Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials: Network, Endpoint, and Cloud (Security 401)"
at http://www.giac.org/registration/gsec

Business Continuity Planning beyond ISO17799

GIAC Security Essentials
Practical Assignment version 1.4
Option 1

Masahito Gotaishi
13 January 2004

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

[0] Abstract
Although there was a tragic and unfortunate terrorist attack on 9/11 2001, and Business Continuity Plan (BCP) is specified in various security standards including ISO17799, quite a few organizations are still unready for contingency. It is assumed that it is because the requirements of ISO7799 are not enough for good BCP. In order to discuss the matter, I looked into the requirement of ISO17799 on BCP and other guidelines on Business Continuity Management.
Consequently I have concluded that the risk assessment procedure for BCM is different from the one for ISMS. More effort should be spent on the Business Impact Analysis (BIA) and Risk Assessment for BCM with more emphasis on the quantitative risk assessment.

[1] Introduction
On September 11, 2001, when the terrorists attacked the World Trade Center, almost all people identified that a disaster is an actual threat to the business process and realized the necessity of business continuity management. However, an article of CFO Magazine[1] reported that a survey found that only two-thirds of the large corporations believed that they are better prepared to access critical data in the wake of a disaster than they were two years ago. Average score of the self-assessment was C+. According to a supplier of business continuity system[2], although organizations were unprepared even for mundane business interruption risk, they were rather reluctant to invest in the business continuity safeguards. According to the recent survey to business continuity managers[3], quite a few companies (39.5%) conduct business impact assessment (BIA) more than once per year. But 43% of the companies answered that they have never done BIA or carried it only once when BCP was developed.

The Section 11 of the ISO17799 security standard specifies the BCP of the information processing activity. Other standards such as HIPAA also require implementing BCP. Although, significant numbers of organizations do not only lack adequate business continuity plan, its very essential processes such as BIA are not properly addressed.

These facts show that it needs more than the codes specified in these guidelines to implement successful BCP. A veteran Business Continuity Consultant pointed out in the interview of Infocon Magazine[4] that ISO17799 was not expected to provide a good template for designing a business continuity management process. According to him, “There are other codes of practice available for BCP, which go beyond ISO17799.” I would like to discuss what other codes are necessary.

[2] BCP in the ISMS

(a) Terminology
There are several technical terms used interchangeably in the business continuity management. I would like to sort out each meaning and mutual positioning:

- Business Continuity Plan (BCP)
  Process of developing advance arrangements and procedures that enable an organization to respond to an event in such a manner that critical business functions continue with planned levels of interruption or essential change.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

- Contingency Plan
  A plan used by an organization or business unit to respond to a specific systems failure or disruption of operations. A contingency plan may use any number of resources including workaround procedures, an alternate work area, a reciprocal agreement, or replacement resources.

- Disaster Recovery Plan (DRP)
  The document that defines the resources, actions, tasks and data, which are required to manage the business recovery process in the event of a business interruption. The plan is designed to assist in restoring the business process within the stated disaster recovery goals.

(from "Business Continuity Glossary" of Disaster Recovery Journal homepage[5])

Considering the definition above, I would like to position each concept in following way:
BCP includes the whole activity including the identification of mission-critical processes, BIA, and development of contingency plans for each process.
Contingency plan is the preparation for any unforeseen event including disaster. It defines how to respond to the contingency in order to continue the business process, and how to restore the normal state of the process afterwards.
DRP is the contingency plan for disasters and typically includes the procedure of securing human safety.

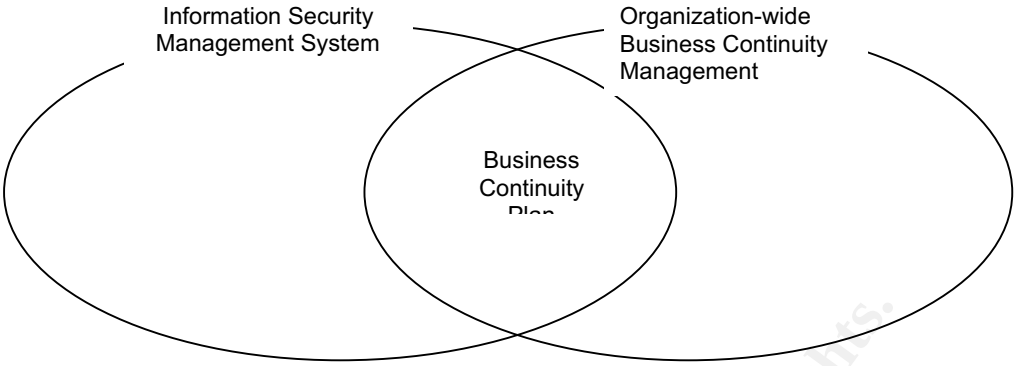
(b) Availability and Business Continuity
Availability is one of the three tenets of information security (Confidentiality, Integrity, and Availability). Therefore availability (=avoiding downtime) of mission-critical IT process such as ERP or groupware is one of major themes of information security. Consequently, it would be sufficient just thinking of maintaining availability of information assets. Why is one independent section spent on BCP? I think that the concept of BCP adds following consideration to the ISMS:

1. One important objective of maintaining availability of information assets is maintaining the overall business continuity. Therefore we need to keep an eye on the role that each information asset plays in the business processes.
2. There are quite a few conventional hazards such as natural disaster among the threats to availability. Such non-IT threats should not be forgotten.
3. Quite commonly these hazards lead to human injury or loss of tangible assets. Therefore we need to assume such cases as 'key personnel becomes unavailable and some members have to immediately succeed him' or 'we must give first aid to the injured people before restoring the process'
4. Unlike information security breaches, quite a few insurance goods cover business interruption. Therefore risk transfer is important in planning business continuity.

BCP might look like a subset or extension of information security management. On the other hand, for most organizations business continuity management (BCM) is the holistic security issue, which influences all stakeholders and includes all business processes. Therefore, we would have to look at the BCP as the overlapping part between ISMS and holistic BCM (Figure 2-1). It should not be forgotten that BCP in the ISMS must be also based on the organization-wide BCM.

Figure 2-1: BCP in the security management should be implemented also as a part of holistic Business Continuity Management

© SANS Institute 2004, Author retains full rights.



[3] Basics of Business Continuity Planning

Before discussing the improvement of BCP, I would like to sort out basic knowledge of BCP and its relationship with information security:

(a) Requirement of ISO17799 to BCP

Section 11 of ISO17799 specifies following matters[6]: (Reverse-translated into English from the JIS X 5080)

11.1.1 Business Continuity Management procedure should be planned, with consideration of following points:

- Priorities of business processes
- Identifying the influence of the process interruption
- Business Interruption Insurance
- Documenting the business continuity strategy
- Testing the plan and procedure
- Holistic BCM included in the organization-wide framework

11.1.2 Business Impact Analysis (BIA) and risk assessment (RA) should be made.

11.1.3 Business Continuity Plan should be made considering following points:

- Identification of all responsibility and emergency procedure
- Contingency plan considering the process recovery
- Education of members
- Test and update of the plan

11.1.4 The framework of BCP should consider following points:

- Condition of executing the plan
- Emergency procedure in case business or human life is jeopardized
- Backup site and procedure
- Recovery plan
- Test procedure and maintenance plan along the test result
- Education
- Individual responsibility

11.1.5.1 BCP should be tested, with at least following test procedure:

- Desktop test
- Mockup test
- Technical recovery test
- Recovery test in the backup site
- Checking (auditing) suppliers' institutes and services

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

- Holistic recovery test

11.1.5.2 BCP should be periodically reviewed and re-evaluated

(b) Prime Elements of BCP procedure
According to the Guideline of Business Continuity Institute (BCI)[7] and the guideline of Australian government[8], BCM should be done with following steps:

Step 1: Project Initiation
Before actual planning work begins, all senior managers of the organization should realize that Business Continuity Management (BCM) is very important to the organization and that it is part of every manager's normal responsibilities.

- The BCM committee should persuade the Board of its importance.
- Managers or senior managers should join the project team (full-time participation is not always required). They should be devoted, at least, in the BIA step.

Step 2: Understanding the Business, or Mission of the Organization
This step is the BIA/RA. It would be the most important in the BCM. Beforehand analysis of the business and identification of the mission-critical process is necessary.

- Mission critical processes and functions should be identified.
- Impact on business of loss of mission critical process should be determined.
- Threats to critical processes/functions should be reviewed
- Risks should be prioritized

Step 3: Developing Continuity Strategies
After the analysis is done, it should be decided how the risk is mitigated.

- Alternatives of the continuities should be listed up.
- Afterwards it should be discussed which strategy to take

Step 4: Implementing Continuity Treatments
When it is decided how they should respond to the contingency, they have to prepare documentation and material during the usual state, including the documented procedure and back-up tapes, etc.

- Preparation for the recovery process, such as taking back-ups, should be implemented in the usual operation.
- Procedure of the BCP should be documented

Step 5: Test and Maintenance of the BCP
In order for the people to become able to execute the procedure in case of emergency, rehearsal is necessary. According to the result of test / rehearsal and the change of business process, the BCP should be also changed. This part is not so different from the corresponding part of ISO17799.

- The BCP plan should be exercised as a walk-through or a full system test
- Plan reviewing / maintenance scheme should be defined

Compared with the recommendation of ISO17799, it is noted that the BCM guideline has more detailed requirements to the project initiation and risk analysis. Most of the BCM guidelines emphasize the importance of executive support and active participation of the senior managers. And they require BIA/RA and specify the detailed procedure.

It should be noted that the result of BIA/RA for information security is not directly

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

used for business continuity plan. Business continuity plan needs its own BIA/RA. Next I am going to examine how Risk Analysis should be done.

[4] Basics of Risk Analysis

Usually risk is expressed in numeric value. Information Security risk is usually assessed qualitatively, although quantitative analysis is also used in quite a few situations. Here both ways are briefly described and compared.

(a) Quantitative Risk Analysis

Quantitative Analysis is expressing the Risk as Annualized Loss Expectancy (ALE). This is calculated by following formula:

ALE={(Asset Value)×(Exposure Factor)} × (Annual Rate of Occurrence) (i)

also expressed as:

ALE=(Single Loss Expectancy) × (Annual Rate of Occurrence) (ii)

(Asset Value× Exposure Factor = Single Loss Expectancy)

Exposure Factor (EF) is the percentage of loss which a realized threat event would have on a specific asset. Annual Rate of Occurrence (ARO) is calculated from the historical data, by dividing the number of occurrence with the observation period.

The Single Loss Expectancy (SLE) is the value describing the damage caused by the disaster / contingency. The Business Impact Analysis can be also defined as "The activity of calculating SLE."

(b) Qualitative Risk Analysis

(1) Theory of Risk Analysis

Qualitative risk analysis method is quite common in analyzing information security risk. No matter qualitative or quantitative, the purpose of risk analysis is to discuss the cost-effectiveness of the given safeguard and make "to implement or not to implement" decision. For that purpose, quantitative analysis calculates the ALE to compare with the cost of the safeguard. Instead, qualitative risk analysis evaluates the threats which the organization faces with some criteria. The cost-benefit evaluation of the safeguard is done with these criteria by rule of thumb. Peltier showed three examples of qualitative risk analysis in his book[9].

In all examples threats are listed and the impacts are examined and expressed, such as on a scale of 1 to 10. Afterwards safeguards are listed and each cost is compared with the risk evaluation. In the process of evaluating risk, the step of evaluating information asset is often included. It is quite natural because it is impossible to evaluate the risk of given threat unless the damage is evaluated. Nonetheless, Peltier also introduced approaches which do not require strict value analysis, such as the "30-minute" risk analysis.

(2) Methodology of Qualitative Risk Analysis

There are several methodologies and software which facilitates the above procedure. Quite a few of them such as COBRA (C & A security systems Ltd.) and SPRINT, SARA (Information Security Forum) are commercial products and consequently their detail is not disclosed to public. Here I would like to introduce two examples, OCTAVE and FRAP, whose information is available. They are originally specialized for assessing the

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

information security risk.

- FRAP

Facilitated Risk Assessment Process (FRAP) was created by T. R. Peltier. Its procedure is described in his book[10]. This methodology is designed for the senior managers themselves to meet together to discuss the risk. Therefore one of its distinguishing properties is finishing the risk analysis within short period, thereby saving mangers' time. Therefore mangers could actually devote themselves to the process. It consists of three parts:

1. Pre-FRAP meeting (about 1 hour)
   Brief meeting to agree on the scope, plan, selection of members, meeting mechanics, definitions of terms
2. FRAP session (about 4 hours)
   Main session to identify and prioritize the risks, and suggest controls against them
3. Post-FRAP process (about 10 days)
   The process of sorting out the result in order to decide how the risks should be controlled (whether to mitigate or accept, etc.)

- OCTAVE(SM)

Operationally Critical, Threat, Asset and Vulnerability Evaluation (OCTAVE)[11] was developed in the Carnegie Mellon University. It has two parts: OCTAVE Criteria[12] and OCTAVE Method. OCTAVE Method was developed as the risk assessment methodology consistent with the OCTAVE criteria. There are also several other methodologies developed by other third-party vendors, but among them, OCTAVE is the only methodology[a] developed by the Carnegie-Mellon University itself. It has 3 phases:
Phase 1: Build Asset-Based Threat Profiles
Phase 2: Identify Infrastructure Vulnerabilities
Phase 3: Develop Security Strategy and Plans
The overall process is accomplished by frequent workshops.
Compared with FRAP, OCTAVE methodology is done in more structured way, and proceeded in asset-based approach. The process begins with the identification and evaluation of information assets and infrastructure.

(c) Quantitative vs. Qualitative, information security vs. business interruption
As long as it is possible, quantitative risk assessment is better than the qualitative. Because_

- If the risk is expressed in quantitative (monetary) terms with supporting rationale, it will be better understood. Consequently the investment on the safeguard acquires organization-wide support.

- Quantitative risk data facilitates the cost/benefit assessment of safeguards, thereby effectively assists the budget decision-making.

The reason why quantitative assessment is not commonly used in information security management is because it is rarely possible. I agree with the past GIAC student[13] that Information Security Risk is usually impossible to quantify. Firstly, information assets / knowledge are difficult to value quantitatively. Secondly, statistical information about the information security threat is by no means enough to

[a] There is another methodology, OCTAVE-s, also developed by Carnegie-Mellon University. This was created by arranging OCTAVE for smaller organization.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

discuss ARO. And finally, EF of security breaches such as unauthorized disclosure cannot be decided objectively.

On the other hand, significant proportion of business interruption risk should be calculated quantitatively. Organizations tend to overlook considerable part of financial loss caused by business interruption and thus they must comprehensively review the whole possibility of the loss. And, as pointed out in the section [2](b), insurance should be considered as an important safeguard. Quantitative discussion is necessary in selecting the insurance. There is a discussion of financial loss incurred by business interruption[14]. In this article, Mr. Imfeld emphasized that the discussion about the effect of the business interruption should not only be focused on the immediate loss but also the consequent decline of market share, increase of churn rate, etc.

[5] Conclusion: Proposal for the better BCP

After the above discussion, I observed following problems in the current BCP:

(a) It is possible that senior mangers leave Information Security risk assessment to specialists. But business interruption risk assessment should be done by the senior managers themselves, because it is necessary to identify which business process is really important in the overall organization.

(b) ISO17799 requires BIA in developing BCP, but it does not specify how to do that. In fact, BIA for the BCP should be done in a different way from the one for information security.

(c) Methodology of risk assessment is different in the BCP (business interruption risk). The risk should be analyzed quantitatively.

So I would like to propose following matters:

(a) BCP needs its own risk assessment besides the one for ISMS.
The process of risk assessment for BCP is significantly different from the one for ISMS. BCP should consider all business activities, including non-IT process. For example, if the manufacturing process cannot tolerate earthquake, it would be meaningless planning the continuity of the production management or MRP system in case of earthquake. Perhaps it would be impossible to integrate the risk assessment for BCP and the one for ISMS. It goes without saying that the one for ISMS cannot substitute the one for BCP. Its methodology should be quantitative, although adjusting the result in qualitative way is also desirable.

(b) Senior managers themselves should be responsible for the risk assessment, including BIA.
The mission-critical process should be discussed along the mission and strategy of the organization. This activity should be positioned as an important management decision. While the guideline of BCI just requires all senior managers understand the importance and support the BCM committee, the CISSP Prep Guide[15] insists that the representatives of senior managers should join the BCP committee. I think that the CISSP Guide's argument is better.

(c) RTO should be made much of in the BIA
In working out BIA for BCP, as Carter explained with an example[16], recovery time objective (RTO) of each function is equally important as its strategic positioning.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Or it would be more important in the majority of the cases. For example, marketing would be strategically no less important for banks than the operation of automatic teller machines (ATM). However, while marketing activity can tolerate interruption for days, ATM downtime for 1 day can cause extensive trouble to customers and it might lead to lawsuits. In this example ATM is more mission-critical than marketing. Although the RTO should be carefully worked out and agreed among senior managers, ISO17799 only implicitly mentiones it.

All companies and public organizations are highly dependent on each other in the current network society. Therefore business interruption makes significant influence to the wide range of stakeholders. Government's guidelines and regulations require companies to maintain business continuity in order to protect nationals, who are important stakeholders of various industries. Nevertheless, guidelines do not really guide organizations to their optimum BCP. For that purpose, additional effort and discussion are necessary. If sound consideration were made, it would be found that good practice of BCP derives competitive advantage to the organization and it is thus worth effort.

© SANS Institute 2004, Author retains full rights.

References

[1] Leibs, Scott, "Two Years Later, Still Adrift?" CFO Magazine September Issue 2003, URL: http://www.cfo.com/Article?article=10545 (29th December, 2003)
[2] Pastore, Michael, CIO Update "People, Planning Key to 'Business Continuity,'" August 5, 2003
URL: http://www.cioupdate.com/trends/article.php/2244581 (29th December, 2003)
[3] Editor of globalcontinuity.com, "BIA survey results," February 11, 2003,
URL: http://www.globalcontinuity.com/article/articleview/331/1/31 (29th December, 2003)
[4] Naef, Wanja Eric, "Business Continuity Planning Interview with David Spinks, EDS," Infocon Magazine Issue One, October 2003,
URL: http://www.iwar.org.uk/infocon/bcp-spinks.htm (28th December, 2003)
[5] Disaster Recovery Journal, "Business Continuity Glossary,"
URL: http://www.drj.com/glossary/drjglossary.html (24th December, 2003)
[6] ISO/IEC 17799 : 2000 Section 11 (Actually its Japanese translation JIS X 5080: 2002 was referred to)
[7] Business Continuity Institute "Business Guide to Continuity Management,"
URL: http://www.thebci.org/Guidelines.doc (28th January, 2004)
[8] Australia Government, "Better Practice - Business Continuity Management, Keeping the wheels in motion,"
URL:
http://www.anao.gov.au/WebSite.nsf/Publications/4A256AE90015F69B4A2568EE0010062B (5th January, 2004)
[9] Peltier, Thomas_R., Information Security Risk Analysis, chapter 2, Auerbach Publications, 2001. pp. 23-46
[10] Peltier, Thomas_R., Information Security Risk Analysis, chapter 5, Auerbach Publications, 2001. pp. 69-90
[11] Alberts, Christopher J., Dorofee, Audrey J., "OCTAVE(SM) Method Implementation Guide Version 2.0," URL: http://www.cert.org/octave/download/intro.html (5th November, 2003)
[12] Alberts, Christopher J., Dorofee, Audrey J., "OCATAVE Criteria, Version 2.0," December 2001, URL: http://www.cert.org/archive/01tr016.pdf (20th January, 2004)
[13] Vuisintine, Vishal, "An Introduction to Information Risk Assessment," SANS GSEC Repository, August 8, 2003, page 8.
URL: http://www.giac.org/practical/GSEC/Vishal_Visintine_GSEC.pdf (10th November, 2003)
[14] Imfeld, Daniel "Keeping an eye on interruption risk," Insurance Risk supplement to Risk magazine, December 2000 issue
URL: http://www.financewise.com/public/edit/riskm/art/art-newsolutions.htm (10th January, 2004)
[15] Krutz, Ronald L., and Vines, Russel D., The CISSP Prep Guide John Wiley & Sons, Inc. pp. 275
[16] Carter, Phil, "Business Impact Analysis: the Starting Block for Business Continuity,"
URL: http://www.infosecnews.com/opinion/2003/01/22_04.htm (5th December, 2003)

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.