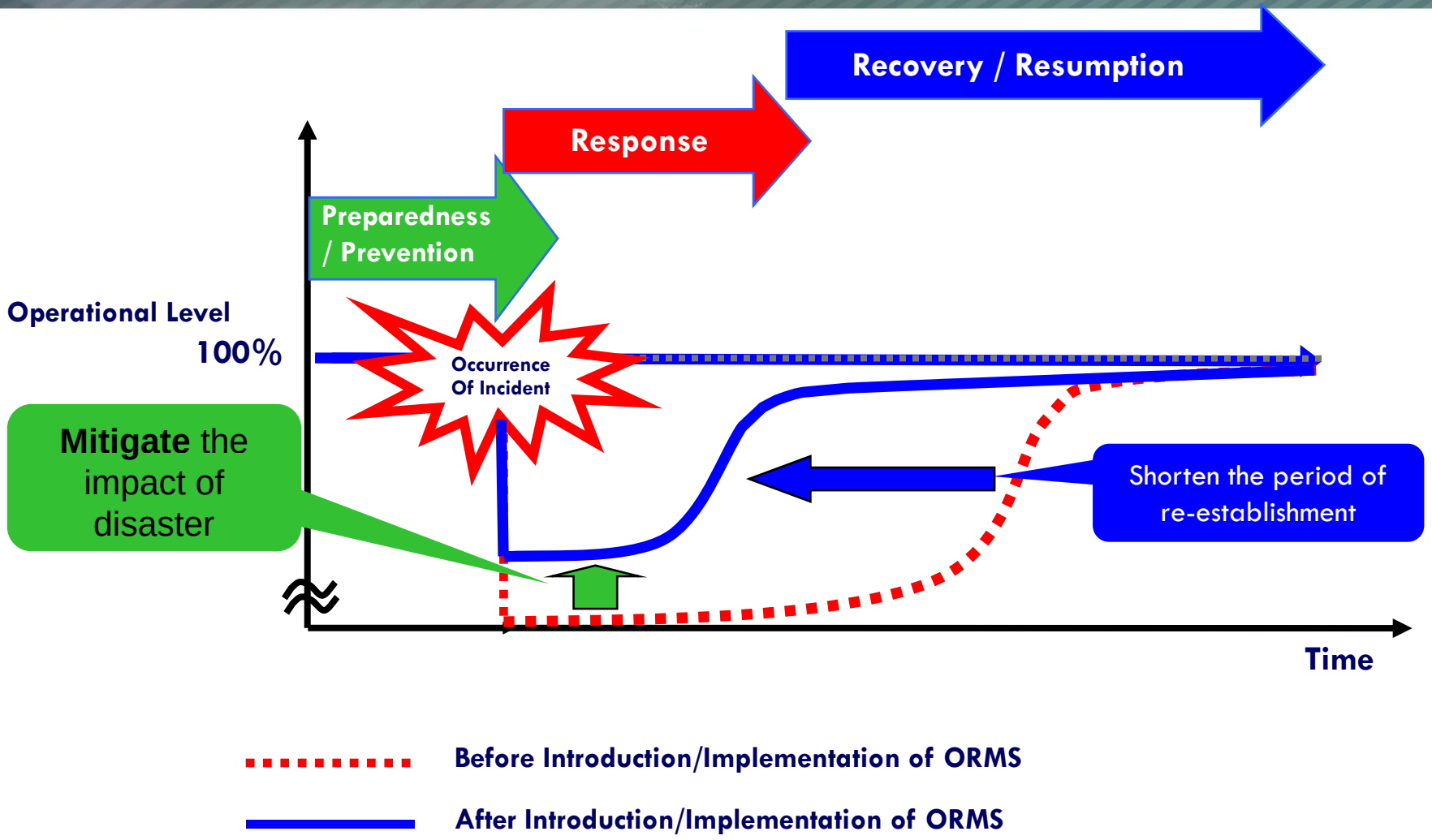
Any Hazards Risk Assessment

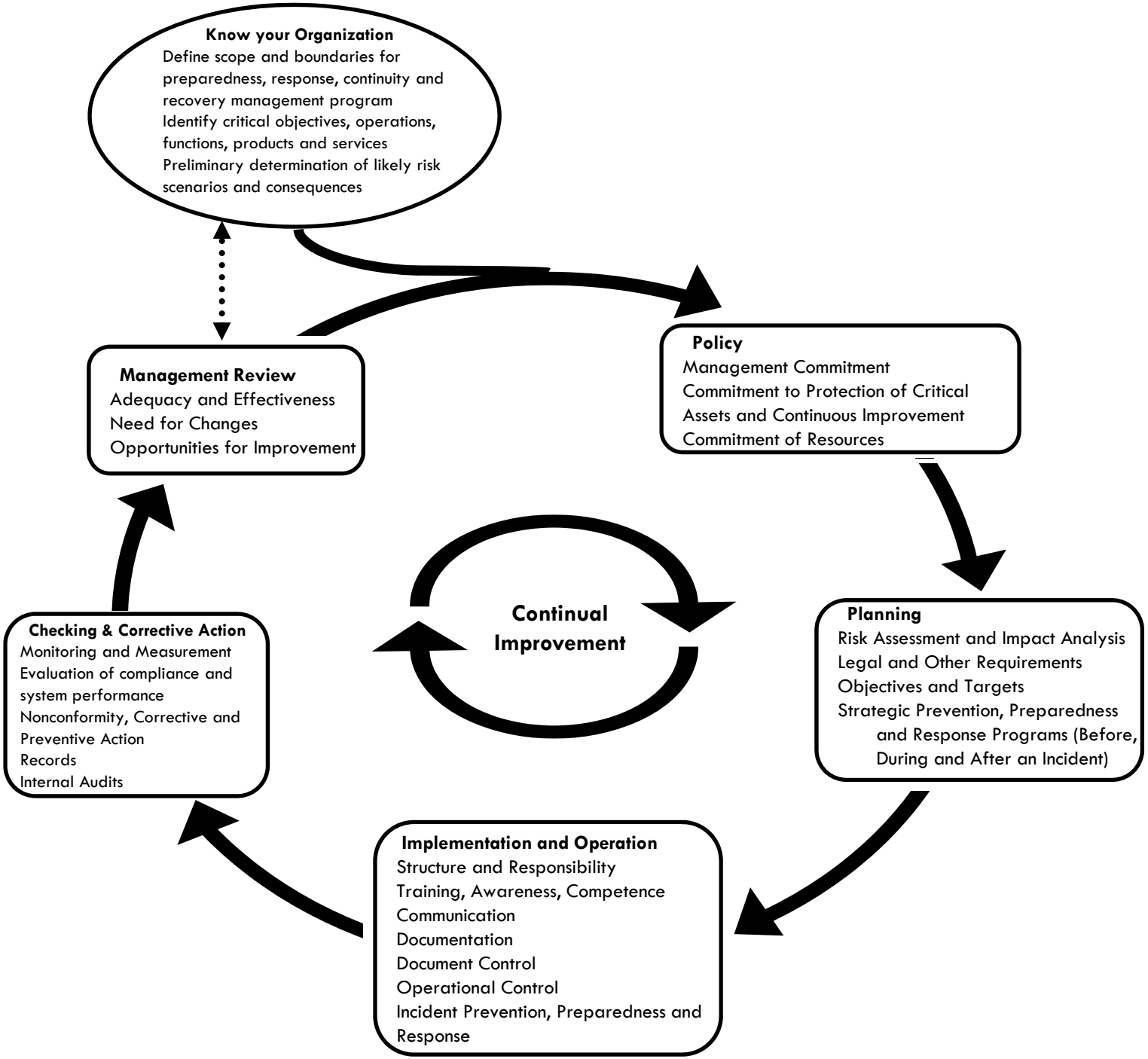
Focus on Protection of Critical Assets and Functions

Incident Management Regardless of Event Trigger



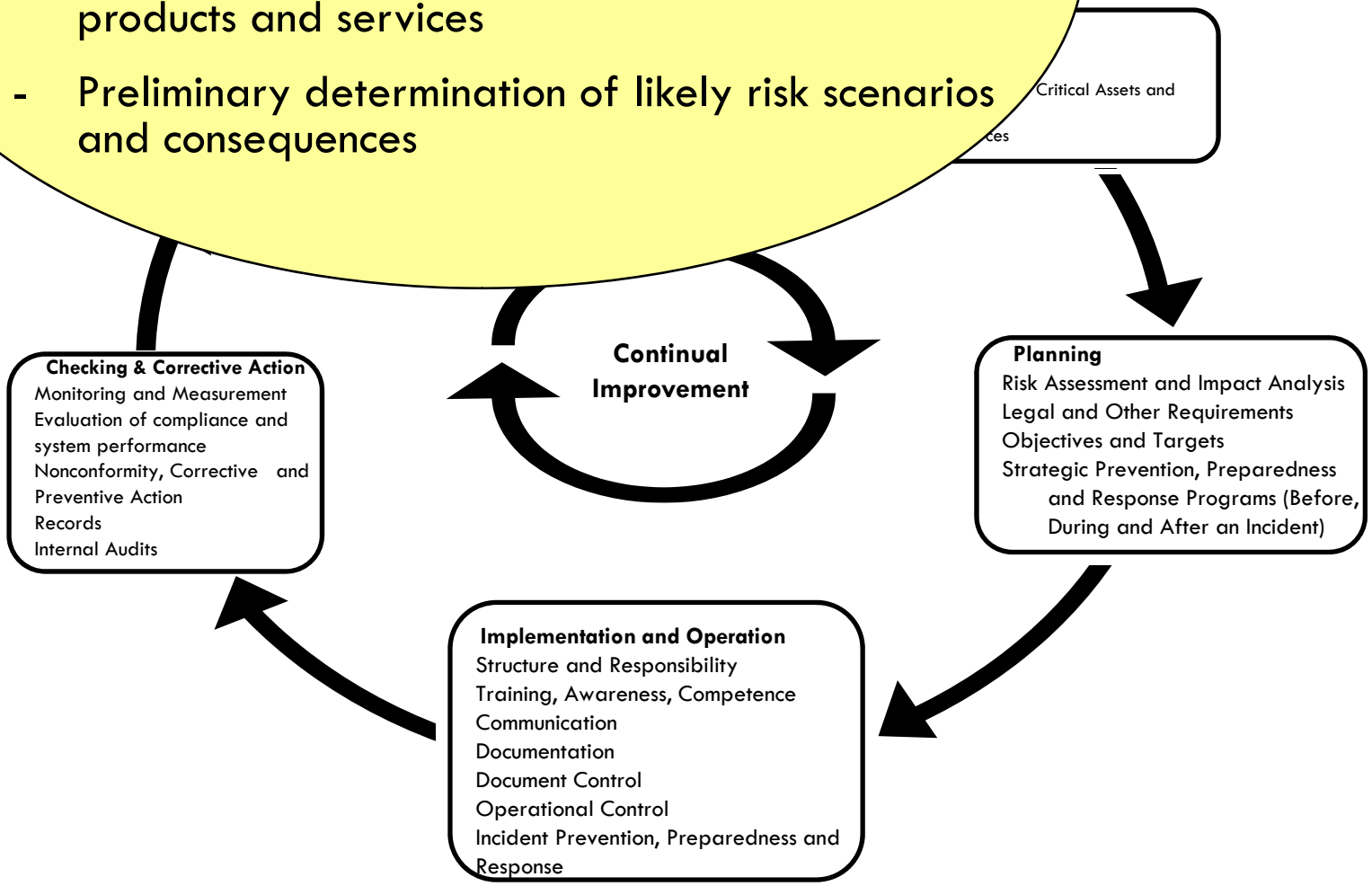
ORMS - Holistic Management Process

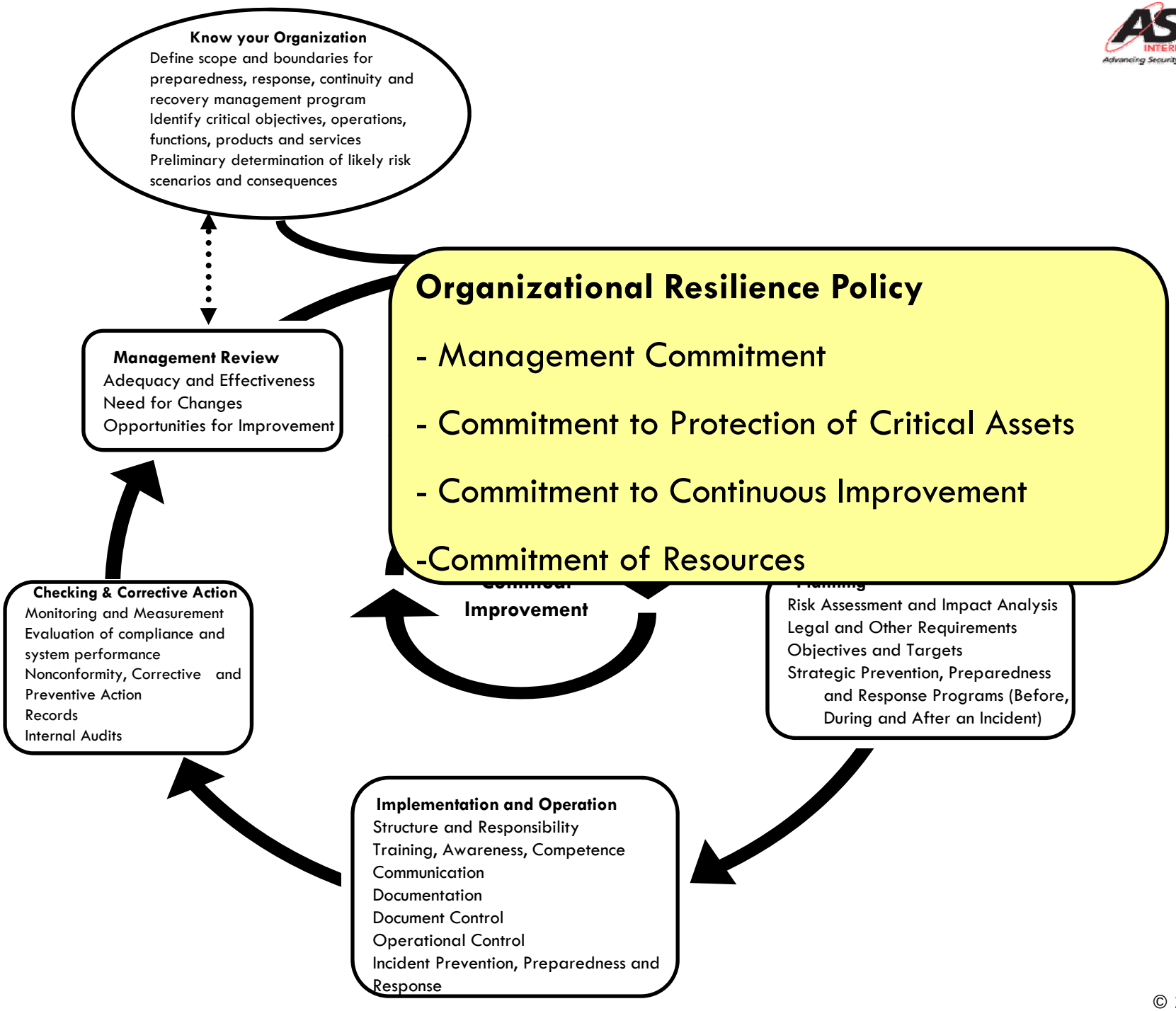


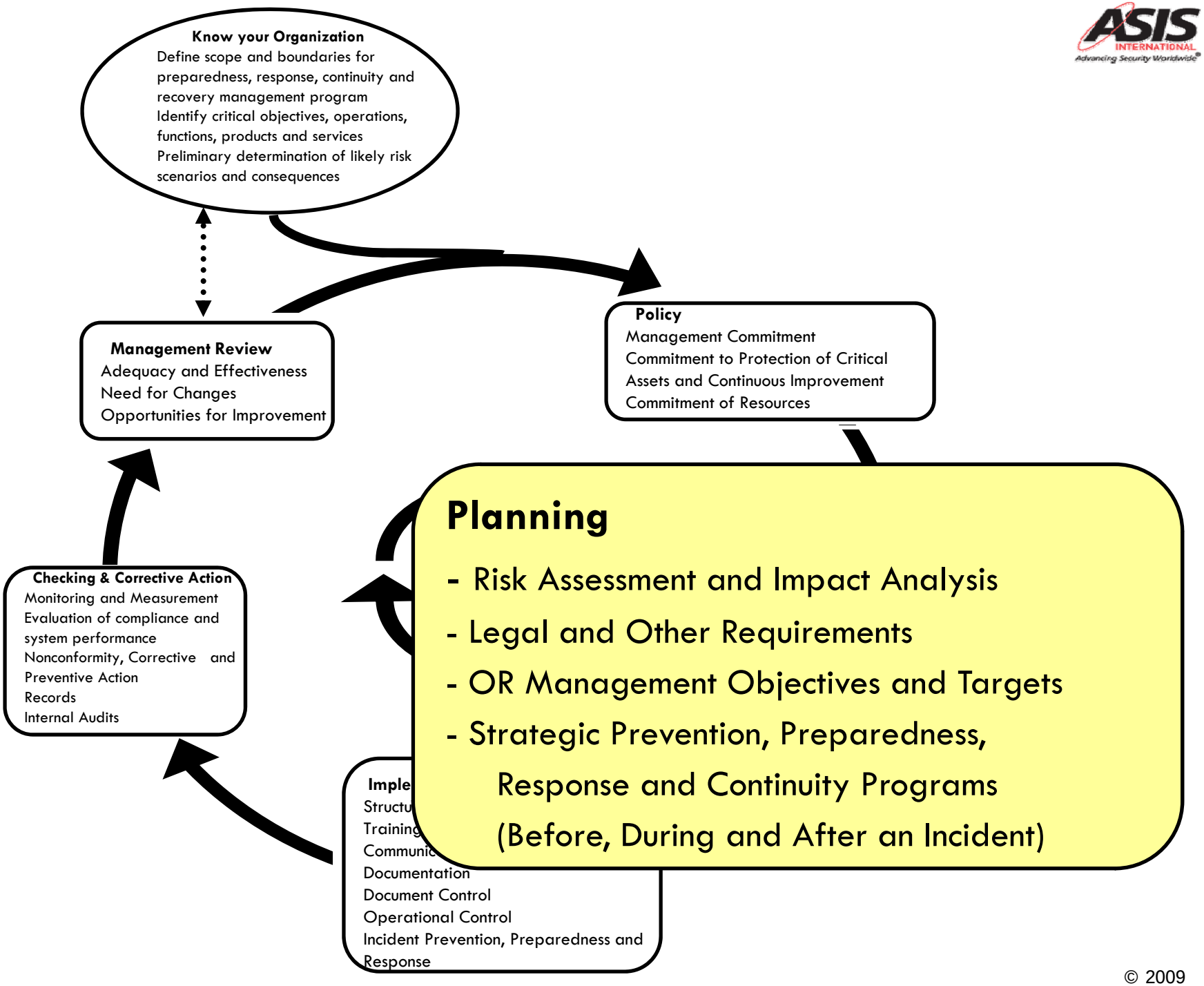

Know your Organization
Define scope and boundaries for preparedness, response, continuity and recovery management program
Identify critical objectives, operations, functions, products and services
Preliminary determination of likely risk scenarios and consequences
Policy
Management Commitment
Commitment 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)
Implementation and Operation
Structure and Responsibility
Training, Awareness, Competence
Communication
Documentation
Document Control
Operational Control
Incident Prevention, Preparedness and Response
Checking & Corrective Action
Monitoring and Measurement
Evaluation of compliance and system performance
Nonconformity, Corrective and Preventive Action
Records
Internal Audits
Management Review
Adequacy and Effectiveness
Need for Changes
Opportunities for Improvement
Continual Improvement

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
Organizational Resilience Policy
- Management Commitment
- Commitment to Protection of Critical Assets
- Commitment to Continuous Improvement
-Commitment of Resources
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
Improvement
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 and 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
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
- OR Management Objectives and Targets
- Strategic Prevention, Preparedness, Response and Continuity Programs (Before, During and After an Incident)
Imple
Structu
Training
Communic
Documentation
Document Control
Operational Control
Incident Prevention, Preparedness and Response
Checking & Corrective Action
Monitoring and Measurement
Evaluation of compliance and system performance
Nonconformity, Corrective and Preventive Action
Records
Internal Audits
Management Review
Adequacy and Effectiveness
Need for Changes
Opportunities for Improvement

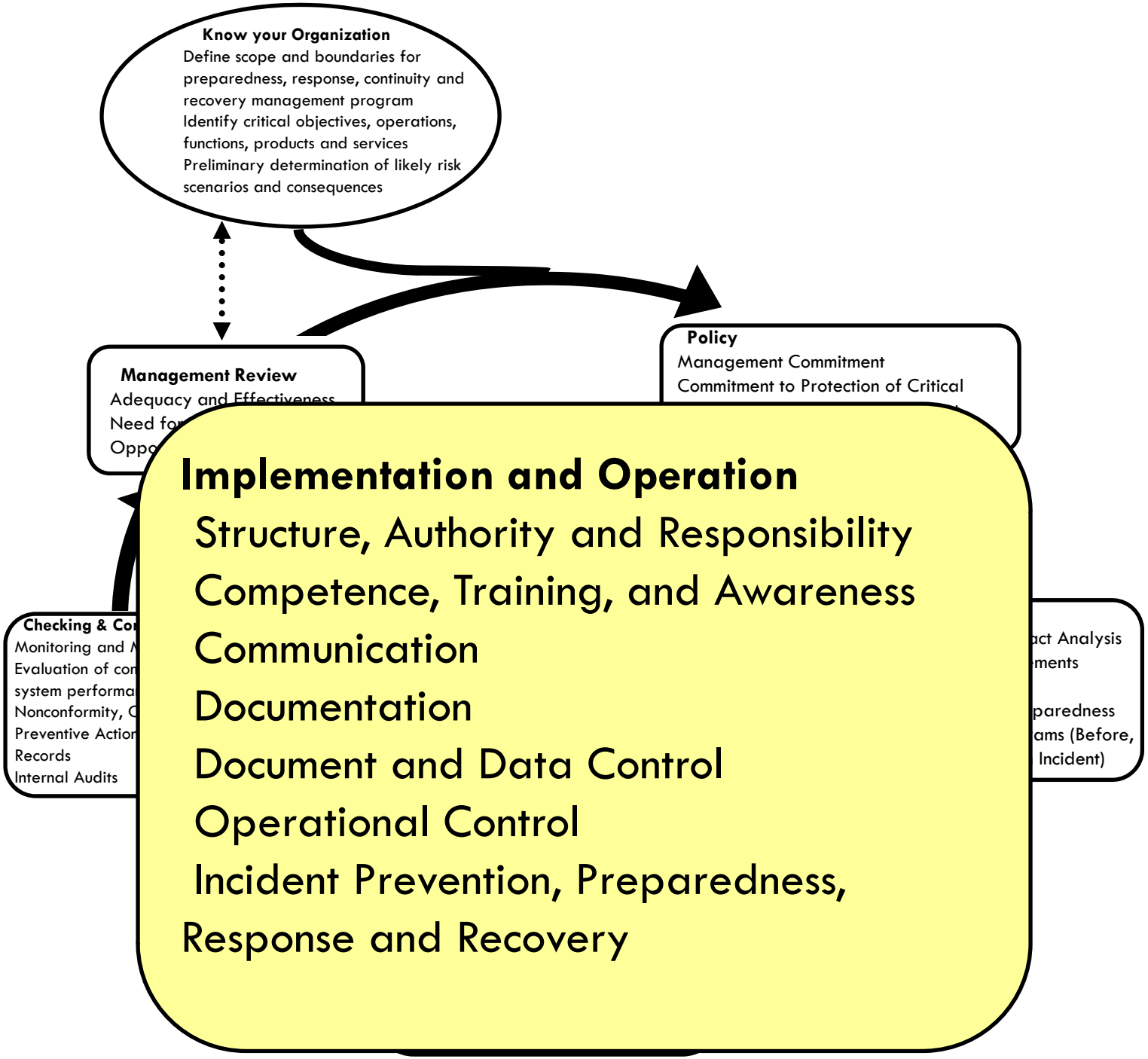
Risk Assessment

- A rational and systematic approach to:
  - Problem Identification
  - Likelihood determination
  - Estimation of potential loss
  - Solution identification
  - System evaluation
- Basis for informed decision-making

Types of Assets

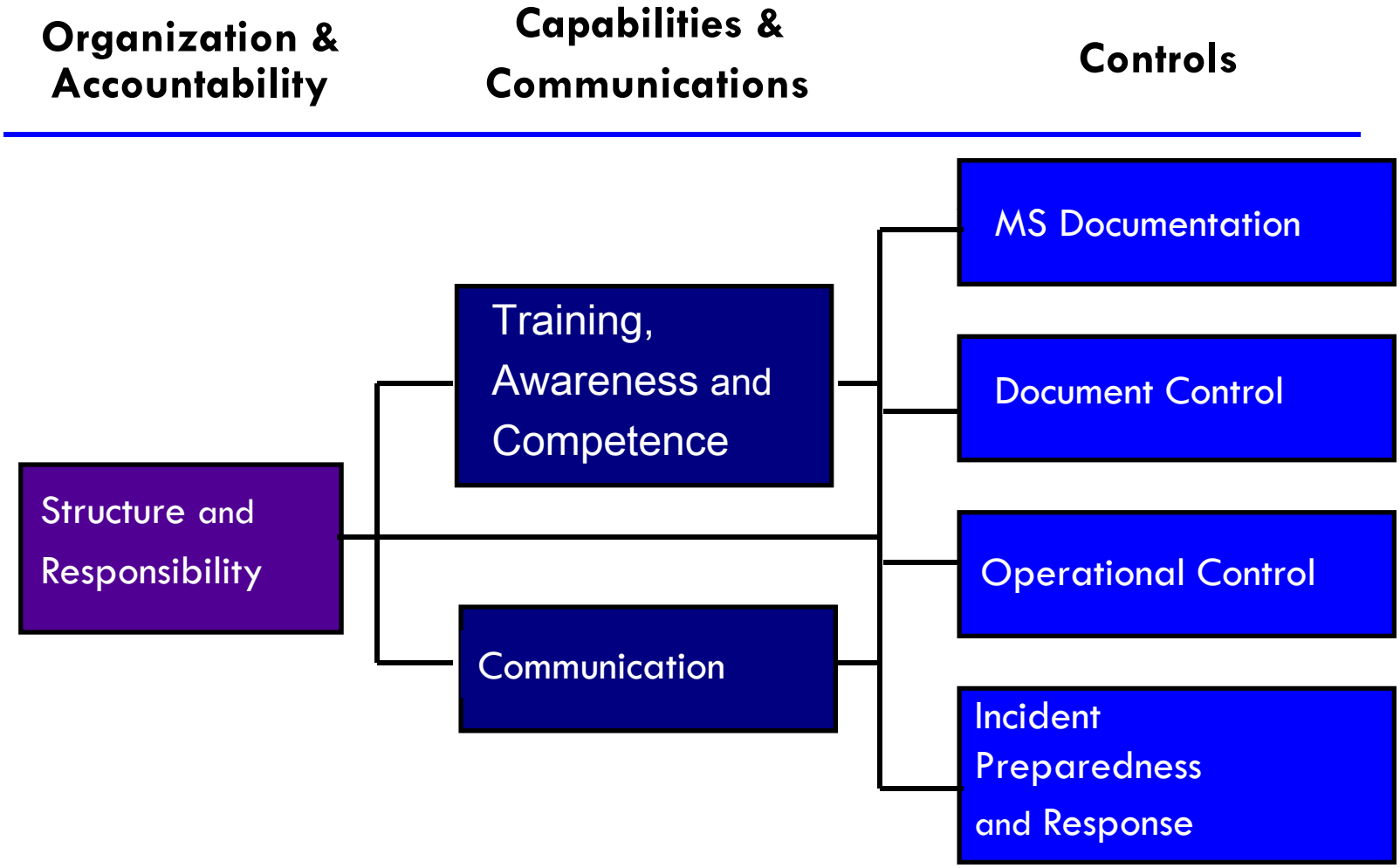
- Tangible:
  - Human
  - Physical
  - Environmental
- Intangible:
  - Image and reputation
  - Data and information
  - Privacy
  - Customer and employee morale and satisfaction

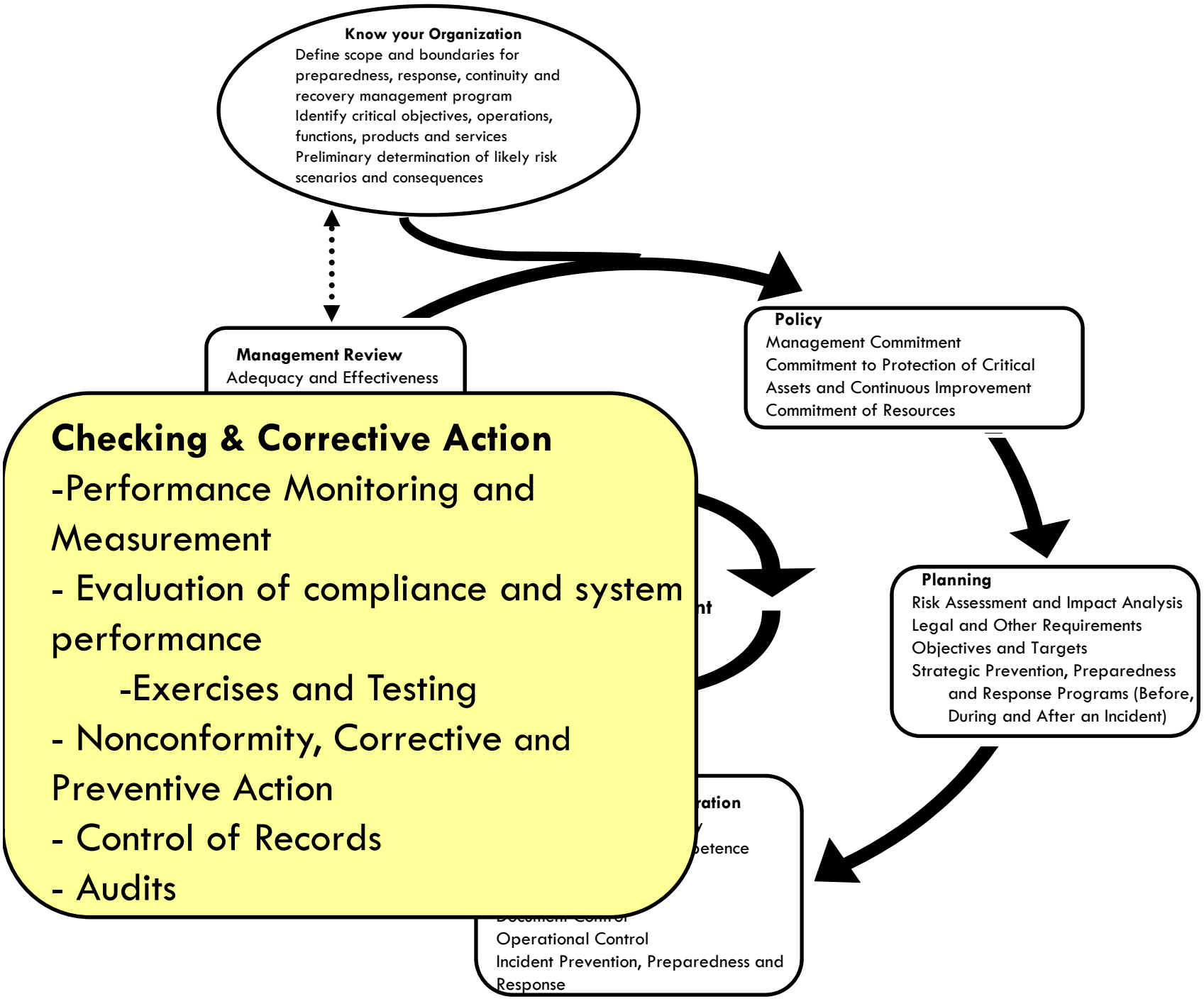
Objectives, Targets and Programs


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
Management Review
Adequacy and Effectiveness
Need for
Oppo
Checking & Cor
Monitoring and M
Evaluation of con
system performa
Nonconformity, C
Preventive Action
Records
Internal Audits
act Analysis
ments
paredness
ams (Before,
Incident)
Implementation and Operation
Structure, Authority and Responsibility
Competence, Training, and Awareness
Communication
Documentation
Document and Data Control
Operational Control
Incident Prevention, Preparedness, Response and Recovery

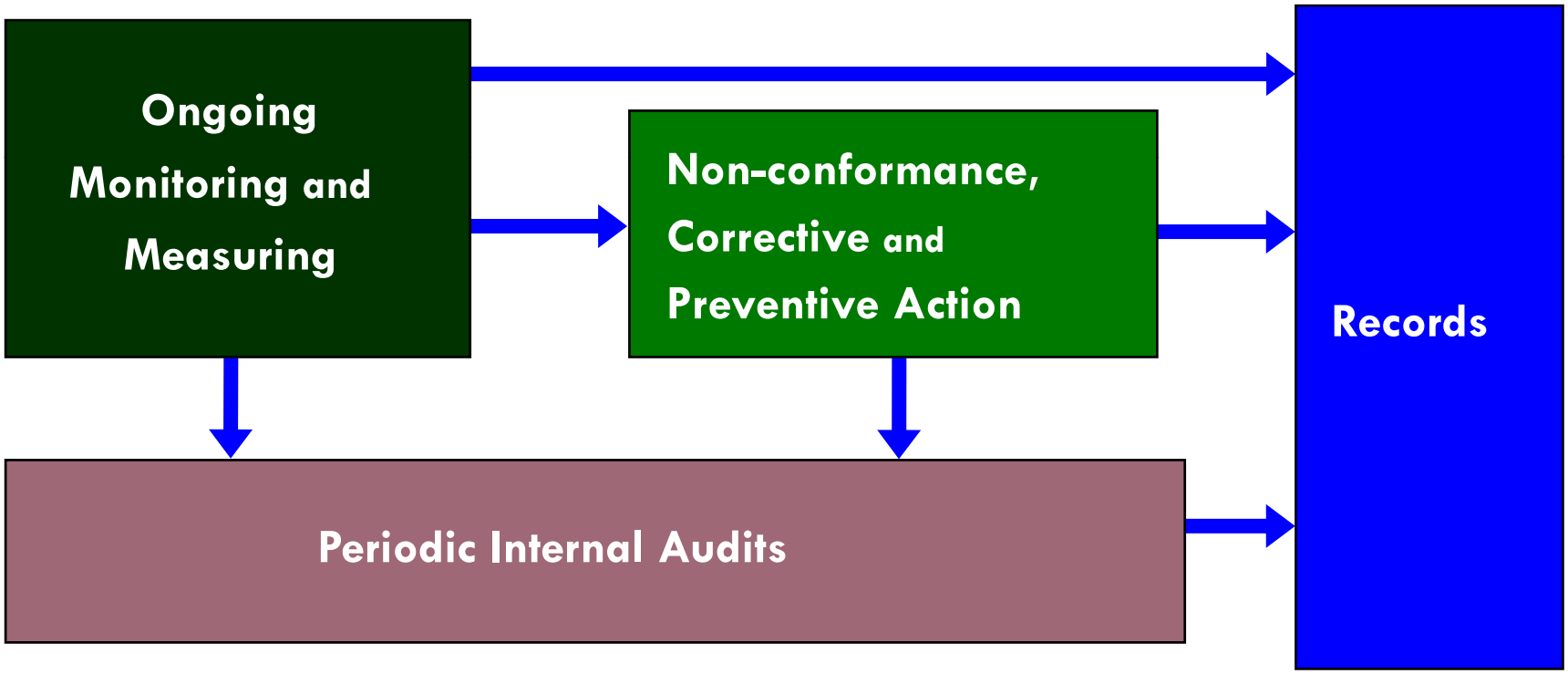
Implementation and Operation

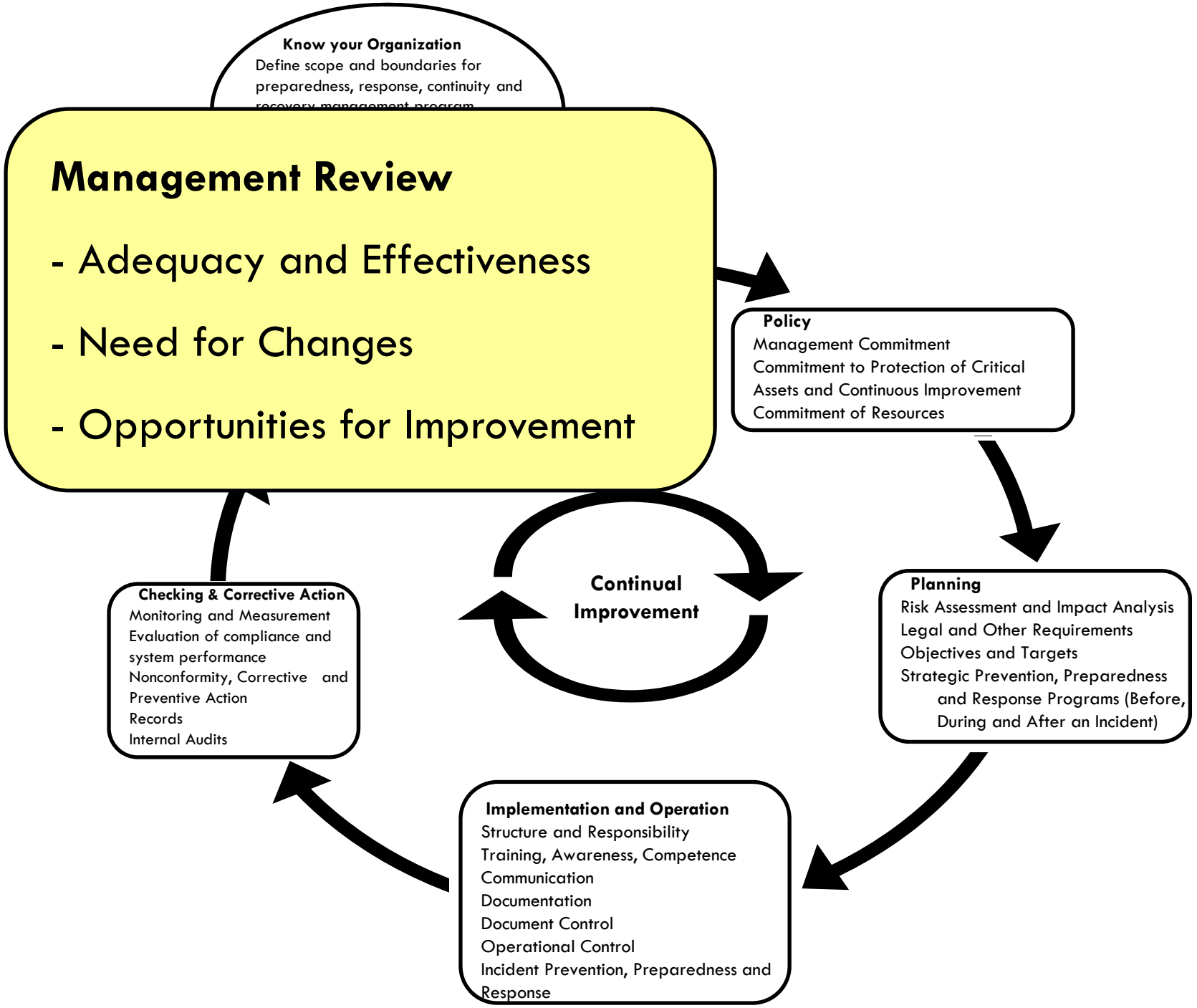
(management support and leadership essential)




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
Management Review
Adequacy and Effectiveness
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)
Operational Control
Incident Prevention, Preparedness and Response

Checking and Corrective Action




Know your Organization
Define scope and boundaries for preparedness, response, continuity and recovery management program
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
Incident Prevention, Preparedness and Response
Checking & Corrective Action
Monitoring and Measurement
Evaluation of compliance and system performance
Nonconformity, Corrective and Preventive Action
Records
Internal Audits
Continual Improvement

Management Review Process

Take account of:

- audit findings
- progress records on objectives changes to facilities
- changes in activities, products or services
- changes in technology
- concerns of interested parties
- other relevant information

To Assess the

- suitability,
- adequacy, and
- effectiveness of ORMS

In order to determine the need for change and improvement to:

- *the ORMS policy*
- *the objectives and targets*
- *other management system elements*

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.

Keep in mind – A 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!

ASIS INTERNATIONAL

ASIS SPC.1-2009

Advancing Security Worldwide

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

ASIS SPC.1-2009

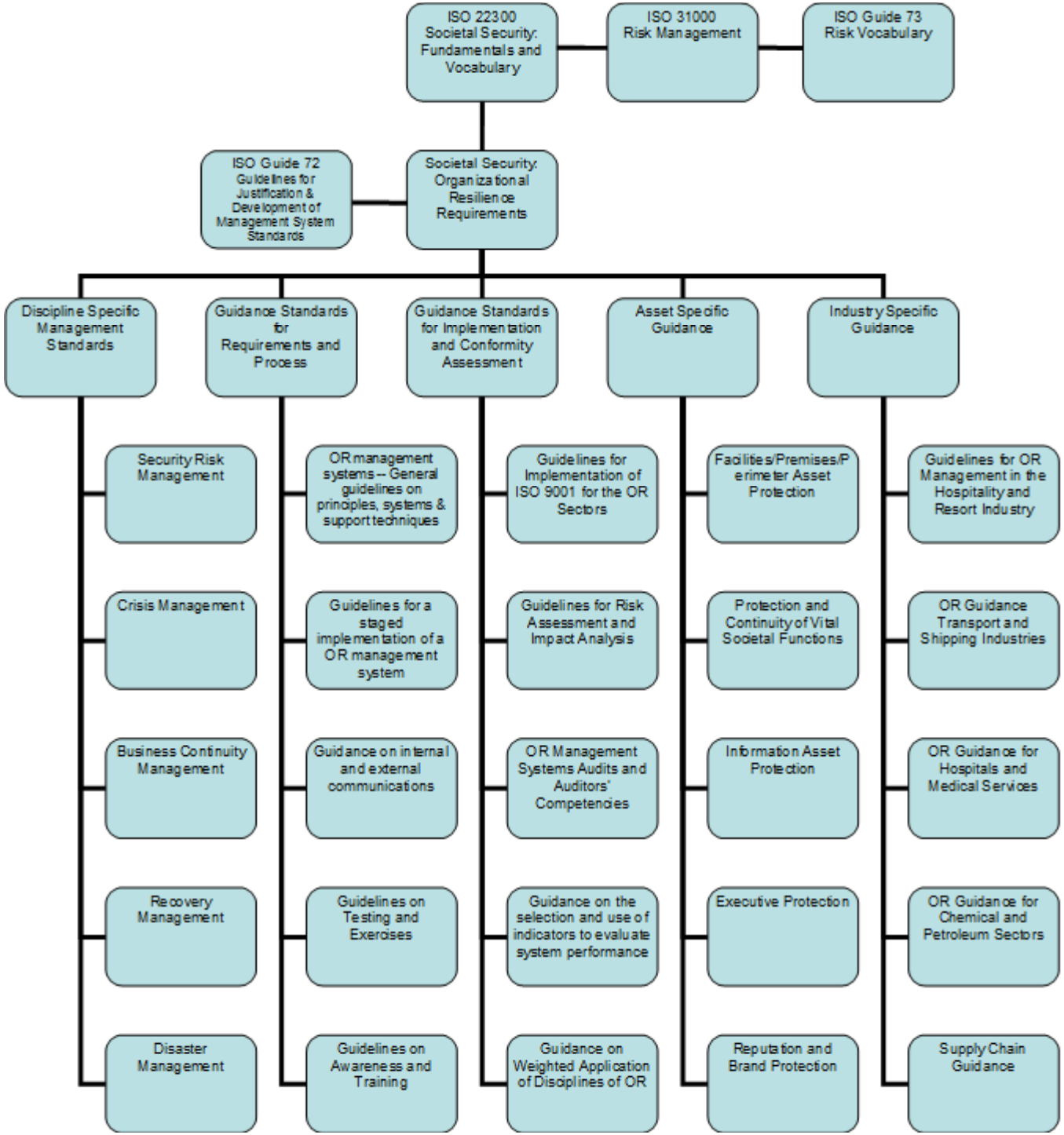
AMERICAN NATIONAL
STANDARD

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

TO DOWNLOAD:

http://www.abdi-secure-ecommerce.com/asis/ps-907-37-1842.aspx

ASIS INTERNATIONAL
Advancing Security Worldwide®


ISO 22300 Societal Security: Fundamentals and Vocabulary
ISO 31000 Risk Management
ISO Guide 73 Risk Vocabulary
ISO Guide 72 Guidelines for Justification & Development of Management System Standards
Societal Security: Organizational Resilience Requirements
Discipline Specific Management Standards
Guidance Standards for Requirements and Process
Guidance Standards for Implementation and Conformity Assessment
Asset Specific Guidance
Industry Specific Guidance
Security Risk Management
Crisis Management
Business Continuity Management
Recovery Management
Disaster Management
OR management systems -- General guidelines on principles, systems & support techniques
Guidelines for a staged implementation of a OR management system
Guidance on internal and external communications
Guidelines on Testing and Exercises
Guidelines on Awareness and Training
Guidelines for Implementation of ISO 9001 for the OR Sectors
Guidelines for Risk Assessment and Impact Analysis
OR Management Systems Audits and Auditors' Competencies
Guidance on the selection and use of indicators to evaluate system performance
Guidance on Weighted Application of Disciplines of OR
Facilities/Premises/Perimeter Asset Protection
Protection and Continuity of Vital Societal Functions
Information Asset Protection
Executive Protection
Reputation and Brand Protection
Guidelines for OR Management in the Hospitality and Resort Industry
OR Guidance Transport and Shipping Industries
OR Guidance for Hospitals and Medical Services
OR Guidance for Chemical and Petroleum Sectors
Supply Chain Guidance

Thank You

Dr. Marc Siegel

Security Management System Consultant

ASIS International

Phone: +1-858-484-9855

Email: siegel@ASIS-Standards.net

siegel@ymail.com