Introduction to
ISO 27001 & ISO 17799:2005
Information Security Management Systems

BSI Management Systems Training
Welcomes Delegates to this Course

shape the future

Issue 4/Sept 2005

BSI Management Systems

General

- Personal property
- Mobile phones, pagers, PDA's and computers
- Smoking
- Safety
- Washrooms
- Breaks and meals

BSI Management Systems

Learning Objectives

To learn about:

- How information security affects you
- Information security standards
  - ISO 27001:2005 and ISO 17799:2005
- ISO 27001:2005
  - Clauses
  - Control objectives and controls
- Implementation of an ISMS
- Certification

BSI Management Systems

Course Structure

- Information Security
- The purpose of the Information Security standards
- Differences between ISO 27001:2005 and ISO 17799:2005
- Clauses within ISO 27001:2005
- Control objectives and controls
- Implementation of an Information Security Management System
- Certification to ISO 27001:2005
- Other BSI Training courses in Information Security

BSI Management Systems

Introductions

- Name
- Company / Department
- Brief résumé of your career
- Information security experience
- ISO 27001:2005 (BS 7799-2:2002)
  - knowledge – rate on scale of 1-10
- Objectives of attending the course

BSI Management Systems

Information Security and Information Security Management

shape the future

Issue 4/Sept 2005

BSI Management Systems

What is Information Security?

- **Information Security**
  - To ensure Business Continuity
  - Minimise business damage by preventing and minimising the impact of security incidents
  - Preservation of Confidentiality, Integrity and Availability of information; in addition, other properties such as authenticity, accountability, non-repudiation and reliability can also be involved

- **Information Security Management System (ISMS)**
  - That part of the overall management system, based on a business risk approach, to establish, implement, operate, monitor, review, maintain and improve information security
  - Is a ***Management*** Process
  - Not a technological process

BSI Management Systems

C. I. A.

Three basic components

- **C – Confidentiality**
  - the property that information is not made available or disclosed to unauthorised individuals, entities, or processes
- **I – Integrity**
  - the property of safeguarding the accuracy and completeness of assets
- **A – Availability**
  - the property of being accessible and usable upon demand by an authorised entity

In some organisations, integrity and/or availability may be more important than confidentiality

BSI Management Systems

Types of Information

Internal

- Information that you would not want your competitors to know

Customer/client

- Information that they would not wish you to divulge

Shared

- Information that may be shared with other trading partners / persons

Activity 1

Discuss within your group

Why do you think Information Security is needed?

Time 15 minutes

BSI Management Systems

Information Security Risks

- (Some) Categories of Information Security Risk:
  - Information theft
  - Intrusion and subversion of system resources
  - Masquerade
  - Denial of service
  - Loss
  - Corruption

BSI Management Systems

Non – IT

- Paper documents:
  - on desks,
  - in waste bins,
  - left on photocopiers
- Whiteboards and flipcharts
- Telephone conversations overheard
- Conversations on public transport
- Social engineering

BSI Management Systems

Activity 2

Discuss within your group

What do you think are the top 10 most common information security mistakes made by individuals?

Time: 30 minutes

BSI Management Systems

Information Security Standards ISO 17799:2005 & ISO 27001:2005

shape the future

Issue 4/Sept 2005

BSI Management Systems

History of Standards

- Industry working group – January 1993
- Code of Practice issued – September 1993
- BS7799 Part One published – February 1995
- BS7799 Part Two published – February 1998
- BS7799 Part 1 and Part 2 – April 1999
- ISO 17799 (BS7799-1) published 2000
- BS7799-2 published 2002
- **ISO 17799:2005 issued**
- **ISO 27001:2005 replacement for BS7799-2**

BSI Management Systems

Comparison Between Standards

ISO 27001:2005	ISO 17799:2005
0 Introduction 1 Scope 2 Normative references 3 Terms & definitions	0 Introduction 1 Scope 2 Terms & definitions 3 Structure of this standard 4 Risk assessment & treatment
Clauses 4 to 8	
Annex A **Control objectives & controls** **A.5 to A.15**	Control objectives & controls 5 to 15
Annex B OECD principles **Annex C** Correspondence between standards	Bibliography Index

BSI Management Systems

ISO 17799:2005

Information Technology – Security Techniques – Code of practice for information security management

- Provides guidance on best practice for ISM
- Prime objectives
  - A common basis for organizations
  - Confidence in inter-organizational dealings
- Defines a set of control objectives, controls and implementation guidance

It <u>cannot</u> be used for assessment and certification

BSI Management Systems

ISO 27001:2005

Information Technology – Security Techniques – Information Security Management Systems – Requirements

Specifies requirements:

- For establishing, implementing, operating, monitoring, reviewing, maintaining and improving a documented ISMS

Designed to:

- Ensure adequate security controls to protect information assets, documenting Information Security Management Systems (ISMS)
- Give confidence to customers & interested parties

It can be used for assessment and certification

BSI Management Systems

Other Documents

A series of books giving guidance on implementing an effective information security management system and guidance for organisations preparing to be certified to ISO 27001:2005

PD3000 series replaced as follows:

- BS 7799-3:2005
  - Publication Dec 05
  - Include text from PD 3002 & PD 3005
- BIP 0071:2005
  - Publication Sept (replacing PD 3001)
- BIP 0072:2005
  - Publication Oct 05 (replacing PD 3003)
- BIP 0073:2005
  - Publication Dec 05 (replacing PD 3004)
- BIP 0074:2005
  - **NEW**
  - Measuring the effectiveness of your ISO 27001:2005 implementations

BSI Management Systems

Clauses within ISO 27001:2005

shape the future

Issue 4/Sept 2005

BSI Management Systems

Clauses within ISO 27001:2005

ISO 27001:2005	ISO 17799:2005
0 Introduction 1 Scope 2 Normative references 3 Terms & definitions	0 Introduction 1 Scope 2 Terms & definitions 3 Structure of this standard 4 Risk assessment & treatment
Clauses 4 to 8	
Annex A Control objectives & controls A.5 to A.15	Control objectives & controls 5 to 15
Annex B OECD principles **Annex C** Correspondence between standards	Bibliography Index

BSI Management Systems

Clauses

- **Exclusions**
  - Excluding any of the requirements specified in Clauses 4, 5, 6, 7 and 8 is not acceptable
  - Reference ISO 27001:2005 (Clause 1.2 Application)

BSI Management Systems

Clauses 4 to 8

- **Clause 4**
  - Information Security Management System
- **Clause 5**
  - Management Responsibility
- **Clause 6**
  - Internal ISMS Audits
- **Clause 7**
  - Management Review of the ISMS
- **Clause 8**
  - ISMS Improvement

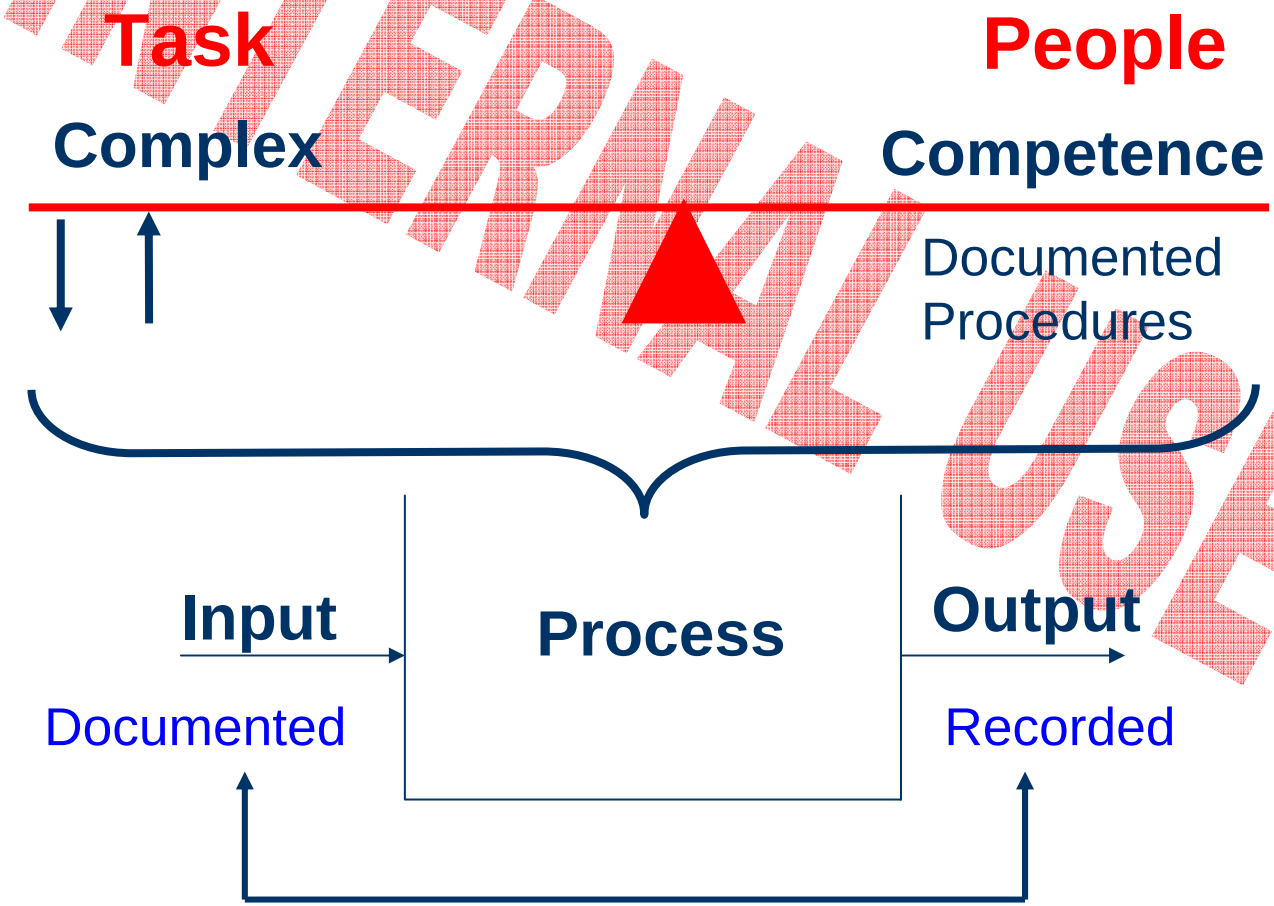
BSI Management Systems

Clause 5
Management Responsibility

- **5.1 Management commitment**
  - Management **shall** provide evidence of commitment
- **5.2 Resource management**
  - 5.2.1 Provision of resources
  - 5.2.2 Training awareness and competency

BSI Management Systems

Competency



Clause 6
Internal ISMS Audits

- **Internal ISMS Audits**

BSI Management Systems

Clause 7
Management Review of the ISMS

- **7.1 General**
  - Management **shall** review the organisation's ISMS at planned intervals
  - **At least once per year**
  - Records maintained
- **7.2 Review input**
- **7.3 Review output**

BSI Management Systems

Clause 8
ISMS Improvement

8.1 Continual improvement

- Continually improve effectiveness of ISMS

8.2 Corrective action

- Eliminate cause of nonconformities in order to prevent recurrence

8.3 Preventive action

- Identify potential non-conformances and causes
- Determine and implement corrective action needed

BSI Management Systems

Activity 3

Discuss within your group

How would you ensure that management:

- Are committed
- Establish roles and responsibilities for information security
- Provide training, awareness and competency
- Carry out reviews of the ISMS

Time: 30 minutes

BSI Management Systems

Clause 4 Information Security Management System

4.1
General
Requirements

4.2
Establish &
Manage ISMS

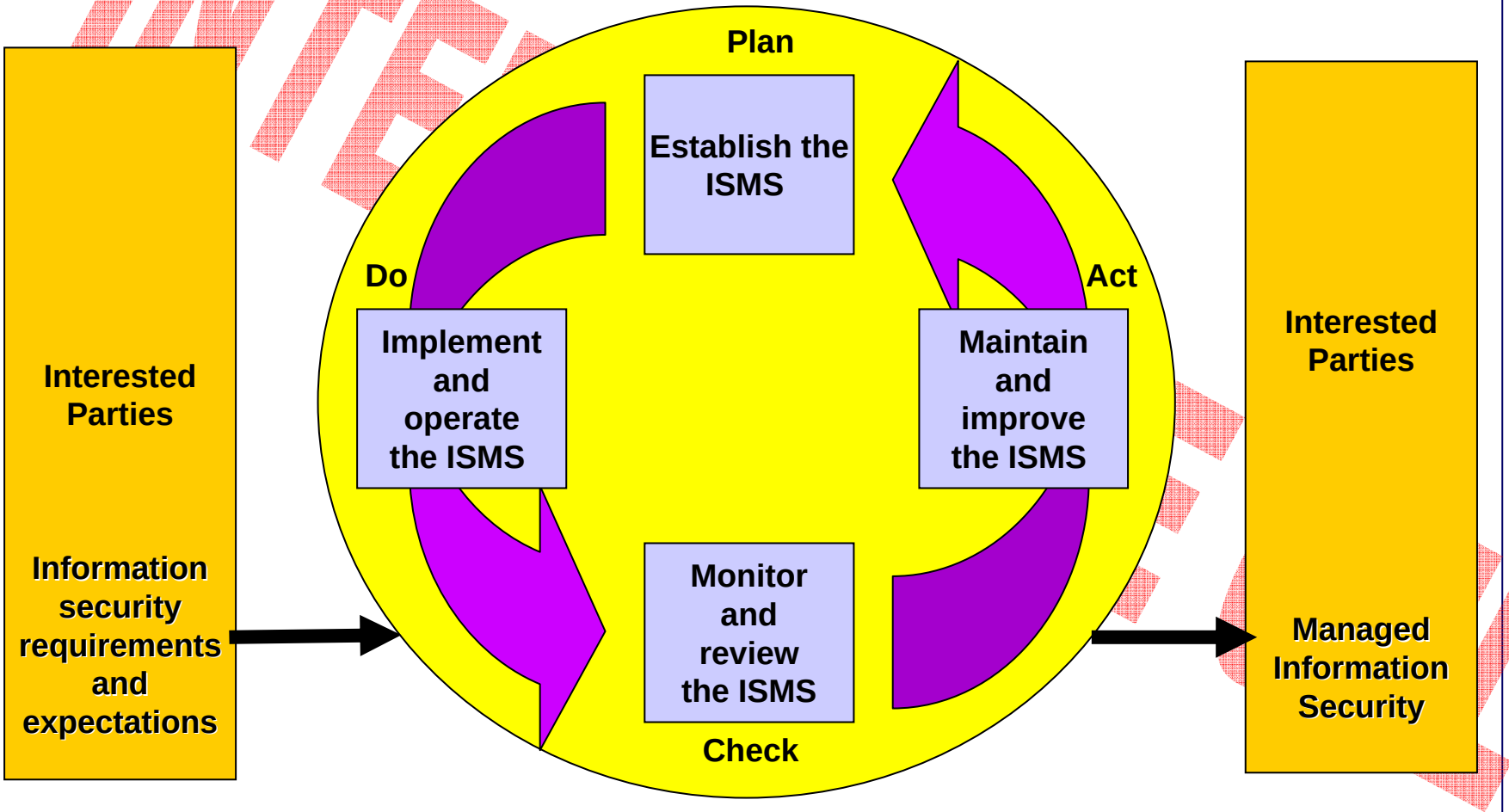
4.2.1 Establish ISMS
4.2.2 Implement & operate ISMS
4.2.3 Monitor & review ISMS
4.2.4 Maintain & improve ISMS

4.3
Documentation
Requirements

4.3.1 General
4.3.2 Document control
4.3.3 Record control

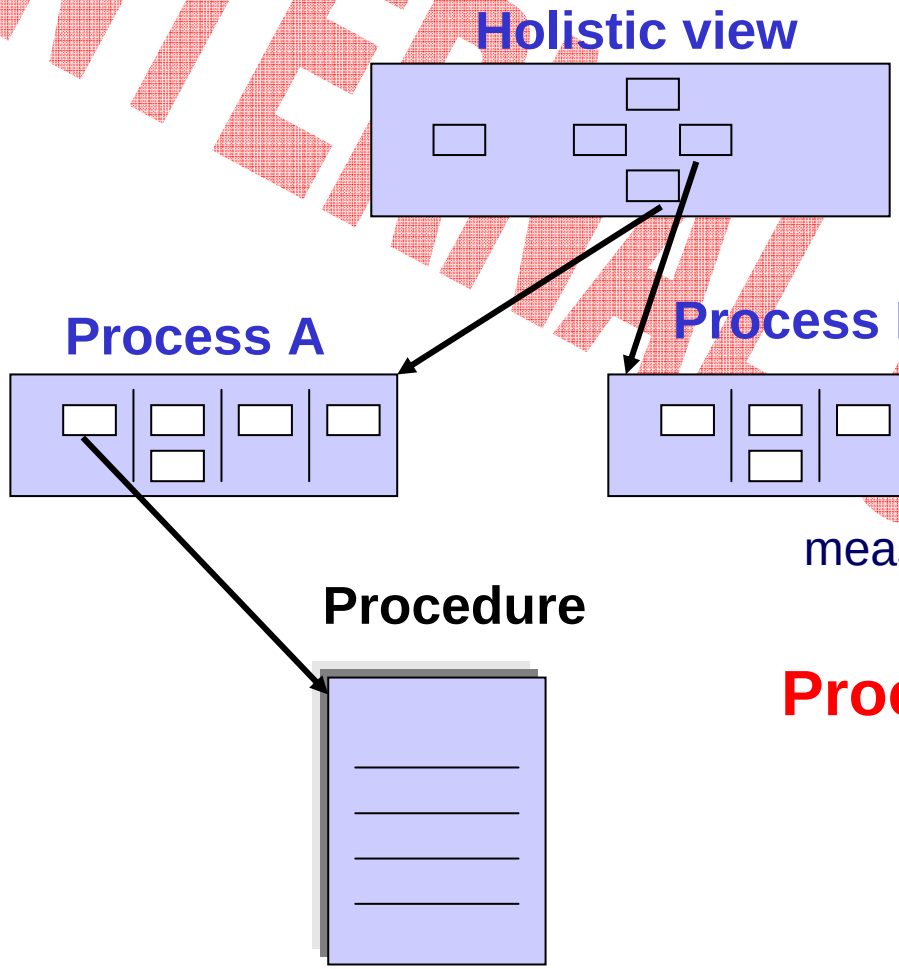
BSI Management Systems

PDCA Model Applied to ISMS Processes



BSI Management Systems

Typical Structure



'measure business performance' , finance, customer, innovation

Top Management

measure efficiency/effectiveness

Process Owner

BSI Management Systems

Clause 4.2.1 (Plan) Establish the ISMS

a) Scope and boundaries
b) Policy - objectives, business and legal or regulatory requirements, strategy, criteria, approved by management
c) Define the risk assessment approach of the organisation
d) Identify risks (assets & owners, threats, vulnerabilities, impacts)
e) Analyse and evaluate the risks (business impact, likelihood, controls currently in place, levels of risk, risk acceptable or requires treatment)
f) Identify and evaluate options for treatment of risks (apply controls, accept, avoid, transfer)
g) Select control objectives & controls for the treatment of risks (select from Annex A)

Clause 4.2.1 (Plan) – (cont) Establish the ISMS

h) Obtain management approval of the proposed residual risks

i) Obtain management authorisation to implement and operate the ISMS

j) Prepare a Statement of Applicability

BSI Management Systems

Clause 4.2.2 Implement and Operate the ISMS (Do)

- Formulate & implement risk treatment plan
- Implement controls
- Training & awareness
- Manage operations & resources
- Implement procedures

BSI Management Systems

Clause 4.2.3 Monitor and Review the ISMS (Check)

- Execute monitoring and review procedures and other controls
- Undertake regular reviews of the effectiveness of the ISMS
- Measure effectiveness of controls
- Review risk assessments at planned intervals
- Review level of residual risk & identified acceptable risk
- Conduct internal ISMS audits at planned intervals
- Undertake management review of the ISMS
- Update security plans
- Record actions and events

BSI Management Systems

Clause 4.2.4 Maintain and Improve the ISMS (Act)

- Implement the identified improvements in the ISMS
- Appropriate corrective and preventive action
- Communicate actions and improvements
- Ensure improvements achieve their intended objectives

BSI Management Systems

Overview of Control Objectives and Controls

shape the future

Issue 4/Sept 2005

BSI Management Systems

Annex A Control Objectives and Controls

ISO 27001:2005	ISO 17799:2005
0 Introduction 1 Scope 2 Normative references 3 Terms & definitions	0 Introduction 1 Scope 2 Terms & definitions 3 Structure of this standard 4 Risk assessment & treatment
Clauses 4 to 8	
Annex A **Control objectives & controls** **A.5 to A.15**	Control objectives & controls 5 to 15
Annex B OECD principles **Annex C** Correspondence between standards	Bibliography Index

BSI Management Systems

Control Objectives and Controls (1)

A5 Security policy

A6 Organization of information security

A7 Asset management

A8 Human resources security

A9 Physical and environmental security

BSI Management Systems

Activity 4

Discuss within your group

What measures would you have in place to ensure secure areas within your own organisation?

Time: 30 minutes

BSI Management Systems

Control Objectives and Controls (2)

A10 Communications and operations management

A11 Access control

A12 Information systems acquisition, development and maintenance

A13 Information security incident management

A14 Business continuity management

A15 Compliance

BSI Management Systems

Selection of Controls (Summary)

- **Additional control objectives and controls:**
  - Organization might consider that additional control objectives and controls are necessary

- **Not all the controls will be relevant to every situation:**
  - Consider local environmental or technological constraints
  - In a form that suits every potential user in an organization

BSI Management Systems

Implementation of an ISMS

shape the future

Issue 4/Sept 2005

BSI Management Systems

Implementation of an ISMS (Summary 1)

- **Establish and manage the ISMS (PLAN)**
  - Scope and boundaries
  - Policy / objectives
  - Define risk assessment approach
  - Identify risks
  - Analyse and evaluate the risks
  - Identify and evaluate options for treatment of risks
  - Select control objectives & controls (Annex A)
  - Obtain management approval of the proposed residual risks
  - Obtain management authorisation to implement and operate the ISMS
  - Prepare a Statement of Applicability

BSI Management Systems

Implementation of an ISMS (Summary 2)

- **Implement and operate the ISMS (DO)**
  - Formulate risk treatment plan
  - Implement risk treatment plan
  - Define how to measure effectiveness of selected controls
  - Implement controls selected to meet control objectives
  - Implement training and awareness
  - Manage operations and resources
  - Implement procedures and other controls

BSI Management Systems

Implementation of an ISMS (Summary 3)

- **Monitor and review the ISMS (CHECK)**
  - Execute monitoring procedures and other controls
  - Undertake regular reviews of the effectiveness of the ISMS
  - Measure effectiveness of controls
  - Review risk assessments at planned intervals
  - Review level of residual risk and identified acceptable risk
  - Internal ISMS audits / Management review
  - Update security plans
  - Record actions and events

BSI Management Systems

Implementation of an ISMS (Summary 4)

- **Maintain and improve the ISMS (ACT)**
  - Implement identified improvements
  - Take appropriate corrective and preventive actions
  - Communicate the actions and improvements
  - Ensure improvements achieve intended objectives

BSI Management Systems

Certification and Other BSI Training Courses on Information Security

shape the future

Issue 4/Sept 2005

BSI Management Systems

Assessment and Certification

Pre-assessment (optional)

Stage 1 – Documentation Audit

Stage 2 – Implementation Audit

Pre-certification

Continuing Surveillance

3-Year Re-assessment

Post-certification

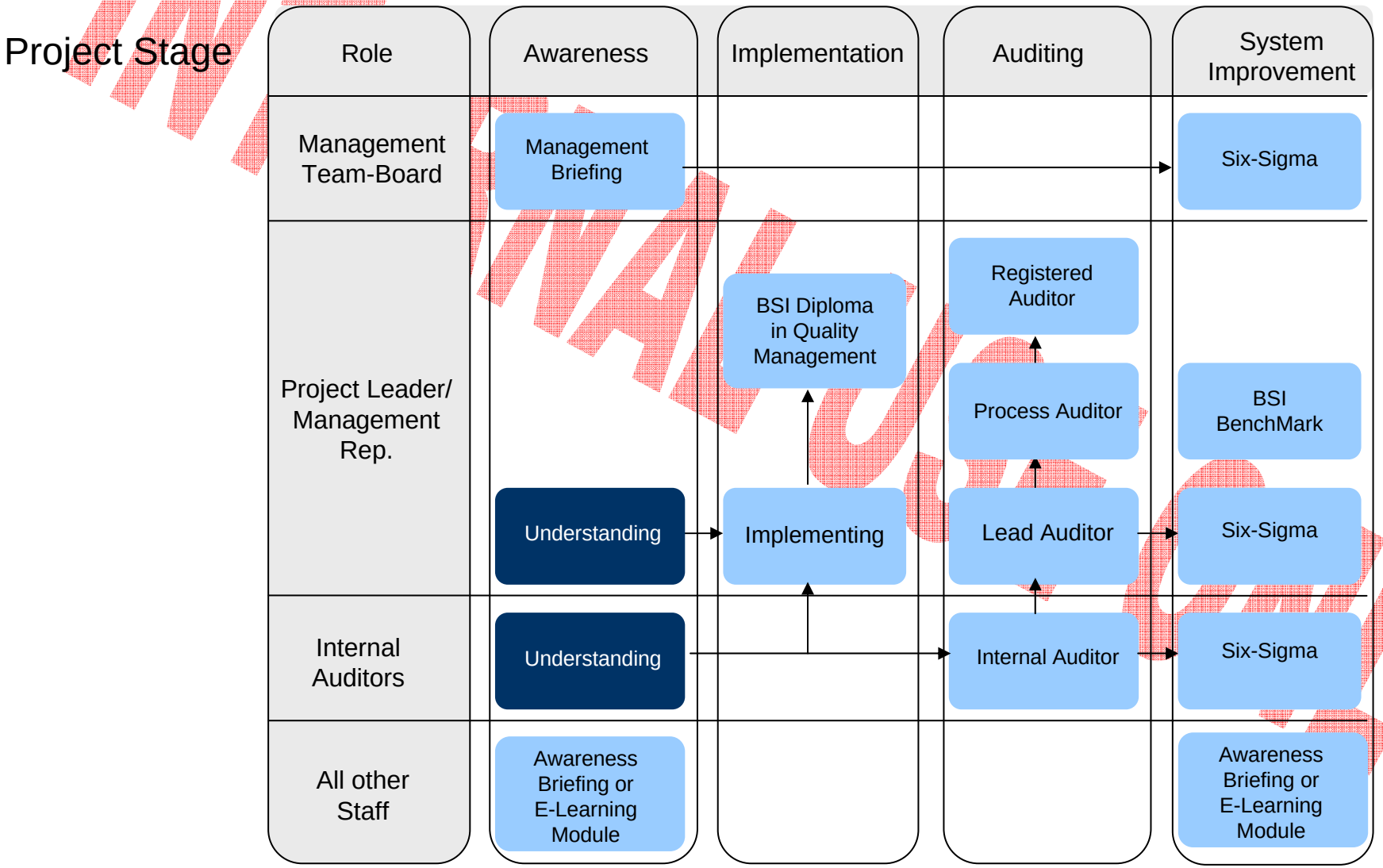
BSI Management Systems

BSI Management Systems Training

- **Open courses:**
  - Held in a wide range of venues worldwide
- **In-house courses:**
  - Can be provided and modified to suite customer's individual needs

BSI Management Systems

Training Course Map



BSI Registered Auditor Qualification:

Management Systems

BSI Registered Auditor - Route to Qualification

Step 4 - Complete the Qualifying Review

Step 3 - Audit Coaching session in the work place

Step 2 - Complete the Process Auditing course

Step 1 - Complete one of the BSI Lead Auditor courses

Management Systems

BSI Registered Auditor Registration

- Supported by the international strength of BSI, the RA Qualification is set to become the benchmark for Quality, Environmental, H and S and ISMS management systems personnel.

- Ensures auditors gain awareness and understanding of best practice in Management Systems Auditing.

- Ensures practices remain up to date.

BSI Management Systems

The BSI Route to Registration

BSI Management Systems MEA
PO Box 26444
Dubai, United Arab Emirates

Tel: 00971 4 3364917
Fax: 00971 4 3360309

www.bsi-me.com

BSI Management Systems