Global Information Assurance Certification Paper

An Information Security Management System
And Policy Framework for Risk Management in Outsourcing Contracts

By
Arran Pearson
For
SANS GSEC Certification Practical Assessment (v1.3)
March 26, 2002

Abstract

This paper presents a generalized framework for allocating responsibilities for various security functions within an outsourcing contract. The framework is based on the outsourcing principles contained within ISO 17799:2000 and divides work along the lines of a risk management structure proposed in ISO13335-3:1998.

The paper also illustrates how the risk management framework proposed conforms to the requirements of ISO 17799:2000. The conclusions are that business control over risk management decisions cannot be outsourced. Whilst Information Security can be maintained in an outsourced environment, this requires a clear delineation of responsibilities between the business and the outsourcer.

1 Introduction

In the current IT environment it is becoming increasingly rare to find an organization that fully owns and operates all parts of its IT operations. From network to applications to business processes, it seems that all parts of the business have become a candidate for outsourcing in one form or another.

However, despite the increasing reliance on external providers to supply critical parts of the IT organization, Information Security has been one area that has been slow to react to the increased complexity that outsourcing places on the organization's Information Security Management Systems. Indeed, it is only recently that information security has become recognized as a candidate for outsourcing itself.

This paper presents framework is presented that outlines an appropriate division of roles and responsibilities for managing an organization's information security risks within an outsourced environment.

2 Outsourcing Security Principles

Outsourcing of critical IT infrastructure has been identified as being of particular concern to regulatory authorities[1] due to the amount of sensitive information that is being placed in the hands of entities external to that of the organization nominally entrusted with its care. This has been recognized within section 4.3 of the Code of Practice for Information Management[2].

This standard defines a set of principles that should be present within outsourcing contracts. A contract with an outsourcer should contain reference to:

1. How any legal requirements are to be addressed, for instance specific data requirements for maintaining the confidentiality and integrity of any personal details[3];
2. The arrangements that are in place to ensure that all parties are aware of their security responsibilities, this must include provisions for any sub-contractors that may be employed by the outsourcer;
3. How the confidentiality, integrity and availability of organizational assets are going to be maintained;
4. Those physical and logical controls which are used to ensure that access to organizational business information is restricted appropriately[4];
5. How service is to be maintained in the event of a disaster;
6. The physical security measures put in place to protect the organization's assets; and
7. The right of audit.

[1] APRA Insight
[2] ISO 17799
[3] Privacy Obligations for Government Contracts
[4] ISO 17799 Section 9

Whilst these principles provide a good foundation for ensuring that Information Security is being addressed in an outsourcing contract, this does not provide sufficient detail to ensure that Information Security is being managed appropriately. The remainder of this paper sets out a generalized model for an Information Security Management System (ISMS) for use when parts of the IT infrastructure have been outsourced.

3 Risk Management in Outsourcing Contracts

When the decision is made to outsource some or all of an organization's IT functions, it is important to ensure that an appropriate risk management strategy is in place to ensure that Information Security is maintained. One of the greatest challenges is how to combine the risk and security management strategies of two separate organizations to ensure that the confidentiality, integrity and availability of the organizations business assets are maintained.

The seven principles outlined in section 2 provide general guidance as to the types of issues that should be present in outsourcing contracts however, the principles themselves do not provide any clues as to how this should be accomplished. The model presented in section 3.1 provides some guidance as to how the various components of information security management can be divided between the business and its outsource provider(s). In section 3.2 it is shown how this model addresses the ISO 17799 outsourcing principles.

3.1 Responsibilities

One of the principals in The Standard[5] states "arrangements will be in place to ensure that all parties involved in the outsourcing, including subcontractors, are aware of their security responsibilities". The Guidelines for the Management of IT Security (GMITS) part 3[6] defines a structure for managing risk within an organization. This model can be adapted to an outsourcing situation. This breakdown is shown in Figure 1 - Division of Responsibilities.

The diagram is adapted from GMITS Part 2[7] with shading added by the author to indicate division of responsibility as appropriate to ensure that risk management responsibilities are appropriately allocated between the outsourcer and the business.

[5] ISO 17799 section 4.3
[6] ISO 13335-3
[7] Figure 1 in ISO 13335-2:1997

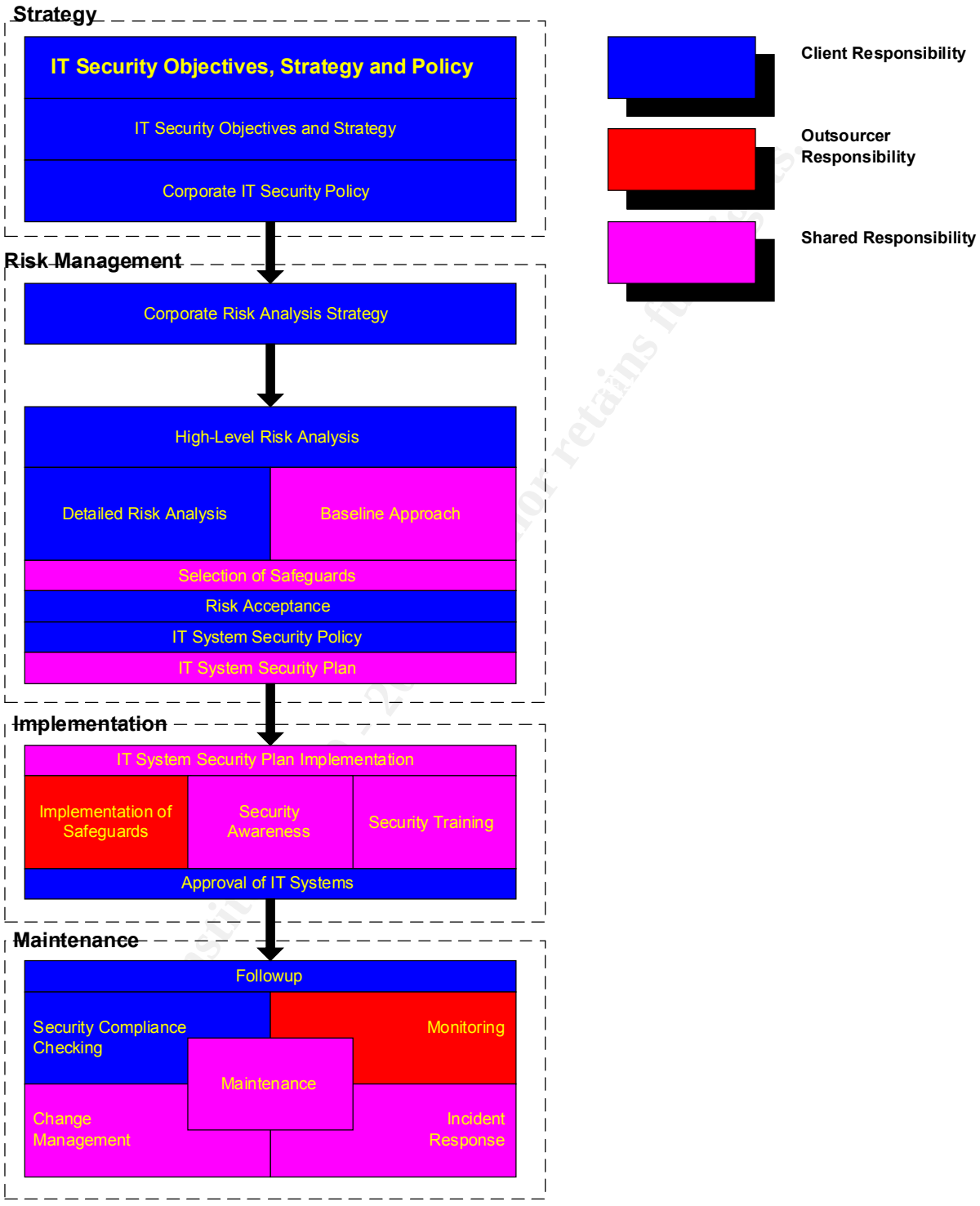

Figure 1 - Division of Responsibilities

3.1.1 Strategy

It is important that Business retain control and responsibility for IT Security Objectives and Strategy. The IT Security Objectives define level of risk that is acceptable to the Business and the Strategy defines how the business will remain within these risk parameters.

Retaining control over this function ensures that the outsourcer has a defined goal to work towards will in turn will assist in the success of the overall outsourcing venture[8].

3.1.2 Risk Management

An important component in the management of risks to business assets is the selection of an appropriate strategy for analyzing risk. Selection of an inappropriate Risk Analysis Strategy can lead to a superficial analysis of the issues or result in overly long and costly risk assessments.

GMITS defines a number of risk analysis strategies that business can use to analyze risk[9]. Of these, the most suitable approach for an outsourcing situation is the combined approach. This approach uses a High-Level assessment to determine whether a more Detailed Assessment is necessary or whether the risk can be analyzed using the existing baseline.

The High-Level Risk Assessment should be performed by the business. The determination of what level of business risk is involved in a particular operation or concept is best left to the business where the impact of any miscalculation of risk will be felt. If a Detailed Risk Assessment is required, this should also be the responsibility of the business.

Should the high level assessment determine that the level of risk is not too significant, the baseline approach is used. Responsibility for a baseline risk assessment is shared between the outsourcer and the business. The outsourcer effectively controls the IT baseline and the business must sign off and be responsible for the level of risk associated with the baseline.

The selection of appropriate safeguards is also a shared responsibility. Safeguards to manage risks will most likely be a mixture of operational and technical controls[10]. Whilst technical controls (for example firewalls and other pieces of security technology), operational controls (such as security policies) will usually remain the responsibility of the business.

Acceptance of risk and the development of any system specific policies should remain with the business. It is a general principle that whilst the assets themselves and even the business process surrounding the asset can be outsourced, the risk associated with the asset is retained with the business.

[8] The Snowball Effect, Section 1.
[9] ISO 13335 Part 2 section 7.1
[10] Standards Australia, HB 231 Section 4.5.3.1

The outsourcer should then produce a System Security Plan that details how the requirements of the System Security Policy are going to be met. Whilst the production of the actual plan itself will be the responsibility of the outsourcer, this item nonetheless remains a shared responsibility, as the business should approve the content of the System Security Plan as part of the general risk management process.

3.1.3 Maintenance

Maintaining IT systems is a matter of balancing many competing priorities such as balancing service levels and controlling cost, the maintenance of IT Security components is no different. Maintenance of IT systems is almost always a shared responsibility. The outsourcer is makes recommendations to the business as to any changes required to maintain and improve service levels and the business evaluates and approves these proposals.

The business is responsible for ensuring that the direction established by the IT Security Strategy and the countermeasures identified during risk management are maintained. For this reason, it is important that the business retain responsibility for Security Compliance Checking. This provides the business with a level of comfort that information security measures are being appropriately maintained.

The responsibility for monitoring should rest with the outsourcer. Monitoring is the means by which the effectiveness of any security controls or processes can be managed. In an outsourced environment, the outsourcer is operating the IT assets and should be providing the business with constant feedback of the performance of all components under their control.

Change management is a shared responsibility. Business should have a role in approving changes to IT systems in response to recommendations made by the outsourcer.

The responsibility for Incident Management is also shared. Typically it will be the outsourcer in their role of custodian of the IT system(s) that is the first stage of any incident response process as often security incidents may manifest themselves as outages or unexplained behavior in IT systems[11].

Once an incident has been identified as having occurred, the business would normally become involved to determine the appropriate steps to resolve the incident. The interactions involved in appropriate incident management are quite complex and beyond the scope of this paper however, in general the business makes the policy and risk management decisions with the outsourcer providing advice and performing any technical changes.

3.2 Correlation to ISO 17799

3.2.1 Legal Requirements

As the organization retains control of IT Security Strategy and overall policy, it is the responsibility of the organization to ensure that the policies are in compliance with any

[11] Carnegie Mellon University

applicable legal and legislative requirements. Organizational ownership of compliance checking provides assurance that any obligations of corporate policies and procedures are being carried out by the outsourcer.

3.2.2 Awareness of Security Responsibilities

Whilst this document does present a framework around which outsourcing services can be agreed, the actual division of work will be defined in the contract between the business and its outsourcer. By working within the framework suggested, both parties will be broadly aware of the distinct Information Security areas that need to be addressed. This will ensure that all parties (not just the outsourcer) are fully aware of their security responsibilities.

3.2.3 Maintenance of Confidentiality, Integrity and Availability

The maintenance of confidentiality, integrity and availability of organizational assets is perhaps one of the most significant challenges during an outsourcing engagement. Outsourcing requires that control of sensitive and business critical information is turned over to a third party who does not necessarily have the same vested interest in ensuring that the data is adequately protected.

The framework suggested ensures that whilst the actual maintenance of security equipment resides with the outsourcer, the business retains control over policy decisions regarding those assets. This division of labor means that it is the business who has ultimate control over decisions regarding the confidentiality, integrity and availability of their assets.

By retaining control over the audit function, the business is also able to ensure that the outsourcer is maintaining the standard required and specified by the business.

3.2.4 Physical and Logical Controls over Access

Where physical controls and logical controls are required to ensure that there is no unauthorized access to company resources, this should be identified as part of the Risk Management activities associated with the framework.

The provisions in the framework show how the business and the outsourcer are jointly responsible for the controls required to manage the business' risk. Whilst the responsibility for implementing the control rests with the outsourcer, policy decisions as to their suitability remain with the business.

3.2.5 Service Maintenance during Disaster

The ISO 13335 framework is not particularly specific about the provision of disaster recovery facilities. However, disaster recovery (DR) and its driver, Business Continuity Planning[12] (BCP) are accommodated within ISO 17799[13]. Both BCP and DR should be considered during the high-level risk analysis activity identified within the model and a decision made as to whether the system falls within the existing baseline (for instance additional on-line services could be incorporated into the existing DR and BCP baseline) or whether a detailed risk assessment is required.

The System Security Policy should contain details of the BCP and DR requirements for the system. This provides the ultimate guide for ensuring that the requirements have been met. It is important to note that ISO 17799 considers that BCP and DR are part of the overall information security management system and thus it is not treated as a separate activity within its own right.

3.2.6 Physical Security Measures

Required physical security measures would be identified and agreed during the Selection of Safeguards activity and then be the responsibility of the outsourcer to implement.

3.2.7 Right of Audit

Auditing falls broadly into the part of the framework identified as maintenance. It is vitally important that the business ensure that appropriate auditing rights are factored into any outsourcing contract. The framework shows that the majority of maintenance activities are identified as being a shared responsibility however; security compliance checking is clearly the responsibility of the business.

Whilst the framework identifies the responsibilities, it is noted that this does not identify the actual rights of audit, however by using the framework this should provide a useful starting point for discussions of audit content and frequency.

3.3 Risk Management and Managed Security Service Providers

Managed Security Service Providers (MSSP) are a specific type of outsource service provider that offers some or all security services to a client. Some of the services that may be offered by a MSSP are:

- Firewall management;
- Intrusion detection;
- Vulnerability assessment and testing;
- Antivirus management;
- Authentication;
- Security intelligence;
- Virtual private network; and
- Public key infrastructure[14].

As the majority of these services directly impact information security, the tendency is to assume that the solution to an organization's security issues is as simple as choosing an

[12] Noakes-Fry and Diamond
[13] ISO 17799 Section 11
[14] Kavanagh, 2001

appropriate MSSP. The thinking is that as information security is complex and non-cost recoverable, this is a function that should be best left to an outsourcer and not left to consume valuable internal resources.

In the author's experience, there is a tendency of businesses to assume that in selecting a MSSP, the information security issues for the organization have been solved. In fact, this is usually far from the case. Too often it is forgotten that the MSSP is there essentially to operate infrastructure[15] and thus is not responsible for the businesses security strategy or requirement. Indeed, organizational control of security strategy is an essential component of Security Outsourcing[16].

The framework shown in Figure 1 is equally applicable to outsourcing the information security function itself. The business must retain control over the decision making process as to what level of risk is acceptable and then be responsible for ensuring that the outsourcer is performing the appropriate actions to ensure that the risk is managed in an appropriate fashion.

3.4 Evaluating the Outsourcer

Having made the decision to outsource some, or all, of the IT Infrastructure, it is important to ensure that an evaluation of the outsourcer's information security practice is included as part of the due diligence process (it sounds straightforward but in the author's experience this is often overlooked). This applies whether the target of the outsource is the security function itself or a general part of the IT infrastructure.

When conducting due diligence on an outsourcer there are a number of key indicators that should be taken into account. These include:

- Does the outsourcer have a clear security policy?
- Is the outsourcer's management clearly and visibly committed to information security?
- Is there evidence that the supplier has assessed the security risks, understood the legal risks and is prepared to implement appropriate countermeasures?
- Does the outsourcer's operational team have a good, demonstrated knowledge and understanding of information security issues?
- Does the outsourcer follow some well-recognized standard for Information Security Management, such as ISO 17799?
- Visible information and data security signals such as appropriate physical security at data centers, security vetting for personnel involved in the management of business resources, password access to IT systems?[17]

One of the challenges in establishing the outsourcing arrangement will be merging the security requirements of the outsourcer with the security requirements of the business it is outsourcing. Although the outsourcer may have its own internal security policies these should be examined to ascertain if there are appropriate provisions for including a client security domain (or indeed multiple client domains) within their (the outsourcer's) policy

[15] Berkman, 2001
[16] Pankowska
[17] Peterson

structure. This issue is illustrated in a diagram developed by the author shown as Figure 2 - Security Domains Within a Data Center.

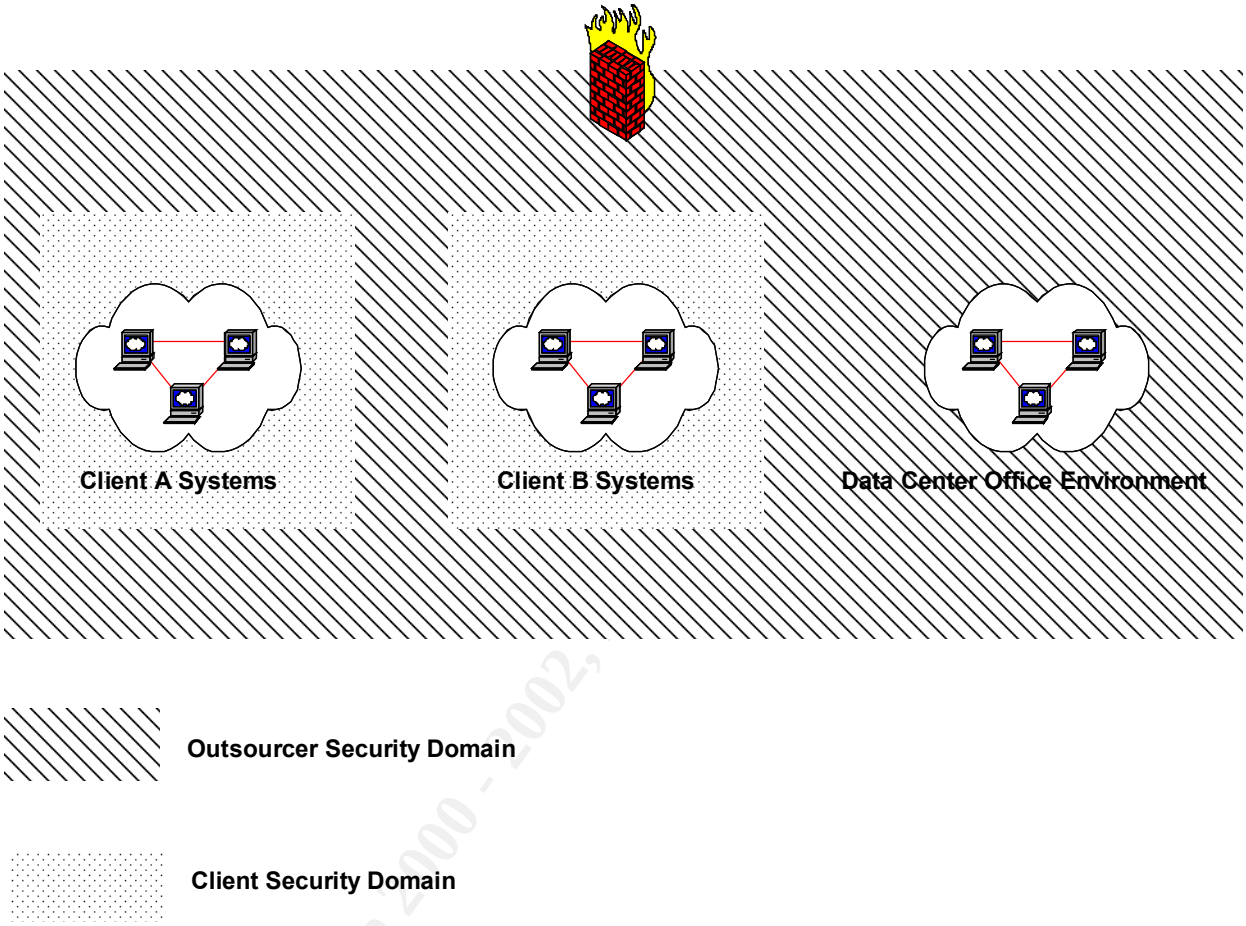

Figure 2 - Security Domains Within a Data Center

Figure 2 shows how an outsourcer might choose to integrate a client's security requirements into their existing data center. Ideally, the outsourcer would have a complete set of security policies and procedures that detail its own information security management requirements; this is depicted as the Outsourcer Security Domain. Everything within the outsourcer's control should be governed by the set of security policies and procedures that govern this domain.

Within the outsourcer's security domain are likely to be a number of client security domains. This reflects the needs and requirements of specific customers within the outsourcing environment. Each client will have different requirements for managing the risk to their business and thus will have slightly different requirements for the way in which information security countermeasures are to be applied for their machines. The outsourcer's security policies should be developed in such a way as to take this into account.

One of the clear indicators as to how well the outsourcer understands the security risks and implications will be the conduct of security due diligence on the business. As

previously stated, outsourcing is a partnership[18] and as such it should be expected that the outsourcer will perform some due diligence activities to assess the various aspects of the business in order to formulate a suitable contract.

As part of the development of the contract, the outsourcer should be taking steps to understand the security requirements of the business. The information security requirements of the business will have a significant impact on the way in which information security is maintained for those assets that are to be outsourced. A robust, thorough Information Security due diligence process by the outsourcer is a good indication that there is a good understanding of Information Security issues and the way in which these issues should be addressed.

4 Conclusions

Outsourcing can offer significant cost reductions to businesses through economies of scale offered by the outsourcer and can provide ready access to knowledge of current industry best practice. However, the decision to outsource parts of the IT infrastructure also brings with it the added difficulties of adequately managing business risk and ensuring that control over that risk is appropriately allocated.

There are a number of ISO Technical Reports, International Standards and private publications that have been collated which provide information on Risk Management although few of these explicitly recognize the reality that outsourcing is increasingly becoming the norm rather than the exception and that our information management systems have to recognize this reality. This is not to say that the information within the current body of knowledge is irrelevant though as the standard approaches to risk management can be easily adapted to suit an outsourced environment.

ISO 17799 provides some high level principals for consideration in outsourcing contracts that, when applied to risk management, provide a good basis for ensuring that information security is maintained even in a complex outsourced environment. Central to this is ensuring that all parties are completely aware of who is responsible for what sections of the information management puzzle. By defining and allocating responsibilities for the various components of risk management puzzle in such a way as to ensure that the business retains control over the information security and risk management strategy (including monitoring compliance), the security of the business can be maintained.

[18] Goolsby

References

1. Australian Prudential Regulatory Authority, "Prudential Issues in Electronic Commerce." APRA Insight. 1st Quarter 2001. URL: http://www.apra.gov.au/Insight/loader.cfm?url=/commonspot/security/getfile.cfm&PageID=2017 (March 2002);
2. International Organization for Standardization, "Code of Practice for Information Security Management." ISO/IEC 17799:2000. (2000);
3. Office of the Federal Privacy Commissioner (Australia). "Privacy Obligations for Government Contracts." Information Sheet 14-2001. December 2001. URL: http://www.privacy.gov.au/publications/IS14_01.pdf (March 2002);
4. International Organization for Standardization, "Techniques for the Management of IT Security." ISO 13335-3:1998, Guidelines for the Management of IT Security Part 3 (1998);
5. Goolsby, Kathleen. "The Snowball Effect: Characteristics of Outstanding Outsourcing Relationships." Outsourcing Center White Paper. February 2002. URL: http://www.outsourcing-requests.com/common/sponsors/4664/The_Snowball_Effect_Characteristics_of_Outstanding_Outsourcing_Relationships.pdf (March 2002)*
6. International Organization for Standardization, "Managing and Planning IT Security." ISO 13335-2:1997, Guidelines for the Management of IT Security Part 2 (1997);
7. Standards Australia. "Information Security Risk Management Guidelines." HB 231:2000 (2000);
8. Carnegie Mellon University. "Monitor and inspect Systems for unexpected behavior." May 2001. URL: http://www.cert.org/security-improvement/practices/p095.html (March 2002);
9. Noakes-Fry, Kirsten and Diamond, Trude. "Business Continuity and Disaster Recovery Planning and Management: Perspective." Gartner Research Technology Overview. October 2001. URL: http://www.availability.com/resource/pdfs/DPRO-100862.pdf (March 2002);
10. Kavanagh, Kelly. "Managed Security Services". Gartner Research Technology. August 2001. URL: http://www4.gartner.com/DisplayDocument?id=339855&acsFlg=accessBought (March 2002);
11. Berkman, Eric. "MSPs Say They'll Do It All For You." IT Outsourcing - CIO Magazine. November 2001. URL: http://www.cio.com/archive/110101/msp.html (March 2002);
12. Pankowska, Malgorzata. "Outsourcing Impact on Security Issues." University of Poland. URL: http://figaro.ae.katowice.pl/~pank/secout2.htm (March 2002);
13. Peterson, Brad L. "Information Security in Outsourcing Contracts." Outsourcing Journal. March 2002. URL: http://www.outsourcing-journal.com/issues/mar2002/legal.html (March 2002).

* Registration Required

Last Updated: May 26th, 2017

Upcoming Training

SANS Stockholm 2017	Stockholm, Sweden	May 29, 2017 - Jun 03, 2017	Live Event
Community SANS Ottawa SEC401	Ottawa, ON	Jun 05, 2017 - Jun 10, 2017	Community SANS
SANS San Francisco Summer 2017	San Francisco, CA	Jun 05, 2017 - Jun 10, 2017	Live Event
SANS Houston 2017	Houston, TX	Jun 05, 2017 - Jun 10, 2017	Live Event
Security Operations Center Summit & Training	Washington, DC	Jun 05, 2017 - Jun 12, 2017	Live Event
SANS Charlotte 2017	Charlotte, NC	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Rocky Mountain 2017 - SEC401: Security Essentials Bootcamp Style	Denver, CO	Jun 12, 2017 - Jun 17, 2017	vLive
SANS Secure Europe 2017	Amsterdam, Netherlands	Jun 12, 2017 - Jun 20, 2017	Live Event
Community SANS Portland SEC401	Portland, OR	Jun 12, 2017 - Jun 17, 2017	Community SANS
SANS Rocky Mountain 2017	Denver, CO	Jun 12, 2017 - Jun 17, 2017	Live Event
SANS Minneapolis 2017	Minneapolis, MN	Jun 19, 2017 - Jun 24, 2017	Live Event
SANS Columbia, MD 2017	Columbia, MD	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS Cyber Defence Canberra 2017	Canberra, Australia	Jun 26, 2017 - Jul 08, 2017	Live Event
SANS Paris 2017	Paris, France	Jun 26, 2017 - Jul 01, 2017	Live Event
SANS London July 2017	London, United Kingdom	Jul 03, 2017 - Jul 08, 2017	Live Event
Cyber Defence Japan 2017	Tokyo, Japan	Jul 05, 2017 - Jul 15, 2017	Live Event
SANS Cyber Defence Singapore 2017	Singapore, Singapore	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Minneapolis SEC401	Minneapolis, MN	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Los Angeles - Long Beach 2017	Long Beach, CA	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Phoenix SEC401	Phoenix, AZ	Jul 10, 2017 - Jul 15, 2017	Community SANS
SANS Munich Summer 2017	Munich, Germany	Jul 10, 2017 - Jul 15, 2017	Live Event
Mentor Session - SEC401	Ventura, CA	Jul 12, 2017 - Sep 13, 2017	Mentor
Mentor Session - SEC401	Macon, GA	Jul 12, 2017 - Aug 23, 2017	Mentor
Community SANS Atlanta SEC401	Atlanta, GA	Jul 17, 2017 - Jul 22, 2017	Community SANS
Community SANS Colorado Springs SEC401	Colorado Springs, CO	Jul 17, 2017 - Jul 22, 2017	Community SANS
SANSFIRE 2017	Washington, DC	Jul 22, 2017 - Jul 29, 2017	Live Event
SANSFIRE 2017 - SEC401: Security Essentials Bootcamp Style	Washington, DC	Jul 24, 2017 - Jul 29, 2017	vLive
Community SANS Charleston SEC401	Charleston, SC	Jul 24, 2017 - Jul 29, 2017	Community SANS
Community SANS Fort Lauderdale SEC401	Fort Lauderdale, FL	Jul 31, 2017 - Aug 05, 2017	Community SANS
SANS San Antonio 2017	San Antonio, TX	Aug 06, 2017 - Aug 11, 2017	Live Event
SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event