Business Continuity

An introduction and perspective on good practice

CHUBB

Alan Beard
Principal Property Risk Engineer
Risk Engineering Services

Agenda

- Presenter introduction
- Background and key message
- Terminology and definitions
- Scope and stakeholders for business continuity
- Business continuity standards and protocols
- Potential approaches and good practice
- Questions

Chubb Risk Engineering Services

- Chubb has a global network of ~550 risk engineers
- 18 Risk Engineers in the UK&I team covering Property, Casualty and incorporating industry practice groups (with a focus on Cyber and Life Sciences)
- An internationally recognised group of experienced risk engineering professionals with multiple qualifications and accreditations
- Average 20 years risk engineering experience
- Many years of provision of risk consulting and loss mitigation services to clients
- Industry and technical expertise with knowledge of both local and global good practice standards and legislation

Chubb's three core Risk Engineering services

Risk Evaluation

We gather and verify data on the client's business to fully understand the threats, controls and potential impact of losses; from the regulatory environment through to business interruption.

We do this primarily with onsite surveys, which we can provide pre-bind, at renewal, or even mid-term if the client's exposures change.

If an onsite survey isn't practical for the client we can complete a telephone interview or desktop study.

Risk Management

We work with clients to reduce exposures, improve risk controls and tackle claim activity, where necessary, by recommending risk improvements.

Risk Partnership

We provide additional services to meet identified client needs and can provide advice, education and training in specific areas of the business. These services help to complete Chubb's holistic cyber risk management solution.

Presenter introduction

Alan Beard
Principal Property Risk Engineer
Risk Engineering Services

- >20 Years as a Risk Engineer at insurers, brokers and clients
- Worked in >30 countries
- Specialist experience in business interruption and business continuity management

CHUBB

Background and key message

Background – Why business continuity?

Some statistics, requests and comments that may be received….

- 'We need a business continuity plan!'
- 'Over 70% of businesses involved in a major fire either do not reopen, or subsequently fail within 3 years of fire.'[1]
- 'Unplanned downtime costs between $926 and $17,244 per minute'[2]
- 'Do you have a BCP template that we can use?'
- 'What's the value of business continuity?'

Some care is required to address items of this nature.

Sources: [1]Continuity Central 'Business Continuity Statistics: Where Myth Meets Fact';
[2]InvenioIT '2017 Disaster Recovery Statistics that Business Must Take Seriously'

Background – Is there value in business continuity?

Yes! Both qualitative and quantitative

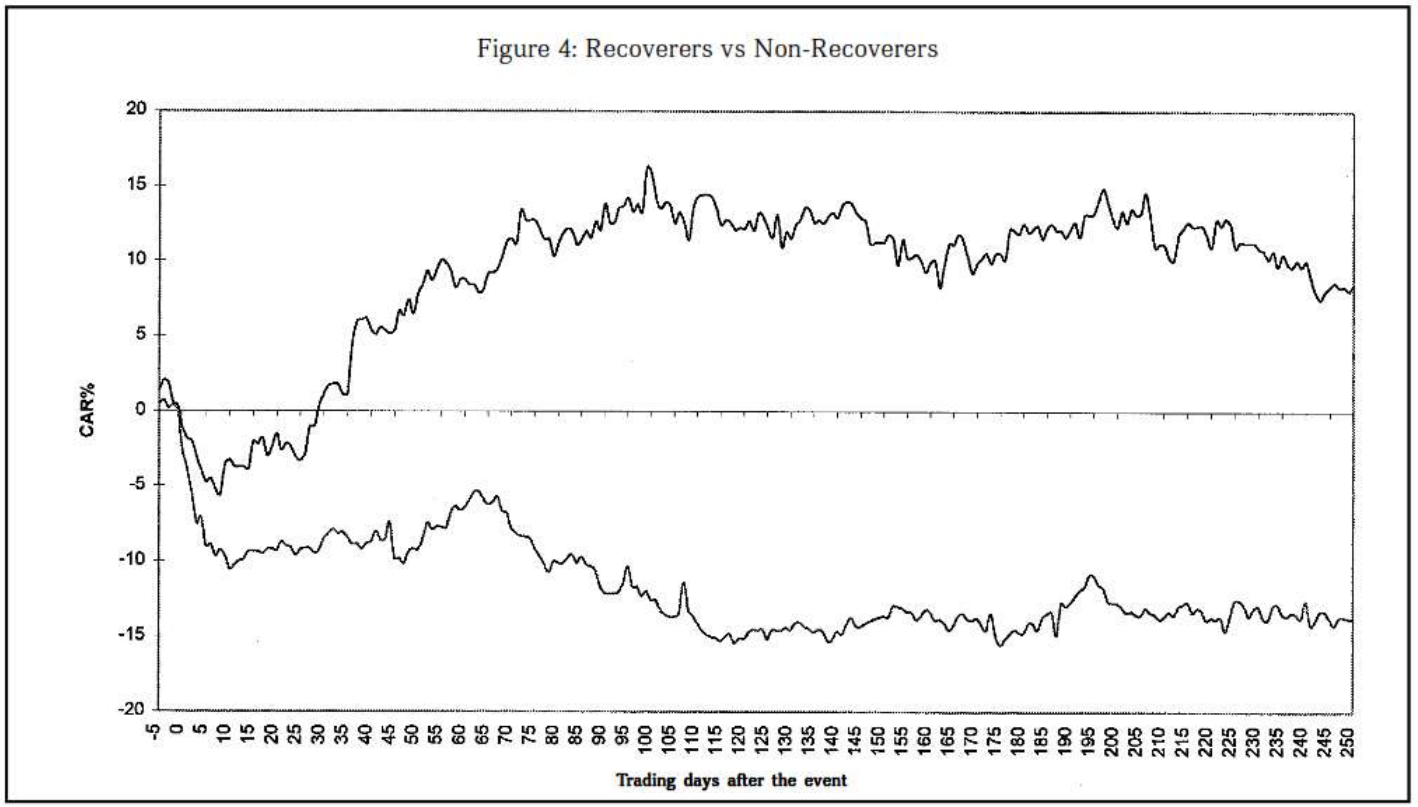
Qualitative:

- A valuable risk treatment of use within a risk management program
- Encourages review of vulnerabilities and risks
- Gives structure to potential response options
- Supports confidence from customers, investors, regulators and other stakeholders
- Favourably reinforces reputation

Background – Is there value in business continuity?

Yes! Quantitative:

- Research by Templeton College, Oxford 1994 sponsored by Sedgewick Group[1]
- '…catastrophes…offer an opportunity for management to demonstrate their talent in dealing with difficult circumstances.'



Sources: [1]Knight and Pretty, Oxford, 'The Impact of Catastrophes on Shareholder Value'.

Background – Key message(s)

Evaluate requests for business continuity support:

- Develop understanding of the objectives
- Agree the scope and any limitations
- Agree the stakeholders and RACI
- Understand Who, How, When and How Much

Attributed to an unnamed soldier by Dwight D. Eisenhower, Supreme Commander of the Allied forces in Europe during World War II and 34th President of the United States of America:

'I have always found that plans are useless, but planning is indispensable.'

CHUBB

Terminology and definitions

Terminology and definitions – Abridged!

A few (of many) definitions and acronyms:

- **Business Continuity Management** ("BCM") is a holistic management process that identifies potential threats to an organisation and the impacts to business operations that those threats, if realised, might cause. It provides a framework for building organisational resilience with the capacity for an effective response that safeguards the interests of its key stakeholders, reputation, brand and value creating activity.[1]
- **Crisis** – A situation with high level of uncertainty that disrupts the core activities and/or credibility of an organization and requires urgent action.[2]
- **Crisis Management (CM)** - Development and application of the organizational capability to deal with a crisis.[3]
- **Disaster Recovery (DR)** - The process, policies and procedures related to preparing for recovery or continuation of technology infrastructure, systems and applications which are vital to an organization after a disaster or outage.[4]
- **Enterprise Risk Management (ERM)** - ERM includes the methods and processes used by organizations to manage risks and seize opportunities related to the achievement of their objectives.[4]

For other definitions the ISO standards, DRJ Glossary and BCI documentation are useful resources.

Sources: [1]ISO22301[2]ISO 22300; [3]BS 11200:2014; [4]Disaster Recovery Journal Glossary; [4]Business Continuity Institute

CHUBB

Scope and stakeholders for business continuity

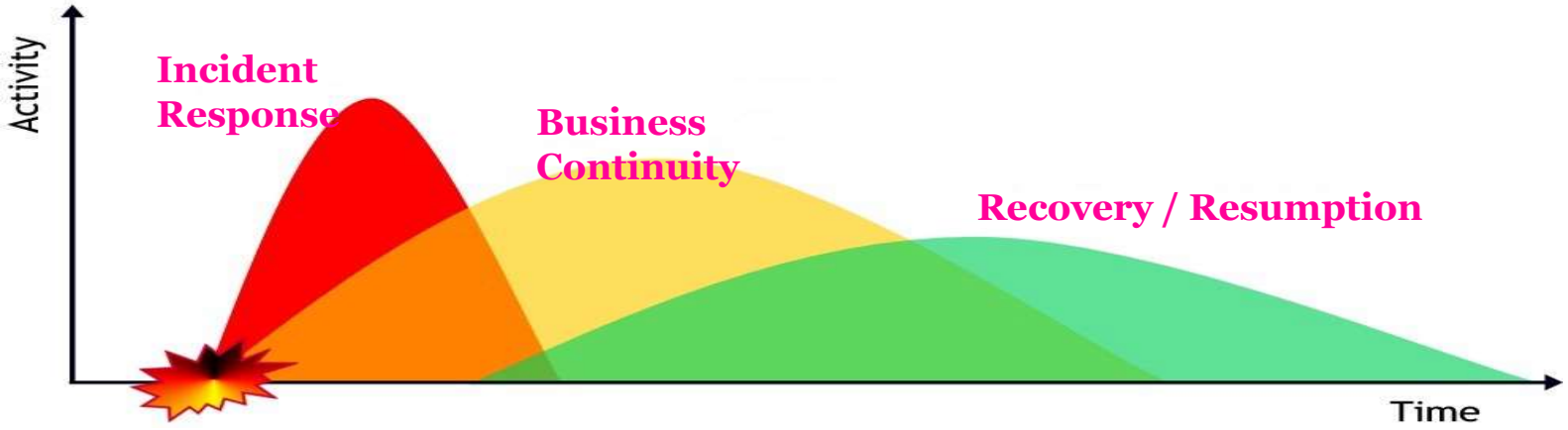
Scope and stakeholders for business continuity

- Why business continuity?

Some potential scope(s) for business continuity:

- Emergency Response
- Crisis Management
- Organisational Resilience
- IT Disaster Recovery
- Business Recovery
- Supplier or Customer Management
- Natural Catastrophe response
- Low frequency/High Consequence events
- Regulatory Compliance
- Support for Enterprise Risk Management

It is recommended that considerable time and focus is applied to the objectives and scope of a business continuity implementation.



CHUBB

Scope and stakeholders for business continuity

- Who is business continuity for?

Some potential stakeholders for business continuity:

- Local Business – Response to credible incidents
- Corporate Business
  - Management reporting
  - Marketing
  - Contractual or Customer requirements
  - Internal audit compliance
  - Regulatory compliance
  - (Enterprise) Risk Management/Sarbox support
- Customer - Reassurance
- Regulators – Proof of compliance
- Insurance Broker – Client marketing
- Insurer – Loss reduction, exposure/capacity management

Managing competing objectives between stakeholders may be a significant issue.

CHUBB

Business continuity standards and protocols

Business continuity standards and protocols

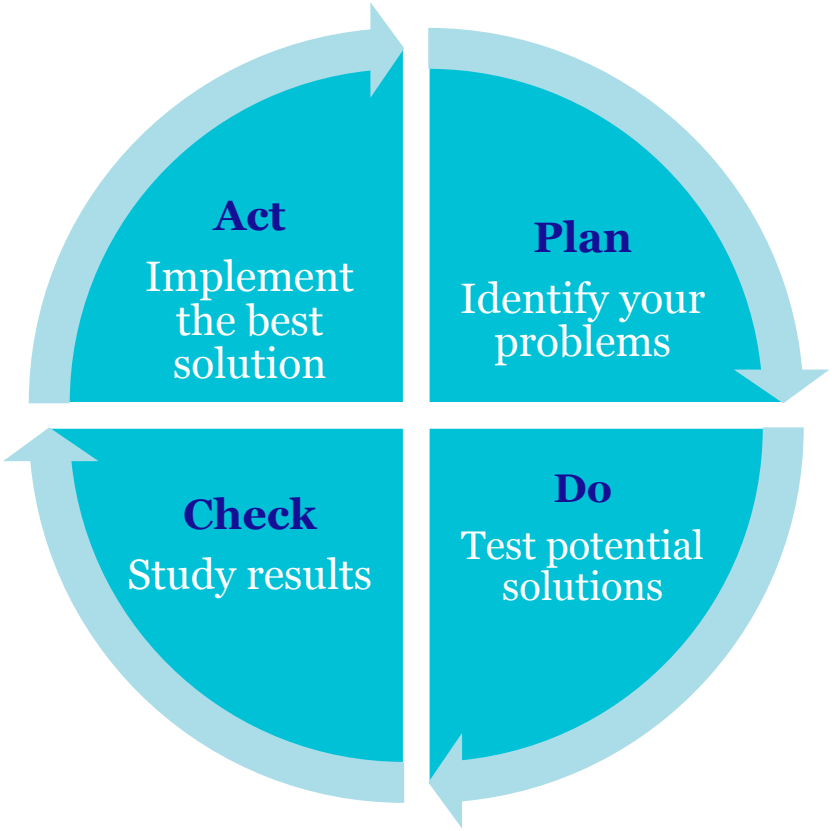
Business continuity is not short of standards and guidance:

- ISO 22301:2012 – Societal security -- Business continuity management systems
- British Standard 25999-1:2006 - Business Continuity Management *(Withdrawn in 2012 due to ISO standard publication)*
- Business Continuity Institute - Good Practice Guidelines 2001-2018 *(Generally aligned with ISO whilst providing guidance across two Management Practices and four Technical Practices)*
- NFPA 1600 Standard on Continuity, Emergency, and Crisis Management 2019
- ISO/IEC 27000:2018 - Information technology. Security techniques. Information security management systems.
- ISO/IEC 27031:2011 Information technology -- Security techniques -- Guidelines for information and communication technology readiness for business continuity
- ISO 22316:2017 – Security and resilience. Organizational resilience. Principles and attributes
- ISO 31000:2018 - Risk management – Guidelines
- PD CEN/TS 17091:2018 - Crisis management. Guidance for developing a strategic capability
- AS/NZS 5050:2010 - Business continuity - Managing disruption-related risk *(also HB 292, HB 293 and APRA CPS 232)*
- Many templates and software systems

Most standards align with the **Plan-Do-Check-Act (PDCA)** continuous improvement cycle developed by W. Edwards Deming and others in the 1950s.

Business continuity standards and protocols

Plan-Do-Check-Act (PDCA) continuous improvement cycle developed by W. Edwards Deming and others in the 1950s.



Business continuity standards and protocols

A ‘standards driven’ approach may be more appropriate for certain organisations and industry sectors

CHUBB

Potential approaches and good practice

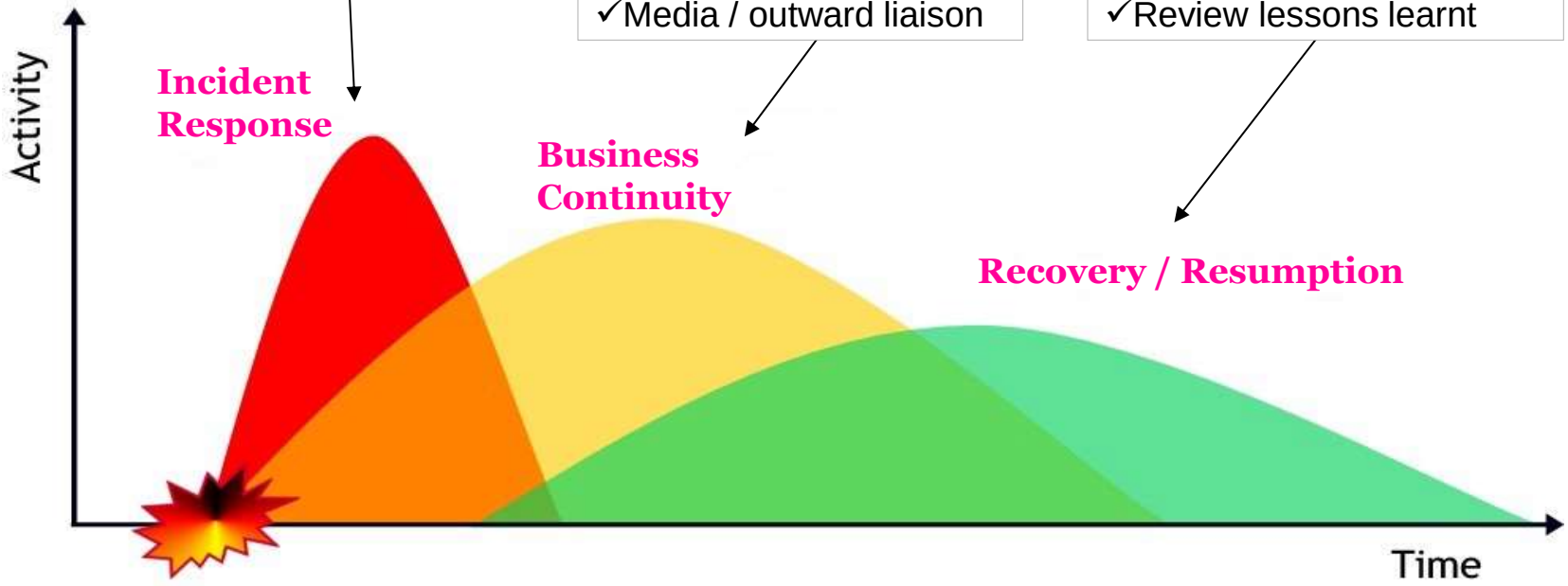
Potential approaches and good practice

All organisations:

Incident Response
Focused on safeguarding people, company assets and the environment
✓Preserving Life
✓Damage assessment
✓Stabilisation & security

Business Continuity
Focused on managing the issues & implications and maintaining operations
✓Strategy perspective
✓Governance & direction
✓Stakeholder management
✓Media / outward liaison

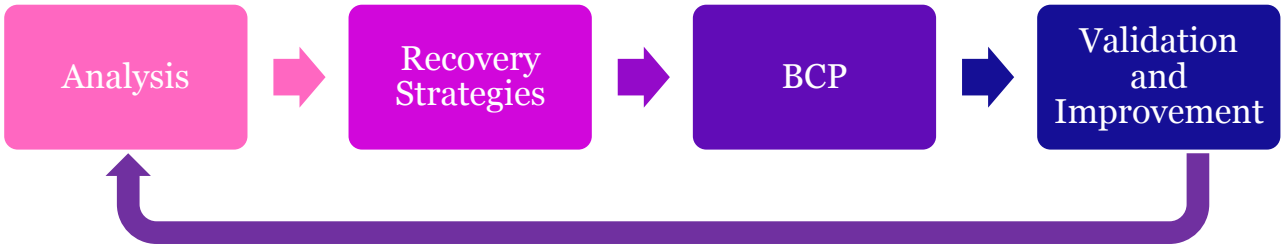
Recovery / Resumption
Focused on phased stabilisation, restoration and recovery of critical business processes
✓Recovery of infrastructure
✓Return to business as usual
✓Review lessons learnt



Potential approaches and good practice

‘Complex’ organisations:

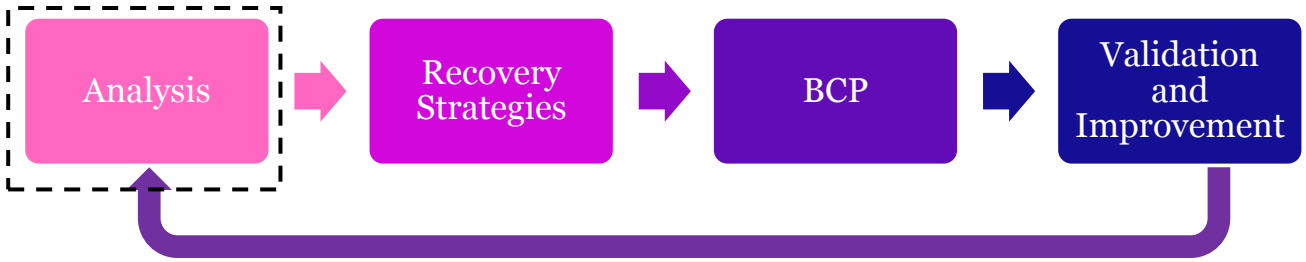
- Consider a standards aligned approach to business continuity
- Organisation-wide management reporting for business continuity
- May require a business continuity management software package to control data and provide reporting
- May require internal or external auditing and certification
- Business continuity lifecycle stages typically include:
  - Analysis (Business Impact Assessment/BIA)
  - Development and decision-making on solution strategies (Recovery/Risk Management Strategies)
  - Business continuity response development (the Plan!)
  - Business continuity exercises, reviews and enhancements (Validation and Improvement)



Potential approaches and good practice

‘Complex’ organisations:

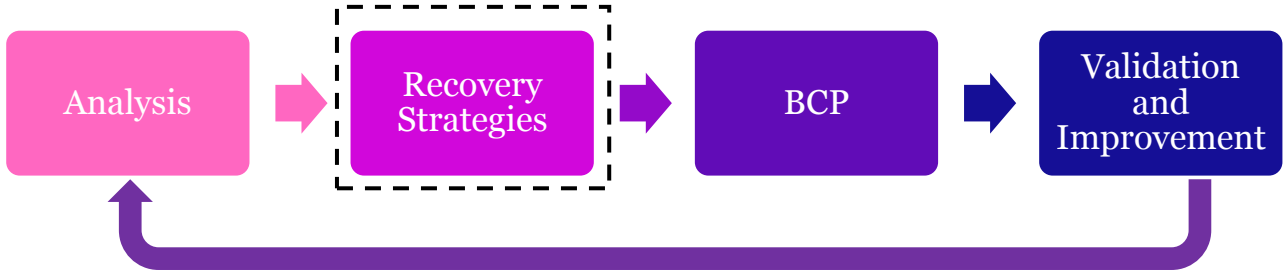
- Analysis (Business Impact Assessment/BIA)
  - Don’t reinvent the wheel
  - Existing risk assessment approaches are recommended to be utilised (eg. corporate Enterprise Risk Management, COSO/SarbOx, ISO/TS 22317:2015)
  - Clear guidance for risk severity and likelihood recommended



Potential approaches and good practice

‘Complex’ organisations:

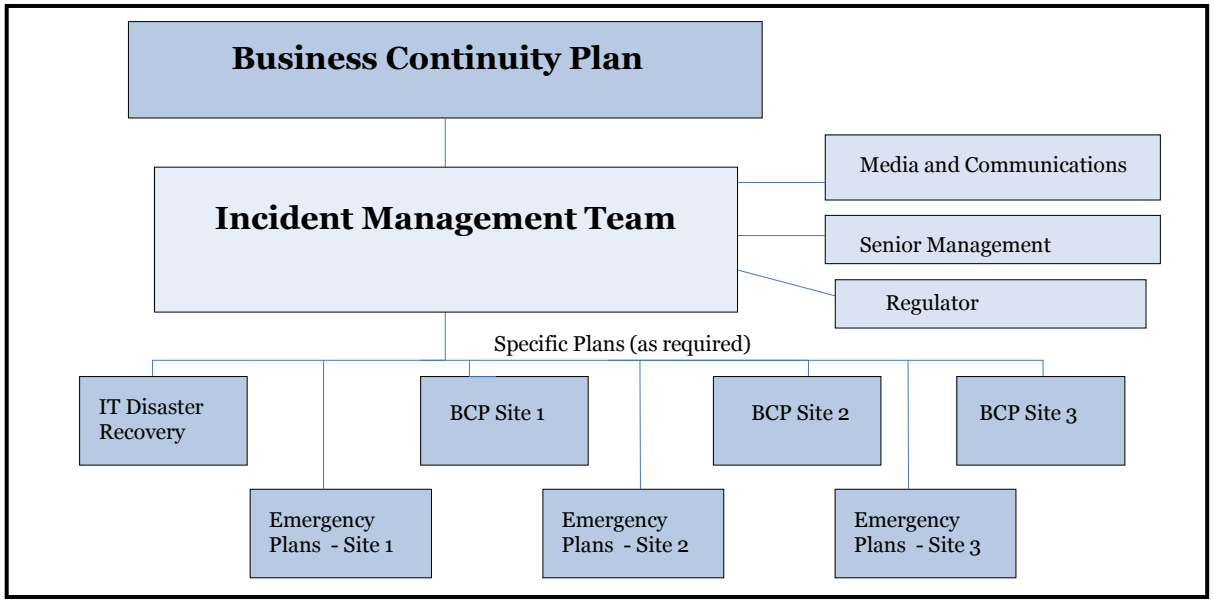
- Recovery/Risk Management Strategies
  - Likely that the same or similar strategies will apply to multiple parts of the organisation (eg. Relocate to alternate location, utilise stockpiled materials, redundant capabilities, etc)
  - Strategies could include: **Avoid, Reduce, Transfer, Accept** (the risk)
  - Beware strategies exposed to failures common to the incident, eg. Automated back-ups corrupted by ransomware along with the live data
  - Recovery strategy and recovery capability alignment is needed (especially IT resource)
  - Discussions on strategy should be managed so that they don’t immediately become plan development

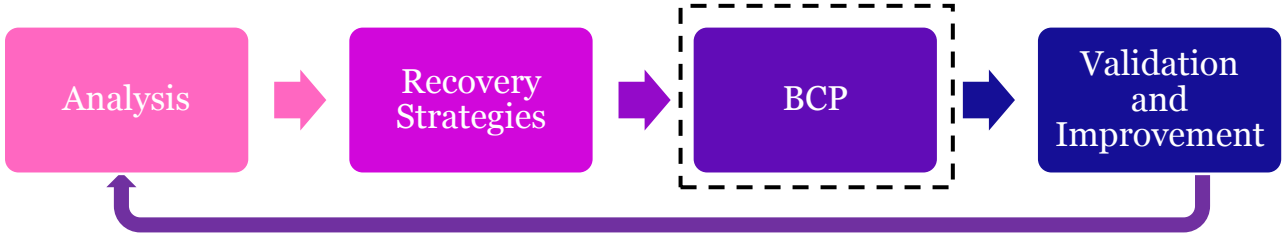


Potential approaches and good practice

‘Complex’ organisations:

- Business Continuity Plans (BCP)
  - Recommended to drive action (not report analysis)
  - Have clarity on authorisation, delegation and escalation protocols
  - Structured to the needs of specific users

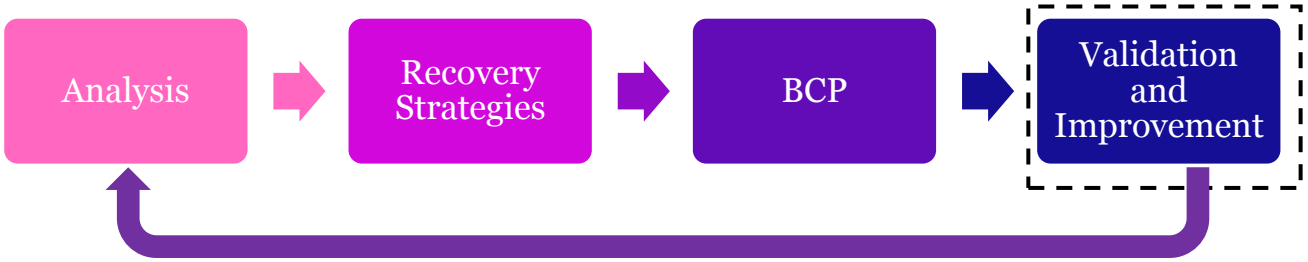




Potential approaches and good practice

‘Complex’ organisations:

- Validation and Improvement stage
- Business continuity exercises, reviews and enhancements
  - Don’t be over ambitious initially, multiple small scale exercises may deliver more value than planning a mega-event
  - Desktop exercises can be valuable, if the correct participants are engaged
  - Some aspects can only be tested at full-scale (eg. IT disaster recovery rather than testing individual systems back-up)
  - There are no failed exercises, every learning is valuable (and better learnt during an exercise than during a real event)



Potential approaches and good practice

Single location, small team or SME organisations:

- Typically incorporate risk management and resilience within the day job
- Relationships with suppliers and customers are often direct
- Often experience rich and time poor
- A focus resilience to known vulnerabilities (eg. Fire, Flood, Utility Outage, Spill) may be effective:
  - Important not to overlook previously unrecognised exposures (consider sourcing information from multiple stakeholders)
- Template BCP may be appropriate
- Approach should be resilient to specific individuals not being available

Summary

- Business continuity is a multifaceted activity and can require careful scoping and planning
- There is real value in business continuity, but beware of unsubstantiated justifications and zombie statistics
- The best approach depends on the type of organisation, the stakeholders and the intended outcome

Alexander Graham Bell (Scottish–born) inventor (1847 – 1922)

'Before anything else, preparation is the key to success.'

CHUBB

Questions

Chubb. Insured.