ResilientiT

IMPORTANCE OF ICT IN BUSINESS CONTINUITY

Presenter: Keivan Memarzadeh

Associate Member of the Business Continuity Institute (AMBCI)

ISO 22301 Lead Implementer, ISO 27001 Lead Auditor

Resilient iT Limited

BASICS

- Objectives of any business

Delivery

- Complete
- Comprehensive
- On Time

Profitability

- Efficient
- Effective
- Business Continuity

Compliance

Value

- What is Business Continuity ?

Capability of an enterprise to continue with the delivery of products or services at acceptable predefined levels following disruptive incident (ISO 22301)

FRAMEWORKS AND GUIDELINES

- Business Continuity Institute – Good Practice Guidelines 2018
  - The GPG takes a collaborative approach to business continuity, ensuring organizations and individuals understand how to work with related management disciplines to successfully implement their business continuity solutions.
- ISO 22301:2012 Business Continuity Management System
  - Specifies requirements to plan, establish, implement, operate, monitor, review, maintain and continually improve a documented management system to protect against, reduce the likelihood of occurrence, prepare for, respond to, and recover from disruptive incidents when they arise.
- ISO 27031:2011 – ICT Readiness for Business Continuity (IRBC)
  - Describes the concepts and principles of information and communication technology (ICT) readiness for business continuity, and provides a framework of methods and processes to identify and specify all aspects (such as performance criteria, design, and implementation) for improving an organization's ICT readiness to ensure business continuity

WHAT IS BUSINESS CONTINUITY FOR?

- **Incident Prevention** - Protecting Products/Services from threats
- **Incident Detection** - Detecting incidents at the earliest opportunity will minimize the impact to delivery of services/products
- **Response** - Responding to an incident in the most appropriate manner
- **Recovery** - Identifying and implementing the appropriate recovery strategy will ensure the timely resumption of services and maintain the integrity of data.
- **Improvement** – Lessons learned from small and large incidents should be documented, analysed and reviewed.

BUSINESS CONTINUITY LIFECYCLE – BCI & ISO

ISO 22301

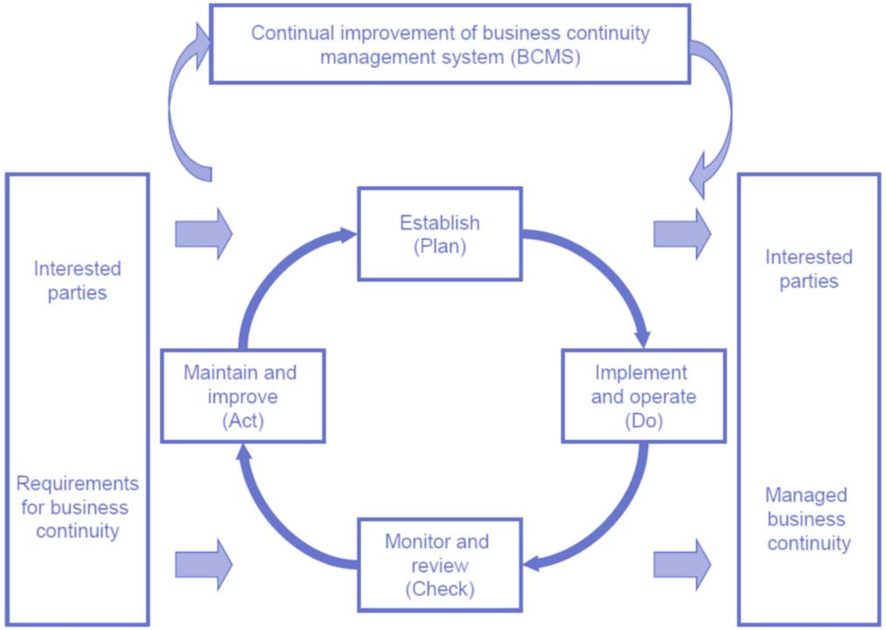
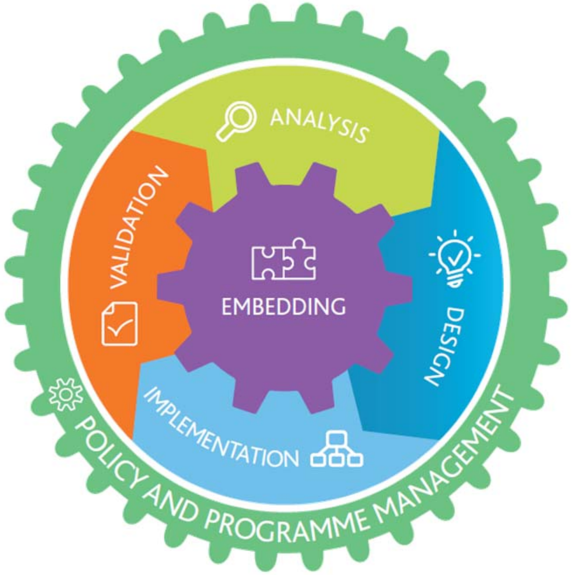
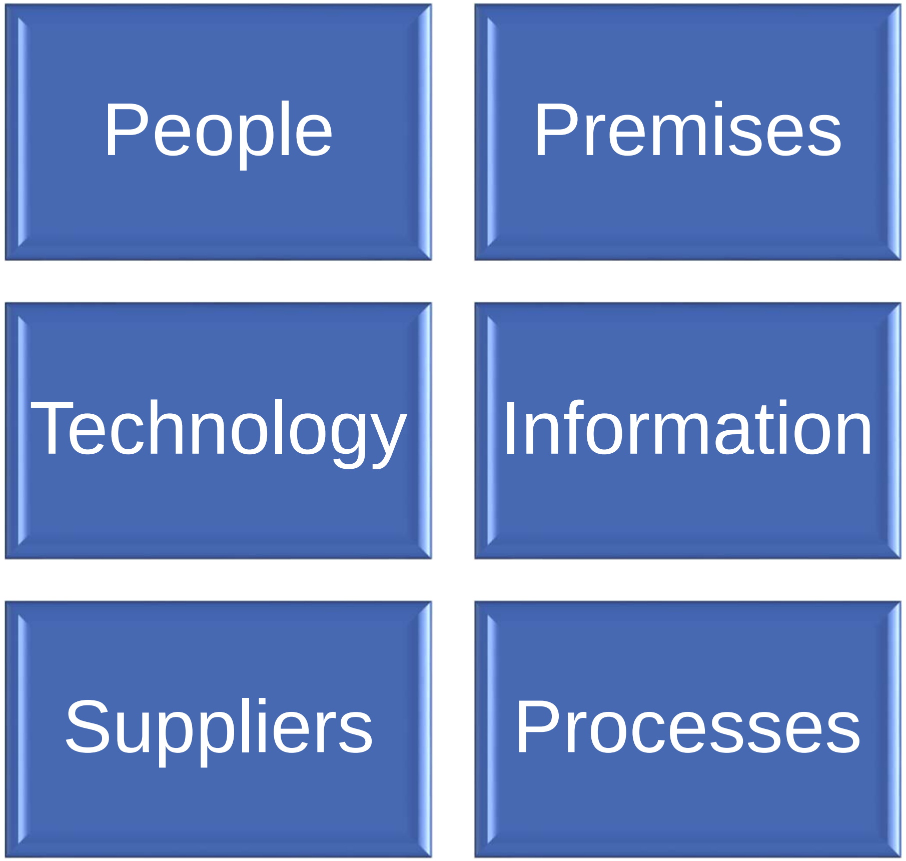

Continual improvement of business continuity management system (BCMS)
Interested parties
Requirements for business continuity
Establish (Plan)
Implement and operate (Do)
Monitor and review (Check)
Maintain and improve (Act)
Interested parties
Managed business continuity

Figure 1 — PDCA model applied to BCMS processes

BCI GPG 2018



KEY PLANNING ELEMENTS



People

Premises

Technology

Information

Suppliers

Processes

BUSINESS IMPACT ANALYSIS – RISK ASSESSMENT

- BIA - Process of analysing activities and the effect that a business disruption might have upon them.

- Use BIA to identify
  - Key processes that deliver a product or service
  - Resource dependencies within the process on
    - People, Premises, Technology, Information, Supplier, Processes
  - Maximum Acceptable Outage (MAO)
  - Recovery Time Objective (RTO)
  - Recovery Point Objective (RPO)

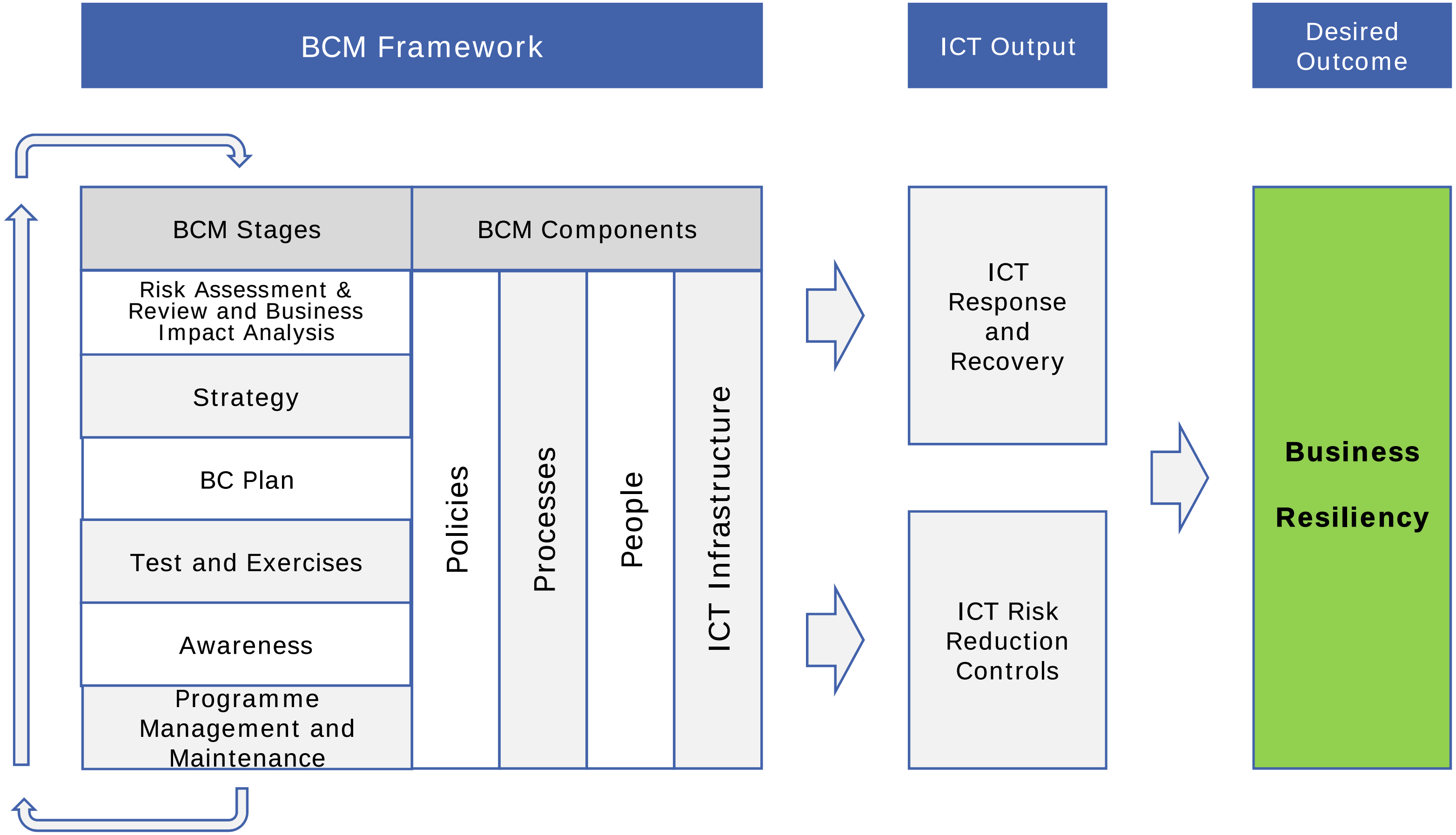
- Conduct Risk Assessment on resource dependencies to identify
  - Single Points of failure
  - Unacceptable concentration of risk in particular areas

DESIGN STRATEGIES

- Mitigation strategies could be
  - Diversification
  - Replication
  - Stand by
  - Post Incident acquisition
  - Do nothing

- Based on needs such as
  - Budget
  - Resource availability
  - Potential costs and benefits
  - Technological constraints
  - The organization's risk appetite
  - The organization's existing BC strategy
  - Regulatory obligations

ROLE OF ICT IN BUSINESS CONTINUITY



BCM Framework

ICT Output

Desired Outcome

BCM Stages

BCM Components

Risk Assessment & Review and Business Impact Analysis

Strategy

BC Plan

Test and Exercises

Awareness

Programme Management and Maintenance

Policies

Processes

People

ICT Infrastructure

ICT Response and Recovery

ICT Risk Reduction Controls

Business Resiliency

BENEFITS OF ICT READINESS FOR BUSINESS CONTINUITY - (IRBC)

- Understands the risks to continuity of ICT services and their vulnerabilities
- Identifies the potential impacts of disruption to ICT services
- Encourages improved collaboration between its business managers and its ICT service providers (internal and external)
- Develops and enhances competence in its ICT staff by demonstrating credible responses through exercising ICT continuity plans and testing IRBC arrangements

BENEFITS OF ICT READINESS FOR BUSINESS CONTINUITY (CONT.)

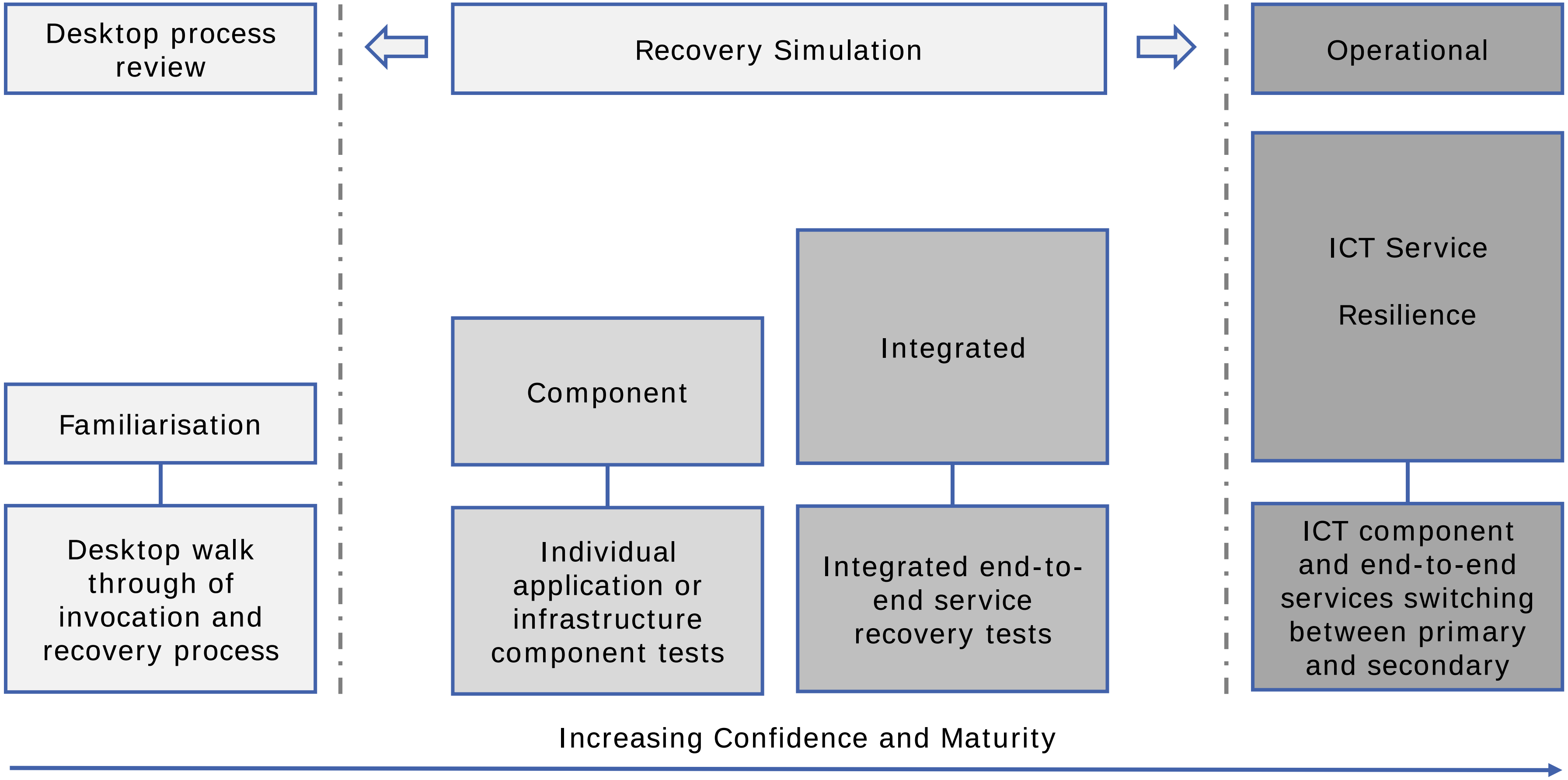
- Provides assurance to top management that it can depend upon predetermined levels of ICT services and receive adequate support and communications in the event of a disruption

- Provides assurance to top management that information security (confidentiality, integrity and **availability**) is properly preserved, ensuring adherence to information security policies

- Provides additional confidence in the business continuity strategy through linking investment in IT solutions to business needs and ensuring that ICT services are protected at an appropriate level given their importance to the organization

VALIDATION & EXERCISE

- Create exercise plans and scenarios to test out recovery readiness


Desktop process review
Recovery Simulation
Operational
ICT Service
Resilience
Integrated
Component
Familiarisation
Desktop walk through of invocation and recovery process
Individual application or infrastructure component tests
Integrated end-to-end service recovery tests
ICT component and end-to-end services switching between primary and secondary
Increasing Confidence and Maturity

MAINTENANCE & CONTINUAL IMPROVEMENT

- Conduct an Audit of BC programme
- Create Measurement criteria – then Measure
- Take corrective action when a failure occurs
- Conduct Management Reviews of audit results, corrective actions, residual risks, lessons learnt and so on

BUSINESS CONTINUITY AWARENESS

Working together to improve organizational resilience

Business Continuity Awareness Week
bci
#BCAW2018
14th – 18th May 2018
DISCUSSION
PLANNING
COOPERATION
MEETING
DEVELOPMENT
COORDINATION
BREAKING SILOS
AGREEMENT
UNDERSTANDING
CHALLENGED
COMMUNICATION
ALIGNMENT
TEAMWORK
PARTNERSHIP
BUY-IN
SHARING
END GOAL
TRUST
TOGETHER
BAU

Join the discussion

@thebceye #BCAW2018 thebci

www.thebci.org/bcaw2018

Business Continuity

Emergency Management | Risk Management | Communications | Health and Safety
Crisis Management | Facilities Management | ICT Security | Human Resources | Physical Security

Q & A

Thank you!

REFERENCES

Business Continuity Institute

www.thebci.org

ISO

www.iso.org