Capgemini
CONSULTING.TECHNOLOGY.OUTSOURCING

SOGETI

End-to-End Business Continuity Testing

Finding the areas for improvement in plans, processes and procedures to protect shareholder value

Performance driven. Quality assured.

Introduction

When it comes to Business Continuity Management (BCM), it is commonly accepted in today's business world that one cannot continue to survive with the belief that *it'll never happen to us*. Business Continuity is an integral part of doing business. Rightly or wrongly, a number of businesses still believe that business continuity is just an offshoot of risk management. One definition of BCM is the "*holistic process that identifies potential threats to an organisation and the impacts to business operations that those threats, if realised, might cause, and which provides a framework for building organisational resilience with the capability for an effective response that safeguards the interests of its key stakeholders, reputation, brand and value-creating activities*[1]". A sub-component is IT Service Continuity Management (ITSCM), which are the processes related to the recovery and continuation of technology-based services to support the business organisation.

BCM and ITSCM utilise risk management practices, but these are just part of the picture – they also use and apply security, project, incident and service management principles. It is planning the processes and activities that the organisation will need to implement to minimise the impact a disruption will have on the enterprise - *when* the disruption occurs.

A holistic continuity management programme addresses all types of scenarios regarding business disruptions :

- sustained loss of environmental resources at either the primary worksite or data centre
- fire, smoke, water damage at the worksite
- loss of critical technology services (including: software and/or hardware problems)
- any event that seriously compromises the security of the property and/or
- staff at the worksite
- acts of God or natural disasters
- terrorism and/or worksite closures

With so many aspects of the Continuity regime to address, a level of document order, hierarchy and integration is essential to enable the organisation to successfully select and deploy the appropriate continuity plans from the myriad of plans available within its arsenal.

Depending on the scale and type of services disruption event incurred, various plans within the Continuity Management System will be invoked. Unless the individual continuity plans include information on how they interoperate and coexist with the other continuity plans, the implementation of the continuity work processes may be as disruptive to the business as the untoward event itself.

1 British Standards: BS 25999-2

Aspects of Continuity Management

Since the inception of the continuity planning concept in the 1970s, originally stemming from IT infrastructure disaster recovery, the Continuity Industry has evolved to cover all aspects of the business organisation, including:

- Crisis management
- Disaster recovery management
- Pandemic planning
- Business continuity planning
- Contingency planning
- Emergency management
- Incident management
- Disruption management
- Business resumption planning
- Business resilience
- IT service continuity planning
- Business process continuity planning.

Originally each of these types of planning had their own unique definitions of terminology, but with time they have been used interchangeably and in contrast to their original meanings.

The definition, and interpretations, of what Business Continuity Management actually is varies from organisation to organisation – as do the supporting objectives and measurements.

The problem is that there is no one standard across all industries and countries. Each has their own interpretation of what is right. That said, however, most leading Continuity industry organisations agree that Business Continuity Management provides the availability of processes and resources *in order to ensure the continued achievement of critical objectives*[2].

It is generally accepted throughout the Continuity industry that each of the plans and/or processes comprise an aspect of the organisational crisis management structure; in similar fashion to that outlined in Figure 1.

Continuity Management is about planning for the continuation of business activities during times of unforeseen disruptions to normal business practices. The efficacy of that planning is evidenced through the presence of documented processes and procedures that will be employed throughout the entire untoward event.

Figure 1: Hierarchy of Continuity Plans

The Business Continuity Management plan endeavours to answer all key critical aspects of keeping the business operating whilst the event is in progress, including:

- **Who**: the Crisis Management Command Structure.
- **What**: which systems and business functions must continue, either via secondary functions or alternate workaround processes.
- **When**: the timing of when to activate different components and aspects of the subsidiary plans.
- **Where**: the locations (and/or secondary locations) that will be used during the disruptive event.
- **How**: the processes and procedures for how to perform the critical aspects during the absence of normal business operations; and the interoperability of the plan types.

Crisis vs. Disaster

Often we find the terms 'crisis' and 'disaster' being used interchangeably. However, in practical terms, the two are quite different. Each term results in a different approach to escalation and the subsequent response to its resolution.

A crisis is where management is required to deliver a proportion of their time, attention, energy and resources away from normal operations to managing an untoward event. If the crisis escalates and overwhelms management capabilities to cope, control becomes lost and the event is regarded as a *disaster*. It is during the time of disaster that Continuity plans are invoked and are expected to function as planned.

2 Standards Australia: HB-221:2004, HB-292:2006

Integration of BCM and ITSCM

Information Technology systems and services have become a critical component of most business processes today, often to the point where many processes are completely unable to function during any disruption to the technology that they are reliant upon.

As IT system services are so essential to the operation of many business processes, it is critical that a holistic end-to-end continuity strategy be developed, implemented and regularly tested, using multiple plans conjointly and concurrently during the tests.

Impact of an IT Service Disruption

During an IT service disruption, one in which the continuity plans are activated, unless regularly reviewed and tested, it is likely that the plans will not be current or contain a sufficient quantity of gaps in processes and procedures to inhibit their usefulness when implemented.

It is for this reason that the Business Continuity Plan, the Business Process Continuity Plans, the IT Service Continuity (Disaster Recovery) Plans and the Recovery Validation Procedures need to be clearly documented, integrated and regularly tested to ensure their currency with today's business operations.

A major or catastrophic IT services disruption will require the activation of one or more ITSC/DR Plans. And, it will mandate the activation of the Business Process Continuity plans, aspects of the Business Continuity Plan and potentially the organisational Crisis Management plan. Continuity documents need to be effectively and accurately integrated, covering all aspects of continuity from time of incident, through Plan activations, data resynchronisation and/or reconstruction, and the eventual resumption of business processing.

In contrast to the traditional DR approach of planning solely for the least probable scenario involving a total loss of the data centre, other resiliency strategies such as high-availability and active-active implementations, disaster tolerant systems, and pseudo-real time data replication across multiple sites are becoming more prevalent in the delivery of IT Service Continuity.

As each new strategy and solution is implemented, the need for integrated continuity planning increases – as does regular testing that the plans continue to maintain their currency with the solutions deployed.

Continuity Testing

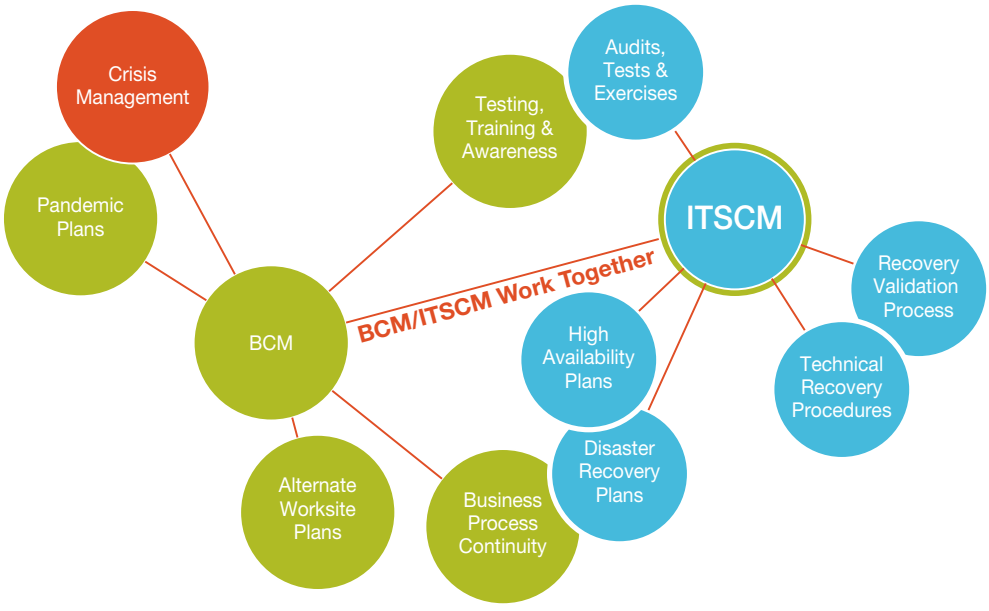
Many organisations perform annual disaster recovery exercises, in an attempt to prove their organisation's (or IT supplier's) ability to recover the IT infrastructure and/or software systems in the event of a catastrophic loss of data centre. During these exercises, more often than not, the systems recovered undergo only a cursory level of unit testing and rarely (if ever) an integrated end-to-end test with the other continuity plans.

In reality, the most likely plan of the Continuity Management programme to be implemented is the Business Process Continuity Plan (BPCP). The BPCP may be activated for any IT services disruption, whether the ITSC/DR Plan is invoked or not. It is the responsibility of this plan to outline the activities the business area will perform throughout the entire event of an IT service disruption - from time of incident to the resumption of normal business function.

Further to the BPCP, the ITSCP/DRP needs to clearly articulate its relationship with the BPCP, and the ITSC/DR Plans of its upstream, downstream and critically dependent systems. Integration of the various continuity plans, processes and procedures (see Figure 2) is an essential factor in providing evidence to the organisational stakeholders that the Enterprise is well prepared to weather any IT services disruption. Far too often, many ITSC/DR Plans rely on the assumed knowledge of the implementer and are rarely revised to maintain currency with changes in technology, system infrastructure or software upgrades.

Leaving the documentation unchecked and unreviewed introduces a new, unforseen and often untested risk that when the time comes to use the documents in a real event – that they will be incorrect, out of date, or contain too much assumed knowledge to provide any real assistance in recovering the system and/or maintaining continuity of business function.

Figure 2: BCM-ITSCM Integration or Interoperability



End-to-End Continuity

Testing for integrated End-to-End Continuity is, ideally, a detailed and systematic review of the organisational continuity plans, processes and procedures to determine their level of adherence to, and compliance with, the organisations pre-established standards and policies, and their alignment with the industry best practices and international continuity standards.

Industry bodies of best practice and standards include: The Business Continuity Institute (BCI), Disaster Recovery Institute International (DRII), International Organization for Standardization (ISO), Office of Government Commerce's IT Information Library (ITIL), British Standards Institute (BSI), Prudential Standard, Standards Australia (SAI Global) and the US National Institute of Standards and Technology (NIST).

A holistic continuity solution anticipates the entire service disruption, end-to-end and employs integration and interoperability of its individual plans. Best practice is to evaluate the Continuity plans, processes and procedures, through simulation of one or more major or catastrophic IT service outage (disaster) scenarios across the entire disruption lifecycle.

Proving the *ability* to recover and teaching exercise participants *how to perform business continuity* are common objectives during most Business Continuity or IT Service Continuity exercises and rehearsals. Testing, on the other hand, is about finding the areas for improvement in the plans, processes and procedures.

Improved Quality

End-to-End testing enables the Test Team to identify risks, weaknesses and gaps within and across the entire breadth of Continuity plans and strategies, and enables the organisation to benefit from its Business Continuity programme.

Tangible Benefits

- Improved protection of shareholder value
- Compliance with regulatory requirements
- Reduced operational downtime
- Lower cost of operation during a disruption
- Reduced losses as a result of a disruption
- More cost effective recovery / continuity implementation
- Improve customer service
- Reduce impact of service disruptions
- Minimise duration of outages.

Intangible Benefits

- Preservation of market base
- Improved operational resilience to unforeseen disruptive events
- Protection of brand reputation
- Improved efficiency in continuity processes
- Managed exposure to risks associated with business disruption
- Provision of competitive advantage
- Improved staff confidence
- Increased shareholder confidence
- Reduction of risk.

Reduction of Risk

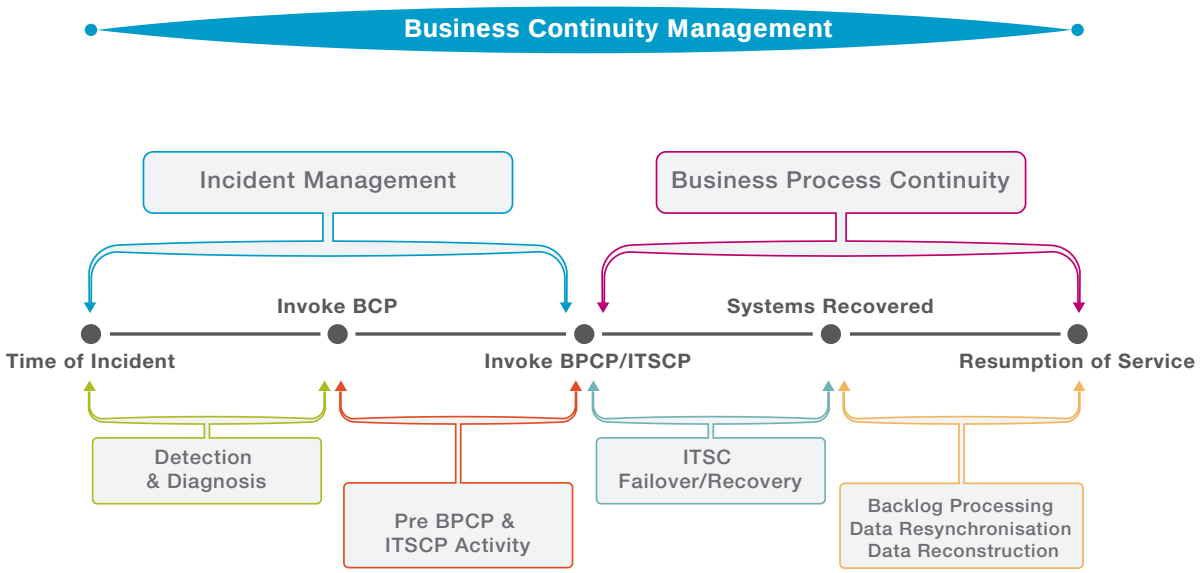
The biggest exposure to risk of any organisation is the implementation of an 'untested' plan, or the expectation that 'untested aspects' of a partially tested plan will function as well as the tested components.

Continuity Plan Validation

End-to-End Continuity Testing is about *validating* the effectiveness, completeness and accuracy of the Plans, holistically and integrated across the suite of Continuity Plans. Its focus is to find as many defects (things that are wrong with the plans) as possible; enabling them to be rectified and resolved – improving both the individual Plans and their integration.

An End-to-End test would span the entire event from time of incident, its detection, and the escalation to failover; all whilst executing the appropriate aspects of business continuity. Figure 3 outlines, at a high-level, some of the plans/processes that may be enacted during the incident lifecycle. Preliminary BCP, BPCP and/or ITSCP activities includes standard incident management processes, where the organisation attempts to resolve/rectify the incident to prevent an untoward invocation of a continuity plan.

Figure 3: Continuity timeline and plans and processes



Capgemini Group employs a range of testing strategies to validate the consistency of the Continuity plans and strategies including:

- Static testing
- Functional testing
- Non-Functional testing
- Point-to-Point (plan to plan) testing
- End-to-End scenario testing
- Cluster (processes and sub-processes) testing
- Black box / White box testing
- Audit and Compliance testing.

A Successful Test?

Successful continuity testing is not the same as successfully executing a continuity or disaster recovery plan. As the goal of testing is to discover defects in the plan, a *successful* test is the test that does not successfully execute all aspects of a continuity or disaster recovery plan; due to the vast quantity of defects revealed. In fact: the more defects identified the more successful the test.

If the organisation is exercising the Plan to *prove* its continued capability in recovering their systems, then a strict test exit criteria is recommended; e.g.

- All planned testing has been completed:
  - 100% of planned test cases executed; or
  - If a planned test case could not be executed, information advising the reason and/or justification for non-execution provided; along with approval by the Continuity Manager
- Nil occurrences of defects which prevent, impede or severely hinder Continuity
- A maximum of five moderate defects, with remediation action plans documented
- A maximum of ten minor defects, with remediation action plans documented.

If 100% of test exit criteria is not, or cannot, be achieved, then the rehearsal exercise is *not* successful. Partially achieved is not achieved.

Summary

Modern business has become so reliant upon Information Technology systems that when IT experiences a services disruption – so does the business. No longer are computers seen as an alternate method to reduce processing times of manual activities. Rather they have become the only method – the manual processes having been long since decommissioned. The business is all but unable to return to a manual process.

Historically the business units accepted, on faith, that their IT service organisations could recover their critical systems – today they require up-to-date and clearly articulated documentation and plans, that undergo regular exercises to confirm continuity. Similarly the enterprise is seeking assurances from its individual business units that they have adequate and proven capabilities of maintaining business operations during any service disruption.

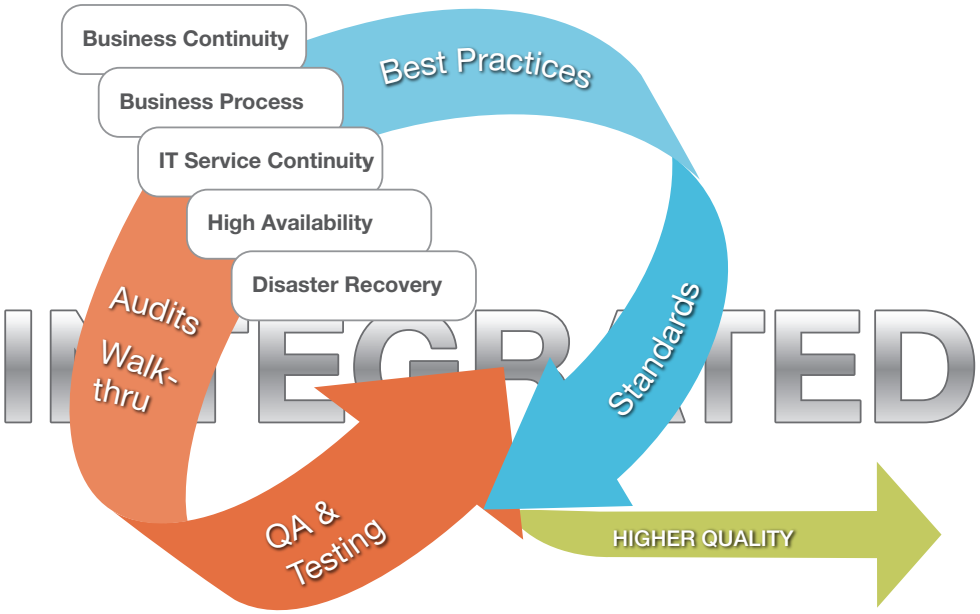
Integrated End-to-End Continuity Testing is essential to ensure a higher degree of consistency with both industry best practices and international standards, such as ISO 9001:2000 (Quality Management Systems), ISO/IEC 27001:2005 (Information Security Management Systems), ISO/IEC 20000:2005 (IT Service Management) and the forthcoming standard ISO 22301 (Preparedness and Continuity Management Systems).

Successful rehearsals of one or more individual continuity plans – in isolation of the other – may provide the organisation with a cursory level of comfort that, should the unthinkable occur, their business and IT groups will handle the incident. But rehearsals do not validate the efficacy of the plans.

Regular audits, walkthroughs and testing of the organisational continuity plans, processes and procedures – combined with understanding of best practices and international standards provide a higher-quality integration continuity solution to the Enterprise and its business (Figure 4).

Beyond conformance to industry standards and best practices, an Integrated End- to-End Continuity Test programme is an indispensable asset toward ensuring that the organisations' Continuity Plans will work when needed most.

Figure 4: The Benefits of Integrated Testing



Capgemini
CONSULTING.TECHNOLOGY.OUTSOURCING

SOGETI

About Capgemini and Sogeti

With more than 125,000 people in 44 countries, Capgemini is one of the world's foremost providers of consulting, technology and outsourcing services. The Group reported 2012 global revenues of EUR 10.3 billion. Together with its clients, Capgemini creates and delivers business and technology solutions that fit needs and drive the results they want. A deeply multicultural organization, Capgemini has developed its own way of working, the Collaborative Business Experience™, and draws on Rightshore®, its worldwide delivery model.

Sogeti is a wholly-owned subsidiary of Cap Gemini S.A., providing local professional services, specializing in Application Management, Infrastructure Management and High-Tech Engineering. Sogeti offers cutting-edge solutions around Testing, Business Intelligence, Mobility, Cloud and Security. Sogeti brings together more than 20,000 professionals in 15 countries and is present in over 100 locations.

The Capgemini Group has created one of the largest dedicated testing practices in the world, with over 11,000 test professionals and a further 14,500 application specialists, notably through a common center of excellence with testing specialists developed in India.

Together Capgemini and Sogeti have developed innovative, business-driven quality assurance (QA) and testing services, combining best-in-breed testing methodologies (TMap® and TPI®) to help organizations achieve their testing and QA goals.

Learn more about us at
www.capgemini.com/testing or
www.sogeti.com/testing

For more information about how Sogeti and Capgemini's Testing Services can help organizations achieve their testing and QA goals, please contact your local Sogeti or Capgemini account manager or our Global Testing Services Team:

Mark Buenen
VP, Business Development
Testing Global Service Line
mark.buenen@sogeti.nl

Kevin Quick
Applications Testing Lead
Capgemini US
kevin.quick@capgemini.com