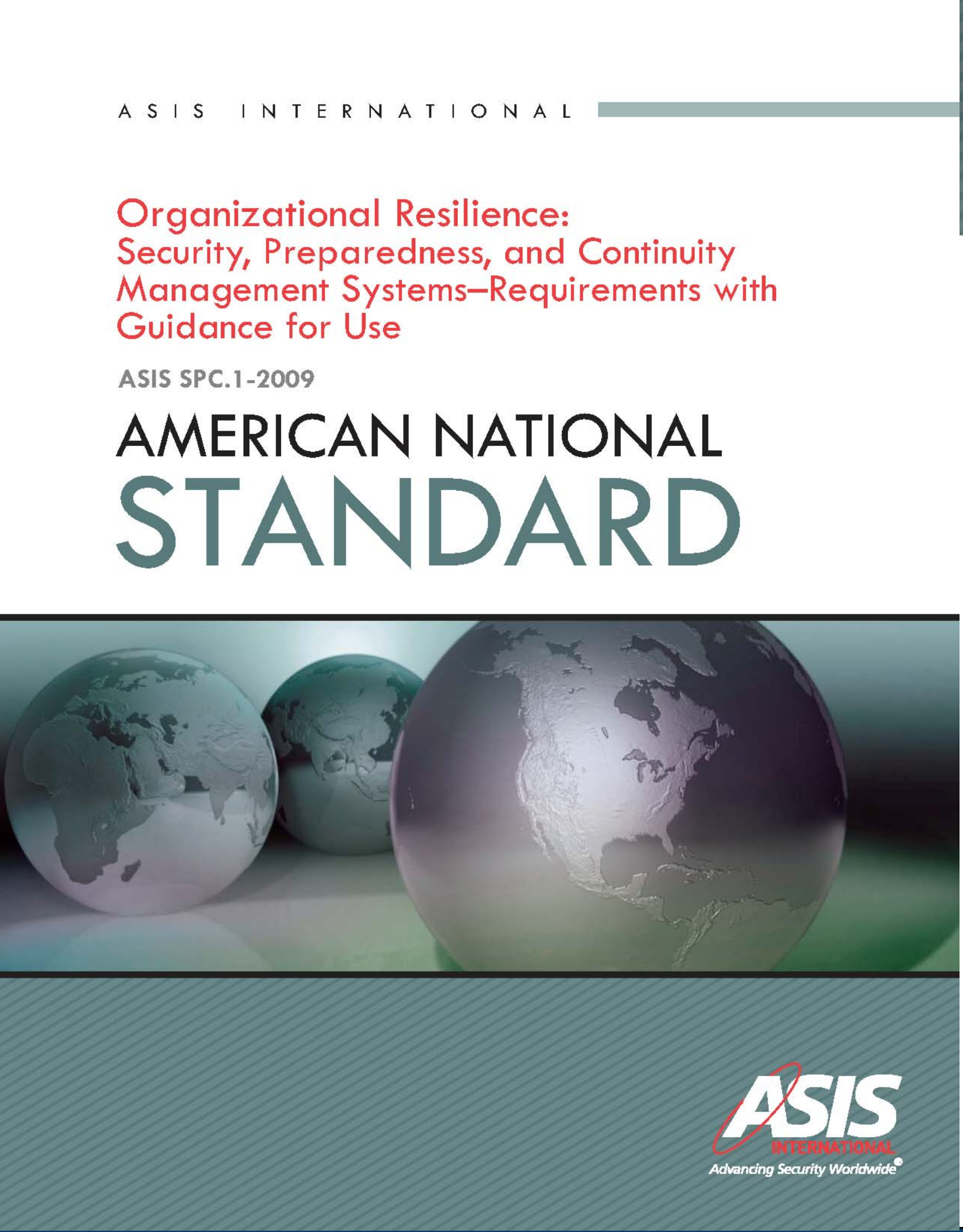
# BEYOND THE SILOS – ORGANIZATIONAL RESILIENCE

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

# Management of Risk

- All organizations face a certain amount of uncertainty and risk.
- In order 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



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®

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

# 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

# What is Resilience?

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

Helps avoid segregating or

# Organizational Resilience

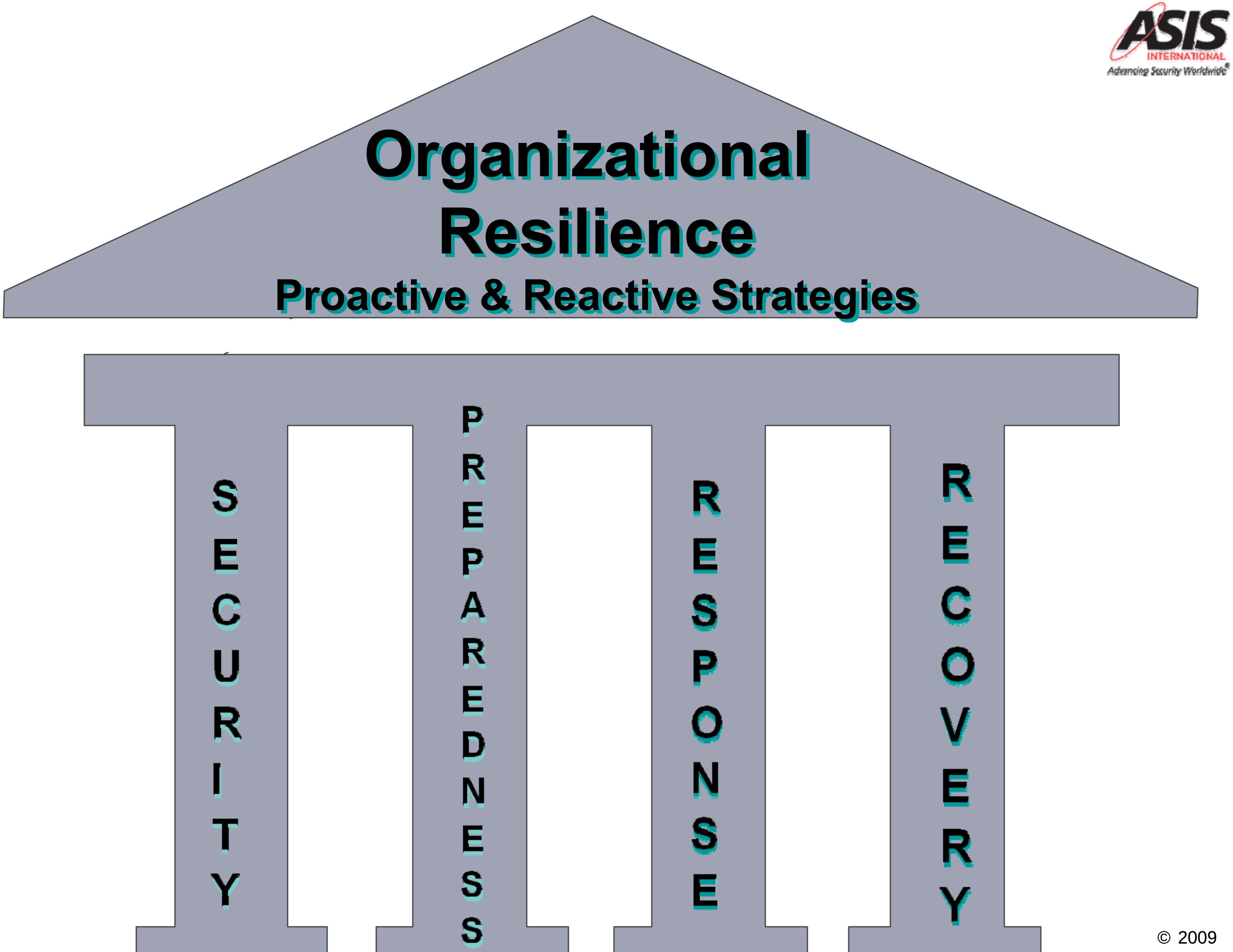
- **Resilience** is the ability of an organization to prevent, resist being affected by an event, or the ability to return to an acceptable level of performance in an acceptable period of time after being affected by an event.

- **Resilience** is the capability of a system to maintain its

# 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

SECURITY

PREPAREDNESS

RESPONSE

RECOVERY

# What Do We Have in the Toolbox?

- Standards can address your organizational resilience needs.

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

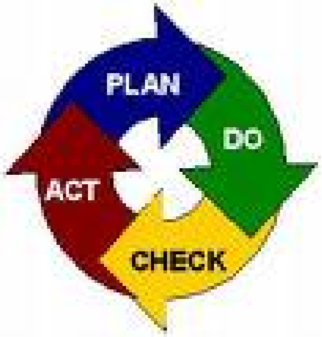
# What are Standards?

- Consensus-based specifications which define materials, methods, processes, services or practices.
- Provide a basis for consistent and reliable performance.
- **S s ations!**

# 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.

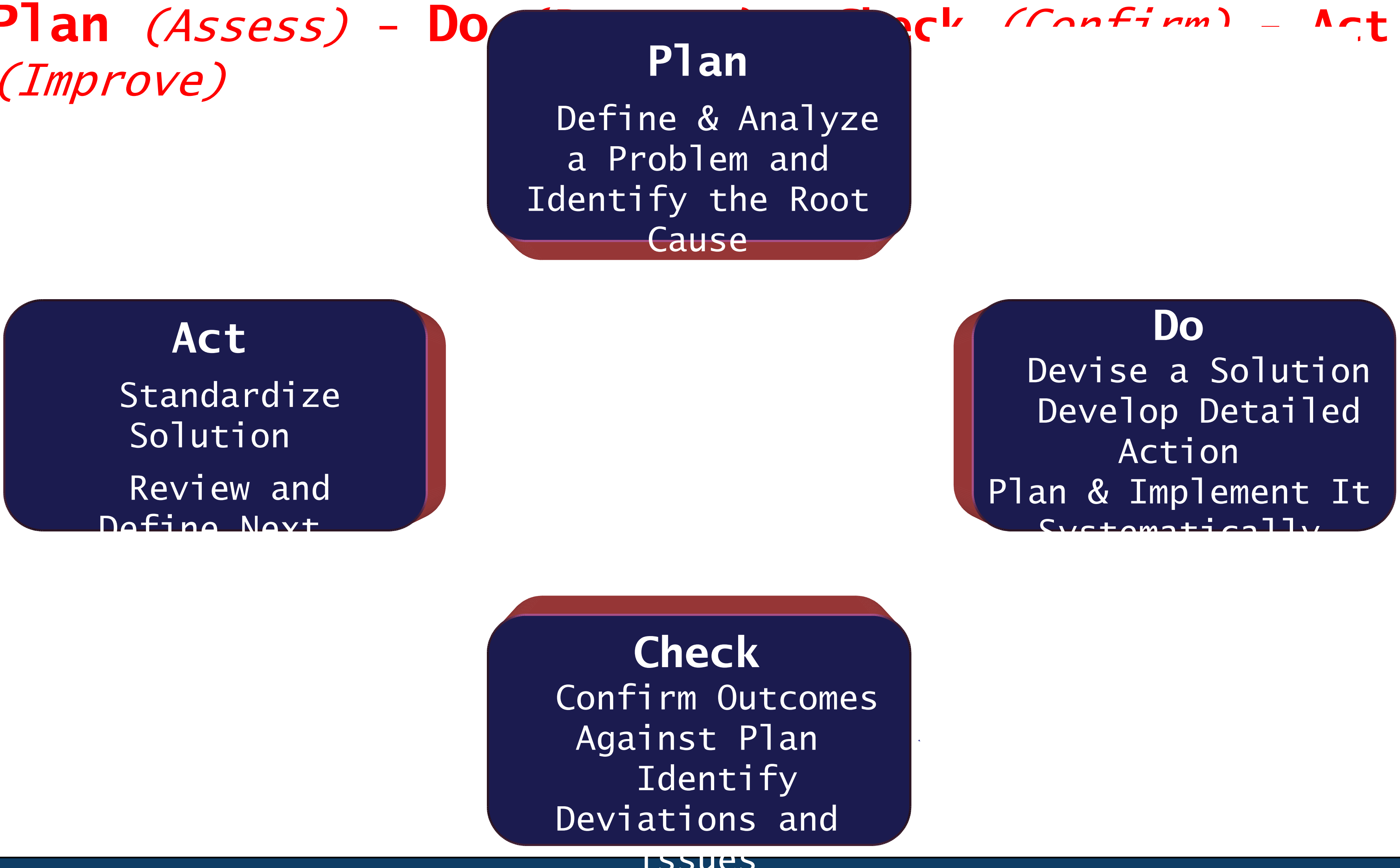
- **Management system standards** provide model to follow in setting up and operating a management system.



# PDCA or APCI Model

*Approach to structured problem solving focused on continual*

**Plan** *(Assess)* - **Do** [illegible] - **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

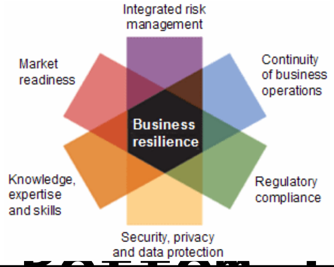
**Act**

Standardize Solution

Review and Define Next

# 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 es
- reputation and brand
- r continual improvement
- Bottom Line: Proactively improve

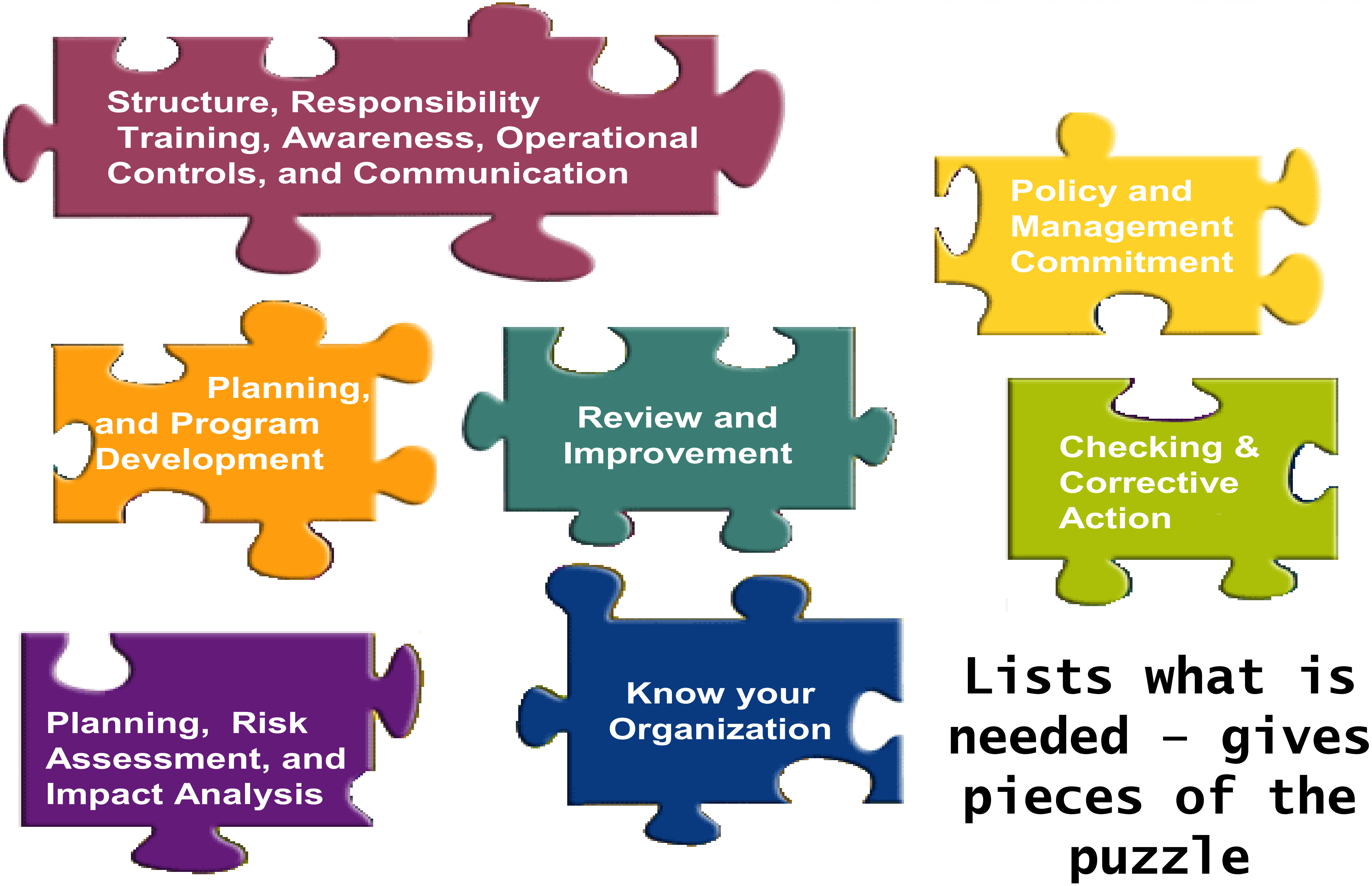

Integrated risk management
Continuity of business operations
Regulatory compliance
Security, privacy and data protection
Knowledge, expertise and skills
Market readiness
Business resilience

# Why Management Systems Work

- Needs focused
- Goals driven
- People oriented
  - Leadership driven
  - Involves people at all
  - 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

Policy and Management Commitment

Planning, and Program Development

Review and Improvement

Checking & Corrective Action

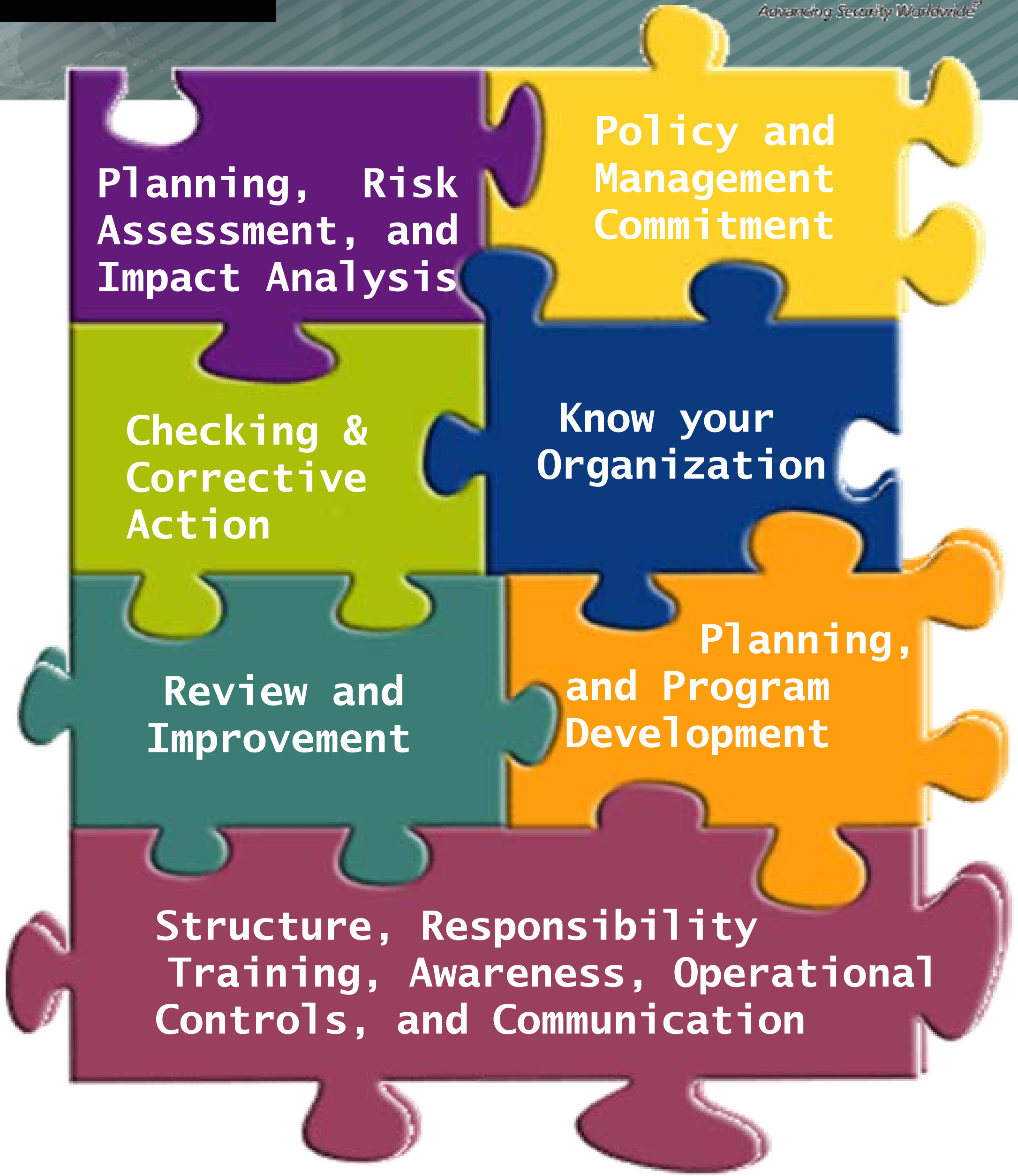
Planning, Risk Assessment, and Impact Analysis

Know your Organization

**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



Planning, Risk Assessment, and Impact Analysis

Policy and Management Commitment

Checking & Corrective Action

Know your Organization

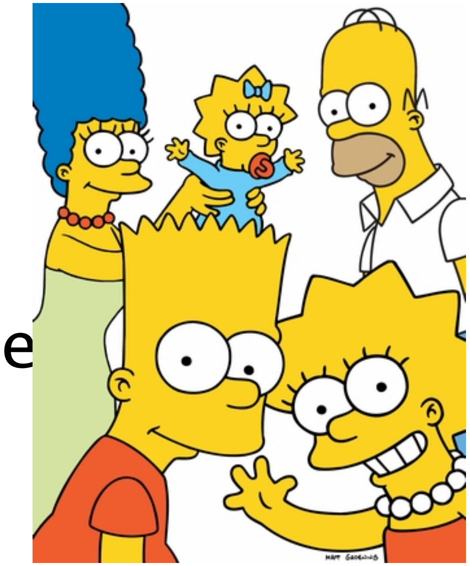
Review and Improvement

Planning, and Program Development

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

# Security/Continuity Management Standards

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



**All ISO Families have evolved from the original ISO 9000 Family**

# Meet the Family

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

INTERNATIONAL STANDARD

ISO 28000

First edition
2007-09-15

**Specification for security management systems for the supply chain**

*Spécifications pour les systèmes de management de la sûreté pour la chaîne d'approvisionnement*

ISO

Reference number
ISO 28000:2007(E)

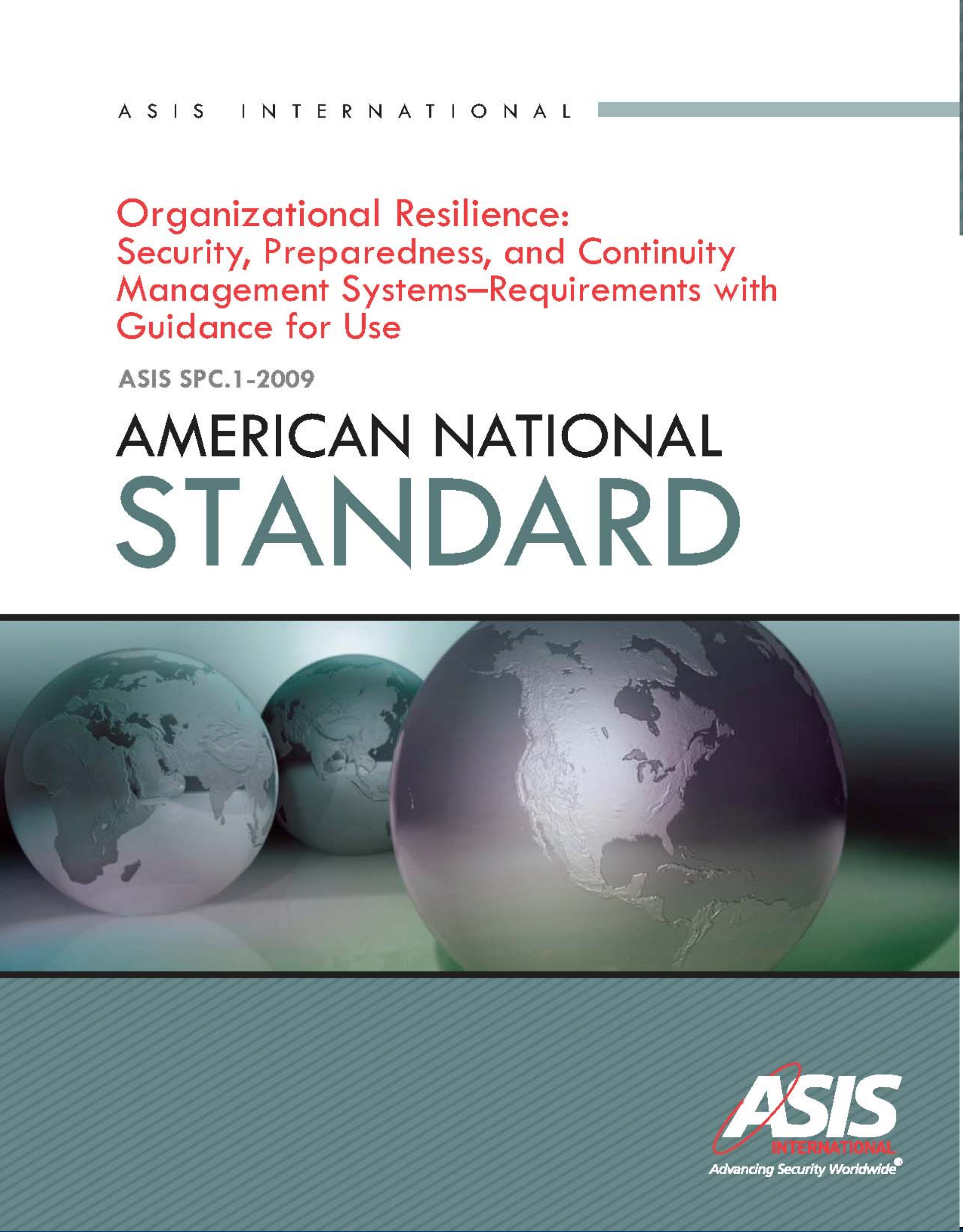
© ISO 2007

# What Does the Future Hold?

ISO 28002, *Resilience in the Supply Chain*

ISO 28005, *Ships and marine technology – Computer applications –*

# ASIS SPC.1-2009



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®

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

# 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

# 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.

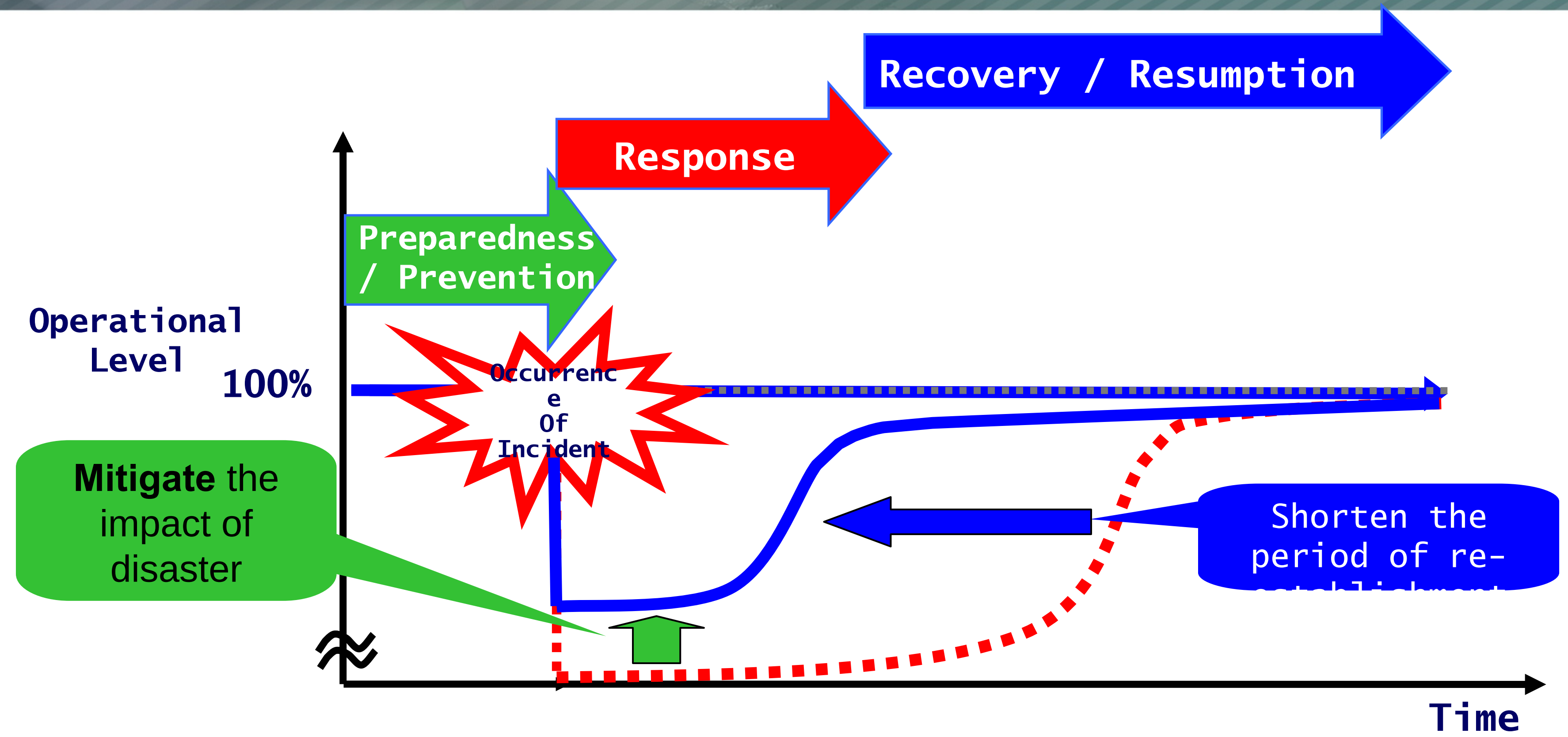
# All Hazards Risk Assessment

*Focus on Protection of Critical Assets and Functions*

*Incident Management Regardless of Event Trigger*

Management of All Hazards Risks

# ORMS – Holistic Management Process



Recovery / Resumption

Response

Preparedness / Prevention

Operational Level

100%

Occurrence Of Incident

**Mitigate** the impact of disaster

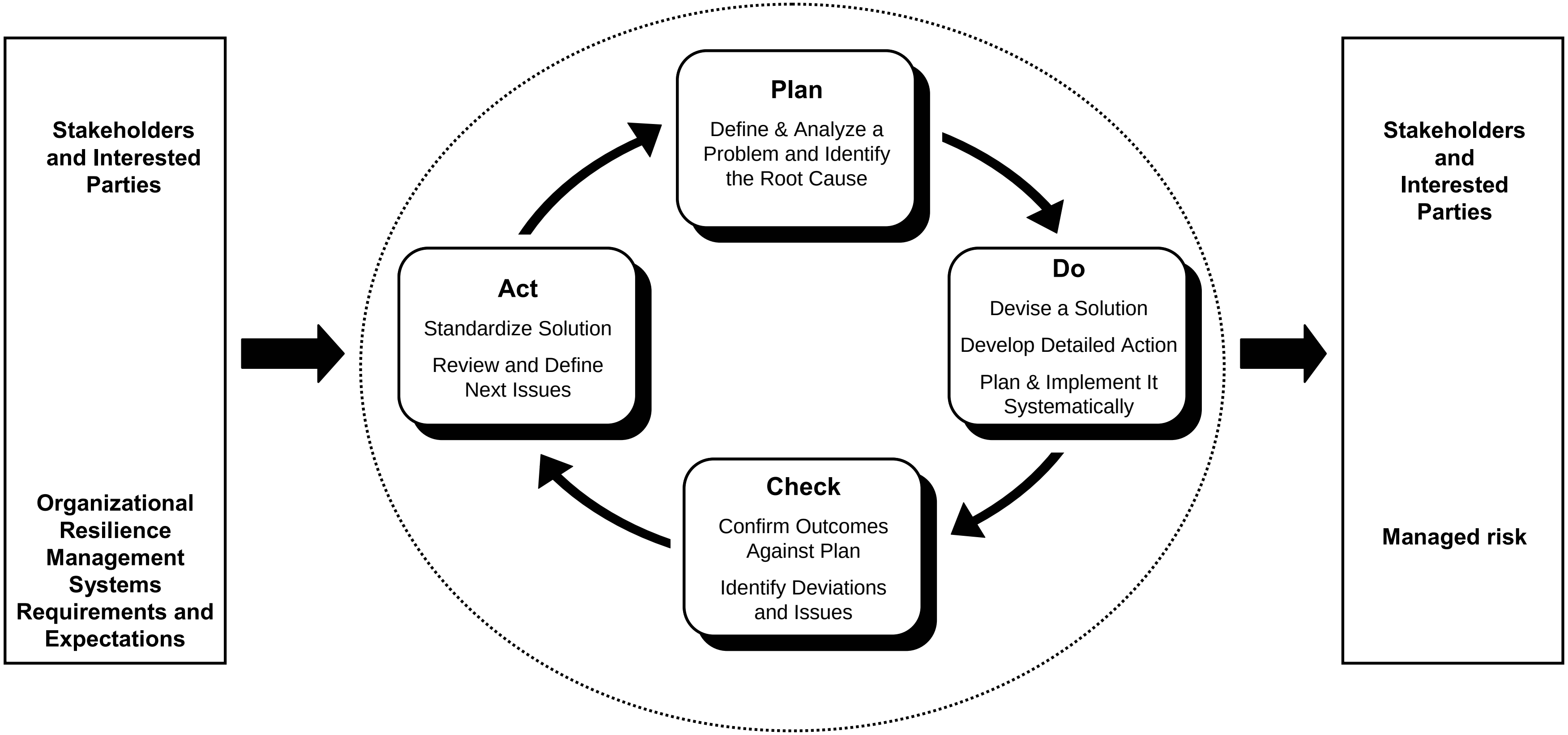
Shorten the period of re-establishment

Time

┅┅┅┅┅ Before Introduction/Implementation of ORMS

━━━━━ After Introduction/Implementation of ORMS

# Builds on the PDCA Model



Stakeholders and Interested Parties

Organizational Resilience Management Systems Requirements and Expectations

**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

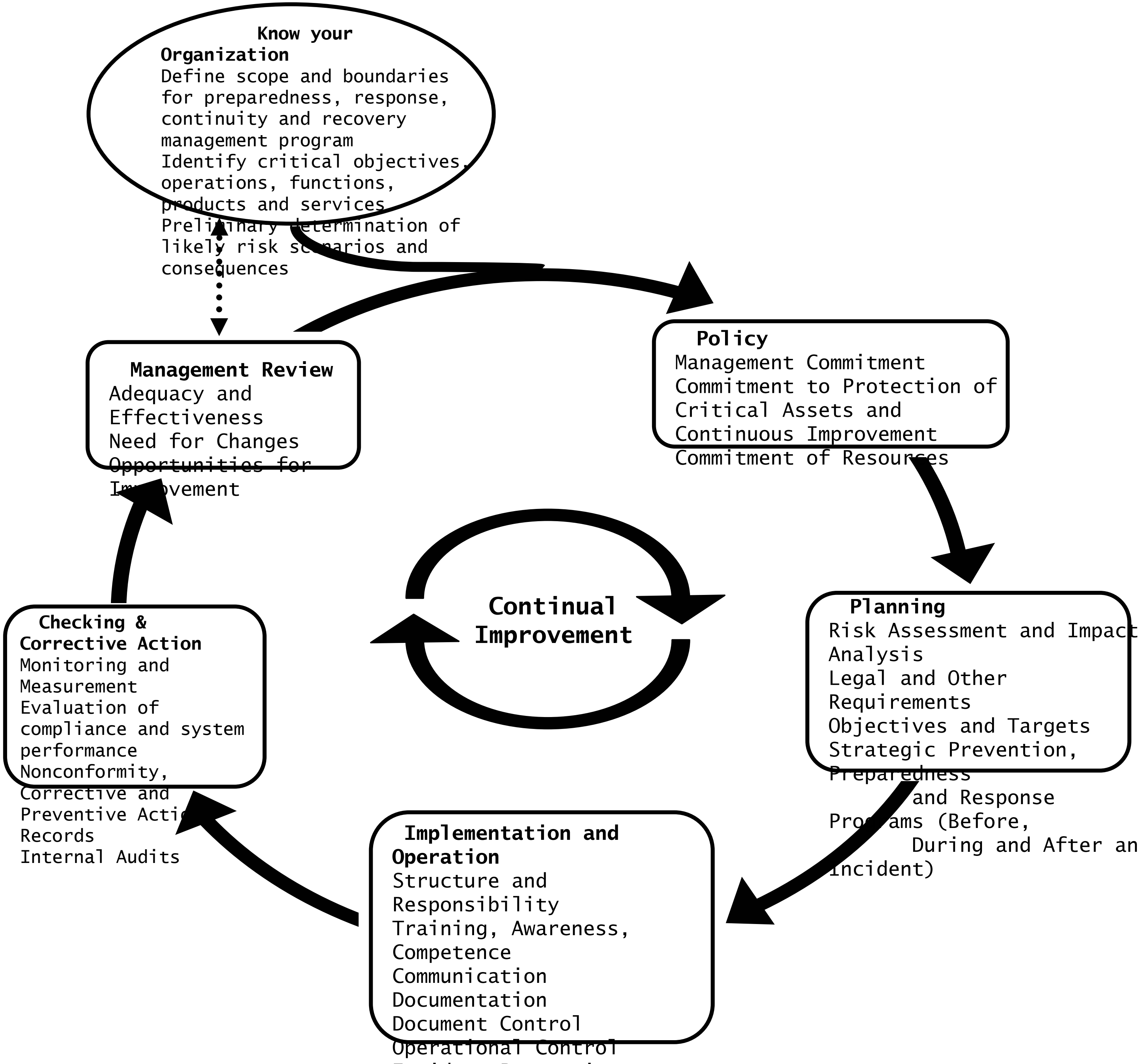
**Act**

Standardize Solution

Review and Define Next Issues

Stakeholders and Interested Parties

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

**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

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

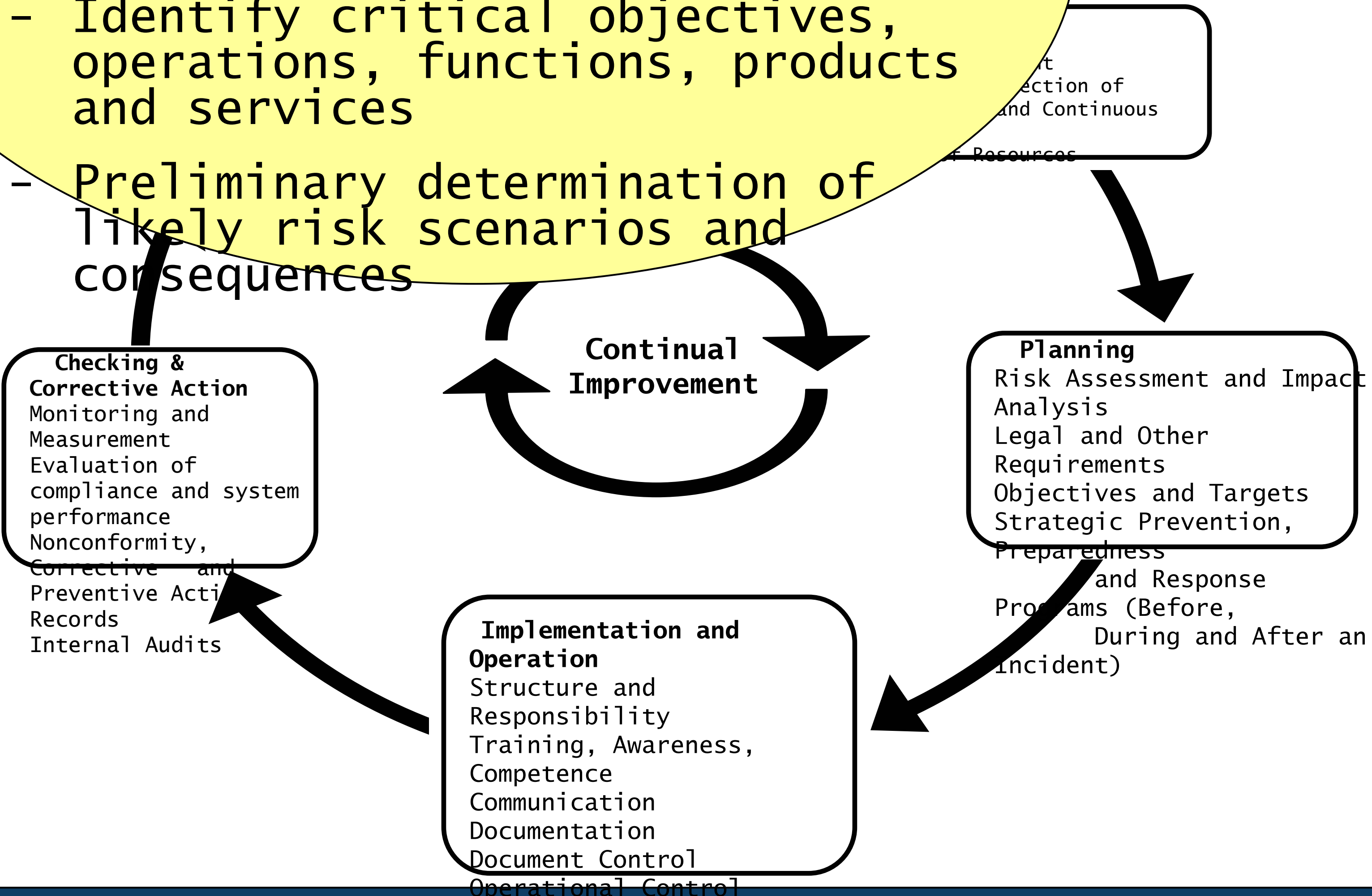
**Management Review**
Adequacy and Effectiveness
Need for Changes
Opportunities for Improvement

**Continual Improvement**

© 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



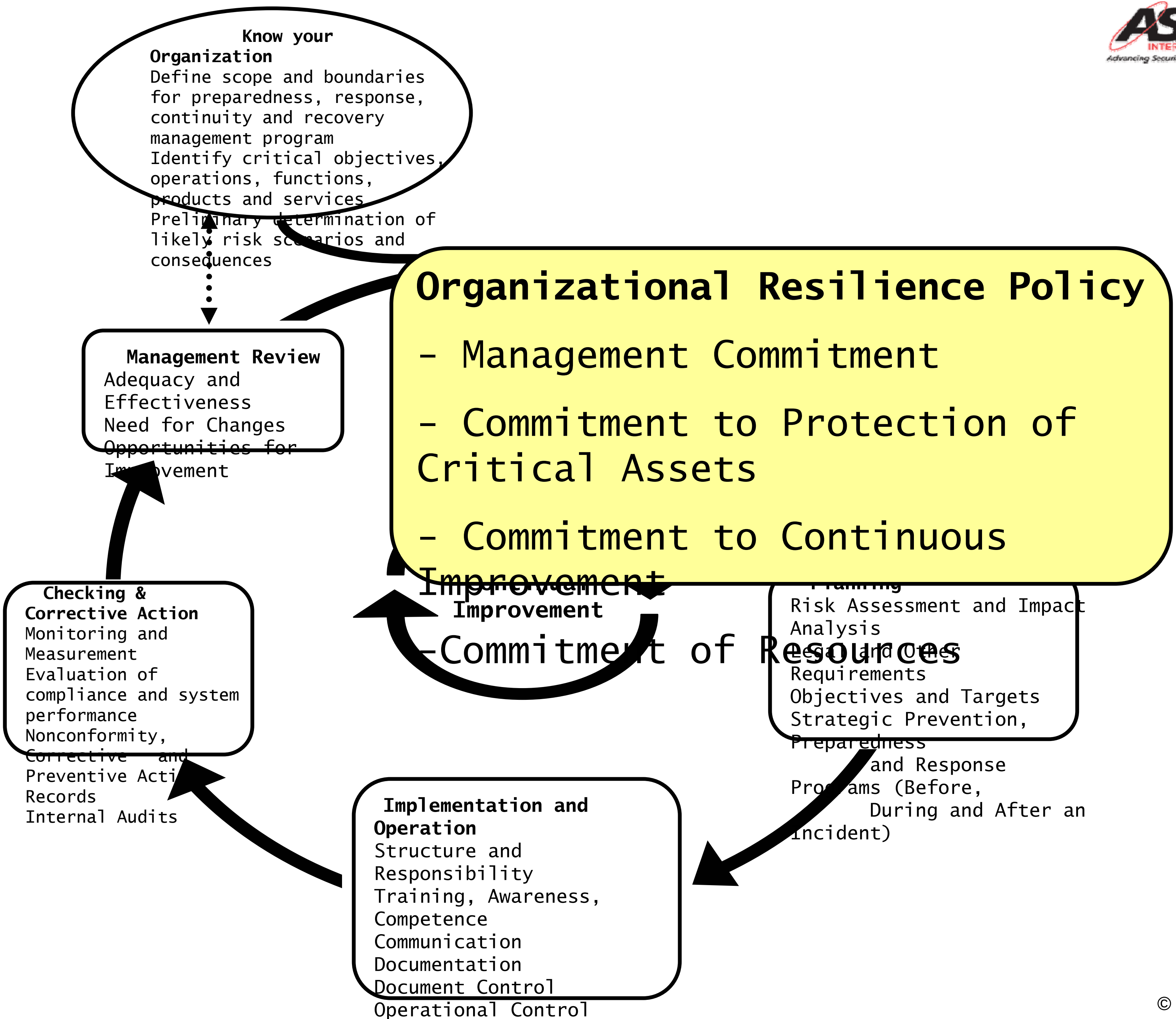
t
ection of
and Continuous
f Resources

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 Acti
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

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

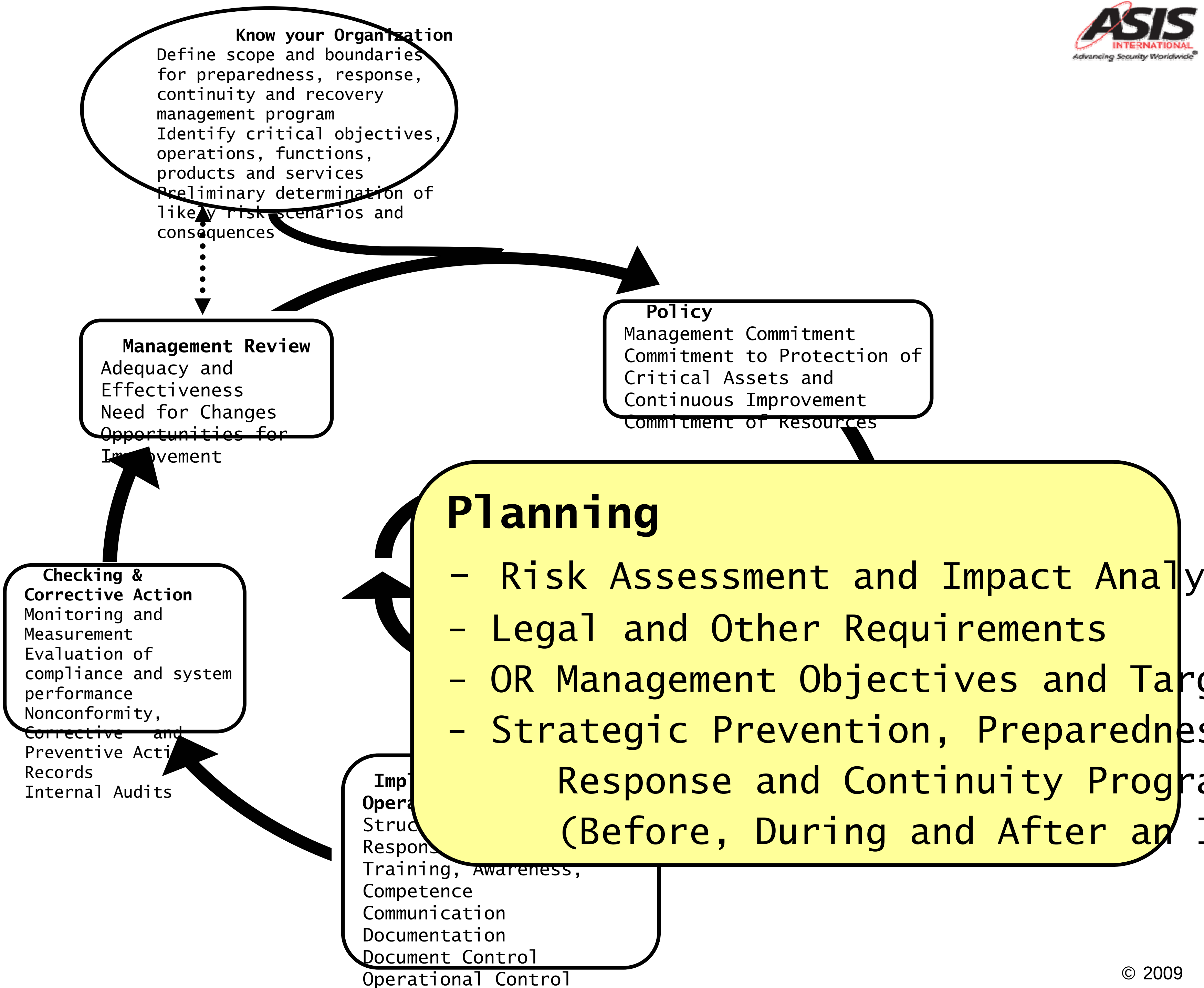
**Management Review**
Adequacy and Effectiveness
Need for Changes
Opportunities for Improvement

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

**Improvement**

**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



**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 Analy
- Legal and Other Requirements
- OR Management Objectives and Targ
- Strategic Prevention, Preparednes
  Response and Continuity Progra
  (Before, During and After an I

**Imp**
**Opera**

Struc

Respons

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 Acti

Records

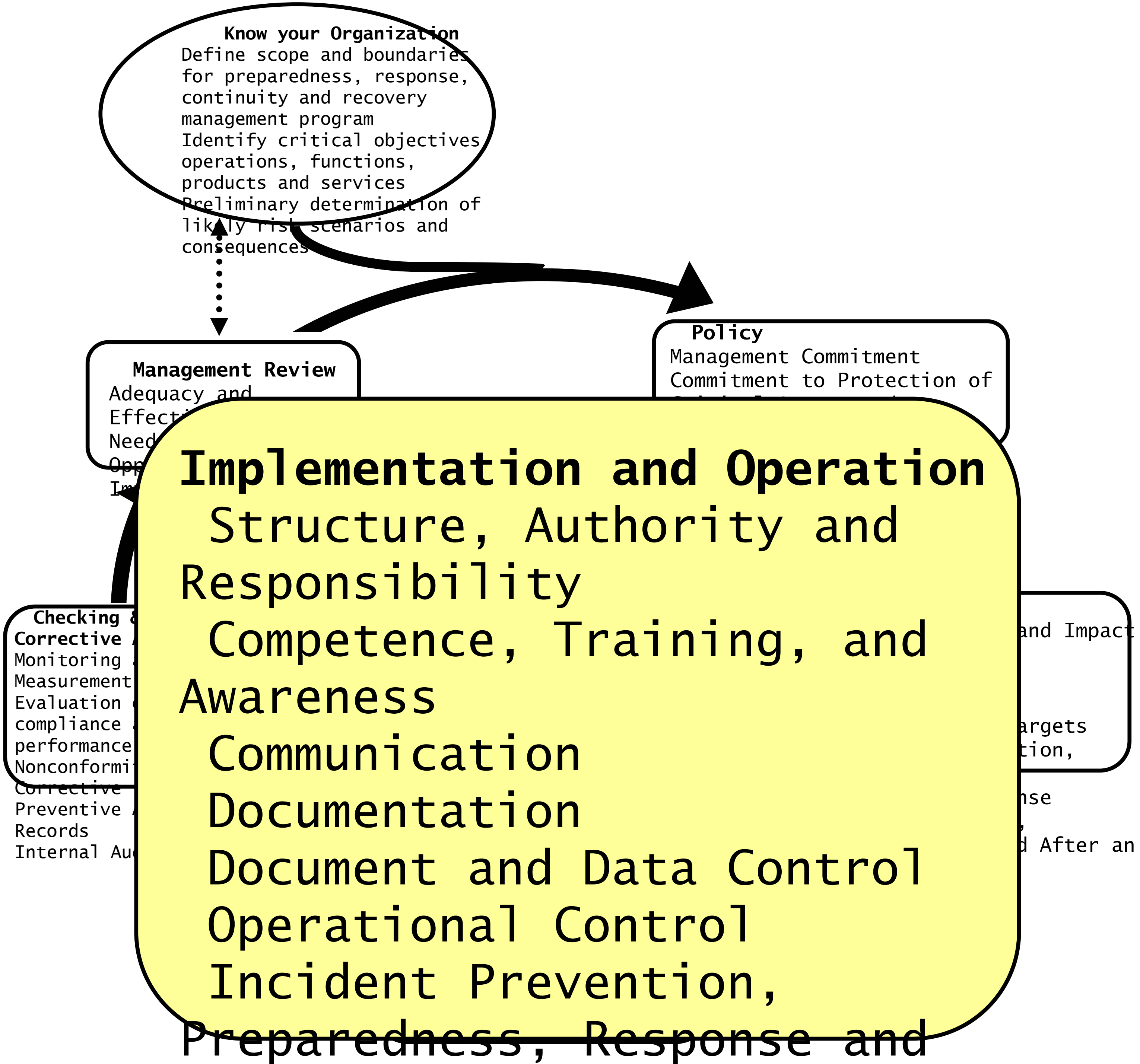
Internal Audits

**Management Review**

Adequacy and Effectiveness

Need for Changes

Opportunities for 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

**Policy**
Management Commitment
Commitment to Protection of

**Management Review**
Adequacy and
Effect
Need
Opp
Im

**Checking &**
**Corrective A**
Monitoring a
Measurement
Evaluation o
compliance a
performance
Nonconformi
Corrective
Preventive A
Records
Internal Au

and Impact

argets
tion,

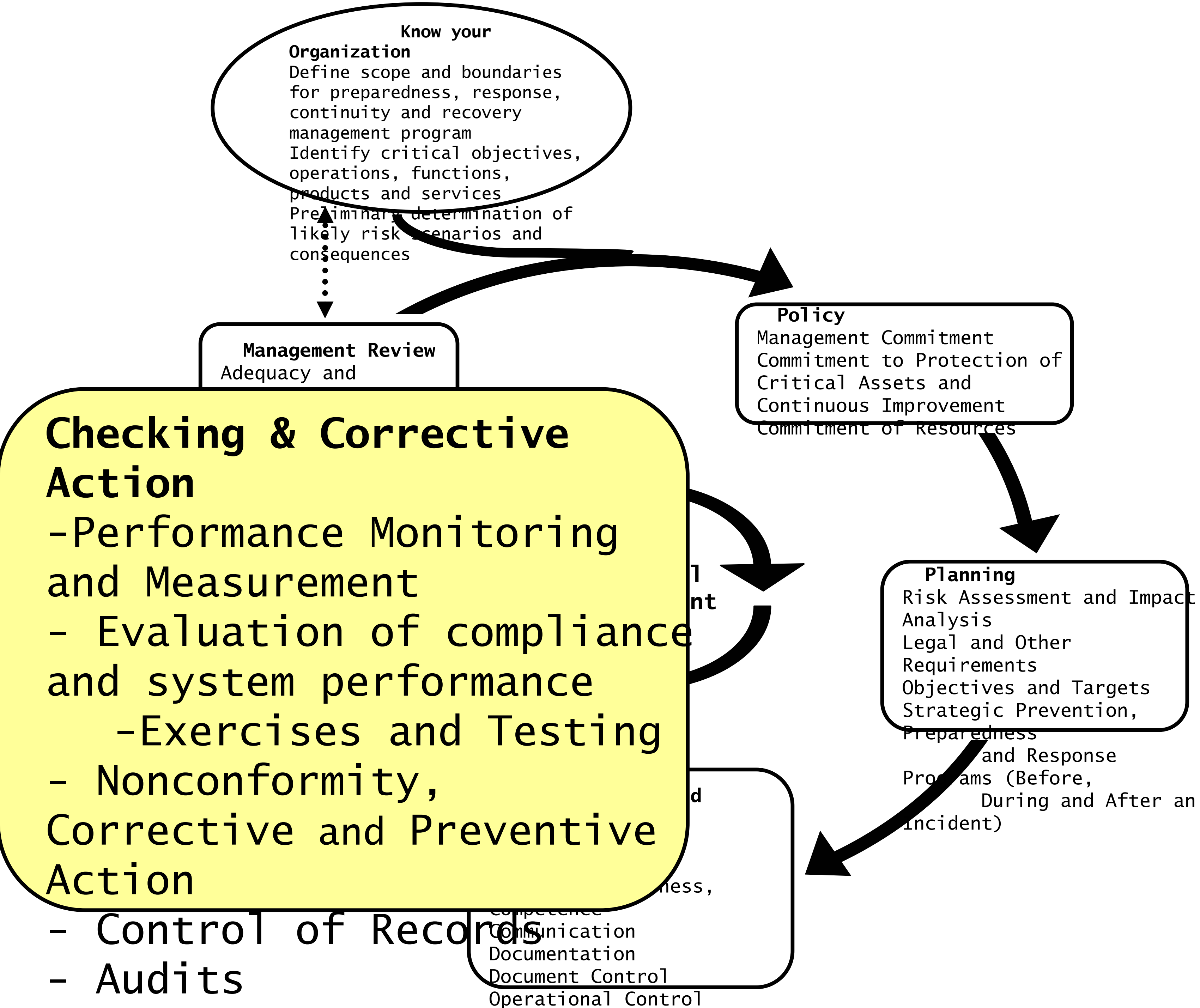
nse

d After an

## Implementation and Operation

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

© 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

**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)

**l**
**nt**

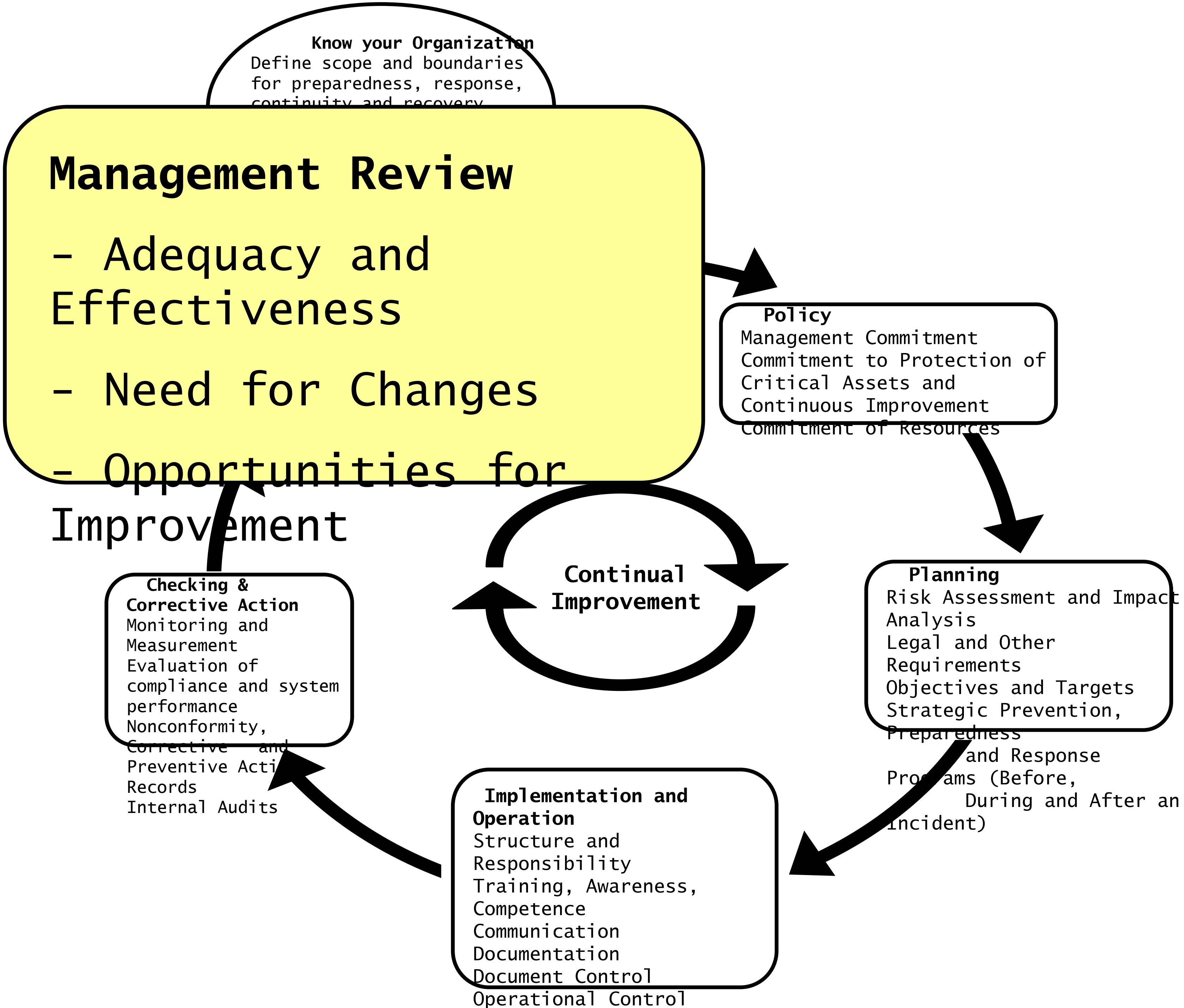
**d**
ness,
Competence
Communication
Documentation
Document Control
Operational Control

## 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

**Management Review**
Adequacy and

© 2009



**Management Review**

- Adequacy and Effectiveness

- Need for Changes

- Opportunities for Improvement

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

**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

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

**Continual Improvement**

# Keep in mind – An ORMS

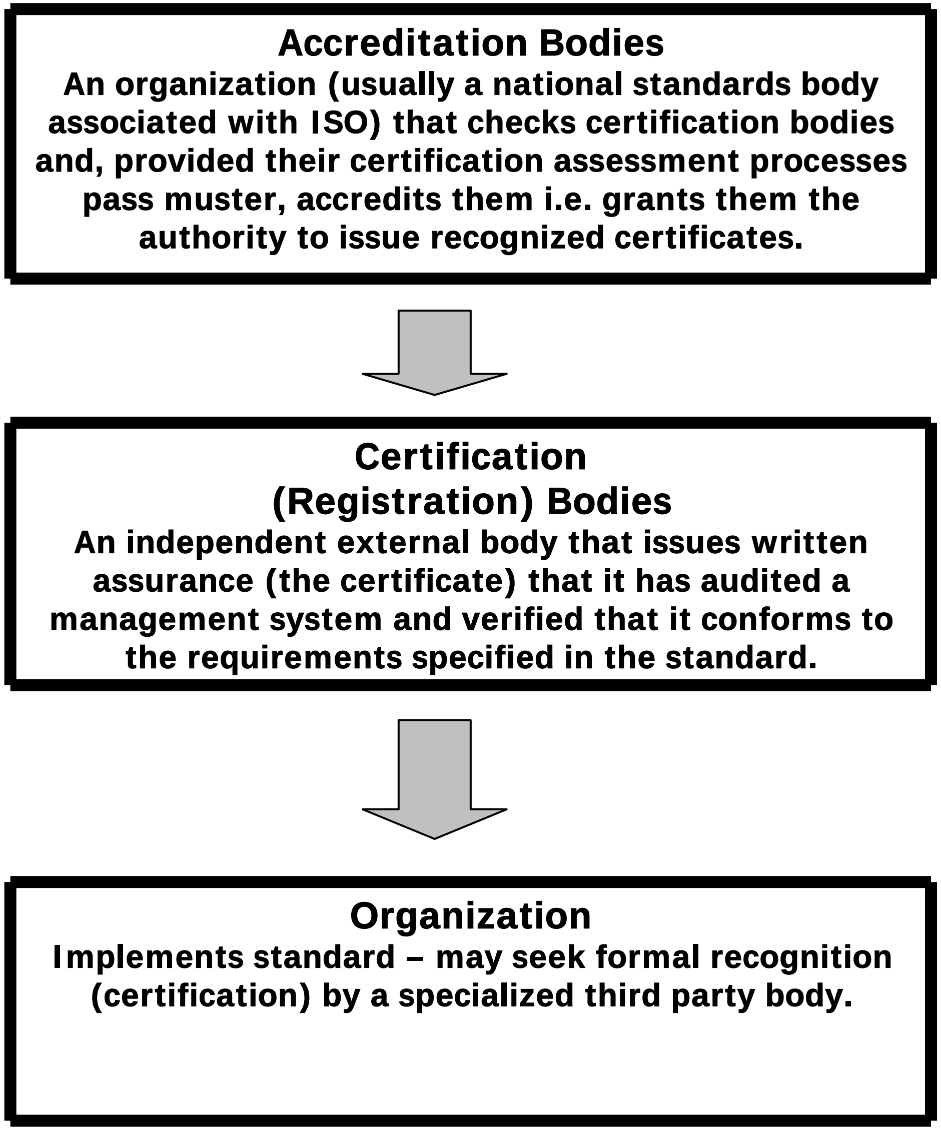
- Is a **<u>dynamic management</u>** system -
  - **THAT'S WHAT MAKES IT WORK!!**
  - Organization must **<u>use</u>** the tools, not just **<u>have</u>** them.
- Is more than compliance - includes safety, energy, water etc. and non-regulated impacts
- **<u>Supports mission!</u>**
- Takes time - it is 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

## Relevant Standards



**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.

**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.

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

**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

**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

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

ASIS INTERNATIONAL
Advancing Security Worldwide®

# Thank You

Dr. Marc Siegel

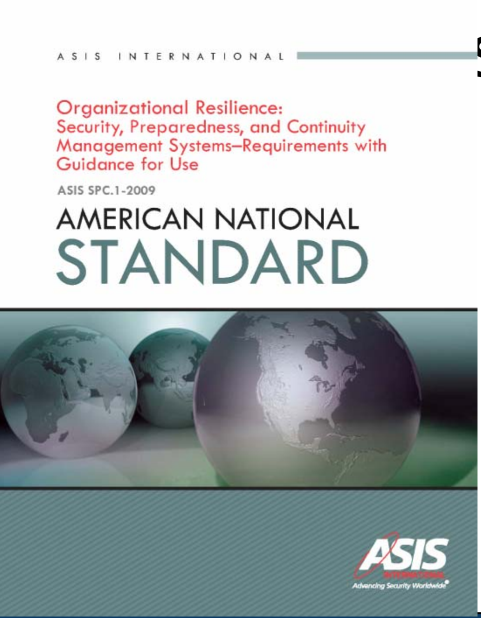
Security Management System Consultant

ASIS International

Phone: +1-858-484-9855

siegel@ASIS-Standards.net

siegel@ymail.co



ASIS INTERNATIONAL

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

ASIS SPC.1-2009

AMERICAN NATIONAL
STANDARD