

# Using Best Practice to Improve Resilience

Richard Stone, Account Director  
Ultima Risk Management (URM)

# URM's Credentials

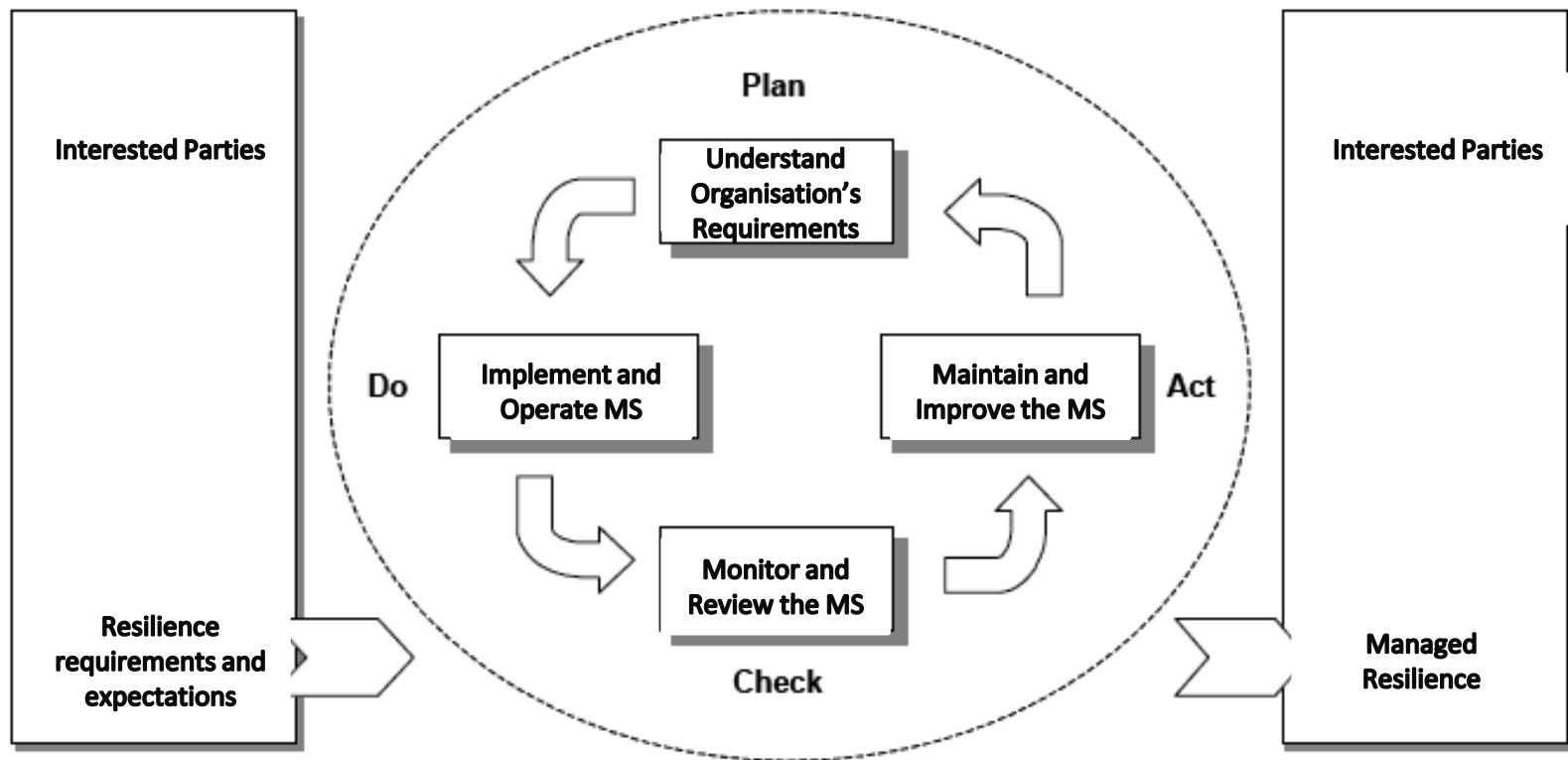
- Information Management, Governance and Security Consultancy
  - Business Continuity- BS 25999
  - Information Security -ISO 27001 and PCI DSS
  - Data Protection
  - IT Service Management- ISO 20000 and ITIL
- Assisted 30 +organisations certify to ISO 27001 and BS 25999
- Accredited as PCI QSA
- Premier BCS /ISEB training provider
- Pragmatic and 'appropriate' approach based on best practice

## Summary of Best Practice

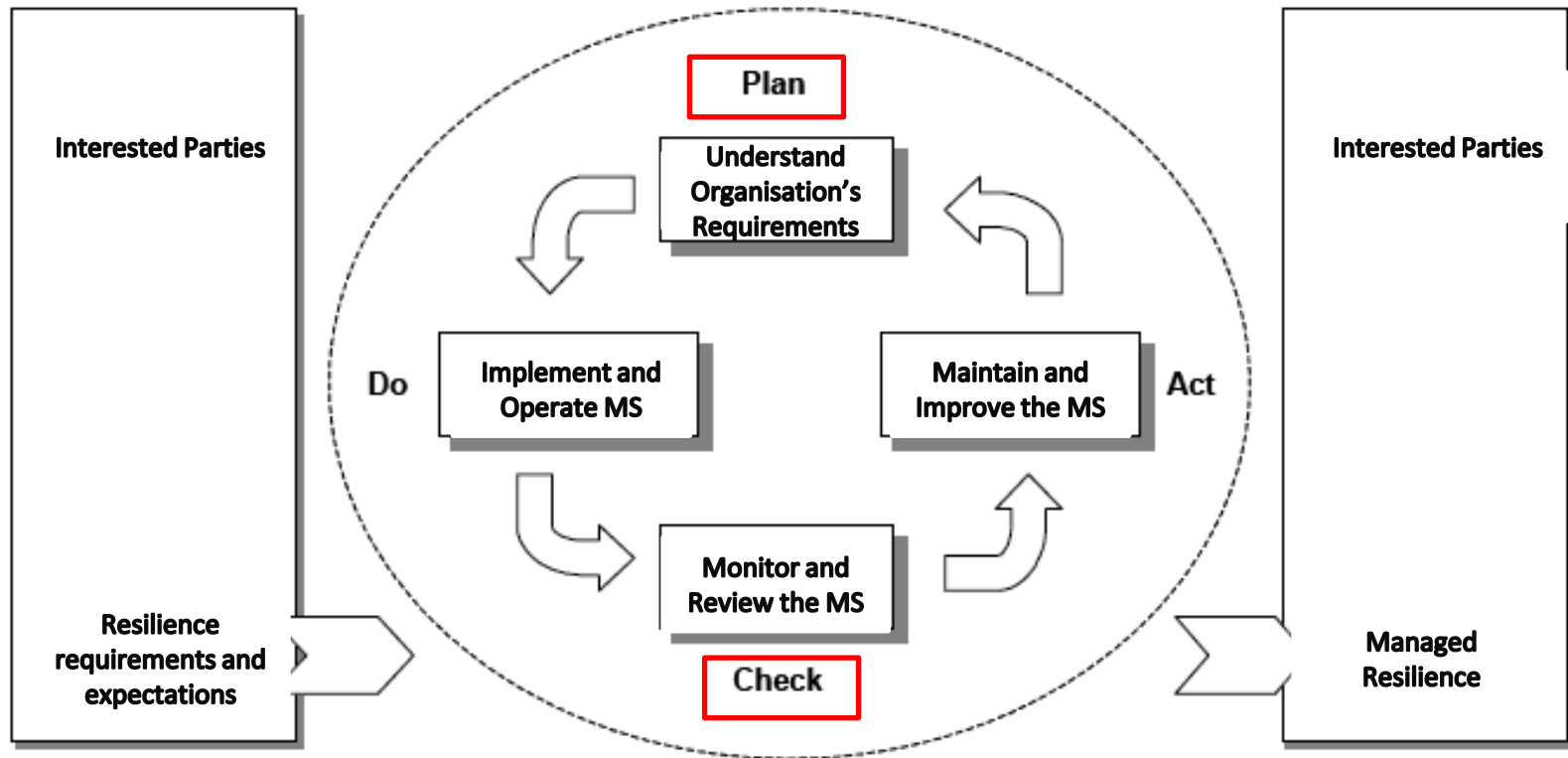
Implementing 'Plan-Do-Check-Act' model of continuous improvement against a documented specification

- ISO 27001 Information security
- BS 25999 Business Continuity

# 'Plan-Do-Check-Act' Model



# Key phases of 'Plan-Do-Check-Act' Model



# 'Plan' Phase Objectives

## BS 25999

- Business Recovery / Maintenance  
Identify requirements that will enable an organisation to respond effectively to a business continuity incident and incorporate this in to BC strategies and plans - **Business Impact Analysis (BIA)**
- Business Resilience  
Identify threats that might lead to an incident or affect an organisation's ability to recover from an incident and identify risk treatment which will reduce the likelihood of threats occurring – **Risk Assessment / Risk Treatment**

## ISO 27001

- Business Resilience  
Identify the impact of an information security incident and identify risk treatment which will reduce the likelihood of threats occurring to an acceptable level – **BIA, Risk Assessment / Risk Treatment**

# 'Plan' Phase Activities

## **BS 25999 BIA Identifies**

- Key products and services
- Critical activities
- Processes supporting critical activities
- Resources required to make the critical activities happen
- Impacts of stopping a critical activity different time periods?
- Resources needed to restore critical activities

## **ISO 27001 BIA Identifies**

- Information Assets
- Impacts of an information security incident on CIA of assets

# 'Plan' Phase Activities

## **BS 25999 Risk Assessment**

- Threats / vulnerabilities that increase likelihood of needing recovery plans
- Threats / vulnerabilities that may hamper the recovery process
- Strategies / controls that will reduce likelihood / impact of threat

## **ISO 27001 Risk Assessment**

- Threats / vulnerabilities that increase the likelihood / impact of an information security incident
- Strategies / controls that will reduce likelihood / impact of threat

**All conducted against the organisation's risk appetite**

# 'Plan' Phase Implementation Methodologies

Approach	Comments
<b>Interviews</b>	Key business representatives are interviewed in order to establish the critical activities and recovery requirements. In large organisations, this can be time consuming and expensive.
<b>Workshops</b>	Key business representatives attend a BIA workshop in order to establish critical activities and recovery requirements. This approach demands a significant time commitment as workshops can last for up to one day.
<b>Questionnaires</b>	The advantage of the questionnaire approach is that it is the most resource efficient. However, the major risk with questionnaires is the potential for unreliable and inconsistent replies from the different respondents.

# 'Check' Phase Objectives

## BS 25999

- Testing of business continuity plans (DR, Business Process and Incident Management)  
To identify a testing schedule that ensures business continuity plans deliver the recovery requirements **identified in the BIA.**
- Auditing of the Management System  
Ensure all elements of the management system are operating effectively

## ISO 27001

- Auditing of Management System  
Ensure all elements of the management system are operating effectively

**With all need to ensure supporting evidence collated**

# 'Check' Phase Activities

## **BS 25999**

- Need appropriate testing schedule – all tested over 3 years
- Selection of appropriate tests
- Clarification of BC roles & responsibilities / competences
- BC audits

## **ISO 27001**

- Clarification of information security roles and responsibilities / competences
- Information security 27001 audits

# 'Check' Phase Implementation Methodologies

## Business Continuity Exercising

BS 25999 requires 'robust' testing of plans, without damaging organisation!

Testing options can include:

- Desk check
- Desktop walkthrough
- Simulation exercise
- Test of individual critical activities
- Testing of individual departmental plans
- Full BC testing

Enhance by using escalating scenarios and removal of key resource.

# 'Check' Phase Implementation Methodologies

## Audit

Audit schedules need to satisfy two key objectives:

- Has organisation implemented information security or business continuity in accordance with documented ISMS / BCMS
- Does ISMS / BCMS meet requirements of ISO 27001 / BS 25999

Can be delivered internally or externally

## **Case Study 1**

### **Service Provider to Automotive Industry**

- ISO 27001 and BS 25999 Certified

# Why Certify?

## ■ Build Customer Confidence

- Experienced separate outages on customer facing systems
- Identified DR solution was a mismatch with customers expectations.
- Outages had appeared in world wide press; not just UK market.
- Sceptical customer base after heavy investment in technology

## ■ Governance

- Increased governance in contracts (FSA)
- Supply chain management (back to back)

# Benefits

- **Credibility in market place**
  - Confidence to do Business with....
- **IT and business alignment**
- **Cultural change**
  - Risk /awareness
  - Ownership and accountability
- **Business efficiency**
  - Formalised processes and controls
  - Measurable / Continuous Improvement
- **Revenue / bottom line protection**

## Case Study 2

### Regional Fire and Rescue Service

- ISO 27001 and BS 25999 certified

## Why Certify?

- Meet its legal obligations
- Meet requirements of Audit Commission who regularly conduct comprehensive performance assessments.
- Address issues raised by internal auditors.
- Meet needs of internal users by providing support to drive the improvement of internal services

## Benefits....

- Stronger operational procedures leading to improved security, resilience and service to internal users
- Greater clarity and simplification of policies
- Greater awareness of information security and business continuity throughout whole organisation
- Created more 'open' culture