INTEGRATING CYBER SECURITY WITH OTHER SURETIES IN A MANAGEMENT SYSTEM

by Paul Baybutt, Primatech Inc.

Presented at the ISA Expo Technical Conference on Manufacturing & Control Systems Security, Chicago, October 26, 2005

paulb@primatech.com
www.primatech.com

OVERVIEW

- Sureties
- Management systems
- Specifications
- Recommended integrated system
- Issues faced

“There are many ways of going forward,
but only one way of standing still.”
Franklin D. Roosevelt

SURETIES

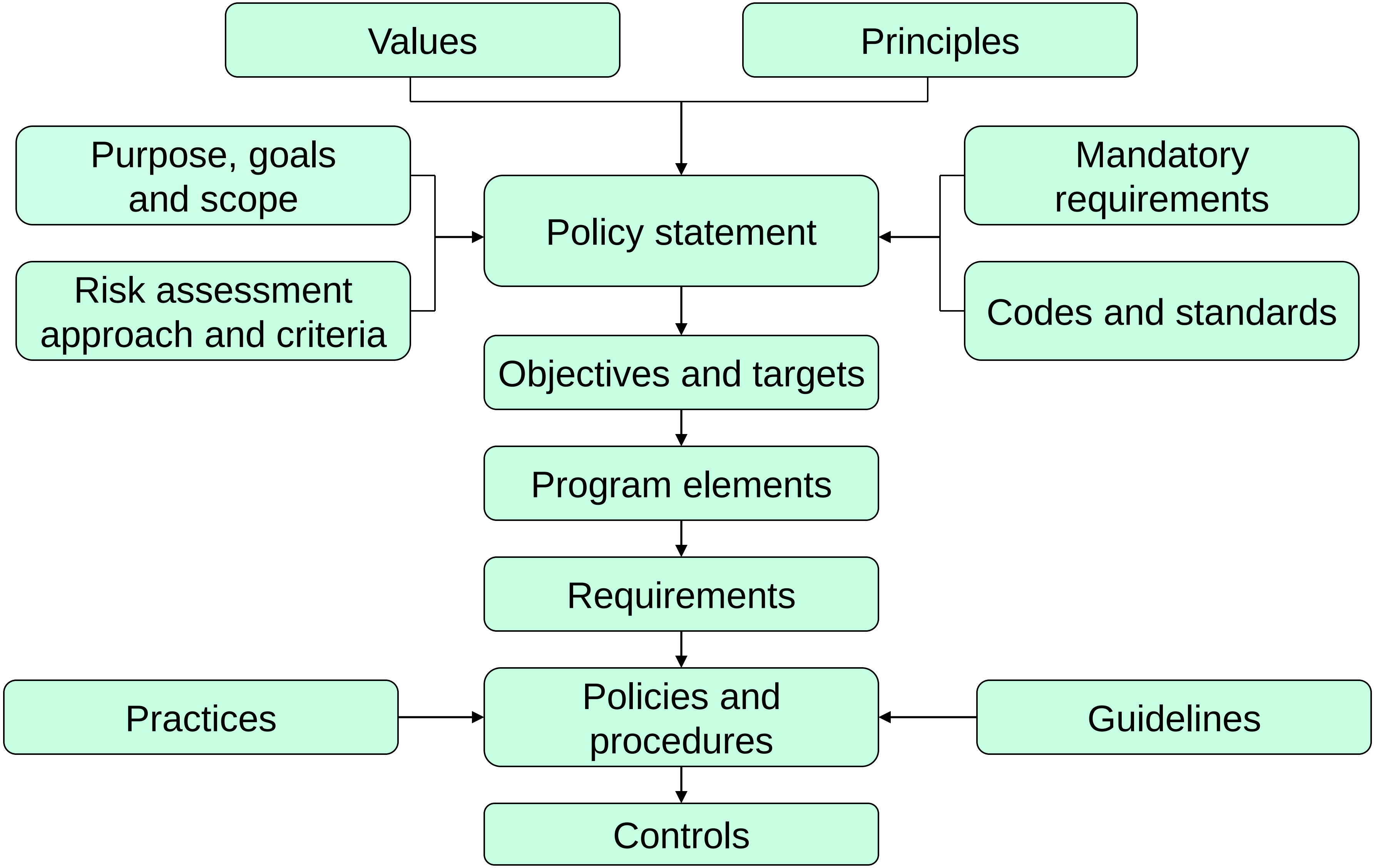
- Manufacturing operations produce products while ensuring a variety of constraints are met, e.g.
  - Costs and profits
  - Quality
  - Safety
  - Environmental protection
  - Security
  - Etc.

- These sureties must be managed to ensure acceptable performance

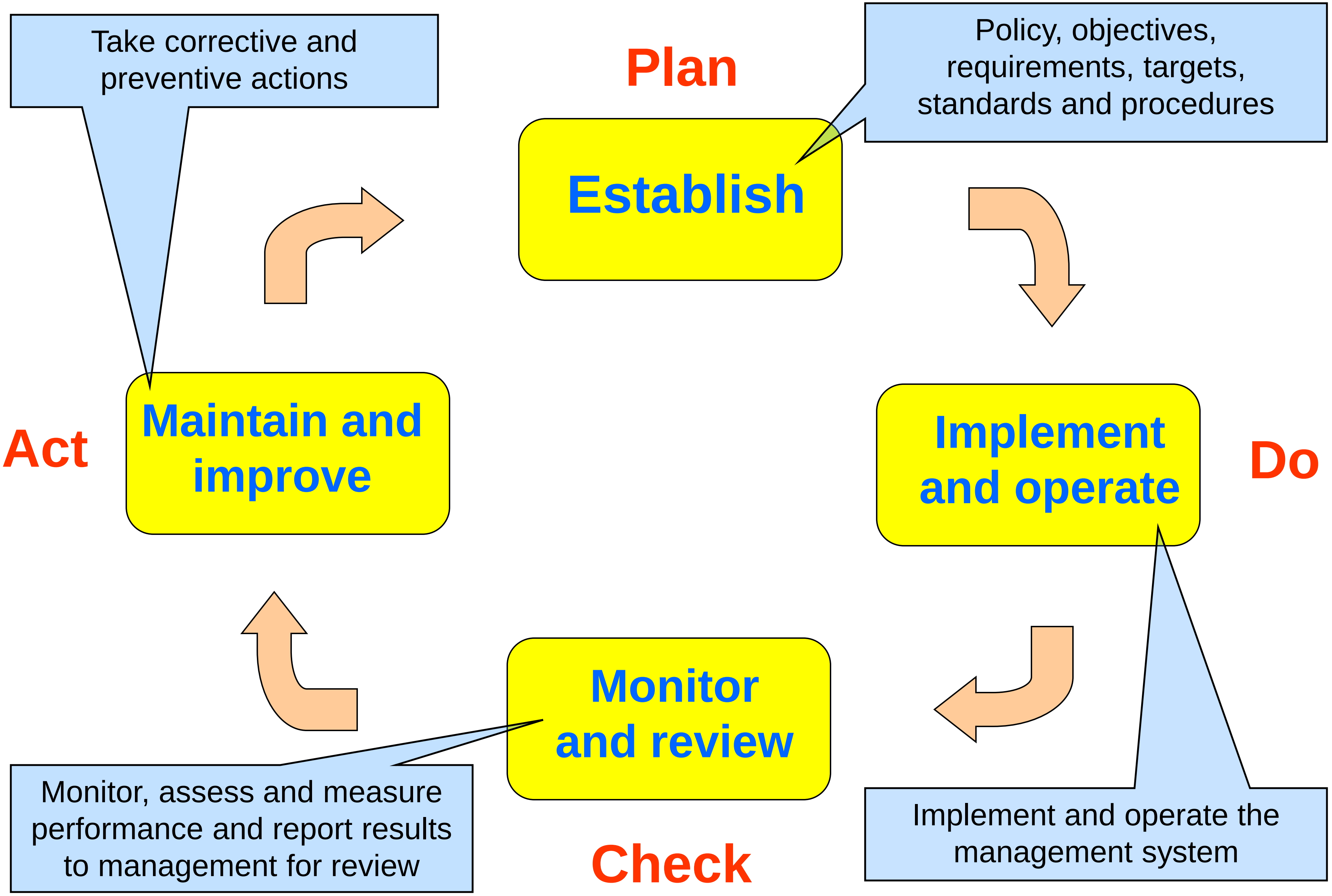
MANAGEMENT SYSTEMS

- Refers to what organizations do to manage their *processes*
  - Activities undertaken to realize a product or a service
- Structured approaches for addressing bottom line performance for sureties
- Tool for use by management

HIERARCHICAL RELATIONSHIP OF ENTITIES FOR A MANAGEMENT SYSTEM



THE PDCA MANAGEMENT SYSTEM MODEL



Plan

Establish

Policy, objectives, requirements, targets, standards and procedures

Do

Implement and operate

Implement and operate the management system

Check

Monitor and review

Monitor, assess and measure performance and report results to management for review

Act

Maintain and improve

Take corrective and preventive actions

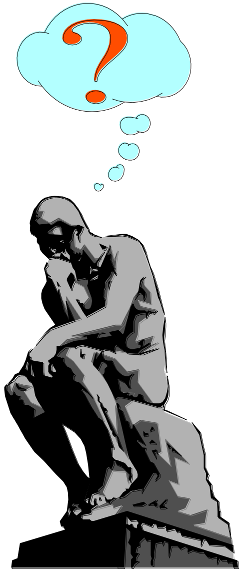
MANAGEMENT SYSTEM SPECIFICATIONS

SURETY	SPECIFICATION	EDITIONS
Quality	ISO 9000	1987, 1994, 2000
Process safety	CFR 1910.119	1992
Environmental protection	ISO 14001	1996
Occupational health and safety	BSI OHSAS 18001	1999
Information security	BS 7799:2	2002
Pollution prevention, distribution, product stewardship, process safety, employee health and safety, security, and community awareness and emergency response	ACC Responsible Care® Management System (RCMS)	2003
Cyber security - chemical sector	CIDX	2004
Food safety	ISO 22000	2005

Note: ISO 14001 was in use by about 37,000 organizations in 112 countries in 2001.

DEVELOPING AND IMPLEMENTING MANAGEMENT SYSTEMS

- Effort involved appears substantial and possibly prohibitive
  - Particularly as more sureties are addressed



APPROACHES FOR MANAGING MULTIPLE SURETIES

SEPARATE	INTEGRATED	UNIFIED
Management of each surety is allocated to different groups	Common elements have the same design	Single system for all sureties
Wastes resources - duplication of effort and additional costs	Generic and specific controls are separated	More effort to design
Systems may conflict	Conflicts are managed	Compromises needed
Sureties optimized individually not collectively	Sureties are optimized collectively	Most efficient and transparent

RECOMMENDED APPROACH

- Leverage off existing management systems
  - Many organizations already have one or more in place
  - Adapt policies and procedures already in place
  - Benefit from experiences in designing and implementing management systems for other sureties

RECOMMENDED APPROACH (CONTD.)

- Combine and rationalize the elements of existing management systems
  - Take advantage of their commonality across different sureties
- Conform to existing management system specifications by mapping them into an integrated system
- Employ ISO philosophies
- Provide the means to incorporate other sureties in the future

INTEGRATED MANAGEMENT SYSTEM

Establish the MS

1.0 Leadership
2.0 Policy
3.0 Specification
4.0 Resource allocation
5.0 Review, documentation and approval
6.0 Implementation plan for the MS

Implement the MS

7.0 Communicate the MS to personnel
8.0 Gap analysis
9.0 Risk assessment
10.0 Risk controls
11.0 Management approval
12.0 Establish individual policies, procedures and guidelines for controls
13.0 Implement controls
14.0 Endorse the MS

Operate the MS

Maintain the MS

Improve the MS

INTEGRATED MANAGEMENT SYSTEM – 1.0 LEADERSHIP

1.1 Design and implementation team

1.2 Source of advice

1.3 Business case

1.4 Management forum

1.5 Management commitment

1.6 Ownership

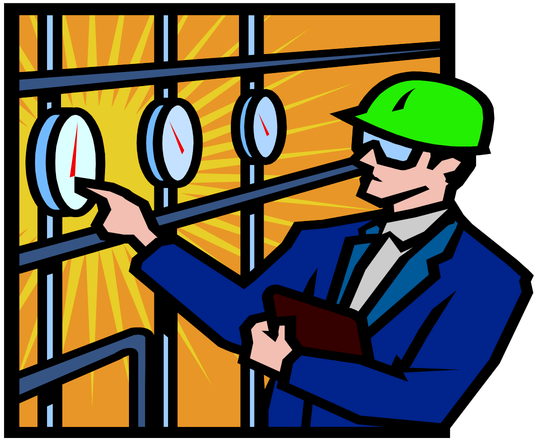
INTEGRATED MANAGEMENT SYSTEM – 2.0 POLICY

2.1 Definitions of terms
2.2 Normative references
2.3 Informative references
2.4 Mandatory requirements
2.5 Expectations and views of stakeholders
2.6 Purpose and goals
2.7 Scope
2.8 Principles
2.9 Overall policy statement
2.10 Objectives and targets
2.11 Roles and responsibilities
2.12 Risk criteria
2.13 Risk assessment approach

INTEGRATED MANAGEMENT SYSTEM - 3.0 SPECIFICATION

3.1 Generic controls
- 3.1.1 Design and inherent surety
- 3.1.2 Personnel competency
  - 3.1.2.1 Competencies needed to perform MS tasks
  - 3.1.2.2 Screening personnel for competency
  - 3.1.2.3 Personnel competency records
  - 3.1.2.4 Initial training of personnel in MS tasks
  - 3.1.2.5 Refresher training of personnel in MS tasks
  - 3.1.2.6 Personnel awareness
- 3.1.3 Personnel management
  - 3.1.3.1 Job responsibilities
  - 3.1.3.2 Employment contracts
  - 3.1.3.3 Performance goals
  - 3.1.3.4 Supervision and accountability
  - 3.1.3.5 Disciplinary process
- 3.1.4 Personnel involvement
- 3.1.5 Communications
- 3.1.6 Information management
- 3.1.7 Risk management
  - 3.1.7.1 Periodic risk assessment
  - 3.1.7.2 Siting
  - 3.1.7.3 Environmental threats
  - 3.1.7.4 Utilities

INTEGRATED MANAGEMENT SYSTEM - 3.0 SPECIFICATION (CONTD.)



3.1.8 Operations management

- 3.1.8.1 Procedures
- 3.1.8.2 Operator logs
- 3.1.8.3 Pre-startup review
- 3.1.8.4 Systems integrity
- 3.1.8.5 Special work and permits
- 3.1.8.6 Management of change
- 3.1.8.7 Third-party involvement
- 3.1.8.8 Protection of trade secrets and intellectual property

3.1.9 Incidents

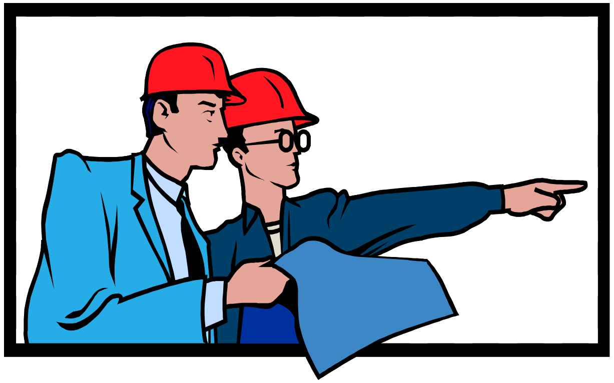
- 3.1.9.1 Reporting and investigation
- 3.1.9.2 Response plan
- 3.1.9.3 Business continuity management

3.1.10 Audits and inspections

- 3.1.10.1 Audits
- 3.1.10.2 Inspections

3.1.11 Coordination with other organizations

INTEGRATED MANAGEMENT SYSTEM - 3.0 SPECIFICATION (CONTD.)



3.2 Specific controls

3.3 Performance considerations

3.4 Capacity planning

3.5 Outreach

3.6 Continual improvement

3.7 Management of preventive and corrective actions

- 3.7.1 Implement actions
- 3.7.2 Communicate the results
- 3.7.3 Review corrective actions taken

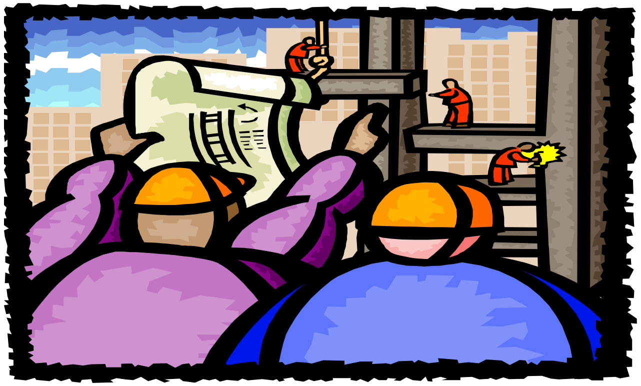
3.8 Control of documents and records

- 3.8.1 Control of documents
- 3.8.2 Control of records

EXAMPLE OF DETAILED SPECIFICATION – 3.1.8.6 MANAGEMENT OF CHANGE

MANAGEMENT OF CHANGE

- *Objective:* Ensure that changes do not compromise the MS.
- *Meaning:* Changes are modifications to an organization’s processes that may alter the risks. They include modifications to equipment, materials, procedures, technology, facilities, etc.



MANAGEMENT OF CHANGE – REQUIREMENTS FOR MOC PROCEDURE

- Types of changes covered.
- Technical basis for the change.
- Evaluation of the impact of the change using risk-based methods prior to their implementation.
- Establishing a system to promptly and effectively address findings and recommendations similar to the system described for the risk assessment element.
- Prompt notification to affected personnel of the changes.
- Ongoing supplemental training of personnel for changes prior to their implementation.
- Consideration of any adverse impacts that may occur as a result of the change process itself.
- Updating procedures as a result of the change.
- Updating information and documents as a result of the change.
- Updating the MS as a result of the change.
- Keeping records of modifications made to the MS in response to changes.
- Schedule for implementing the change.

MANAGEMENT OF CHANGE – REQUIREMENTS FOR MOC PROCEDURE (CONTD.)

- Management approval of the proposed change.
- Verification that the change has been implemented correctly.
- Determination that the system functions correctly after the change has been made.
- Maintenance of a log of the changes made.
- Briefing of personnel on the management of change procedure.
- Considering distinguishing between major and minor changes and adjusting practices accordingly.
- Consideration of both temporary and permanent changes, and emergency changes.
- Establishing and monitoring a time limit for temporary changes.
- Ensuring the process is returned to its original or designed conditions at the end of a temporary change.
- Integration with other change management programs, as appropriate.

MANAGEMENT OF CHANGE

- *Documents:* Management of change (MOC) procedure.

- *Records:*
  - Change requests.
  - Records that show a sound technical basis for each change.
  - MOC reviews.
  - Records that show how the impact of the change was evaluated.
  - Records showing notification of personnel of changes.
  - Records showing supplemental training of personnel for changes prior to their implementation.
  - Records showing briefing of personnel on the management of change procedure.
  - Records showing updates to procedures, training, information and other parts of the MS.
  - Records of modifications made to the MS in response to changes.
  - Log of changes.

ISSUES FACED

- Existing groups with ownership of specific sureties
  - May feel threatened
- Need for compromise on how management system elements are handled for different sureties
  - Form an integration group
- Decisions are needed on conflicting requirements
  - Management involvement
- Meeting regulatory requirements
  - Both national and international

SUMMARY

- Organizations must manage many sureties
- Formal management systems should be used
  - Range from simple to complex
- Best accomplished using integrated approaches

FURTHER INFORMATION

- Technical papers on cyber and process security and management systems:

  www.primatech.com

- Contact info:

  paulb@primatech.com

FEATURES OF ISO MANAGEMENT SYSTEMS

- Provide a model with generic requirements
- Make possible a structured approach for:
  - Setting performance objectives and targets
  - Achieving them
  - Demonstrating they have been achieved
- Do not specify performance levels
- Applicable to any organization regardless of its type, size, or the nature of its business
- Continual improvement is a key aspect