HOUTKIN & ASSOCIATES
TECHNICAL PROJECT MANAGEMENT
PROCESS ENGINEERING

WHITE PAPER

Creating Synergy Between the Business Continuity and Disaster Recovery Process

Creating Synergy Between the Business Continuity and Disaster Recovery Process 3

Introduction 3

Preliminary Ground-Work 3

Management Support 3

Defining the Disciplines and New Requirements for Their Fulfillment. 5

Business Continuity. 5

Safety 5

Business 5

Business Continuity - New Concepts 6

Disaster Recovery 8

Technical Requirements 8

Alternate Data Center 9

Alternate Seating Office 9

Disaster Recovery - New Concepts 9

In summary 10

Defining Synergies 11

Synergies with Production Technical Processes/Procedures and their Support of the Business. 11

Synergies between the Business Continuity and Disaster Recovery Process 11

Sub-Process: Site Risk Assessment. 11

Synergy with the Disaster Recovery Process. 12

Sub-Process: Business Impact Analysis: Total at Production Site. 12

Synergy with the Disaster Recovery Process. 12

Sub-Process: Business Continuity Plan. 13

Synergy with the Disaster Recovery Process. 13

Sub-Process: Business Evacuation Drill/Call Tree Testing/Accountability Drill. 13

Synergy with the Disaster Recovery Process. 13

Summary 14

Creating Synergy Between the Business Continuity and Disaster Recovery Process

Introduction

There is a very strategic relationship between the Business Continuity and Disaster Recovery disciplines and processes. Many use the terms interchangeably or confuse the two disciplines altogether. Disaster Recovery is often inter-twined with the Corporate Technology environment but is not often integrated into the life-cycle process of supporting the business. Business Continuity is primarily about understanding the business and its risks and methods of mitigating this risk but the plans are actually manifested through the Disaster Recovery process. We have tried to fit Business Continuity processes into the existing Risk Management process and Disaster Recovery processes into the existing technology processes but we have come to understand that there are aspects of both disciplines that are not responded to with existing processes and we can no longer continue to fit a square peg into a round hole.

In the private sector, Business Continuity and Disaster Recovery processes and procedures form an end-to-end process that begins with business continuity process and continues with the manifestation of the resulting plans into logistical and technical solutions. There is never really an end point to the process as there is a continual looping as the business changes and annually, when the failover process is tested on all levels: physical, network, infrastructure, operating system, fail-over of the replicated repositories; invocation of application and database processes at the alternate site and application-level testing ensuring all up-and down-stream dependencies are present in tangible form at the alternate site: staging servers, circuits, firewall configurations, etc. So, Business Continuity and Disaster Recovery changes as the production business changes.

To identify the compatible elements between the two processes, we need to first understand:

1) How to define the two disciplines by the sub-processes and procedures that comprise them.
2) the new elements that both the Business Continuity and the Disaster Recovery processes bring to existing business, risk assessment and technical process and where and how they are to be integrated.
3) Where elements of the business continuity process directly funds the Disaster Recovery process (the bridge, if you will between the two disciplines).

Preliminary Ground-Work

The way that I choose to define a discipline is to understand, by delineation, those primary and sub-processes that are performed to complete the whole. There are two “givens” to clarify before we attempt to define each term by its sub-processes and procedures:

- Disaster Recovery logistical and technical solutions are driven by the business and defined by the Business Continuity plan however, the processes that are used to implement, maintain, support and test may already exist within the technology side.
- The set of Disaster Recovery solutions must combine those solutions that support the enterprise / business and those that that support individual businesses. Without looking at the individual requirement mapped to the enterprise supported solutions, the environment will be costly and inefficient.

Management Support

Management support is the fundamental concept that underlies both the Business Continuity and Disaster Recovery process. Because our goal is to integrate the alternate logistical and technical solutions into a single enterprise-wide

solution, there are certain policies that are required. I mention these as Business Continuity and Disaster Recovery often take a back-seat and without firstly, support from Senior Management, the baseline policies may not be defined and implemented, making it very difficult to pursue and maintain both a Business Continuity program and disaster recovery best practices.

So, imperative to both Business Continuity and Disaster Recovery definitions, is that Senior Management has defined a mission to support both Business Continuity and Disaster Recovery and that this mission and support is communicated to the Business Heads, related Managers, CTO and Technical Heads.

The result of Management Support is far-reaching and crucial for continued success of the private sector Business Continuity and Disaster Recovery program.

Defining the Disciplines and New Requirements for Their Fulfillment.

Business Continuity.

It is has been my experience that Business Continuity is defined by those processes and procedures performed to ensure resiliency of the business and its staff through any incident. The end result of these processes is the identification/documentation of the mission critical process, its Recovery Time Objectives and functions that perform this process resulting from an in-depth impact analysis and risk assessment of the business based against various scenarios that could possibly impact the core of its business process.

The sub-processes and procedures include:

Safety

1. Safety process, whether in-line with those created by the Corporate Security/Building Management Fire/Safety Director that include both Evacuation and Accountability of Staff.[1]
2. Risk Assessment of the Building from a Security Perspective.

Business

1. Analysis of the Business Processes and procedures and prioritizing them by Mission Critical, Critical and Priority
2. Analysis and delineation of those functions that perform the Business Process
3. Analysis and delineation of those tools that support the Business Process
4. Overlaying the Business Processes, functions and tools onto a schedule that comprises a timeline of "0 hour to 2 business weeks" to understand what processes are required within prescribed periods within the 2 weeks (0-4 hours; 4-8 hours; 8-24 hours; 24-48 hours, etc); the skill-set (and number of staff) required to perform them and those tools that used to support them.
5. Business Impact Analysis of Each Business within the Company and of the Total Business.
6. Risk Assessment of each Business and the overall Business Business Process from the perspective of 1) the business as its own entity; 2) the business within that particular facility
7. Resulting Plans/Requirements[2]:
    a. Business Continuity Site Plan
        1. Overview of the Business within that Facility
        2. Overview of the Business within that Facility in relation to the overall business
        3. Overview of the Business within that Facility in relation to the industry
        4. The 3 scenarios of Disaster Recovery and specific instructions on how to respond:
            - Scenario 1: Facility is Impacted During BAU
            - Scenario 2: Denial of Physical Access
            - Scenario 3: Shelter-in-Place
        5. Risk Assessment of the Building
        6. The Crisis Management Team, Process and Contact Listing of Crisis Management Team
        7. Evacuation Plan for the specific building
        8. Assembly point in-line with local laws
        9. Accountability Process that includes a phased-in approach to accountability including nightly business-level conference calls to determine status of mission critical process at time of incident and

---

[1] You cannot recover from a Disaster if you do not have the staff to do it. It is imperative that the safety process and the staff accountability process become part of the Business Continuity/Disaster Recovery process.

[2] I should note that I personally like to summarize those processes that everyone in the business requires through a document that I call the Business Continuity Site Plan. This plan has any and all information that anyone in the business needs in case of an incident. I also keep a tightly documented spreadsheet that becomes a dashboard for program management and audit requirements. The Business Continuity Site Plan is differentiated from the Business Continuity Plan in that the Business Plan is business-specific and the number of these plans are determined by the number of businesses within an overall Company.

who will fulfill the business continuity plan

10. The full process from 0-hour of an incident through to the first 48 hours including instructions for each milestone in that 0-48 hour process
11. All methods of travel away from the area
12. Areas in the vicinity to avoid - (soft-targets)
13. Areas to go for safety if you cannot leave the area: Fire / Police Departments, Hospitals, Post Offices, etc.
14. Listing of other offices within the country or region and their contact information
15. Description of the Alternate Seating Site with Seating Chart, Business Allocation, Access Methods and general Rules/Regulations of the Site
16. Directions to the Alternate Seating Site (All methods of travel)
17. Listing of hotels, restaurants, hospitals, shopping venues

b. Business Continuity Plan for Each Specific Business

1. Description and History of the Business
2. Ranking of the Business within the Company
3. Ranking of the Business within the Industry
4. Business Process flow
5. Business Process verbal description
   - Process Entities
   - Functions that perform the process
   - Tools that support the process
   - Up-stream/down-stream dependencies
6. Delineation of the Mission Critical, Critical and Priority Business Process and those Skill-Sets and tools that perform these processes based against a timeline of 2 weeks - by Recovery Time Objective (RTO)
7. Call Tree Contact Listing
8. Call Tree/Accountability Process
9. Business Continuity Seating Requirement (Seating requirements within the facility or another office within the same vicinity in case of a localized event);
10. Alternate Seating Requirements (number of seats; tools on the desk; tools on the workstation image)
11. All systems and technology that supports the mission critical and critical business process
12. All systems and technology that support the mission critical and critical business process mapped to Recovery Point Objective
13. Third Party Business dependencies (both up-stream/down-stream) and related tools, software, contact information, support numbers and methods of communication
14. Third Party Business contact listings
15. Vendor Licensing, Leasing and Contact Listings
16. Office Supplies including business-required tools (calculators, etc)
17. Hotel Requirements including needs for family and pets
18. Medical Requirements
19. Testing History: Plan Walkthrough; Call Tree Testing; Evacuation Drills; Accountability Process Drill

Business Continuity - New Concepts

Many of the new concepts that are introduced through the Business Continuity Process includes the following policies that are required to help the Business through the analysis, planning and documentation of their plans.

- The Business Continuity Mission; e.g. 1) The RTO for the complete business; 2) Continue or maintain normal business process within the RTO
- Crisis Management Team and Process

- Remote Access as an accepted form for working
- Distributed Model[3] of Production Seating
- Creation of Human Resources policies and processes regarding: remote access; use of holidays/vacations in light of a catastrophic event; counseling and support; and use of benefits for injured, hospitalized and deceased
- Creation of policies and processes in working with Corporate Security or local agencies re: search and rescue; death certificates and family counseling

[3] The distributed model permits use of the alternate seating site as a microcosm of the production environment and is designed to be in use during normal business process. In this way, the business can meet the need to be resilient, rather than just continue after an event. By delineating the mission critical business process, the Business Head can identify those skillsets that can work from the alternate seating site on a normal business day while the majority of the business works from the production site.

Disaster Recovery

Disaster Recovery may be defined as the process of mapping business Requirements to technology policies and methodologies to define and deploy logistical and technological solutions to ensure that the Business can meet their resiliency expectation that they defined in their plans. Note that Disaster Recovery includes Planning and Deployment and testing. The Disaster Recovery sub-processes and procedures include:

- Analysis of the complete site risk assessment, business requirement and each individual business requirement to get an overall "picture" of the total breadth of the solution
- Analysis of the business requirement mapped to the existing technical environment
- Creation of those logistical and technical solutions that manifests the business planing requirements
    - Technical Requirements
    - Alternate Data Center
    - Alternate Seating Requirements

Technical Requirements

- Analysis of the production network environment
    - LAN architecture and any current issues that require a re-design or resolution
    - Internet and up-load/down-load capacity requirements
    - FTP or other file transport requirements
    - Methods of "communicating" with regulators, if applicable
    - Point-to-point connections to upstream/downstream business or vendor partners (market data; counter-parties; custodians; third-party data hosting) and all infrastructure supporting this relationship (staging servers, etc.)
    - Firewalls and configurations
- Estimated network requirements for the alternate site
    - LAN architecture and any current issues that require a re-design or resolution
    - Internet and up-load/down-load capacity requirements
    - FTP or other file transport requirements
    - Methods of "communicating" with regulators, if applicable
    - Point-to-point connections to upstream/downstream business or vendor partners (market data; counter-parties; custodians; third-party data hosting) and all infrastructure supporting this relationship (staging servers, etc.)
    - Firewalls and configurations
- Current backup processes and procedures
- Current tape backup and retrieval processes and procedures
- Complete listing of applications mapped to server names/types/replication methodology, schedule and total payload replicating across the network
- Analysis of each application including architecture, all core and dependent components resulting in number of required servers for deployment
- Overlay of both the business process and the application/system process onto the architectural analysis of the application
- The disaster recovery delivery process in use for this technology culture
- The approval of these solutions by the Stakeholders of the Business;
- The design, procurement and deployment of the solutions
- Documentation of the Run-Book or Invocation Document for each Technical, System and Application
- The Disaster Recovery process and delineates the order of technical processes to be performed from 0 hour to failover the site mapped to ownership
- Testing of these solutions: infrastructure; technical testing (shakedown); application functionality (core); application functionality with upstream/downstream dependencies; End User Testing; Site Failover (Technical); Site Failover (Technical and Business)
- Vendor Management

Alternate Data Center

- Location
  - Risk Assessment of the Area: Terrorism, History of Civil Unrest, Weather-Related Issues
  - Distance from the Production Data Center
  - Distance from the Production Business Seating Site
  - Distance from the Alternate Seating Site
  - Ability to Reach the Site by all modes of travel
- History of the Hosting Company
- History of the Data Center Facility including any issues and method of resolution
- Use of Hosting Company technical resources for maintenance; fail-over
- Price per square foot
- Environmentals methodologies and notification processes in case of an issue
- Price for power, cooling other environmentals
- Notification/Escalation Processes and procedures
- Discretionary Capabilities of Hosting Company
- Footprint requirement
- Restrictions by the local Office of Emergency Management
- Vendor Management
- Impact to the Production Data Center environment: Is server consolidation now a consideration. If so, what is the methodology: VM; RAC?
- Impact to the Production Architectural Method. Is this the time to start considering High Availability? To start clustering servers?

Alternate Seating Office

- Review of all functions supporting the mission critical business process mapped to those who perform them and their home locations to find the best place for an alternate seating site
- Ease of travel to the site including all methods to meet all requirements
- Proximity of hotels, restaurants, shopping venues; hospitals; doctors, drug stores, etc. to the site
- History of the Hosting Company
- History of the Facility including any issues and method of resolution
- Number of seats
- Analog requirements: Fax, for example
- Local construction laws
- Local loop offerings, price and relations to MAN/WAN carriers
- MAN/WAN offerings, price and relations to local loop carriers
- Firewall requirements
- Vendor Management
- Access Control: Physical
- Location of Third-Party Technical Support
- Location of Business / Vendor Partner Alternate Business locations (public facing)
- Decontamination Services

Disaster Recovery - New Concepts

As with the business, the Technology team must make some decisions and policies that will ultimately impact their production environment and possibly the CIO's vision of the production technical environment that supports the Business. Why? Since we no longer view Disaster Recovery as a single point in time but as an aspect of the production environ-

ment, we now have to reconsider the overall network design for 2 sites and the relationship between the two data centers and possibly between the alternate seating sites; use, placement and configuration of infrastructure services and related hardware; application architecture possibly over a MAN or WAN and now, replication. Here are some of the points that are new to the production environment but require attention and integration into the existing technology environment.

- Mapping of the alternate application environment to production (configuration/capacity) on an application-level
- Status of the alternate data center? Hot Site/Cold Site?
- Replication Methodology. Dual-path (synchronous or asynchronous); Host-based; block-level; database-level (Data Guard, SQL Transaction-Log shipping); replication solutions per database type or a single solution
- Network Architecture: Load-Balanced or fail-over
- Application-Level Architecture: High-Availability (co-located); High-Availability over a WAN/MAN; load-balanced (with dual-path replication)
- Client-Server Architecture: Thin/Thick Client
- Workstation Image. Single image with hidden applications/one image for each business
- Server Consolidation: VM? RAC?
- System/Application Access Controls in times of an Incident
- Fail-over methodology.
    - Use of automated means to fail-over:
        - DNS re-direct, for example and those standards required to support failover:
        - Replication (block-level)
        - Use of alias names in front-end odbc files; sql.ini files; tnsnames.ora files rather than hard-coded ip addresses or server names
        - Use of thin-client vs. thick client; e.g. ensuring that processing is performed on the server to lessen the amount of data that is transported to the client if working remotely
    - Consideration of smart-sourcing to handle failover of those manual processes and procedures supporting the failover process
        - Performing the DNS push
        - Isolating the injured site to ensure that
        - If the site is not isolated, Stopping Replication processes in the production site and Stopping (if applicable) database processes in the production site
        - Changing the personality of the alternate data repositories and mapping storage to the appropriate servers
        - Starting database processes at the alternate site
        - If using Citrix, promotion of the alternate site permissioning
        - Promotion of User logon-scripts at the alternate site, if required
        - The support paradigm for both production and the alternate site
        - Inter and intra-disciplinary cross-training

In summary

1. Business Continuity Planning sub-processes output to various documents that delineate the plan for the business.
2. The Business Continuity Plan must be manifested and tested in order for the plan to be viable otherwise it exists in document state only.
3. Disaster Recovery Planning is driven by the Business Continuity Plan as well as the current production business and enterprise solutions and manifests these plans and requirements into cost-effective technical and logistical solutions
4. Both Business Continuity Planning and Disaster Recovery Planning are based on certain policies that the Company must respond to as guidelines for both planning, deployment and maintenance.

Defining Synergies

So, where are our compatible elements? Firstly, look at the existing production environment and those methods, processes and procedures that support the Business. By supporting the Business, the Business Continuity Plan is also supported.

I find that technology often assumes that existing operating processes/procedures; software development life-cycle processes and technology deployment, testing and maintenance processes and procedures can support Disaster Recovery. This is not true. If we look again at the new aspects that Disaster Recovery can bring to Technology, we see that existing processes and procedures do not support Disaster Recovery most basic precepts: the fail-over process and methodology - let alone other aspects of Disaster Recovery.

Synergies with Production Technical Processes/Procedures and their Support of the Business.

- The production support organization.
    1. Help-desk Support
    2. Desktop Engineering: Workstation Image; Methodologies re: market data; one-off's on the client
    3. Infrastructure Support: Infrastructure services: Add Wins, DNS, DHCP, domain controller configuration information to all servers supporting both the production and alternate environments
    4. Telecom Support: Define those production fax numbers and phone numbers that are mission critical to the business
- The production technology charge-back process. Integrate pricing for the alternate environment including:
    1. Seating requirements: workstation, phone, network connection
    2. Special requirements: turrets, broker lines
    3. Storage
- The production Software Development Life-Cycle
    1. Integrate Business Continuity requirements into the Business Requirements and Business Project Initiation Document
    2. Integrate Disaster Recovery infrastructure architectural, device configuration and storage requirements into the production technical specifications document
    3. Integrate deployment of the Disaster Recovery solution along with the production solution.
    4. Integrate disaster recovery testing into the deployment process as a sign-off action.
- The Change Management Process
    1. Integrate Disaster Recovery infrastructure changes into the Change management process
    2. Integrate Disaster Recovery application changes into the Change management process
    3. Integrate Disaster Recovery database changes into the Change Management process
    4. Add replication changes into the Change Management process
    5. Add Disaster Recovery desktop image and one-off applications into the Change Management process
    6. Add Disaster Recovery storage changes into the Change management process
    7. Business Outputs and how they are manifested in production

Synergies between the Business Continuity and Disaster Recovery Process

Sub-Process: Site Risk Assessment.

The Facility or Site Risk Assessment is usually performed by Corporate Security or the Building Managements' Fire/Safety Director along with local City Agencies: Office of Emergency Management, for example. This Assessment gives us an idea of:

2. If the building is a soft-target or is situated within the vicinity of soft targets;
3. If the building or area is subject to flooding or bad-weather.
4. If the building is subject to electrical problems.

5. Whether the City Agencies will lock-down the complete City. and subsequent response.
6. What processes Corporate Security or the Fire/Safety Director may follow.
7. Any physical security risks in the building or in the vicinity.

Synergy with the Disaster Recovery Process.

This information directly impacts the Disaster Recovery process. If we know that technology staff may have a problem leaving the building because they are locked-in or leaving the area after an evacuation, we may need to identify more automated processes to fail-over the environment and possibly, a smart-sourcing solution for the first 0-3 hours to perform the actual fail-over of the environment.

This will also help technology staff to focus on their safety rather than the data center - which unfortunately took lives on 9/11.

Sub-Process: Business Impact Analysis: Total at Production Site.

Here, it is important to ensure that we have a total view of the business so that we can understand how the business are ranked within a Company and within the industry.

Synergy with the Disaster Recovery Process.

Risk is measured in terms of: Operational; Reputation; Terrorist-Related; Industry; Weather-Related; Civil Unrest.

1. Operational risks could impact the reputation of the company with regards to their inability to either meet financial obligations; meet market or regulatory requirements and/or accrue penalties of fines for this impact.
2. We look to see what steps will mitigate these risks: Identifying mission critical business functions that tools that will help to mitigate these risks. As well, whether cross-training is required and by mapping the mission criticality of the process with the RTO, whether critical business staff should have a setup at home (as long as it meets with regulatory guidelines) and most importantly, whether the distributed model would mitigate these risks on a day-to-day basis.
3. If we see concerns regarding reputation, we must ensure that we have a Communications representative on the Incident Management Team who is accountable for third-party communications to stabilize bad press. As well, we need to ensure that there is a well-documented plan that has both a primary and alternate owner for communication to clients and internal staff in other regions/countries.
4. If the Business industry is a target of terrorists or civil unrest, it is important that we choose a building and location that does not further attract these concerns. As well, that we follow very strict communication and policies regarding discretion with staff regarding locations of various alternate sites and data centers. Important as well, we need to look at travel opportunities to and from the building in case the Business is dependent on deliveries.
5. If there are weather concerns, we need to look at travel opportunities around the city to facilitate evacuation and permit staff to actually travel to the alternate sites. Here, several small sites may be required or deployment of the distributed model may mitigate risks that staff may be stuck on roads during evacuation.
6. A difficult issue to deal with is industry-related risk and the “disgruntled” staff problem - only because they bring in Human Resource elements that may not be appropriate for the Business Continuity team to raise in a Risk Assessment as it is the job of Compliance and internal audit to manage the actual day-to-processes practiced by anyone business in the Company.

   The Risk Assessment should present the results of a cursory study of the industry to look at any recent issues in the industry that could potentially impact the Company’s bottom line -- or if there are any current investigations that are being performed within the Company or by regulatory bodies. The sub-prime problem is a good example. However, trying to ask the Business to identify any practices that could impact the business may not work. The best we can do is perform our research with reputable sources and identify any industry-wide practices in the Risk Assessment.

Sub-Process: Business Continuity Plan.

Here, it is important to ensure that we have a total view of the business so that we can understand how the business are ranked within a Company and within the industry.

1. Business process delineated by Mission Critical, Critical and Priority.
2. Functions that support the Business Process
3. Up-/down-stream dependencies to the Process
4. All business application requirements, tools
5. Office requirements

Synergy with the Disaster Recovery Process.

1. Definition of the seating design for the alternate site; number of seats
2. Definition of the overall RTO for the business.
3. Which businesses are supported by the highest ranking business or which business support the highest ranking business to better define a complete seating environment - resulting in a complete end-to-end business microcosm that supports the complete end-to-end business process.
4. Definition of fax machines and phone numbers that will need to be re-directed to the alternate site.
5. Identification of applications and systems that are mission critical to the business and consequently . . .
6. The Recovery Point Objective and the replication methodology, schedule and fail-over process.
7. Identification of all up- and down-stream dependencies that are mission critical to the business including all related infrastructure and transport.
8. Possibility expansion over the next 6-months, 1 year, etc that directly effects: number of seats and supplies; voice circuits; bandwidth for replication and usage; storage requirements for both production and disaster recovery, etc.
9. Whether there is a need to review architectural standards to support the results of the Impact Analysis.

Sub-Process: Business Evacuation Drill/Call Tree Testing/Accountability Drill.

I only bring these drills, walk-throughs and tests into play as they have become very important since the 9/11 incident. I noted as many do now, that people do not recognize themselves during an incident. Those we may rely on may be the first to leave. Others may leave and not return - and not communicate at all. Or, the saddest are those who do not deal with their experience and ultimately suffer illness in years after the event as the incident left indelible marks on their physiology.

Synergy with the Disaster Recovery Process.

I find that the Business Continuity walkthrough, the Call Tree test, the evacuation drill and the Staff accountability drills help me to see who may have issues with a catastrophic event either from past experiences or by internal fears. This is important information - although it may not be communicated directly in words. Anger, absenteeism, arrogance towards the process tell me that we may need to identify who we may need to keep an eye on during an event and . . .

1. identify a buddy system during evacuation
2. that we may need to change the various processes to better ensure that staff will use them
3. that we need to reach staff on a regular basis through monthly presentations and tear sheets, to get buy-in to the process of having staff communicate their status
4. that we may need to carefully review the Accountability process and ensure that only staff who feel clearly capable are actually primary/alternate callers and finally
5. That we carefully review who become members of the Crisis Management, Disaster Recovery and Fire Warden teams

This information is not in any plan so we have to be careful to look at the signs and be ready to make changes in our Safety plans.

Summary

Business Continuity and Disaster Recovery are clearly two distinct disciplines that are further confused by attempts to integrate them into existing Business, Risk Management and Technology Departments and processes and procedures. Agreed, there are some overlaps, but the differences with existing processes and procedures need to be acknowledged and responded to if we are to be successful.

The Business must think about their process, with already defined risks, within a facility and what it takes to replicate the complete process somewhere else when the greatest variable is the status of their staff, the incident itself and any associated variables: communication and travel. Each variable adds another risk to their ability to maintain resilience.

Technology cannot support a Disaster Recovery environment without considering the particulars of Disaster Recovery; e.g. fail-over process and methodology, replication, vendor management, out-sourcing of mission critical process, alternate seating, alternate networks and alternate data centers. The addition of Disaster Recovery can actually change the complete vision for the Technology team and how it supports the business from how it architects the application to how it supports both Business and operational process.

If we are true to our business, we have the ability to benchmark it at various stages of growth. Integration of a Business Continuity and Disaster Recovery program into an existing business is another level of growth. There is too much to lose to consider Business Continuity and Disaster Recovery as an insurance program.

If we look at Business Continuity and Disaster Recovery as a single end-to-end process, as part of the production business and technology process, we can modify existing process to integrate the new concepts without impacting our resources. We will truly see the flow between the two disciplines rather than looking at them as two separate concepts. The more we separate Business Continuity and Disaster Recovery principles the more difficult it becomes to perform the work that they are in existence to perform and the two disciplines begin to cause yet another set of issues that further take a business from focussing on its well-being and its ability to weather any incident that may cross its path.