Global Information Assurance Certification Paper

Disaster Recovery and Business Continuity Plans and advantages for undertaking major infrastructure changes

By

Iain Segall

November 2003

GIAC Security Essentials Certification (GSEC) Practical Assignment
Version 1.4b Option #1

Contents

1. Introduction and Overview

In this paper I discuss the advantage of good Disaster Recovery Plan (DRP) and Business Continuity Plans (BCP) in ensuring smooth running business and IT infrastructure. These plans are often thought of as something undertaken by a business as a method to plan solely for a major disaster or system failure. In this paper I look at how using these can aid in everyday activities. I discuss their importance when undertaking a major infrastructure upgrade and the processes that can be followed to avoid common mistakes of allowing upgrades and changes to over-run causing service disruption.

I draw on personal experiences and discuss how, with a correctly documented and planned infrastructure, unknown and predicated events can be correctly planned for to avoid serious issues.

2. What is Business Continuity and Disaster Recovery Planning?

BCP and DRP are often terms and processes that are regularly thought as being one and the same. However they are quite different and are defined as:

Business Continuity Plan – This is a plan, which is created to ensure that if an unknown situation or disaster affects a business, the service is restored in the quickest and smoothest of fashions. This plan covers the business as a whole, and can include anything from the recovery from a minor flood affecting one room or an office as a whole.[1]

Disaster Recovery Plan – This is a plan to ensure that if computer systems fail they are brought back up in the quickest timescale.

3. Business Awareness of the Need for BCP/DRP

The process of BCP/DRP is one in which there was increased business awareness in their importance as part of Year 2000 planning, and more recently post the September 11th 2001 terrorist attacks.

When undertaking work for the year 2000 a lot of companies used it as a multi stage process, which included the following:

- Review and audit of systems
- Legacy system replacement to avoid Y2K problems
- Definition of system priority
- Backup procedure updates

[1] http://www.nccglobal.com/consultancy/security/bcp.htm

- Business continuities and disaster recovery plans to cover the period of roll-over to the year 2000

The level of BCP and expenditure by companies and organisations for Y2K varied depending on the type of company or organisation, and where in the world it was located. In developed countries such as the USA, larger expenditure was necessary especially by financial organisations, whereas in countries such as the Gambia the need for mass work and expenditure was not necessary[2]. This was partly related to the perceived loss in business, reputation, as well as an organisations reliance on technology.

In the lead up to the 1999/2000 rollover, BCP formed a major part of many companies expenditure. In many cases this led to the formation of a dedicated team for Year 2000 compliance and continuity planning. These teams were in-effect a BCP planning team. Very soon after the rollover, teams were often disbanded with their roles for BCP planning either moved back into the general business with no central responsibility, or even completely abandoned. This meant that the major work and organisational changes put into place were often lost with their benefits.

As a result of the tragic events of the September 11th terrorist attacks, BCP was brought back to the forefront of business budgets. Whereas for Year 2000 a lot of planning was done to look at one specific event, namely the rollover between one year and the next, the focus of what should be included in BCP has changed to include[3]:

- **Operation Efficiency Initiatives:** Organisations have moved towards having a smaller number of operations centres which run more efficiently whilst being able to take on additional workload if required. This has brought about not only the advantage of efficiency savings but also the possibility of higher security.

- **Increased Focus in User/Client Recovery:** The loss of a user's workspace was not previously seen as a problem. With recent developments there is more emphasis on ensuring that a user base can be relocated, which includes home working and relocation to disaster recovery sites.

- **A Reduction in Site Separation:** There previously was a trend to have a recovery site a distance away from the site being recovered. It is now more favoured to place recovery sites nearer to ensure that if a disaster occurs normal business can be started as soon as possible. It takes account of the fact that staff, suppliers and clients will not have to travel a great distance compared to the normal site location, reducing costs and delays. There is a trend away from employing a third party to host recovery sites, in the case of site unavailability, as businesses

[2] http://www.scoop.co.nz/mason/stories/HL0001/S00007.htm
[3] http://www.csoonline.com/analyst/report484.html

now plan for critical business restoration across sites compared to that posed by totally catastrophic site loss.

4. The Planning Process for BCP/DRP

The planning process for BCP/DRP is dependant on what sort of incident is being planned for. If a system is located and hosted by a third party, then the planning required is very different to that used for planning for a complete site recovery.

There are a number of national and international standards that have been developed and adopted for ensuring system integrity and security. In my experience in the UK and Europe, it is now common to adopt a combination of two standards, which are ISO 9001 and BS7799/ISO7999 when undertaking BCP/DRP work. These standards are defined as:

ISO 9001 – International Standards for Quality Management Systems

This is a set of standards for quality management systems that has worldwide acceptance, and has been adopted worldwide in more than ninety countries[4]. This is a general business process standard and not an IT standard, used by any business, not just for IT systems. With ISO 9001 processes are put in place and audited to ensure that they meet an acceptable standard.

BS7799/ ISO 17799 - Information technology — Code of practice for information security management

BS7799 was the first security standard for commerce, which provides a framework for information security 'Good Practice'. It was born out of ISO 9001 heritage and was drafted in 1995 and then again in 1999 in the UK by the DTI (Department of trade and industry)[5]. BS7799 is a British Standard consisting of two parts:

- Part 1: Code of practice for information security management.
- Part 2: Specification for information security management systems.

Part 1 has been adopted as an international standard and is now known as ISO/IEC17799 – Information Technology – Code of Practice for Information Security Management. Part 2 has yet to be adopted by the international community. Part 2 is the specification against which a system is audited.

[4] http://www.isoeasy.org/

[5] http://www.ffwlaw.com/%5BResources%5D/Publications/BTMT/Technology_Law/technologyupdatesummer2003.pdf

It consists of ten sections that are[6]:

1. *Security Policy*
2. *Organisational Security*
3. *Asset Classification and Control*
4. *Personnel Security*
5. *Physical and Environmental Security*
6. *Communications and Operation Management*
7. *System Access Control*
8. *System Development and Maintenance*
9. *Business Continuity Management*
10. *Compliance*

With both IS0 9001 and ISO17799/BS7799 a company can get an external company to audit them for compliance. This includes an initial assessment to standard and then a periodic check to ensure continuance of compliance.

Compliance auditing is quite a common practice for ISO 9001, but it is not so common with ISO17799/BS7799. For ISO17799/BS7799 it is common for a company, or even just a department within it, to create and follow the standards and principals defined within it.

In meeting both standards a major part of the process is auditing. This often consists of visiting different departments/sections within a company and using an audit checklist to check for compliance. The following is an example form that may be used by an auditor when assessing user access control for ISO17799/BS7799:

Section	Question	Answer
User registration	Is there a formal registration process for users on the systems?	
	Are unique IDs used?	
Passwords and user access	Are passwords for systems stored centrally, and what controls are in place to ensure that unauthorised access does not take place to these passwords?	
	How often are individual user rights reviewed?	

[6] Information technology — Code of practice for information security management - ISO/IEC 17799 First edition, ISO, Geneva Switzerland. December 2000

	What is in place to ensure that users are de-registered from systems as needed?	
System Access logging	Are there procedures to monitor system use, and how often are they reviewed?	

Often a team is specially set-up within a company to audit against compliance principals. There are a number of products available to assist them in checking security of systems. One commonly used product is COBRA[7], which was developed by "C&A Systems Security Ltd" as a system for general risk analysis. It has been developed into a system, which can be used for the insurance that systems meet compliance to the BS7799/ISO17799 standards.

5. Business Continuity Management as Defined in ISO 17799

Within ISO 17799, Section 11 defines Business Continuity Management and the processes that can be used to ensure proper Business Continuity. By using and adhering to the processes in ISO 17799, a company can define procedures covering all aspects of good BCP. By following the procedures in order and adapting to individual needs and requirements, it helps to mitigate risks involved when undertaking major infrastructure changes.

The processes in Section 11 of ISO 17799 can be summarised as:

Section 1.1 - Business continuity management process

This defines putting in place a process for development and maintenance of Business Continuity throughout an organisation. It also details insurance of the following areas:

- Risk impact analysis – The analysis of risks, their impact which includes identification and prioritisation of critical business processes
- Understanding the impact which interruptions would have on a business
- Purchasing of suitable insurance as part of the business continuity process
- Formulation and documentation of a business continuity strategy and plans consistent with the agreed business objectives and priorities
- Periodic testing and updating of plans
- Integration of processes into organisation management structure at the appropriate level

Section 1.2 Business continuity and impact analysis

This defines that Business Continuity should begin by identifying events that can cause interruptions to business processes, which include:

[7] http://www.riskworld.net/

- Equipment failure
- Flood and fire.

Once this is done, a risk assessment to determine the impact from interruptions should be undertaken. It also says that this activity should be done in conjunction with all teams involved in a system. If it is found necessary from risk assessment, a strategy plan should be developed to determine the overall approach to Business Continuity. This should always get management endorsement.

Section 1.3 Writing and implementing continuity plans

This section it describes the writing of continuity plans and identifies that they should include the following sections:

- Identification and agreement of responsibilities
- Emergency procedures to allow recovery and restoration
- Documentation of procedures and processes
- Staff education in the agreed emergency procedures and processes
- Testing and updating of the plans

Section 1.4 Business continuity planning framework

This details creating a single framework of business continuity plans, which should include:

- Activation processes
- Emergency procedures
- Fallback procedures for re-location to alternative premises
- Resumption procedures to re-turn to normality
- Maintenance schedule for plan
- Awareness and education activities for BCP
- Responsibilities of individuals/Teams

Section *1.5 Testing, maintaining and re-assessing business continuity plans*

This section describes two important areas, and how by using them, plans can be kept up to date and relevant.

Testing the plans – The importance of ensuring that the plan is regularly tested for relevance, being up to date and effective is described. This should involve all affected teams. When testing a number of processes, it is recommended that simulation, tabletop testing and supplier facility testing is included, as well as the complete rehearsal of activation of BCP processes and DRP contained within them.

Maintaining and re-assessing the plans – This is probably the most important part of a BCP. A plan should be updated and re-assessed after a number events, including changes in:

- Personnel
- Addresses or telephone numbers
- Business strategy
- Location, facilities and resources
- Legislation
- Contractors, suppliers and key customers
- Processes, or new/withdrawn ones
- Risk (operational and financial)

6. The Cost Implications of Putting in BCP/DRP

It is not an uncommon view within a company that Business Continuity planning has only costs without any actual gain[8]. The following are areas that should be taken account of when considering BCP/DRP:

- What are the costs of part of a business/process being unavailable?[9] This consist the following areas:
    - Tangible Costs identified as actual items such as lost revenue and wage costs for idle workers
    - Lost Revenue and productivity from not being able to conduct business
    - Late Fees, Penalties and legal costs for delays in work delivery
    - Indefinable costs. This includes loss in new business opportunities
    - Remedial expenses such as additional staff expenses and additional marketing required when recovering from a loss in brand confidence

- Is the correct BCP/DCP process being planned? It is not uncommon to decide to go along the route of implementing BCP/DRP processes and taking it too far. It is a careful balancing act between putting in the correct processes to over coverage where there are too many procedures in place.

An area that is not often taken into account is the potential gain for a business in the implementation of standardised procedures. Gains include:

- **Easy to follow processes** – A good process can be followed by someone not usually working in the area failed within the business. It will also cut down on wasted time looking for information.

[8] http://www.guardian.co.uk/online/story/0,3605,1022649,00.html
[9] http://www.contingencyplanning.com/PastIssues/MayJun2002/1.asp

- **Improvements in security of systems** - It is not uncommon that when a major system fails and it is not correctly documented or backed up, for best practice to be dropped. With the pressures of recovery of services or processes, it can often seem more important to bring back a service by switching off or reducing controls such as Firewalls or not security patching machines to cut down on time delays involved in bringing systems back.

7. The Importance of BCP/DRP for Major Infrastructure Changes

With the correct procedures in place, consistency from good BCP/DRP can bring about major advantages to not just businesses but also the planning process for a major IT infrastructure change.

In the example of an e-commerce system it is common for it to cover a number of different disciplines and technologies. Areas and technologies may include:

- Security Systems - Firewalls, Intrusion detection and Anti-virus
- Networking – Routers, switches and cabling
- Operating systems – Unix and NT based. Different teams often support these
- System Monitoring – Network availability systems such as TNG, SNMPc and Cisco Works
- Database systems – SQL server and Oracle
- Applications – Dependant on the site used
- Web servers

Different teams or individuals often support these areas. It is common for there to be little communication between teams or individuals on a day-to-day basis with communication only happening at times of need, such as system failure.

By following industry best standards for BCP/DRP, defence in depth and reliability of infrastructure can be achieved. From my experience, following the principals of standards such as BS 7799/ISO17999 will gain in the following areas:

- **Procedures are regularly reviewed** – If best practices for change control are followed, then when a change is undertaken the approval process will trigger updates in documentation. At the regular audit review period then a complete review of all documentation will be put into place.
- **Security patching is kept up to date** – With adherence to standards, the monitoring should be in place for security alerts for systems. These can come from both vendors or mailing lists such as bugtraq (http://www.securityfocus.com)

- **Upgrade planning process is simplified** – When undertaking an upgrade, the planning process is usually more difficult than the actual work involved. In the example of an e-commerce infrastructure, an upgrade or change to a Firewall and then the work involved will normally cover more than just the Firewall. Even though a change to a Firewall in its simplest form may be only a case of upgrading with security patches, there can often be unknown effects. If vendors bring out an emergency patch to close serious security flaws it can bring about other affects such as changing functionality of systems or even resetting default settings. By knowing the full set-up of machines and infrastructure, workarounds can more easily be achieved which may involve other teams in altering functionality such as application settings.
- **System downtime is reduced** – In the above example of a Firewall change, it is unavoidable to undertake this without some system downtime. Whilst work may be scheduled during a known reduced activity period such as overnight on a weekend, due to the nature of the Internet and the 24-hour society, there is no time that would not cause some potential effect for loss in business. With correct documentation and procedures, the unpredictable can be taken into account and the potential downtime reduced. It is a common mistake when undertaking work to plan for the known, such as what needs to be done, with those involved engrossed in their work and then not noticing an overrun. Even in the case of an upgrade failing, a good set of BCP and DRP procedures will cover the event of how to back-out and restore business in a quick and reliable way.
- **Business profile is kept high** – When winning and maintaining business, the ability to show that systems and processes are correctly documented and adhered to, gives a good impression about the company or system and its inherent security to clients and customers. There will then be a likelihood of requests for undertaking future business.

8. Conclusions

I have discussed in this paper the considerations that should be taken for planning for business continuity and disaster recovery, and how they can actually produce gain, in financial savings and also to its reputation and profile.

In summary, good BCP/DRP is not just a case of producing a set of procedures and processes. The main goal always should be to implement easy to follow, relevant and appropriate procedures and practices, which bring into place reliable and secure well maintained systems and processes.

References

"Business Continuity Planning BCP " URL: http://www.nccglobal.com/consultancy/security/bcp.htm (29 Oct 2003)

"Y2K: the Benefits exceeded the Costs" URL: http://www.scoop.co.nz/mason/stories/HL0001/S00007.htm (1 Nov 2003)

"Trends in Business Continuity Planning: Not What everyone Expected" URL: http://www.csoonline.com/analyst/report484.html (28 Oct 2003)

"What are ISO 9000 and ISO 9001?" URL:http://www.isoeasy.org/ (2 Nov 2003)

"Technology Law Update: September 2003" URL : http://www.ffwlaw.com/%5BResources%5D/Publications/BTMT/Technology_Law/technologyupdatesummer2003.pdf (30 Oct 2003)

Information technology — Code of practice for information security management - ISO/IEC 17799 First edition, ISO, Geneva Switzerland. December 2000

COBRA – Security Risk Assessment and Security Risk Analysis URL: http://www.riskworld.net/ (31 Oct 2003)

"Pay now, live later" URL: http://www.guardian.co.uk/online/story/0,3605,1022649,00.html (3 Nov 2003)

"The True cost of Downtime". URL: http://www.contingencyplanning.com/PastIssues/MayJun2002/1.asp

Last Updated: September 24th, 2017

Upcoming Training

Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
Community SANS New York SEC401^	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
SANS DFIR Prague Summit & Training 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
SANS Phoenix-Mesa 2017	Mesa, AZ	Oct 09, 2017 - Oct 14, 2017	Live Event
SANS October Singapore 2017	Singapore, Singapore	Oct 09, 2017 - Oct 28, 2017	Live Event
SANS Tysons Corner Fall 2017	McLean, VA	Oct 14, 2017 - Oct 21, 2017	Live Event
SANS Tokyo Autumn 2017	Tokyo, Japan	Oct 16, 2017 - Oct 28, 2017	Live Event
CCB Private SEC401 Oct 17	Brussels, Belgium	Oct 16, 2017 - Oct 21, 2017	
SANS vLive - SEC401: Security Essentials Bootcamp Style	SEC401 - 201710,	Oct 23, 2017 - Nov 29, 2017	vLive
SANS Seattle 2017	Seattle, WA	Oct 30, 2017 - Nov 04, 2017	Live Event
San Diego Fall 2017 - SEC401: Security Essentials Bootcamp Style	San Diego, CA	Oct 30, 2017 - Nov 04, 2017	vLive
SANS San Diego 2017	San Diego, CA	Oct 30, 2017 - Nov 04, 2017	Live Event
SANS Gulf Region 2017	Dubai, United Arab Emirates	Nov 04, 2017 - Nov 16, 2017	Live Event
Community SANS Colorado Springs SEC401~	Colorado Springs, CO	Nov 06, 2017 - Nov 11, 2017	Community SANS
SANS Miami 2017	Miami, FL	Nov 06, 2017 - Nov 11, 2017	Live Event
Community SANS Vancouver SEC401^	Vancouver, BC	Nov 06, 2017 - Nov 11, 2017	Community SANS
SANS Sydney 2017	Sydney, Australia	Nov 13, 2017 - Nov 25, 2017	Live Event
SANS Paris November 2017	Paris, France	Nov 13, 2017 - Nov 18, 2017	Live Event
SANS San Francisco Winter 2017	San Francisco, CA	Nov 27, 2017 - Dec 02, 2017	Live Event
SANS London November 2017	London, United Kingdom	Nov 27, 2017 - Dec 02, 2017	Live Event
Community SANS St. Louis SEC401	St Louis, MO	Nov 27, 2017 - Dec 02, 2017	Community SANS
Community SANS Portland SEC401	Portland, OR	Nov 27, 2017 - Dec 02, 2017	Community SANS
SANS Khobar 2017	Khobar, Saudi Arabia	Dec 02, 2017 - Dec 07, 2017	Live Event
SANS Munich December 2017	Munich, Germany	Dec 04, 2017 - Dec 09, 2017	Live Event
Community SANS Ottawa SEC401	Ottawa, ON	Dec 04, 2017 - Dec 09, 2017	Community SANS
SANS Austin Winter 2017	Austin, TX	Dec 04, 2017 - Dec 09, 2017	Live Event
SANS Bangalore 2017	Bangalore, India	Dec 11, 2017 - Dec 16, 2017	Live Event
SANS vLive - SEC401: Security Essentials Bootcamp Style	SEC401 - 201712,	Dec 11, 2017 - Jan 24, 2018	vLive