BS 25999 – a framework for resilience and success

Robert Whitcher
BCI Webinar June, 2009

raising standards worldwide™

Management Systems

Scope of Presentation

- The Standards process
- Drivers for BCM and BS 25999
- BS 25999 development
- Overview of BS 25999 Part 1
- Break
- Overview of BS 25999 Part 2
- Certification
- Conclusions

What is a Standard?

What is a Standard?

- A full consensus of all interested parties, so not imposed (includes Government, business, trade associations, Non Government Organizations and consumers)
- Updated on a regular cycle
- *Best* practice not general practice, therefore a goal
- Certification or audit is available, if required

Standards pyramid

The standards process

- Starts with formation of a Technical Committee (TC) after recognition of business ‘need’
- All interested stakeholders invited to join the TC
- Work programme agreed with input from the National or International standards body
- TC can operate purely for National Standards or can ‘mirror’ European and ISO committees
- Draft standards go for public consultation
- Emphasis is on building consensus among key stakeholders about what is best practice

Why formal standards

- Standards are a powerful tool for organizations of all sizes, supporting innovation and increasing productivity.
- Effective standardization promotes forceful competition and enhances profitability, enabling a business to take a leading role in shaping the industry itself.
- Standards allow a company to:
  - Attract and assure customers
  - Demonstrate market leadership
  - Create competitive advantage
  - Develop and maintain best practice

Why a formal standard

- We live in a more uncertain world with new and evolving risks
- Ensuring the survival of an organization is a top management priority
- More Board awareness of business disruptions and their impact on profits
  - Organizations have far more interdependency between countries
  - Organizations rely on longer and more risky supply chains and frequently rely on single-source suppliers

Why a formal standard

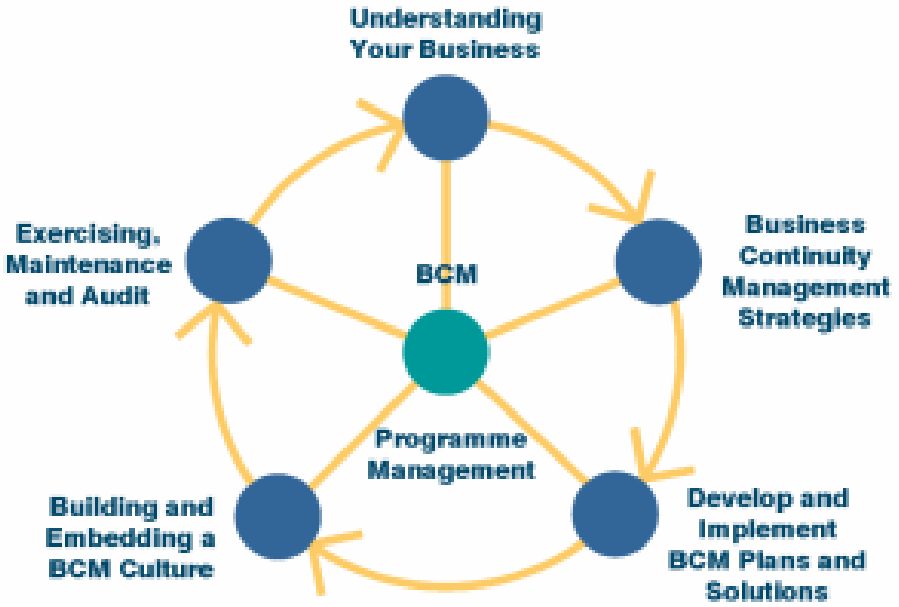
- Provides a common framework, based on internationally accepted best practices for implementing and managing business continuity
- Provides a framework for organizations of any type, size and location
- Improve operational effectiveness of an organization
- Allows for the proactive management of business risks
- Help demonstrate applicable laws, regulations and contractual requirements are being observed
- Brings a common understanding to the marketplace

BS 25999 Part 1

PAS 56

- Predecessor to BS 25999
- Developed in conjunction with:
  - The Business Continuity Institute (BCI)
  - Insight Consulting, and
  - British Standards Institution (BSI)
- Published March 2003
- Now withdrawn

Original BCM Lifecycle



BS 25999-1:2006

- Code of practice for business continuity management
  - Establishes the BCM processes, principles and terminology
  - Provides a basis for understanding, developing and implementing business continuity within organizations of any size or from any sector
  - Provide a comprehensive methodology based on BCM best practice and the whole BCM lifecycle
  - Business driven

Benefits of BS 25999

- Provides a common framework, based on international best practice, to manage business continuity
- Proactively improves your resilience when faced with disruptions to your ability to achieve key objectives
- Provides a rehearsed method of restoring your ability to supply critical products and services to an agreed level and timeframe following a disruption
- Delivers a proven response for managing a disruption

BS 25999 Code of practice contents

1	Scope and applicability
2	Terms and definitions
3	Overview of business continuity management (BCM)
4	The Business Continuity Management policy
5	BCM Programme Management
6	Understanding the organization
7	Determining business continuity strategy
8	Developing and implementing a BCM response
9	Exercising, maintaining and reviewing BCM arrangements
10	Embedding BCM in the organization's culture

BS 25999 Code of practice contents

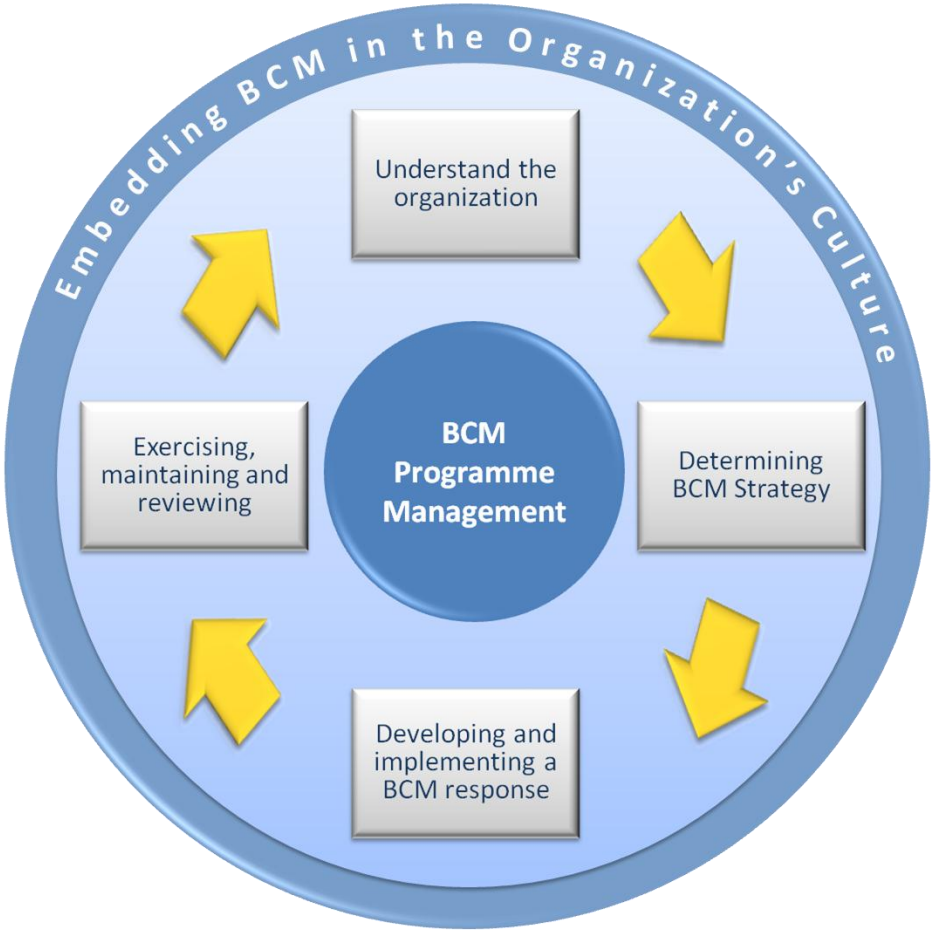
1	Scope and applicability
2	Terms and definitions
3	Overview of business continuity management (BCM)
4	The Business Continuity Management policy
5	BCM Programme Management
6	Understanding the organization
7	Determining business continuity strategy
8	Developing and implementing a BCM response
9	Exercising, maintaining and reviewing BCM arrangements
10	Embedding BCM in the organization's culture

What is Business Continuity Management?

"Business continuity management is a holistic management process that identifies potential impacts that threaten an organization and provides a framework for building resilience and the capability for an effective response which safeguards the interests of its key stakeholders, reputation, brand and value creating activities"

Source: *BS 25999-1*

Business Continuity Lifecycle



The BCM policy

- The objectives of establishing a BCM policy are to:
  - ensure that all BCM activities are conducted and implemented in an agreed and controlled manner;
  - achieve a business continuity capability that meets changing business needs and is appropriate to the size, complexity and nature of the organization; and
  - put in place a clearly defined framework for the ongoing BCM capability.

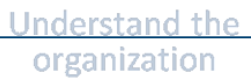
BCM programme management

Purpose

Programme management is at the heart of the BCM process. Effective programme management establishes the organization's approach to business continuity.

- Achieves the objectives defined in the policy
- Involves three steps:
  1. assigning responsibilities (governance);
  2. implementing business continuity in the organization;
  3. ongoing management of business continuity

Understanding the organization

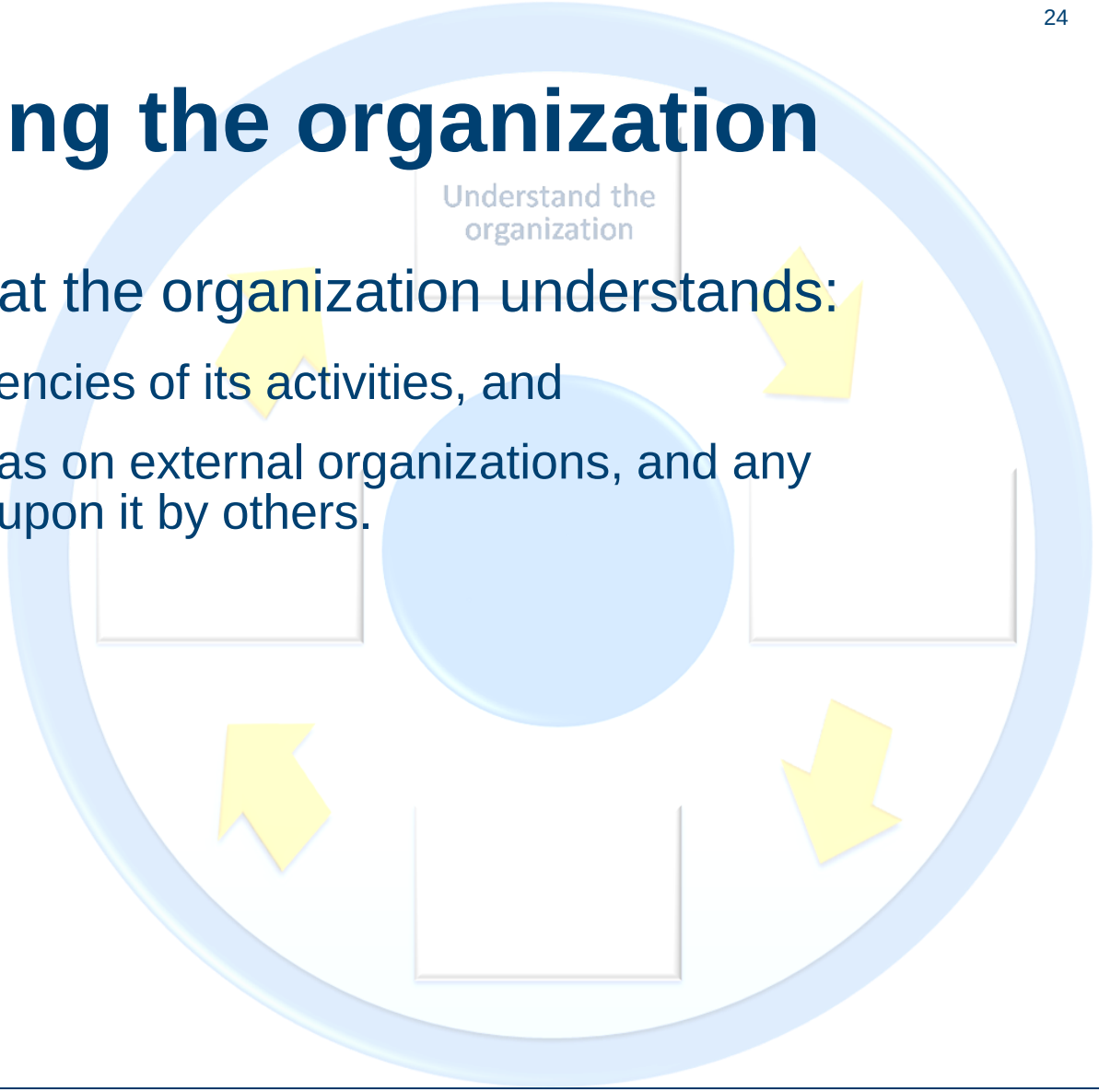


Purpose

To assist the understanding of the organization through the identification of its key products and services, and the critical activities and resources that support them.

- Business Impact Analysis
- Identification of critical activities
- Determining continuity requirements
- Evaluating threats to critical activities
  - Undertake a risk assessment
- Determine choices
- Approvals

Understanding the organization



- It is important that the organization understands:
  a) the interdependencies of its activities, and
  b) any reliance it has on external organizations, and any reliance placed upon it by others.

Determining business continuity strategy

Purpose

As a result of the analysis conducted in “understanding the organization”, an organization will be in a position to choose the appropriate continuity strategies to enable it to meet its objectives.

- Strategy options will depend on a range of factors:
  - the maximum tolerable period of disruption of the critical activity;
  - the costs of implementing a strategy or strategies; and
  - the consequences of inaction.

Determining business continuity strategy

- Strategies might be required for the following organizational resources:
  - people
  - premises
  - technology
  - information
  - supplies
  - stakeholders
  - civil emergencies

Developing and implementing a response

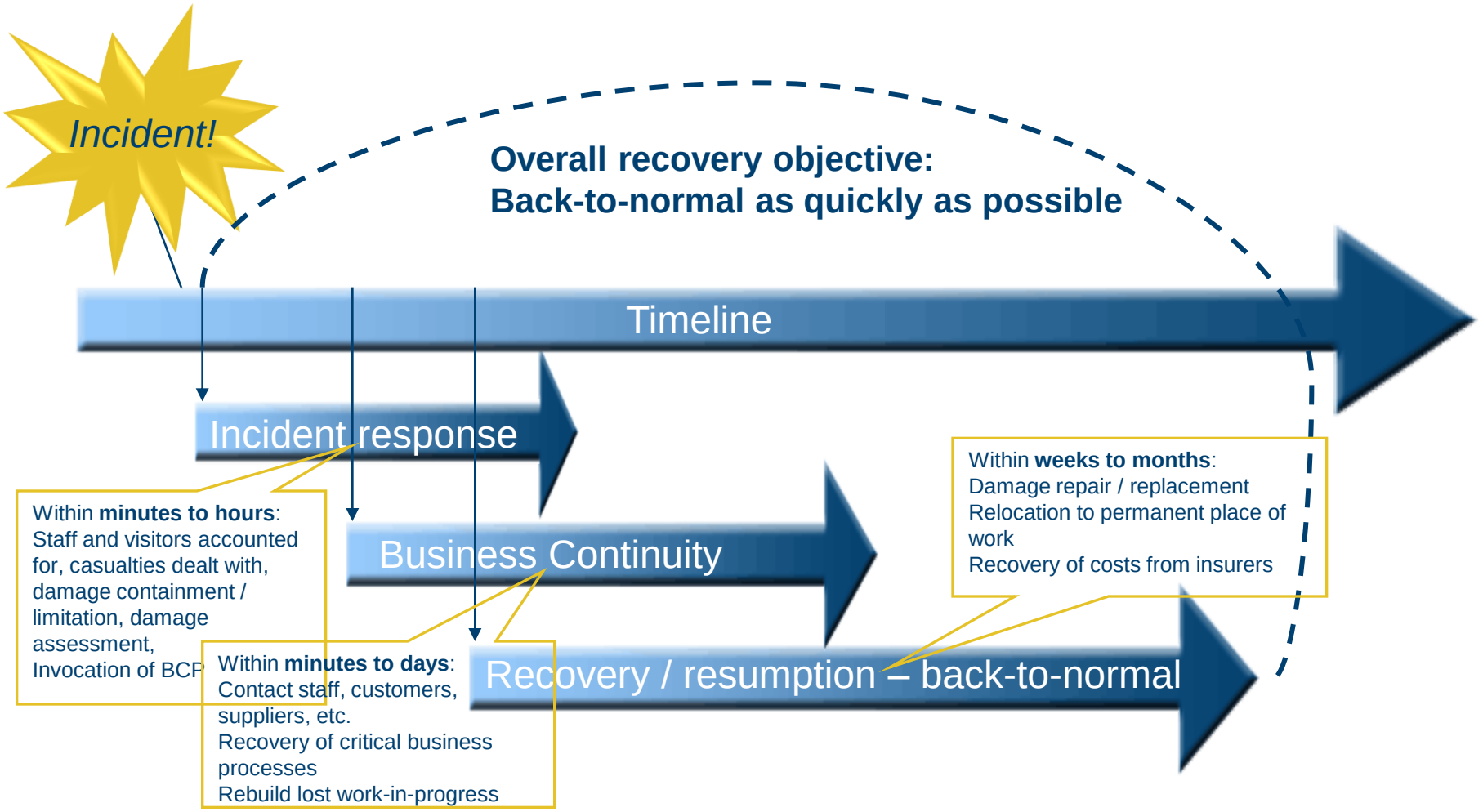
Purpose

Development and implementation of appropriate plans and arrangements to ensure continuity of critical activities, and the management of an incident.

- Identify critical activities
- Evaluate threats to those critical activities
- Choose appropriate strategies to reduce the likelihood and impact of incidents; and
- Choose appropriate strategies that provide for the continuity or recovery of critical activities

The range of threats to be planned for should be determined by the organization's risk appetite.

Incident timeline



Developing and implementing a response

- A small organization may have a single plan that encompasses all requirements for the business and which covers its entire operations
- A very large organization may have many plans, each of which specifies in detail the recovery of:
  - a particular part of its business;
  - particular premises; or
  - a particular scenario.
- May include separate documentation for the incident, continuity and recovery phases

The Incident Management Plan (IMP)

Purpose

The purpose of an IMP is to allow the organization to manage the initial (acute) phase of an incident.

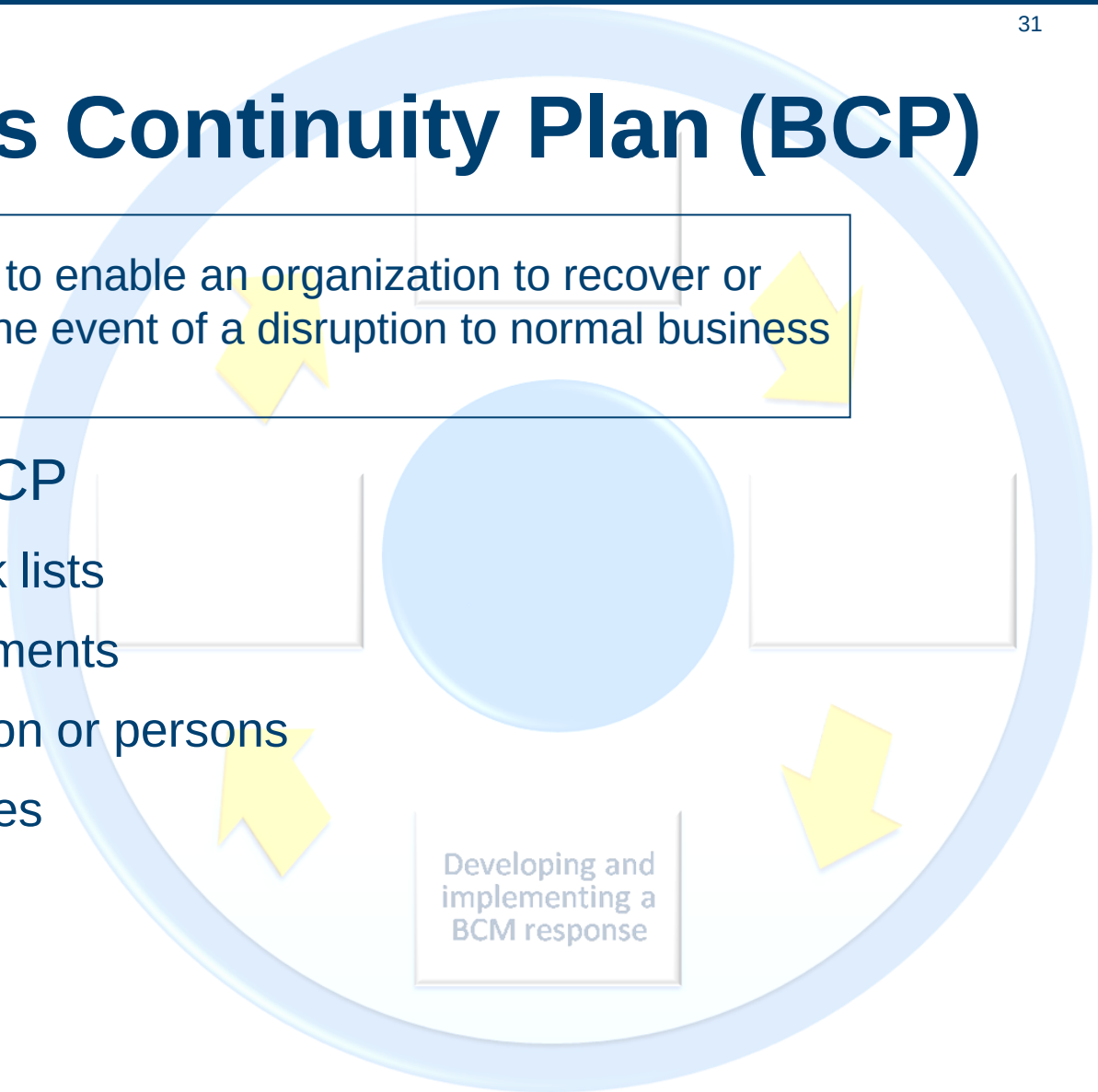
- The IMP should:
  - Be flexible, feasible and relevant;
  - Be easy to read and understand, and
  - Provide the basis for managing all possible issues, including the stakeholder and external issues, facing the organization during an incident.

The Business Continuity Plan (BCP)

Purpose

The purpose of a BCP is to enable an organization to recover or maintain its activities in the event of a disruption to normal business operations.

- Contents of the BCP
  - Action plans / task lists
  - Resource requirements
  - Responsible person or persons
  - Forms and annexes



Exercising

Purpose

This element of the BCM lifecycle ensures that an organization's BCM arrangements are validated by exercise and review and that they are kept up-to-date.

- Exercises provide demonstrable evidence of business continuity and incident management competence and capability
- Time and resources spent proving BCM strategies by exercising BCPs will lead to a fit-for-purpose capability
- No matter how well designed and thought-out a BCM strategy or BCP appears to be, a series of robust and realistic exercises will identify areas that require amendment

Embedding BCM into the culture

Purpose

To be successful, business continuity has to become part of the way that an organization is managed, regardless of size or sector. At each stage of the BCM process, opportunities exist to introduce and enhance an organization's BCM culture.

- Ensures that BCM becomes part of the organization's core values and effective management
- Creating and embedding can be a lengthy and difficult process
- All staff have to understand that BCM is a serious issue for the organization and that they have an important role to play in maintaining the delivery of products and services to their customers

BS 25999 Part 2

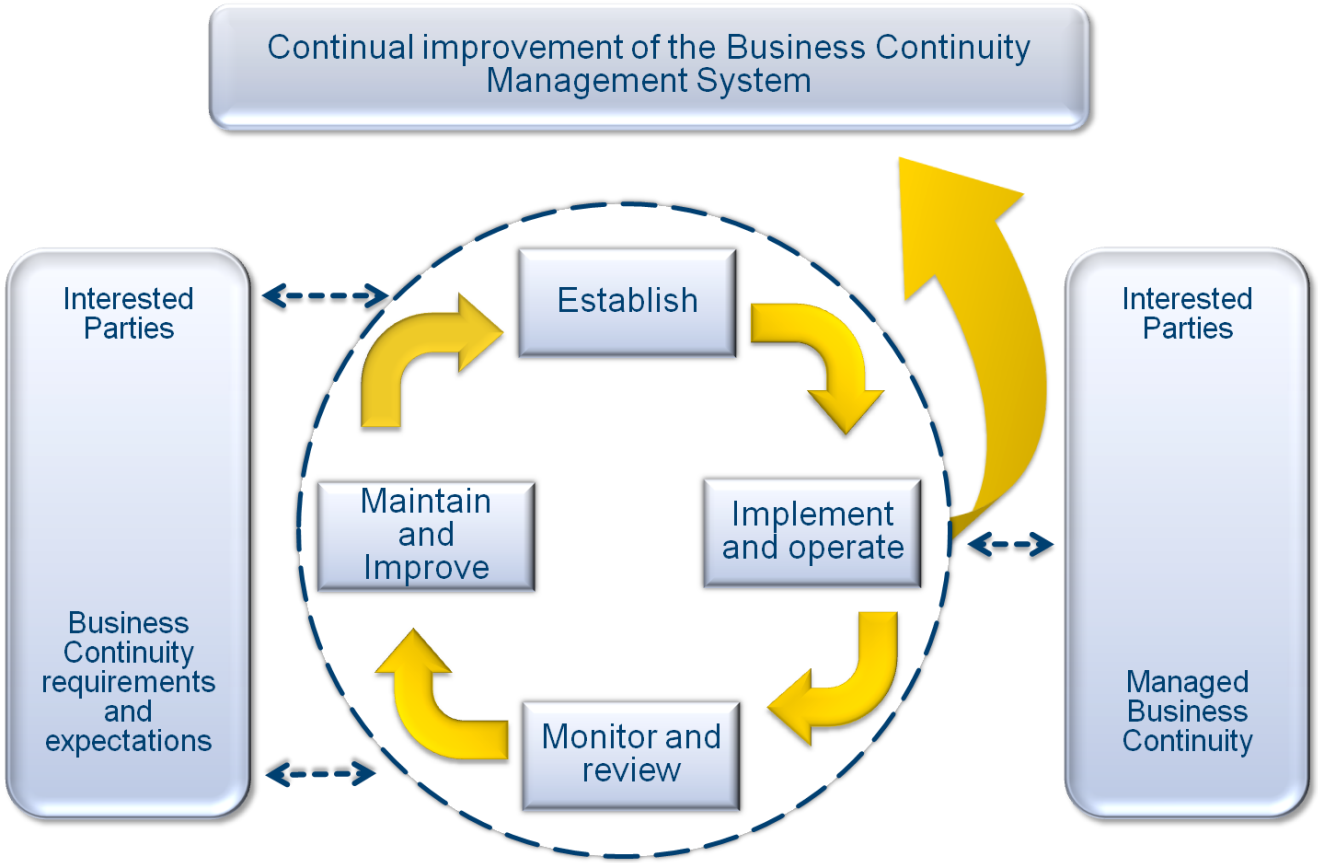
Understanding BS 25999

- BS 25999 Part One, a Code of Practice, provides BCM recommendations
- BS 25999 Part Two, a Specification, provides an auditable management system framework for managing business continuity

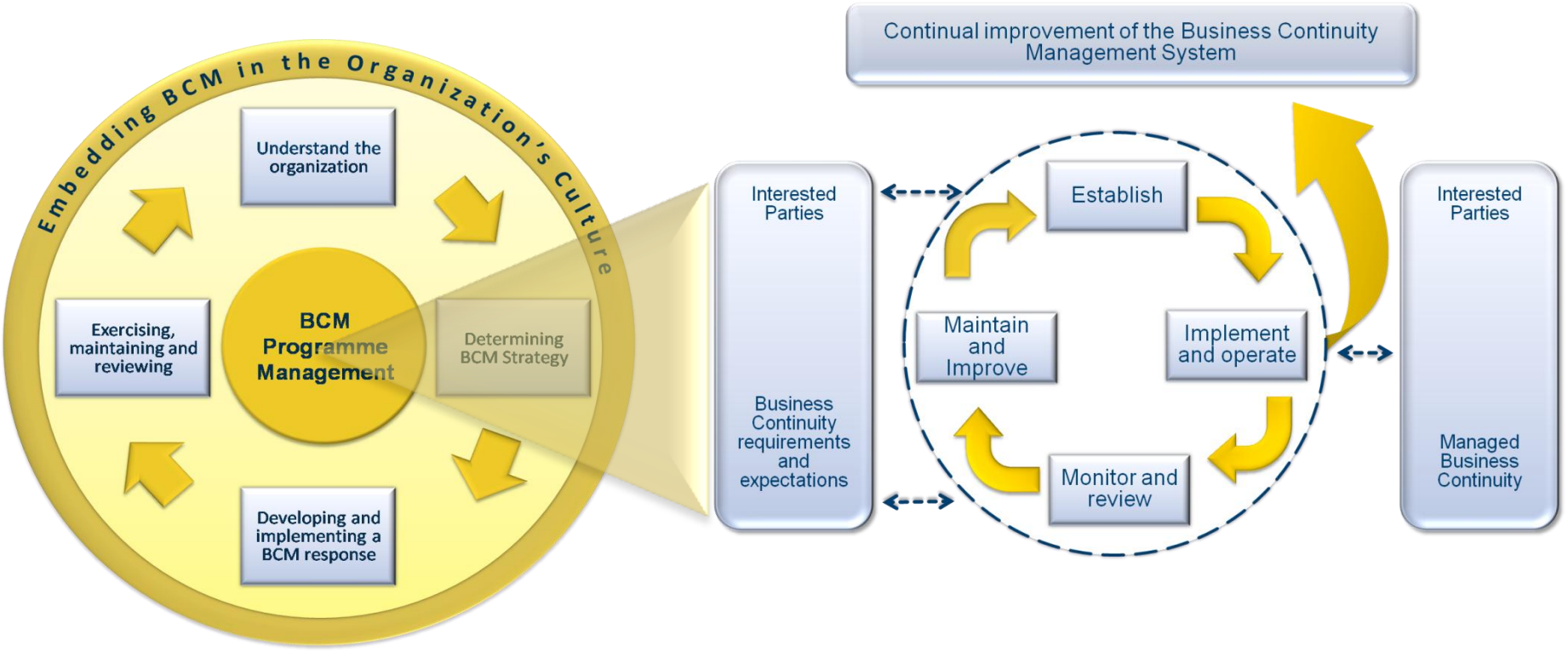
BS 25999-2 Specification

- Specifies the requirements for:
  - establishing, implementing, operating, monitoring, reviewing, maintaining and improving a documented BCM system (BCMS) within the context of an organization's overall business risks.
  - the implementation of business continuity controls customized to the needs of individual organizations.

The Business Continuity Management System (BCMS)



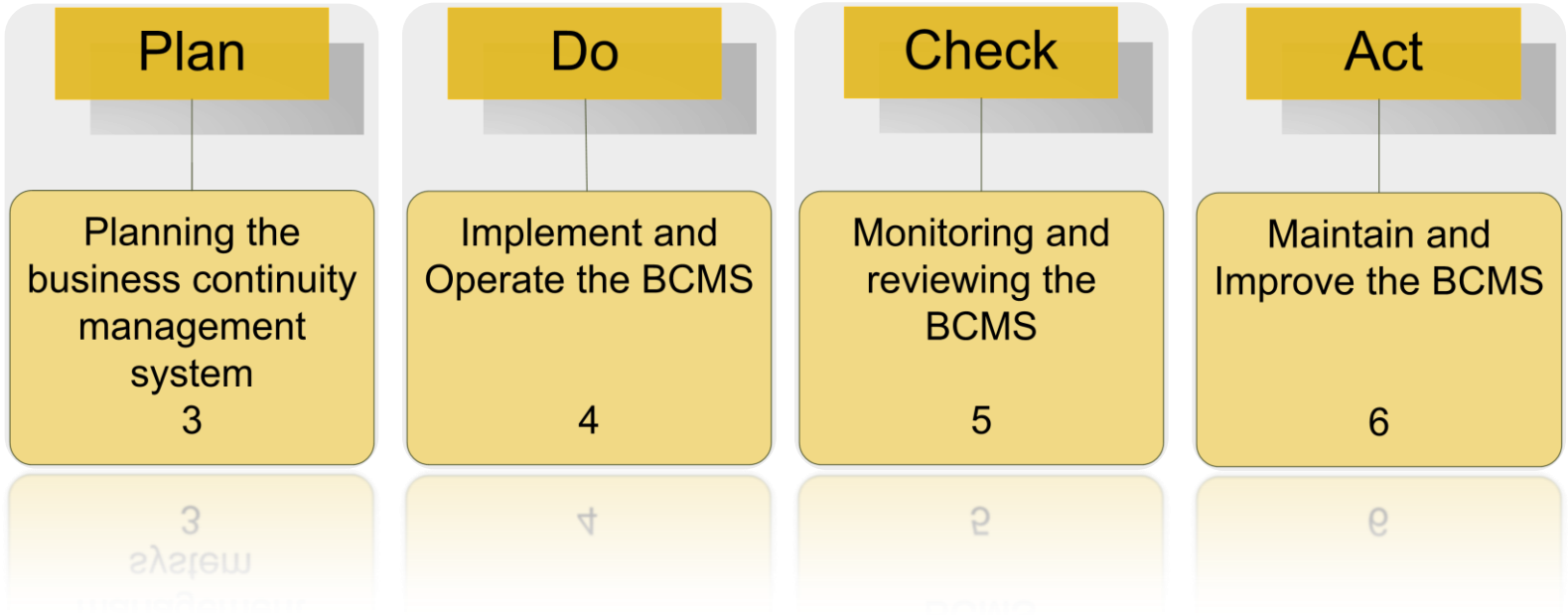
What's the difference between BCM and a BCMS?



BCM Lifecycle

BCMS

BS 25999-2 layout



Establishing and managing the BCMS (Plan)

- To define the scope and boundaries of your BCMS, and to ensure that:
  - Your organization's objectives are clearly stated, understood and communicated,
  - Top management's commitment to BCM is demonstrated,
  - Proper resources are allocated, and
  - those with BCM responsibilities are competent to perform their role.
- To ensure that your organization embeds business continuity into your routine operations and management processes

Establishing and managing the BCMS (Plan)

- Provide clear evidence of the effective operation of your BCMS and your organization's implementation of Business Continuity Management.

Implementing and operating the BCMS (Do)

- To enable you to identify critical activities and the resources needed to support your key products and services
  - understand the threats to them and choose appropriate risk treatments
- Identify BCM arrangements that will enable you to recover your critical activities within the recovery time objectives you set
- Enable you to develop and implement appropriate BCM plans and arrangements
  - to manage any incident and
  - to continue running your critical activities

Maintaining and improving the BCMS (Act)

- Maintain and improve the effectiveness and efficiency of your BCMS
- Taking corrective and preventive actions, as determined by the management review

Implementing and operating the BCMS (Do)

- Verify the ongoing effectiveness of your BCM arrangements
- Provides you with greater assurance following an incident that critical activities will be recovered as required

Monitoring and reviewing the BCMS (Check)

- To ensure that your management:
  - monitor and review the effectiveness and efficiency of your BCMS
  - review the appropriateness of your business continuity policy, objectives and scope, and
  - determine and authorise actions for remediation and improvement

Certification

Why Certification?

Competitive advantage	Supply chain requirement	Respond to shareholders, investors, analysts	Financial benefits and savings (insurance, audits…)
Reduce costs of tendering	Certified businesses outperform	Recruitment and retention	Rigour and independence of the audits
Consistency across sites	Ensure staff are complying with procedures	Protect brand and reputation	Drive continuous improvement

What is certification?

- Certification involves a third-party, such as BSI Management Systems, visiting an organization, assessing their management system against the requirements of a standard.
- This – hopefully - results in the issuing of a certificate of registration to show that the organization abides by the principles set out in the standard, so following industry best practice.

Why is certification important?

- Lets you reduce the cost of evaluating suppliers
- Helps you develop, implement, maintain and improve a management system – a proactive and proven approach to reducing risk
- Continual improvement - achieved through regular assessments of the management system
- Demonstrates that your organization is exercising duty of care
- Provides a goal for your organization to work towards

Why is certification important?

- Demonstrates to stakeholders that:
  - key services and products can continue to be delivered
  - applicable laws, regulations and contractual requirements are being observed
- Offers global consistency in BCM implementation
- Protects the interests of shareholders, brand and reputation
- Mandating certification from suppliers and outsource partners can help reduce supply chain risks

Why is certification important?

- Reduces the overall burden of internal and external BCM audits
- Adds value to the business by identifying opportunities for improvement
- Cost savings through
  - Fewer audits
  - Reduced insurance?
- **Above all, certification demonstrates a commitment to business continuity and is an investment in your survival.**

End of Presentation

Additional Optional slides

BS 25999 Part 1 - Code of Practice

- The code of practice for business continuity management
  - Establishes the BCM processes, principles and terminology
  - Provides a basis for understanding, developing and implementing business continuity within organizations of any size or from any sector
  - Provide a comprehensive methodology based on BCM best practice and the whole BCM lifecycle
  - Business driven
- Published in November 2006

End of Presentation