Global Information Assurance Certification Paper

IS Risk Assessment
&
Risk Management Processes in Large Organisations

Author : Naume Srbinoski

Course : GSEC Option 1, Version 1.4b

Date : June 2004

Table of Contents

Table of Figures

1 ABSTRACT

Viruses, worms, Trojans, inappropriate access, malicious code and identity theft, are just a small number of factors that can threaten organisations in today's highly computer dependent society. As an organisations' exposure to these risks increases so to do the potential consequences, ranging from no or very little impact, to legal action or affecting the organisations reputation or share price.

Although management generally addresses risks associated with general business functions such as financial or legal fraud, it is rare that critical computer systems are provided similar treatment. By neglecting computer systems in this way dishonest individuals have a greater opportunity to exploit these systems and compromise the overall security of many organisations.

The intent of this paper is to assist organisations in the understanding of and the need for a pragmatic risk assessment methodology, in addition to the requirements for an incident handling process. The existence of both of these processes will ensure an organisations exposure to risk is minimal and in the event of a threat materialising the incident handling process will provide clear and agreed procedures to promptly address incidents.

2 INTRODUCTION

Although many organisations address business related risks such as those related to financial, legal or safety, computer system are not generally afforded a similar high profile and hence lack many of the important risk mitigation processes. Much of this is due to the fact that many Information Services (IS) groups have historically been technically focussed with very little business or process knowledge.

Today Chief Information Officers are increasingly sought to provide the business with a strong business focus, account for all expenditure and liase with upper management in business terms. These factors and the high reliance on Information Technology (IT) have raised the profile of the Information Services department.

This new profile, growing frequency and consequences of attacks on large organisations have changed the focus for many IT departments. This has resulted in a number of changes including the need for processes and policies and a growing importance and the need to address risk management. Both of these changes now feature prominently in IT business plans and are a growing requirement for legal requirements. The risk management output is also an important input into risk mitigation strategies and the business justification for the prioritisation and allocation of funds.

Risk management alone will not, and does not attempt to address all risks, as policy, process or technical countermeasure cannot be 100% effective. Hence the incident management process is essentially very closely linked to the risk management process by providing a procedure that addresses IS related incidents and minimises the impact of such incidents upon the business.

3 RISK MANAGEMENT OVERVIEW

Risk is defined as 'the chance that something happening will have an impact upon objectives and is measured in terms of consequences and likelihood' [1]. A risk management policy is an integral part of the management process and must be relevant to an organisations' strategic goals, objectives and the nature of its business. It must be part of the overall risk management plan and in order for the plan to be effective it must be clearly understood, implemented and maintained.

A very important differentiator between a risk management process and many other processes, including audits, is the frequency at which the review is carried out. Audits generally consist of a once-off investigation that is usually quite focussed and more often than not locked away and never looked at again. On the other hand risk management is an iterative organisational improvement process performed and reviewed on a regular basis. With each cycle risk criteria can be strengthened to achieve progressively better levels of risk management.

It must be noted that there are a number of existing risk management frameworks that can be used in the development of a customised process. These include but are not limited to the OCTAVE (http://www.cert.org/octave/) and Intel processes. The first of these is the Operationally Critical Threat & Vulnerability Evaluation, better known as the OCTAVE process and jointly developed by the US Department of Defence and Carnegie Mellon University. The OCTAVE process is an exceptional methodology for evaluation and assessment of threats and vulnerabilities. Unfortunately it does not provide metrics to measure risk and can be quite a cumbersome and time-consuming process.

The second notable and well-established process is that developed by Intel Corporation in the US. This process is a more pragmatic implementation that also incorporates useful metrics, which are relative measures, for the measurement of risk. This addresses the issue faced by many organisations, i.e. you cannot control what you cannot measure. The Intel process introduces the iterative two-loop process and is based upon Business Assets.

A key attribute of these frameworks is the use of relative measures of the magnitude of threats and vulnerabilities. While the question of 'how likely is it that something will occur' is difficult to answer, it is usually possible to make a reasonable assessment of whether a certain threat is more likely than another. This assessment and measurement process is an effective and practical means of prioritising investment in risk mitigation.

By combining the two frameworks and existing risk management standards, the case study discussed in this paper details the process developed by a large international corporation. The resultant process assisted the organisation to fully understand and mitigate the risks to the business associated with information systems.

4 KEY INFORMATION RISK MANAGEMENT TERMS

There are a number of key terms that must be understood prior to understanding and developing a risk management process. Some key terms include, threats, vulnerabilities, risks, assets, etc.

Threats can be defined as any event that may prevent or inhibit an organisations' ability to meets its business objectives (http://online.standards.com.au/online/autologin.asp). A threat has the potential to cause an unwanted incident that may result in harm to a system or organisation and its assets. Given that IS assets support the Business Assets, factors that threaten IS assets are threats to the business asset. Threats mainly come from the environment, other systems or people and can originate internally or externally from the organization. The threat may be an act of nature, accident or an intentional act. In general a threat could result in:

- Destruction, theft of loss of an asset
- Corruption or modification of an asset
- Disclosure of an asset
- Interruption of services.

Organisations cannot control the existence of threats. Effective risk management is about recognizing the existence of threats, and stopping them from materialising by:

- Understanding the sources of threats.
- Understanding the impact on realizing value from assets.
- Predicting the likelihood of occurrence

Examples of threats include, viruses, worms, brute force attack, natural disasters, corporate sabotage, malicious code, etc.

Vulnerabilities are defined as weaknesses associated with an organisations assets that allow threats to materialise. Vulnerabilities consist of security gaps in current process, systems, technologies or practices that lend themselves to being exploited. Remediation of vulnerabilities reduces risk exposure but it is impossible to address all vulnerabilities for a variety of reasons. These may include the fact that there are too many, they are not yet fully understood, they have yet to be identified or there are budgetary or business constraints.

The approach to risk mitigation is to prioritise remediation on the basis of the value at risk, i.e. mitigate risks that have the highest consequence first. As not all vulnerabilities can be mitigated, they should be investigated and mitigation costs assigned. If mitigation is a higher cost than the value at risk the vulnerability may be best controlled through awareness and manual processes rather than costly technical solutions.

In the context of an enterprise IT infrastructure the following are examples of vulnerabilities; inappropriate access, wireless access points, weak passwords,

poor or lack of relevant procedures, etc. With so many viruses and worms being released into the wild, a vulnerability that many organisations can relate to is poor Operating System security patching processes and procedures. This vulnerability allows worms and viruses to penetrate organisations defences and depending upon the destructive capabilities of the threat, result in either very little impact or cause major financial losses as a worst-case scenario.

Critical Business Assets can be defined as a logical grouping of process, plant, system, people or business function. Key identification criteria may include the fact that the asset:

- Has a Business Continuity Plan (BCP) associated with it
- Is known to be critical to the company's operations
- Is likely to have a direct impact on the company's performance in the event of failure or malfunction
- Has revenue-generation or revenue-management significance

An IS Asset is a logical grouping of Information Systems, not necessarily a physical instance of software or hardware. IS Assets can be identified by the following behaviour;

- Typically exposed to same vulnerabilities and threats
- Typically support the same set of critical Business Assets
- Whose failure could have significant on company's operations
- Are known to contribute to the company's exposure to risk
- Typically supplied and supported by a single vendor

Correct grouping prior to embarking on a risk, threat, and vulnerability assessment is critical. The more groupings of IS Assets underlying a Business Asset, the higher the IS risk level, which is to be expected, as the more IS components that a Business Asset depends on the greater the IS risk level,

Potential IS groupings for a risk management framework include the following:

- Mainframe - Hardware, operating system and applications that reside on it.
- Network - Cables, active & passive network hardware, switches, firewalls and other associated equipment
- Midrange – Hardware such as VAX and NT servers, and applications that reside on it
- Workstations - Workstations should be considered at a group-wide level, as the policy for their use and configuration is set at this level. Where a workstation, or group of workstations differ from the group standard they should be included as a grouping. Workstations should also be considered if hosting any applications that are required for the operations of the Business Asset

Risk is the potential that a given threat will exploit vulnerabilities to cause loss or damage to an asset or group of assets, and hence directly or indirectly to the organisation. Risk is also a measure of human, environmental impact or economical loss, in terms of both an incident likelihood and the magnitude of that impact or loss. In general, a risk should be considered in terms of known controls that will affect its likelihood. Additionally if an incident has occurred and mitigations have been put in place – the strength of these controls should be considered.

Threats and vulnerabilities are closely related and one cannot affect an organisation without the presence of the other. In the earlier example, a virus could not have infected computer systems had the operating system patching vulnerability not existed. Threats can come from anywhere and the objectives may also differ, similarly vulnerabilities may also be large and varied. Security efforts are complicated further by the shorter length of time between the discovery of new vulnerabilities and when it is first exploited. It is for these and many other reasons that an effective risk management process is required for today's modern and always connected enterprise.

4.1 IS ASSET FAILURE MODES

It is generally accepted that IS assets, can only fail in four general ways, these are as follows:

- Disclosure – The IS asset is compromised in such as a way that sensitive intellectual property is available to unauthorised users or resources
- Modification – The IS system or information contained on that system is modified either deliberately or accidentally in a manner that caused a failure of the IS asset.
- Loss/Destruction – The IS asset is permanently disabled and normal service will not be restored. This may be the result of a major fire or severe environmental incident.
- Interruption – Differs from loss and destruction in that normal service of the IS asset will be resumed. An example of a common interruption is power loss.

These IS asset failure modes are used by many organisations to develop threat and vulnerability assessments that are an integral part of the risk management process.

5 RISK ASSESSMENT & EVALUATION

There are many ways of calculating IS risks and indeed risks in general, the main objective is to ensure consistency during the evaluation process and to ensure that the results are both valid and useful when comparing results. The following description is used as a basic introduction in order to introduce and present the entire risk management process.

Risk management standards are available that detail possible methods of evaluation (http://online.standards.com.au/online/autologin.asp). Two ways that are widely accepted and used throughout the IT industry include the use numbers and the other uses a criticality scale. In general both these methods essentially use a simple formula to produce a risk rating. This formula adds or averages the consequence and the likelihood of a certain scenario. The two examples are as follows:

Sample Risk Quantification 1:

- Likelihood – Almost Certain (A), likely (L), moderate (M), unlikely (U)
- Consequence – Critical (C), high (H), medium (M), Low (L)
- Risk – High (H), medium (M), low (L)

Sample Risk Quantification 2:

- Likelihood – Almost Certain (5),Likely (4), Possible (3), Unlikely (2), Rare (1)
- Consequence – Critical (5), Major (4), Moderate (3), Minor (2), Low (1)
- Risk – Extreme (9,10), High (6,7,8), medium (4,5), low (1,2,3).

It is this second risk quantification process that has been used to demonstrate the usefulness of the risk management process and has been used at a major organisation. Further details cannot be supplied due to IP related issues.

Consequence →	Low (1)	Minor (2)	Moderate (3)	Major (4)	Critical (5)
Likelihood ↓					
Almost certain (5)	High (6)	High (7)	Extreme (8)	Extreme (9)	Extreme (10)
Likely (4)	Moderate (5)	High (6)	High (7)	Extreme (8)	Extreme (9)
Possible (3)	Low (4)	Moderate (5)	High (6)	Extreme (7)	Extreme (8)
Unlikely (2)	Low (3)	Low (4)	Moderate (5)	High (6)	Extreme (7)
Rare (1)	Low (2)	Low (3)	Moderate (4)	High (5)	High (6)

Figure 1. Risk Assessment, Consequence & Vulnerability Matrix

Note that the risk management process would prioritise risk mitigation based upon the abovementioned results, i.e. extreme, followed by high, moderate and low and allocate funds accordingly. The business may never address the low and moderate risks as they may consider these acceptable.

6 CASE STUDY : RISK MANAGEMENT OVERVIEW

Taking many of the previous methodologies into consideration, OCTAVE, Intel and relevant standards, a risk management process was recently developed for a large international organisation. It was subsequently piloted, implemented and formed a key component of a balanced IS scorecard that was then communicated to senior management. The outputs of this process are now being used to effectively plan, prioritise and address high-risk issues. As previously mentioned much of the finer detail has been omitted as it is considered sensitive and private information.

The risk management process essentially produces a metric that is relative and is of no use on its own. The process is driven by a number of threat and vulnerability assessments that take into consideration the previously mentioned failure modes and the risk assessment processes. The process can be driven by spreadsheets or databases, or specialised manually and although the output is a raw score that is the output of a formula, much of the benefit is in the conversation associated with each risk assessment. Hence it is of the utmost importance that this dialogue is captured and documented to assist with the next iteration of the process and to provide background material that justifies the raw score.

The metric that has been produced is defined as iRRL, Relative Risk Level due to IS. It is a metric that measures relative exposure to risk and can be used as a guide for risk mitigation activity. The iRRL should be higher if there are threats more likely to occur that will threaten business value. Mitigation of vulnerabilities should lower the iRRL, but it is unreasonable to expect that an iRRL would fall to zero if all mitigations are made as value is at risk and all vulnerabilities and threats are not known.

$$iRRL = \frac{(\text{Value-at-Risk}) \times (\text{Likelihood of Threats})}{(\text{Control over Vulnerabilities})}$$

Figure 2. iRRL Equation

6.1 PROCESS INTRODUCTION

In order to identify, manage and reduce risk a process is required to continually reduce the exposure of a Business Asset to risk. The most effective approach to reducing the enterprise risk level (iRRL) is to reduce vulnerabilities and control threats for those IS assets that contribute the highest level of risk to the overall enterprise risk score.

Identifying a 'top N' list of Business Assets is an initial step and it should actually identify the to Business Assets based upon their dependence on IS.

To obtain this data a business asset must be scored as to how it contributes to the business value and then analysed to ascertain how that relative score could be impacted by IS system outages or interruptions. Note that N is an arbitrary number, which is dependant upon the size of the organisation. Having identified the to N Business Assets that depend upon IS, the next step is to mitigate the vulnerabilities in the IS Assets that support the to N Business Assets. This identification and mitigation approach has lead to the definition of an iterative two-loop, eight step process as depicted below:

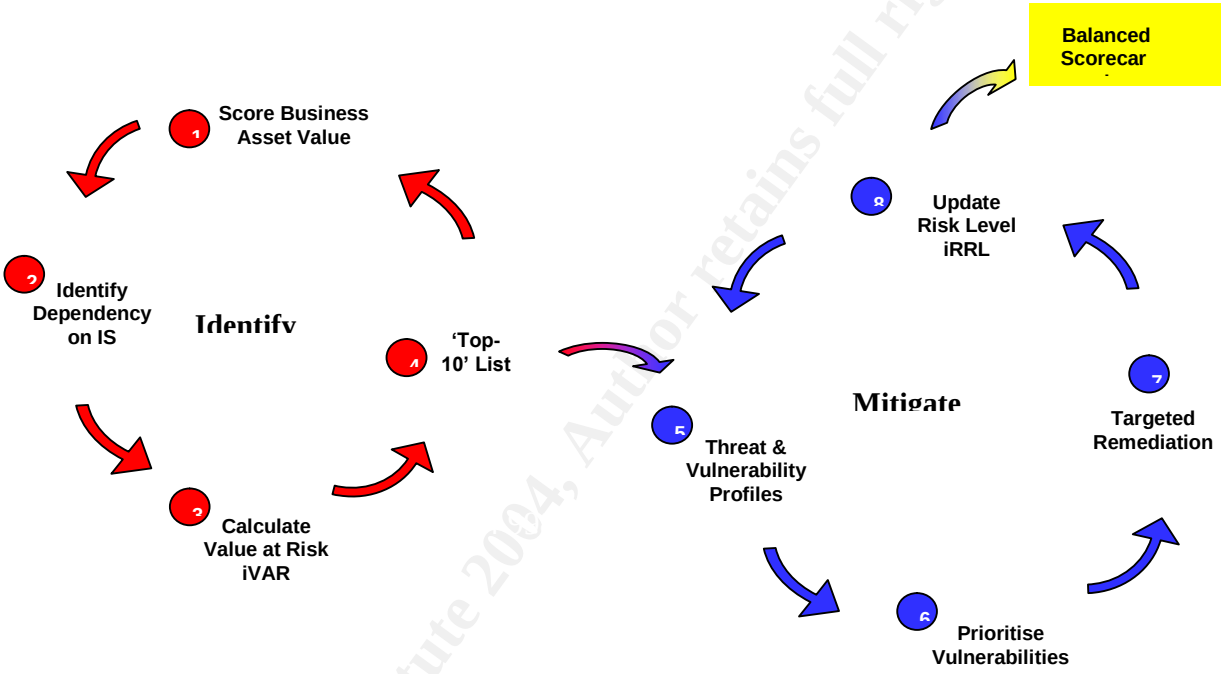

Figure 3. Risk Management Process, Two-Loop Representation

The initial loop identifies high value, high priority Business Assets that have the greatest dependence on IS assets and potentially the greatest impact in the event of the assets failing. Hence not every Business Asset will need to go through the detailed analysis that is required in the mitigation loop. This part of the process involves hundreds of questions that address IS threats and vulnerabilities. Once this has been completed it is followed by targeted remediation, which then changes the iRRL score and feeds back into the Balanced Scorecard. Note that the Balanced Scorecard is a high level reporting mechanism back into upper level management.

Another way of graphically representing the process is as follows:

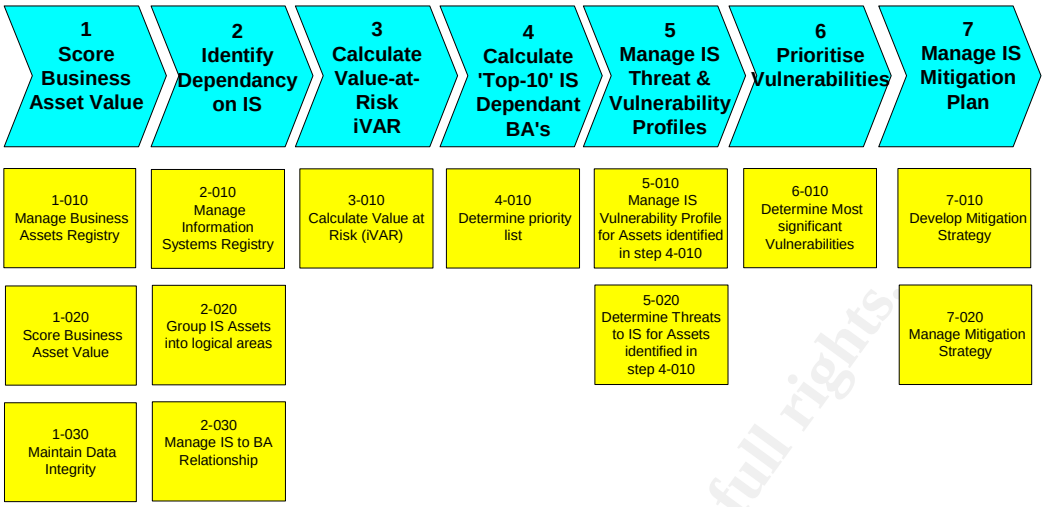

Figure 4. Risk Management Process Flow

6.1.1 Phase 1 – Identification

This phase identifies the top Business Assets in terms of their contribution to the business, then scored based upon dependence on IS. An initial measure of risk is produced, iVAR, which is the business value that is at risk due to an IS failure, forming the basis of the 'top-N' list. As Business Assets and supporting IS Assets do not change very frequently, it is suggested that this phase is undertaken annually and driven by the Business Units. An overview of each step of the process is described below:

Step1 : Score Business Asset Value – Based upon factors that are important to the organisation a likelihood and consequence evaluation is performed for failure scenarios to ascertain the value of the business and the potential value that is at risk. These factors may include financial losses, customer impact, legal action, safety, HR, etc and are usually linked back to the organisations bond.

Step2 : Identify Dependence on IS – This step assesses the Business Assets reliance on IS, the four categories mentioned previously may be used as a basic guide, i.e. Mainframe, Midrange, Network, PC's or any other groupings that may be useful.

Step3 : Value at Risk – Having identified Business Assets and the IS Assets that support them the next step is to determine the level of dependence that a Business Asset has on those IS Assets. The four failure modes that were previously discussed are used as the basis of this evaluation and the value produced is known as the iVAR.

Step 4 : Top N List – The 'Top-N' list is then the direct result of the iVAR value of Step 3. This sorted list will indicate which Business Assets should be targeted and prioritised for remediation.

6.1.2 Phase 2 – Mitigation

This phase essentially analyses the top business assets in order to mitigate these risks and reduce the iRRL, which subsequently feeds into the balanced scorecard. It is suggested that the mitigation phase also be performed on an

annual basis or as desired. This part of the process must be driven by the Corporate IS Security team but the actual remediation is carried out by the IS owners.

Step 5 : Threat & Vulnerability Profile – This is done using lists of well known threats and can be performed for each IS Asset that supports a Business Asset. A likelihood and consequence score is assigned to each threat and these can normally be grouped into Environmental, Human External, Human Internal and System. Similarly vulnerabilities are also grouped corresponding to each threat and these can be grouped into Organisation, Physical, Policy/Procedure, Technical & 3rd Parties. Again these are scored from 1-5 depending upon the level of controls over the vulnerabilities.

Step 6 : Prioritise Vulnerabilities - Highest contributing threats and vulnerabilities are then extracted to prioritise remediation.

Step 7 : Targeted Remediation – Common vulnerabilities across Business Units should be clear and projects may be initiated to mitigate these. Other vulnerabilities will only be mitigated based upon cost versus risk reduction comparisons.

Step 8 : Update iRRL - The final step in the mitigation loop is the recording of the iRRL and to ensure that projects that have been initiated in previous steps are in actual fact reducing the iRRL.

6.2 ISSUES & KEY LEARNINGS

In addition to a pragmatic risk management framework, two of the biggest challenges in developing and implementing risk mitigation strategies are management support, and 'buy-in', or support from the business. Without either of these the risk management process will fail from the onset. The two tend to be complementary and one cannot be effective without the other.

Generating business support can be a difficult task at the best of times, as the business often believes that they have far more important tasks to address. It is only through effective communications, training and management support that this can be achieved. Once the business people have been through the full process it is only then that they realise the effectiveness of the process and are often pleasantly surprised by the benefits.

Another key ingredient for success is the establishment and understanding of key roles for each step of the process. It is imperative that the business owns and manages the risks. The corporate IS departments' role tends to be more governance oriented and technical in nature, particularly during the mitigation phase of the process. The exact roles and responsibilities will be dependent upon the size of the organisation and its structure.

Prior to full-scale implementation of a process it is also good practice to run a pilot implementation. This pilot will ensure the process is appropriate for the business and meets all requirements. Finally it must be acceptable to all parties and more importantly must be formally signed off and agreed to.

7 CONCLUSION

Most large organisations are heavily reliant on Information Technology for their day-to-day operations. This reliance has also exposed the organisation to various threats and vulnerabilities, which are changing rapidly and also growing in number. This changing risk profile, dependence in IT systems and increasing regulatory and legal requirements has driven many organisations to develop and deploy risk management processes.

Many risk management processes are basically very similar to the case study detailed in this paper. Although the case study is based upon the Intel, Octave and relevant standards they essentially exist in order to provide the organisation with a clear understanding of IT risk and as a tool to minimise this risk by proactively and iteratively addressing and reducing relevant risks. It must be noted however that risks, consisting of threats and vulnerabilities, cannot be completely mitigated and it is not the intent of the risk management process to mitigate all risks. The risk management process is designed to document known risks and to address those that may have the greatest and unacceptable consequence for an organisation. The risk mitigation costs must also provide clear and measurable business benefits, i.e. if the cost of mitigating risk is greater that the consequence then an organisation may choose to accept this risk.

By far the biggest risk to any organisation is the lack of a risk management process that is regularly reviewed, i.e. lacking an understanding of or documenting the threats and vulnerabilities associated with it's IS assets. This paper has introduced the reader to the key concepts associated with risk management and has also presented a case study that has hopefully demonstrated the application of these principles and the importance of a risk management process.

By effectively implementing a risk management process an organisation regularly reviews and addresses risks associated with it's IS assets and indeed it's business. This proactive approach essentially reduces the organisations exposure to known threats and vulnerabilities, but does not eliminate or mitigate all risks. In the event of an incident due to any number of factors including a breakdown of controls, the presence of an effective incident management plan will minimise business impact and ensure business continuity is maintained.

8 REFERENCES

Standards Australia/Standards New Zealand, HB231:2004 Information Security Risk Management Guidelines, Second Edition 2004
URL: http://online.standards.com.au/online/autologin.asp

Standards Australia/Standards New Zealand, AS/NZ 4360:1999 Risk Management, 12th April 1999
URL: http://online.standards.com.au/online/autologin.asp

Working Council for Chief Information Officers, Trends in Information Security & Business Continuity Planning, 2003,

PriceWaterHouseCoopers, Information Security, A Strategic Guide for Business, Nov 2003

Organisation ABC, Company Code of Practice, Hazard and Aspect Risk Management, 2003,

Alberts, Christopher, Dorofee, Audrey, Stevens, James, Woody, Carol, Introduction to the OCTAVE Approach, August 2003
URL: http://www.cert.org/octave/

Various authors and papers have been referenced
URL: http://www.sans.org/

AusCert, Australian Computer Crime & Security Survey, 2003
URL: http://www.auscert.org/