Contents

Business ContinuITy

Foreword

Yes, this is about IT Business Continuity. The main focus is IT as a function within a business enterprise, in contrast to IT as a separate business. IT business is unique not only in its nature but also the IT Business Continuity is characterized by distinct features that do not apply to other businesses/functions. This paper explains the implementation of the Business Continuity Management from an IT perspective, taking into consideration the IT specific characteristics.

While this paper focuses on IT as a business, it doesn't differentiate between the Information Technology, Information Systems, Business IT and Infrastructure IT. I will try to address aspects related to all these areas.

Introduction

All enterprises depend on IT in one way or other. For most, IT is essential to their existence – not only commercial banks, insurances, airlines and retail but also increasingly pharmaceuticals, engineering, railways and power suppliers depend on computerized systems for their core business processes from supply chain management to sales to finances to other supporting functions. Even IT Consulting companies and IT departments in large enterprises themselves are increasingly depending on IT systems.

Few years ago, a CIO of a global Pharma company in Basel stated the business of IT as "We keep our company running!" Indeed, her simple but powerful mission statement summarizes all what we do. IT Business continuity is about ensuring that this mission is fulfilled even under adverse conditions.

Typical IT organization structurally mimics the business organization to which it belongs. For example, a company's IT typically has departments like Research IT, Development IT, Supply-Chain IT, Finance IT etc. This is where the comparison stops - IT is different. Different in its internal organizational structure, services, technologies, dependencies, lifecycle (e.g. "we have our 3rd reorganization in less than that many years!") and last but not least, it's people. Further, all the business IT departments typically depend on the common Infrastructure IT that provides datacenter facilities, network, servers, clients (PC's), telephony and mobile devices. Of course, operation of all these belongs to Infrastructure IT too. Hence, Infrastructure IT is the single largest area of focus for IT Business Continuity. This is because all other functions including IT itself, depend on it.

While most IT components nowadays are inherently made resilient right from the architecture, it is not always transparent how resilient an IT system is, as a chain of infrastructure components make the final service (e.g. an application or a website) to the end-user. The final service is as available as the least available component or service in the chain. For example, an application depends on a server (90% available), database server (99% available), network (99.999% available) and any PC (100% available), the application cannot be available for more than 90%! Similarly, the datacenter may be a fortress but the application is still not available if the road-workers on the street cut the optical cable while digging (this happened even in Switzerland more than once in the past 3 years). My point is, take chains of dependencies into account for making an IT service available to the business, not just the application server or the network. Ensure redundancies in all components and services leading up to an IT service – the weakest links are usually the low hanging fruits.

What is Business Continuity Management?

Based on the BS25999-1:2006, BCM in the context of IT can be defined as a framework for building organizational resilience with capability to continue if only at a pre-defined lower levels, IT operations and services when threats are realized. In other words, this would include (but not limited to):

- The organization has a pre-defined plan of what to do in case of an adverse event – a plan including who plays what role, contact information, emergency processes and communication, necessary infrastructure (e.g. remote working), priorities that are pre-aligned with business (or business IT) and necessary instructions for trained personnel.
- Reduced Service Levels (DOO – Degraded Operational Objective) during emergency
- Process for back-to-normal operations

Components of IT Business Continuity Management

The following sections describe the components of the Business Continuity Management, from the IT point of view.

1. BCM Policy: The main purpose of the BCM Policy is to provide the high level objectives and scope, based on which the Business Continuity Management (BCM) capability is designed and built. It also helps document the risk appetite of the management, principles (policy statements), assumptions and the Governance and for the implementation of BCM for the IT organization. The Policy will also outline the approach taken to implement BCM. The BCM Policy may be perceived as an unnecessary formality but is very useful as it describes the scope of the BCM and clearly articulates what can be expected from the organization’s BCM.
2. Organizational Understanding: This includes Business Impact Analysis (BIA) and Risk Assessment (RA). Together, these (BIA and RA) give rise to the Business Continuity Requirements. The BIA documents the impact of the unavailability of each IT component/process/system/person on the IT’s ability of providing services or keeping the systems running. For example, what is the impact

of not having email or their ERP system on any business? Within hours, the consequences of lost productivity, lost business become unacceptable. Even worse, GxP/SOX compliance aspects will cause enormous effort fixing the issues even after the systems are brought up again. Now consider the loss of a whole Datacenter. The BIA systematically documents impact of the IT components on business, helping identify mission critical components (infrastructure, data, applications and so on) and people. BIA also helps set the maximum tolerable period of disruption (MTPD), which in turn helps build the BCM strategy for the component/person.
The Risk Assessment (RA) documents risks (vulnerabilities and threats) along with their impacts, probabilities of realizing.

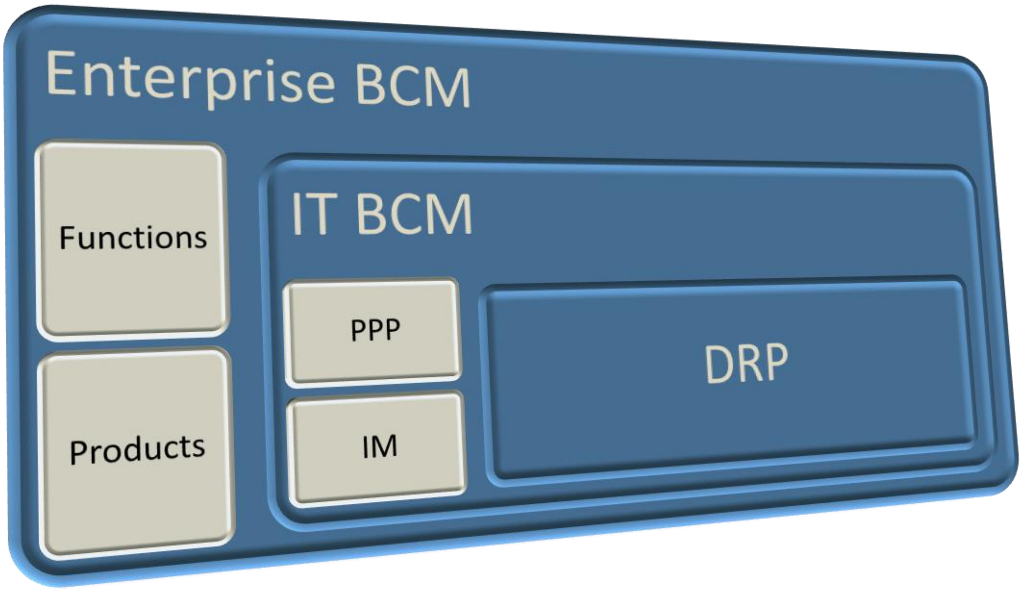
The combination of the BIA and RA gives most of the Business Continuity requirements. Other considerations include risk appetite, DOO, RTO/RPO set by the business or business IT, constraints and inherent strengths of the organization in terms of resilience (e.g. having an IT organization spread across many locations is more resilient compared to having the whole IT organization and the Datacenter in one building, irrespective of minor loss of performance due to geographic distance).

3. Business Continuity Strategies: In many IT departments, most important building blocks of the IT business continuity exist already – Disaster Recovery Plans (DRP) for Datacenters, business critical applications like ERP, CRM and others supporting main business processes. The development of BC Strategies includes documenting how these are used (sometimes referencing the DRP is sufficient), in addition to determining and documenting continuity strategies for other key components. Another aspect is to ensure that the vendors that provide business critical services also have strategies implemented for the continuity of their services at agreed service levels. Business Continuity Strategies include:

   - Accept (Tolerate the risk and potential impact),
   - Transfer (transfer the risk thru an insurance policy or outsourcing or transferring to another function within the organization),
   - Terminate (e.g. implement a process change or a new technology to avoid the risk) and
   - Mitigate.

   The mitigation of the risk implements measures to reduce the risk or the impact of the risk when realized. The residual risk after the mitigation is usually accepted.

4. BCM Response: The BCM Response is documented in the Business Continuity Plan (BCP). For IT, this encompasses all plans (e.g. Disaster Recovery Plan/DRP, Pandemic Preparedness Plan/PPP, Major Incident Management Process/IM etc.) and is referred to by the BCP(s) of the main business functions.



For smaller IT organizations, the IT BCP could be a single document addressing all elements of the BCM.

There are three main topics in the IT BCP.

- First is the plan itself: scope, validity, plan maintenance process, location(s) where it is stored physically or electronically, how to access the plan, test documentation and any templates required during the execution of the plan.
- Second, a clear procedure for managing a major incident. This includes emergency management team structure, roles and responsibilities, call chains, contact information, stakeholder lists, communication plan and interfaces to other incident management processes (e.g. Business or vendors).
- Finally, procedures to bring operations back-to-normal.

5. Testing, Reviews, Exercises and updating IT BCM: The IT environment is very dynamic. Not only do the changes in the business and business organization affect the IT organization but also the emergence of new technologies, development of new services, consolidations and globalization impact the IT landscape. In addition, outsourcing and off-shoring initiatives transform and re-distribute the roles and responsibilities in an IT organization.

   In order to preserve the value of the BCM framework, it is essential to keep it up-to-date and review the contents of a BCP and its subordinate components against the objectives and scope. The frequency of the reviews varies depending the size and complexity of the IT organization as well as the scope of the BCM.

   Testing and exercising the BCP is essential to ensure that the plan is executable. Testing varies from a simple desk-check by the author of the plan to walk-through's conducted involving key players of the execution to end-to-end tests and rehearsals. The BCM tests often refer to the unit-tests of the subordinate components (e.g. Fire drills, DR testing etc.).

Reviewing, Exercising and Updating on an annual basis is recommendable. In addition, the BCM should be reviewed and necessary revisions are made immediately after major changes to the IT organization, IT Landscape (e.g. implementation of ERP or CRM) or post a major incident.

Role of Vendors in BCM

Vendors play a key role in any IT organization's Business Continuity Management, as most organizations depend on basic infrastructure services provided by vendors. For most IT organizations, telephony (fixed or mobile, including the blackberry services) is fully outsourced, whereas the internal organization is playing the role of an interface to the external service providers (aka internal service management). Email exchange servers are still operated in-house by many large organizations but increasingly outsourced to managed-service providers (e.g. MS-Online) as well. The LAN may often be operated in-house but extended LAN (across different locations within a city) and WAN are provided by global network vendors (except that the last-mile connection is often provided by a local telephony vendor).

With basic services, the contract may be out of scope. However, it is important for the Business Continuity Officer (BCO) to understand the service levels and any force majeure clauses so that these can be considered as constraints while developing the business continuity plans.

Where operational IT services are outsourced to vendors it is important to ensure that the service levels include necessary clauses related to Business Continuity Scenarios.

Bringing BCM to your IT Organization

Often BCM is talked about a lot and in some organizations specific aspects of the BCM are also partly or fully implemented. Typically in IT, Incident Management and Disaster Recovery are often in place. Thanks to recent Flu Pandemic, many IT organizations implemented Pandemic Plans. Some other aspects of BCM like having key people backed up or succession planning are often in place as well. However, very few organizations have a Business Continuity Management – the fabric that binds all these individual pieces into a single framework without re-creating or necessarily re-organizing the responsibilities.

The BCM can be brought to your organization without large investments and without allocating several FTE's for the job. The sophistication of the tools is in my view, far less important compared to having the discipline to bring it to the organization thru appropriate training and to keep the Business Continuity Plan (BCP) up-to-date. Implementation of the BCM is more about a change to the culture of the organizations rather than implementing yet another tool that contains information that was last updated several years ago.

It is recommendable that the BCM is brought to an organization in multiple cycles in a few years rather than a single large project. With a large project, the IT organization runs the risk of losing the value of the initial investment over a period of two years unless high level of management focus and considerable continued investments are maintained. It is better to invest steadily over two to three years and embed BCM into the organizational culture. One exception would be when the IT organization aims at achieving BS25999 (or similar) certification and intends to maintain the certified status.

I recommend the following approach for an IT organization. It is not necessary but not uncommon to engage a BCM Consultant for guiding and supporting the internal BCM responsible thru the above process. The role of a consultant is mainly advisory bringing in knowledge of best practice, but not executing the BCM implementation process, for which an internal project manager is much more suitable. His/her effort should be limited to a few person-weeks stretched through out the duration of the BCM program, especially as the consultant should add value by using existing templates, sample documents and other artifacts.

- Before determining on the approach for implementing BCM, it is necessary to understand the IT organization's reasons for implementing the BCM. Start with interviews with one (the sponsor) or more senior IT Managers (CIO/CTO and direct reports, depending on the scope of the BCM. Outline the following approach to the sponsor/senior manager(s) during the meeting and seek their feedback. Document the outcomes in the preliminary draft of BCM Policy.
- Prepare for a BCM workshop. A workshop will jump-start the BCM program and reduce the implementation time greatly. It will also help send the message about the BCM in a single voice.
    - Create the agenda
    - Introductory presentation,
    - Gather already existing information about the organization, business critical processes, people, assets (facilities, infrastructure etc.), systems and data
    - Create necessary templates for collecting and organizing the information relevant to the BCM
    - Draft BCM Policy (essential is that there is an agreement on the scope of the BCM that is being implemented
    - Logistics of the workshop
- Conduct BCM Workshop
    - All senior IT managers (CIO/CTO and their direct reports) participate. Where key IT services are outsourced/off-shored, the vendors may attend the workshop but typically they are represented by the internal vendor managers. Key process/asset/system portfolio owners (e.g. Head of Application or Infrastructure Operations, irrespective of the level in the organization) should also participate in the workshop.
    - After the common session, workgroups (formed based on the scope of the BCM) to identify business critical processes, systems, data, infrastructure and facilities and document MTPD (Maximum Tolerable Period of Disruption), RTO (Recovery Time Objective) and RPO(Recovery Point Objective).
    - Validate information previously gathered, approve BCM Policy.
    - Risk assessment and developing BCM strategies for mission critical processes and components, if time permits.
    - Agree on BCM roles and responsibilities (e.g. Business Continuity Officer(BCO)/Manager, Emergency Management roles etc.)
    - Outline next steps.
- Draft BCP (there are many samples in the internet – pick one that is most suitable for your organization)
- Review cycles of the BCP
- Conduct training and exercises (BCM testing) as needed (either individually or in small groups)

- Perform periodical (e.g. BCM review/BCP update etc.) and continual (e.g. thinking of BCM aspect for changes to organization, projects etc.)

Conclusion

- IT Business Continuity is an essential part of any enterprise's Business Continuity Management.
- IT BCM need not be developed from scratch, as key components (e.g. DRP) are often already in place. Re-using the existing processes and frameworks improves maintainability and achieves high value for a low investment
- It is better to have a usable and up-to-date BCM with a limited scope than to implement a complex framework that cannot be maintained.