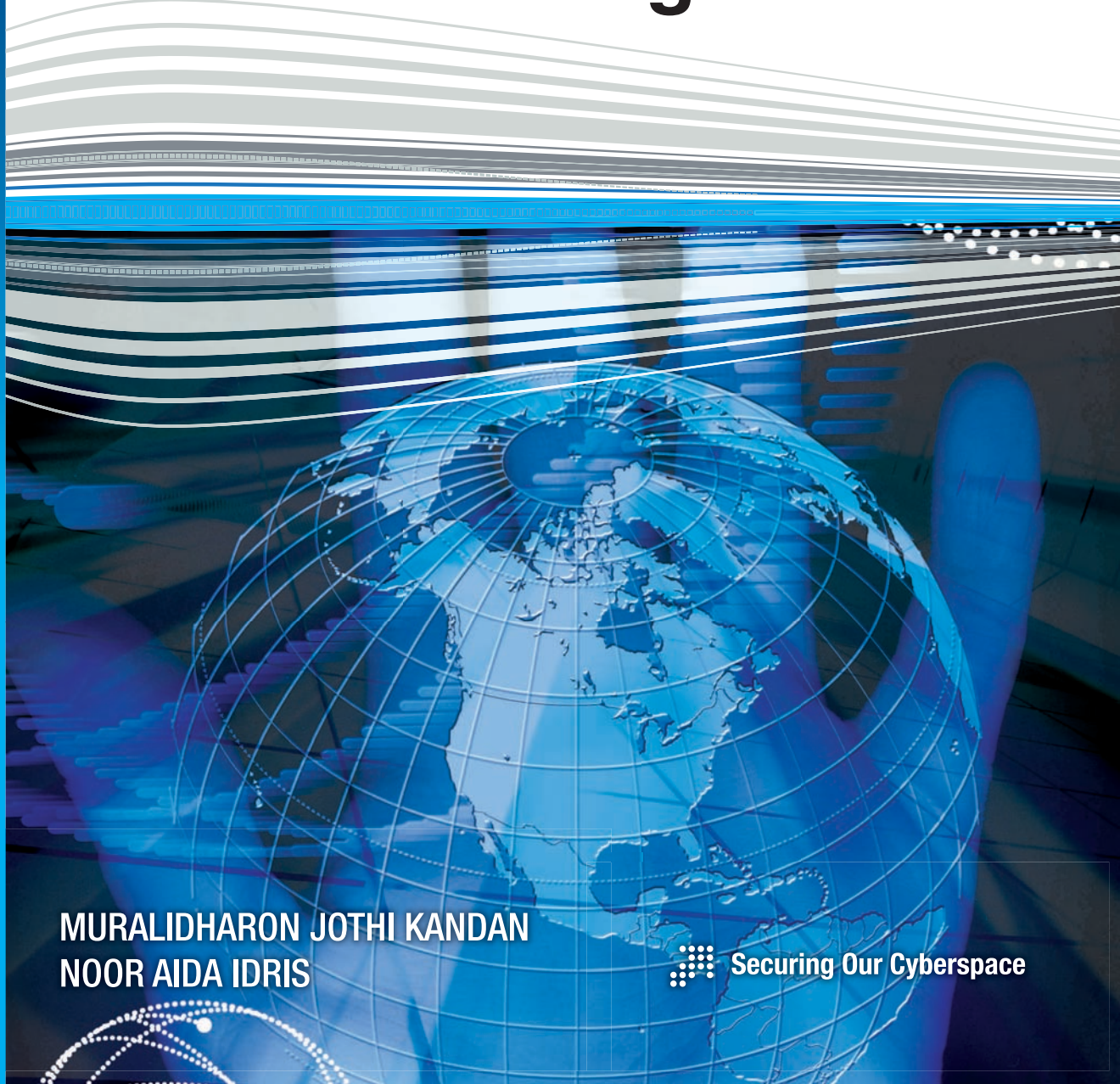
CyberSecurity MALAYSIA
An agency under MOSTI

Guidelines on Information Security in ICT Outsourcing



MURALIDHARON JOTHI KANDAN
NOOR AIDA IDRIS

Securing Our Cyberspace

CyberSecurity MALAYSIA

An agency under MOSTI

Guidelines on Information Security in ICT Outsourcing

MURALIDHARON JOTHI KANDAN
NOOR AIDA IDRIS

COPYRIGHT

NO ENDORSEMENT

Products and manufacturers discussed or referred to in this document, if any, are presented for informational purposes only, and do not in any way constitute product approval or endorsement by CyberSecurity Malaysia.

TRADEMARKS

All terms mentioned in this document that are known to be trademarks or service marks have been appropriately capitalised. CyberSecurity Malaysia cannot attest to the accuracy of this information. Use of a term in this document should not be regarded as affecting the validity of any trademark or service mark.

WARNING AND DISCLAIMER

Every effort has been made to make this document as complete and as accurate as possible, but no warranty or fitness is implied. The information provided is on an “as is” basis. The author and CyberSecurity Malaysia shall have neither liability nor responsibility to any person or entity with respect to any losses or damages arising from the reliance to the information contained in this document.

REGISTERED OFFICE:

CyberSecurity Malaysia
Level 8, Block A, Mines Waterfront Business Park,
No 3, Jalan Tasik, The Mines Resort City,
43300 Seri Kembangan, Selangor.
Phone: +603 – 89460999
Fax: +603 – 8946 0888
http://www.cybersecurity.my

Printed in Malaysia

Acknowledgement

CyberSecurity Malaysia wishes to thank the panel of reviewers (Internal & External) who reviewed drafts of this guideline.

Internal Reviewers

Chia Won Chee **(InfoSecurity Professional Development)**

Maslina Binti Daud **(Security Management & Best Practices)**

Rosly Yahil **(Cyber Consulting Group)**

Sabariah Binti Ahmad **(Security Management & Best Practices)**

External Reviewers

A Fattah Yatim **(Teknimuda (M) Sdn Bhd)**

Dr. Dzaharudin Mansur **(Microsoft Malaysia)**

Puteri Nor Shatirah Binti Mohamad Zabri **(Malaysian Airport Technologies Sdn Bhd)**

Ummi Kalsom Abdul Rahim **(Securities Commission)**

Table of Contents

Abstract

ICT outsourcing creates wide opportunities for both organisations and outsourcing providers. Organisations might consider outsourcing an ICT service to an outsourcing provider for several reasons, such as lack of the required capabilities in the organisation, value for money, or anticipated technology and skills transfer to the organisation from the outsourcing provider. By outsourcing an ICT service, performance standards can be improved tremendously and the organisation can focus on its core business.

However, as ICT outsourcing services grow, so does information security risks in relation to outsourcing activities. These risks, if left unmanaged, will give a negative impact to the organisation as well as the ICT outsourcing industry as a whole. While potential benefits from outsourcing can be enjoyed, organisations should balance them against the risks that outsourcing may create.

If and when organisations decide to outsource an ICT service to outsourcing providers, both organisations and outsourcing providers should carry out the roles and responsibilities provided in this Guideline. This will ensure that all risks that could cause an impact on confidentiality, integrity and availability of the ICT service to be outsourced can and will be mitigated.

Introduction

Outsourcing is widely chosen as the preferred alternative in carrying out an organisation's business services or functions. Usually, organisations outsource a non-core business service or function to another service provider (i.e. outsourcing providers) specialising in those areas. This is to ensure that they can free up resources (such as personnel), time and facilities to focus on their core business functions or services.

ICT outsourcing can be defined as means of contracting out of a defined ICT function or process to external service provider for an agreed period[1]. The outsourcing areas cut across all types of ICT services including but not limited to developing and maintaining application systems, helpdesks, servers and network operations, Disaster Recovery Centres, etc.

Some of the reasons why organisations may choose to outsource are:

- Increase focus on core business functions.
- Improve cost effectiveness and financial efficiencies, thus conserving capital for other business ventures.
- Obtain specialised expertise especially in technology centric areas (this expertise is usually just needed during the outsourcing project, hence may not be cost-effective to hire permanent staff).
- Increase availability and quality of services offered to the customers.
- Increase ability to acquire and support current technology.

Whenever organisations decide to outsource an ICT service, it is essential to ensure that confidentiality, integrity and availability (CIA) of information are preserved throughout the outsourcing process.

1 http://www.bundesrechnungshof.de/publications/booklets-guidance/ictguide.pdf

1

Chapter Contents

1.1 Objective

The objective of this Guideline on Information Security in ICT Outsourcing is to provide guidance to organisations in managing and ensuring information security is preserved when choosing to outsource an ICT service to an outsourcing provider. It should be noted however that this Guideline does not in any way address the overall management of ICT outsourcing itself; and is not intended to replace or supersede existing information security standards and guidelines produced internally by organisations or regulators.

The use of this guideline can differ according to the size, nature and complexity of an organisation, as well as the objective and scope of each ICT service to be outsourced.

1.2 Scope

This Guideline focuses on the following requirements in ICT outsourcing:

- Outsourcing risk assessment
- Information security requirement
- Outsourcing planning
- Outsourcing provider selection
- Outsourcing agreement
- Physical and environmental security
- Security of information and system
- Information security incident management
- Security arrangements
- Training

This Guideline provides recommendations on roles and responsibilities of organisations and outsourcing providers in three phases of outsourcing: pre-outsourcing, during outsourcing, and post-outsourcing. Their roles and responsibilities are directly related to the above information security requirements only.

1.3 Target Audience

This guideline is recommended for the following audience:

- Organisations that plan to outsource their ICT service to an outsourcing provider.
- Individuals with an overall responsibility of managing information security during outsourcing process.
- Individuals who are the information security personnel, whose responsibilities include information security planning and monitoring of the organisation's outsourced ICT service.

1.4 Document Structure

This guideline is structured as follows:

- Section 1 introduces objective, scope and target audience of the guideline.
- Section 2 defines Terms and Definitions used in the guideline.
- Section 3 lists the Acronyms and Abbreviations used in the guideline.
- Section 4 provides an overview of ICT outsourcing which includes outsourcing risks and the three phases in ICT outsourcing.
- Section 5, 6 and 7 describe in detail the information security requirements of ICT outsourcing in three phases: pre-outsourcing, outsourcing and post-outsourcing phases respectively.
- Appendix A provides Key Risks in Outsourcing.
- Appendix B provides References

Terms & Definitions

A glossary of terms is usually located at the back of a book and referred to only when necessary. However, the terms and definitions for this guideline are placed here for easy reference. Users of this Guideline are recommended to spend a few minutes to familiarise or refresh themselves with the following computer and technical jargons.

2.1 Computing related equipment

Computers, networks, telecommunications and peripheral equipments that support the information processing activities and dissemination of an organisation. Some examples are personal computers (PCs), personal digital assistants (PDAs), thumbdrives, printers, video cameras, game consoles and multimedia devices.

2.2 Information and Communication Technologies (ICT)

The study, design, development, implementation, support or management of computer-based information systems, particularly software applications and computer hardware[2].

2.3 Information and Communication Technologies (ICT) service

A service being supplied via an ICT system[3].

2.4 Information and Communication Technologies (ICT) system

A set up consisting of hardware, software and firmware of computing related equipment and the people who use them. ICT system includes any computing related equipment or other electronic information handling systems and associated equipment or interconnected systems that are used in the acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission or reception of data/information.

2 searchcio-midmarket.techtarget.com/sDefinition/0,,sid183_gci928405,00.html
3 www.cmpp.net/CMS/Media/Docs/ITIL/ITIL%20Glossary%20of%20Terms01.doc

2

2.5
Information security

Preservation of confidentiality, integrity and availability of information; in addition, other properties such as authenticity, accountability, non-repudiation and reliability can also be involved[4].

2.6
Malicious Code

A program that is inserted into a system, usually covertly, with the intent of compromising the confidentiality, integrity, or availability of the victim's data, applications, or operating system or of otherwise annoying or disrupting the victim's regular mode of activity[5].

2.7
Organisations Outsourcing

Public or private registered entities that outsource an ICT service to an outsourcing provider.

2.8
Outsourcing

Contracting out a defined ICT function or process to external service provider for an agreed period[6].

2.9
Outsourcing Providers

Entities that provide outsourcing services to other entities.

2.10
Patch

A piece of software designed to update or fix problems with a computer program or its supporting data. This includes fixing bugs, replacing graphics and improving the usability or performance.

2.11
Threat

A probable impending danger or warning of impending danger which may exploit a vulnerability to cause harm to organisation.

2.12
Vulnerability

A weakness in an ICT system which potentially allows an attacker to violate the integrity of the ICT system.

4 ISO/IEC 27001 – Information Security Management Systems
5 NIST SP800-83 Guide to Malware Incident Prevention and Handling
6 http://www.bundesrechnungshof.de/publications/booklets-guidance/ictguide.pdf

Acronyms & Abbreviations

ICT	Information and Communication Technologies
IEC	International Electrotechnical Commission
ISO	International Organisation for Standardisation
IT	Information Technology
NDA	Non Disclosure Agreement

3

Background

Outsourcing, if managed effectively, may help many organisations focus on their core businesses to deliver optimum business results to satisfy their customers, while managing other non-core services. It may also provide organisations with opportunities to increase business productivity and at the same time save their time and money. This can be achieved by completing a number of activities prior to outsourcing, such as conducting risk assessment (to assess risks on outsourcing), having a structured project plan for outsourcing, and/or selecting a qualified and capable outsourcing provider. However, information security needs to be managed diligently during the process. Both organisations and outsourcing providers should play their respective roles in managing information security in ICT outsourcing.

4.1 Phases in ICT Outsourcing

There are three phases in ICT outsourcing: pre-outsourcing, during outsourcing, and post-outsourcing. See table 1 below.

Process	Description
Pre-outsourcing	Pre-outsourcing phase is the first phase in ICT outsourcing. In this phase, organisations decide which ICT service should be outsourced. Planning involving scope of work, time-line, resources and information security requirements for the ICT outsourcing project should be done in this phase. This is the phase where organisations evaluate and select the most appropriate outsourcing provider that meets their requirements to deliver the outsourcing project. Finally, terms and conditions related to the outsourcing exercise are developed and accepted by both organisations and outsourcing providers, usually via a signed agreement.

continue Pre-outsourcing

4

Chapter Contents

Process	Description
Pre-outsourcing	The terms and conditions should also include the expected deliverables during and upon completion of the outsourcing exercise. It is also important in this phase, for an organisation to know the details of the outsourcing provider's personnel that will be involved in the outsourcing exercise particularly the project manager, and that all the personnel are vetted. An NDA (Non disclosure agreement) should also be signed by all personnel involved in this phase.
During Outsourcing	During the outsourcing phase, the chosen outsourcing provider performs the outsourcing task based on the scope of work. Organisations should monitor and provide assistance to the outsourcing provider (if required). Prior to the engagement, organisations should ensure the existence and adoption of adequate audit procedures to protect the security of their physical and environmental premises, security of their information and information systems, as well as procedures for managing information security incidents.
Post-outsourcing	In this phase, final outsourced ICT service is delivered to organisations, or in the case of physical data centre, returned to the organisation. However, depending on the agreed terms in pre-outsourcing phase, outsourcing providers may be responsible to provide maintenance and/or training to organisations. In addition, all physical and logical access rights provided to outsourcing providers are removed and assets belonging to organisations are returned in this phase.

Table 1 : Three phases in ICT outsourcing

4.2 Information Security Risks in ICT Outsourcing

Managing information security in ICT outsourcing environment is not an easy task. Information is an asset, like other physical business assets, that is essential to be appropriately and adequately protected. Information exists in many forms; either printed or written on paper, stored electronically, transmitted by post or other electronic means, shown on any medium (film, software presentation), and even spoken during conversation.

In ICT outsourcing, information security is critical due to the fact that numerous information being exchanged between organisations and outsourcing providers. It is suggested that organisations identify outsourcing security risks prior to outsourcing a particular project to make sure that sufficient security strategies, staffing and reporting mechanisms are in place. Even so, if the security risks outweigh the benefits, organisations may want to reconsider the approach or re-visit the previously identified scope.

ICT Outsourcing is becoming a trend nowadays. Despite increasing number of organizations that involve in ICT outsourcing, it should be noted that ICT outsourcing is not a panacea. It comes together with risks. The risks, if not managed, will lead to outsourcing failure. Even though other areas have adopted risk management as their patching material, the application of risk management in ICT outsourcing was not quite accomplished. Risk management should be conducted in ICT outsourcing as it will foresee risks that might disturb the smooth flowing of ICT outsourcing and prevent or reduce the impact of risks if they occur. It should be conducted at early stage and should be continuously performed until the end of outsourcing life cycle. This paper presents a conceptual framework to manage risk in ICT outsourcing. The framework will cover the process in risk management in ICT outsourcing as well as the risk management

principle that should be conducted at each and every phases of ICT Outsourcing life cycle. A set of questionnaire was distributed to organizations to validate the conceptual framework. The findings showed that the consequences of not practicing risk management would result in poor controlling and managing of ICT outsourcing projects. Based on the findings, future empirical and exploratory survey will have to be conducted and risk management in ICT outsourcing framework has to be developed.

Table 2 below lists several examples of information security risk in ICT outsourcing.

Information Security	Sample of Information Security Concerns
Confidentiality	Level of protection provided by the outsourcing provider may not be adequate to protect sensitive or confidential organisations' information such as intellectual property or trade secrets from being viewed or accessed by unauthorised parties including personnel within the outsourcing provider.
Integrity	Inability to protect access particularly involving outsourcing providers' personnel who may need access to systems to perform their tasks/projects at non-official circumstances. These accesses may result in tampering of any data intentionally or unintentionally, hence risking a compromise to the integrity of such data.
	Similarly, access granted to the outsourcing providers' personnel to perform his/her tasks may be used to change information belonging to the organisation without authorisation thus compromising the integrity of the data.
Availability	Inadequate backup and recovery plan resulting in improper backup by the outsourcing provider. Any data corruption or lost, may not be able to be recovered without proper and timely backup that are tested frequently and successfully leading to the risk of unavailability of data.
	Removal of an organisation's confidential data from outsourcing providers' system and any leased system without the organisation's approval.
	Inadequate or not yet tested business continuity plans by outsourcing providers may risk the continuity and availability of the outsourced ICT service.

Table 2: Information Security key area in ICT Outsourcing

Please refer to **Appendix A: Key risk in Outsourcing** for further information on overall key risks in outsourcing. Key risks in Outsourcing should not be considered as either a complete or an accurate reflection of all the risks that may exist in outsourcing. Instead, organizations should build on and amend their own key risks through internal and external consultation to capture all relevant risks.

Pre-outsourcing

A pre-outsourcing phase allows organisations to prepare and plan for the ICT outsourcing project. In this phase, organisations develop strategic decisions on which ICT service or scope of service that needs to be outsourced and how it should be outsourced. Risk assessment involving information security confidentiality, integrity and availability should be performed and mitigating factors should be elaborated and accepted. If the risks are high and the mitigating factors are not satisfactory, an organisation should opt not to continue. If the risks and mitigating factors are accepted, an organisation may pursue the exercise of choosing the outsourced provider. Depending on the organisation's procurement policies/procedures if any, it is also recommended that an organisation undertake a thorough tendering process, either closed or open tender, in order to provide real opportunities for the organisation to understand the level of services and expertise available in the market. This will provide a wide spectrum of information for selecting the most appropriate and suitable outsourcing provider for a certain outsourcing exercise. Once an outsourced provider is chosen, both parties must enter into an agreement which includes all conditions required by the organisation to mitigate all the risks identified in protecting the organisations' information C,I,A (Confidentiality, Integrity, Availability) .

5.1 Assessment of Risks of Outsourcing

Before the decision to outsource is acted upon, information security risks related to ICT outsourcing should be identified and assessed. Risk assessment can be performed and is vital to ensure that the organisation understands information security risks related to ICT outsourcing. A risk assessment is a process of identifying, quantifying and prioritising risks against the known criteria for risk acceptance and objectives relevant to the organisation[7]. The primary goal of conducting risk assessment in the pre-outsourcing phase is to identify risks and mitigate (or accept) them.

5

Chapter Contents

5.1.1 Roles & Responsibilities for Organisations

Roles and responsibilities for organisations in conducting risk assessment should include, but not limited to, the following:

- Identify the business processes and functions of ICT service to be outsourced.
- For each of the ICT service to be outsourced, carry out risk assessment to understand the impact of loss of confidentiality, integrity or availability.
- Present risk assessment report to senior management to ensure that the management is aware of all the risks involved.
- Produce risk treatment plan to take steps to treat identified risks (where appropriate); where risks are accepted, conduct ongoing monitoring of risks.

5.2 Information Security Requirements

When the decision for outsourcing is approved, organisations should define the security requirements of the outsourcing activities. The security requirements shall commensurate with the confidentiality, integrity and availability needs of organisations as show in section 4.2 Table 2 : Information Security key area in ICT Outsourcing.

5.2.1 Roles & Responsibilities for Organisations

Roles and responsibilities for organisations in defining requirements include, but not limited to, the following:

1. Define all the requirements. It is recommended for organisations to refer to controls described in MS ISO/IEC 27002 Code of practice when identifying the information security requirements and security measures that may be implemented within the outsourcing context.
2. Ensure the identified information security requirements are in line with the following:
   - Organisations' business functions and processes
   - Organisations' security policies and procedures
   - Compliance, regulatory, standard requirements
3. Ensure the requirements are endorsed by senior management.
4. Ensure the requirements are included in Request for Proposal (RFP) which will be given to potential outsourcing providers.

5.3 Outsourcing Planning

Once a risk assessment has been performed and a risk treatment plan has been implemented or is being implemented, organisations should develop an outsourcing plan.

5.3.1 Roles & Responsibilities for Organisations

1. Produce outsourcing plan. The outsourcing plan should include the following:
2. Description, objective, and scope of work of the ICT service to be outsourced
3. Identified security requirements
4. Outsourcing project time-line and milestones
5. Mechanisms to track the outsourcing plan implementation
6. Ensure the plan is endorsed by senior management
7. A team that consists of key personnel from various areas, typically from the following functions or equivalent:
   - Human Resources Department (HRD)
   - Physical Security Department (PSD)
   - Information Technology Services and Security Department (ITSSD)
   - Risk Management Department (RMD)

7 MS ISO/IEC 27001:2007 – Information Security Management System

- Legal & Compliance Department (LCD)
- Finance Department (FD)
- Procurement Department (PD)

This team, ideally, should have decision-making authority but may also provide a channel through which information security issues can be passed to senior management (for decision making), for issues that cannot be resolved or agreed at the team level.

5.4 Outsourcing Provider Selection

Organisations should select the best outsourcing provider to perform the ICT outsourcing project. Outsourcing providers are responsible to provide sufficient team members with relevant background to form an outsourcing team.

5.4.1 Roles & Responsibilities for Organisations

Roles and responsibilities for organisations in selecting an outsourcing provider include, but are not limited to, the following:

1. Select an outsourcing provider that is Information Security Management System (ISMS) certified (in accordance to MS ISO/IEC 27001: 2007) and the scope of certification covers the outsourced service of interest. This is to ensure the selected outsourced provider meet its information security management needs and requirements and is relevant to the service area being outsourced.
2. Acquire an outsourcing provider that agrees to comply with the organisation's policies and procedures and willing to be audited periodically by a third party auditor.
3. Verify the outsourcing provider's team members. The team members' names and profiles including their relevant knowledge, skills, experiences and certifications (either professional certifications or product or technology specific certifications) should be verified (include both background and technical verifications) by organisations. The verification guideline should include:
   - At least two references
   - A criminal record check
   - Checking the accuracy of Curriculum Vitae's (CVs)
   - Positive confirmation of academic and professional qualifications
   - Positive identity check (sight of Identity card or passport)
   - Bind outsourcing provider with a Non-Disclosure Agreement (NDA) to protect sensitive and confidential information and information derived from it.

5.4.2 Roles & Responsibilities for Outsourcing Providers

Roles and responsibilities for outsourcing providers in outsourcing provider selection include, but not limited to, the following:

- Provide the team members' name and details to organisations concerned. Extends any changes to the profile, to the organisation, in a timely manner.
- Sign NDA for the outsourcing provider as well as ensure that each member signs the NDA prior to the start of the outsourcing project.
- Define clearly each team member's role in the outsourced activity including, where necessary, the backup personnel to cover the absence of primary staff. It is acceptable that primary staff can be a backup for another primary staff in another role, depending on role or function, while not violating the principle of segregation of responsibilities.
- Provide one focal point of contact to report and respond on issues.

5.5 Outsourcing Agreement

Organisation should prepare agreements that include all the terms and conditions related to the outsourcing activities as agreed by both organisation and outsourcing provider. Developing an agreement involves documenting specific terms and conditions as agreed by both organisations

and outsourcing providers into a formal document. The requirements should be set out in clear, unambiguous and mutually beneficial contract. To ensure the agreement is complete and legally binding, it is recommended that it is reviewed by a qualified legal counsel before it is signed.

The following security requirements shall include, but not limited to the following agreement:[8]

(a) Controls to ensure asset protection, including:
   1. Procedures to protect organisational assets, including information, software and hardware;
   2. Any required physical protection controls and mechanisms;
   3. Controls to ensure protection against malicious software;
   4. Procedures to determine whether any compromise of the assets, e.g. loss or modification of information, software and hardware, has occurred;
   5. Controls to ensure the return or destruction of information and assets at the end of, or at an agreed point in time during the agreement;
   6. Confidentiality, integrity, availability, and any other relevant property of the assets;
   7. Restrictions on copying and disclosing information, and using confidentiality agreements.

(b) Responsibilities regarding hardware and software and maintenance;

(c) Access control policy, covering:
   1. The right to audit responsibilities defined in the agreement, to have those audits carried out by a third party, and to enumerate the statutory rights of auditors;
   2. Responsibilities with respect to legal matters and how it is ensured that the legal requirements are met, e.g. data protection legislation, especially taking into account different national legal systems if the agreement involves co-operation with organisations in various other countries;
   3. Intellectual property rights (IPRs) and copyright assignment and protection of any collaborative work;
   4. Involvement of the third party with sub-contractors, and the security controls these sub-contractors need to implement.

5.5.1 Roles & Responsibilities for Organisations

Roles and responsibilities for organisations in developing outsourcing agreement include, but not limited to, the following:

1. Ensure the agreement adequately reflects identified security requirements for handling of confidential data, business information, or any other protected information.
2. Clearly define responsibilities for day-to-day security management (both organisation and outsourcing provider) in the agreement.
3. Include in the agreement to attain rights of inspection and audit during ICT outsourcing period.
4. Clearly address in the contract how security and exit clause to be identified will be managed in event of termination and/or transition. The following terms can be considered for inclusion in the agreement:[9]
   - A contingency plan of the outsourced ICT service should be in place in case either party wishes to terminate the relationship before the end of the agreement;
   - Re-negotiation of agreements if the security requirements of the organisation changes;
   - Upon termination of the agreement, there should be expertise and knowledge gap that needs to be filled to enable `Business as Usual`. An organisation needs to have a comprehensive exit plan in place.

8 ISO/IEC 27002:2005 Code of Practice for Information Security Management
9 ISO 27002:2005 Code of Practice for Information Security Management

- Current documentation of asset lists, licenses, agreements or rights relating to assets used during the outsourcing agreement
- A transition process on how the outsourcing provider will work with new outsourcing provider (if applicable).

5.5.2 Roles & Responsibilities for Outsourcing Providers

Roles and responsibilities for outsourcing providers in outsourcing agreement include, but not limited to, the following:

- Read and understand terms and conditions in the agreement before signing it.
- Outsourcing provider should be contractually obliged to provide organisations regular reports on performance of the outsourcing activities:
- Risks which have been identified prior to the outsourcing process.
- Possible risks factors which may arise during the outsourcing process.
- Incidents which may occur during the outsourcing process.
- Emerging threats which may arise during the outsourcing process.
- Changes to the current environment (e.g. resignation of the Project Manager) that may affect both organisations as well as the outsourcing providers.

During Outsourcing

In this phase, the outsourced ICT service is performed based on the agreed scope of work and agreement. Outsourcing providers are responsible on performing tasks in delivering the outsourcing project; however organisations should manage the overall outsourcing project and/or assist (if required) the outsourcing providers during the duration of the outsourcing project.

6.1 Physical and Environmental Security

Organisations should enforce the physical and environmental security during the outsourcing engagement. This plan needs to weigh the option of having the outsourcing process in the organisations' or at the outsourcing providers' premises.

(Note: The following roles and responsibilities cover the scenario where the outsourcing project or service is performed in the organisations' premises only. If the outsourcing project or service is performed at the outsourcing providers' premises, organisations should carefully read and understand the outsourcing provider's policies and procedures relating to physical and environmental security.)

6.6.1 Roles & Responsibilities for Organisations

Roles and responsibilities for organisations in developing outsourcing agreement include, but not limited to, the following:

- Develop policies and procedures related to physical and environmental security (e.g. Physical Security Policy, Access Control List, etc).
- Provide pictorial identification badges that clearly identify the outsourcing providers' team members.
- Assign different responsibilities to team members for accountability. These accesses should be given to a specific system, network or computer equipment, which are necessary to the outsourcing project only. The access control list should be documented and reviewed periodically.
- Lock file cabinets and/or rooms to prevent unauthorised access to an organisation's sensitive and confidential data.
- Provide sufficient office space and office equipment for the outsourcing provider to perform their services; a restricted area is preferred.

6

Chapter Contents

- Produce 'Assets Tracking Form' that lists all organisational assets which are borrowed by/provided to outsourcing providers.
- Monitor CCTV at relevant locations and periodically check the CCTV recordings/logs to protect assets that may be affected by this outsourcing exercise.

6.1.2 Roles & Responsibilities for Outsourcing Providers

Roles and responsibilities for outsourcing providers in physical and environmental security include, but not limited to, the following:

- Read and comply with organisations' policies and procedures related to physical and environmental security (e.g. record attendance in visitors log book).
- Display picture identification badges all the time while in organisation's premises.
- Avoid sharing physical and/or logical access with other team members (especially if the member is not part of the outsourcing project), and be held accountable for all access under your name.
- Sign and maintain the 'Assets Tracking Form' for all organisational items borrowed. This is to ensure all movements of assets are properly monitored.
- To sign the non-disclosure agreement.

6.2 Security of Information and System

Organisations and outsourcing providers should be responsible to protect the organisation's information and system as well as the organisation's customers' information collected during and after performing the outsourcing exercise. Outsourcing providers should adhere to the signed agreement to ensure the confidentiality, integrity and availability of the organisation's information and systems related to outsourcing activities.

6.2.1 Roles & Responsibilities for Organisations

Roles and responsibilities for organisations in the security of information and systems include, but not limited to, the following:

- Provide file encryption tools to protect digital information in media (e.g. hard disks, thumb drives).
- Run and/or test the backup produced by outsourcing providers periodically. These backups need to be protected against tampering and unauthorised changes.
- Ensure change management controls are applied and monitored to control changes to the organisations' systems as a result of outsourcing projects.
- Regularly monitor log files to ensure there is no unauthorised or accidental access to the organisations' information and systems.

6.2.2 Roles & Responsibilities for Outsourcing Providers

Roles and responsibilities for outsourcing providers in the security of information and systems include, but not limited to, the following:

- Read, understand and adhere to the organisations' policies and procedures related to security of information and systems.
- Use the provided file encryption tools to protect digital information in media (e.g. hard disks, thumb drives) and/or when transmitting the organisations confidential information.
- Create periodically back-up of information related to outsourcing activities.
- Follow the organisations' change management procedures when updating systems/software.
- Outsourcing providers should also carry out periodic backups of the outsourcing activities. Furthermore, they should keep logs recording each member's activities (e.g. login/logout). These logs are important for reviewing and identifying possible information security threats.

6.3 Information Security Incident Management

Organisations should provide formal incident reporting procedures for outsourcing providers to abide by. This is to ensure timely measures can be carried out to respond to information security incidents relating to ICT outsourcing operations.

Outsourcing providers should report any information security incident to the organisation via formal incident reporting procedures. This is to ensure all incidents are logged and timely measures can be carried out to respond to information security incidents relating to ICT outsourcing operations.

6.3.1 Roles & Responsibilities for Organisations

Roles and responsibilities for organisations in information security incident management include, but not limited to, the following:

- Produce formal incident reporting procedures (e.g. template forms and the individuals to report to).
- Review the reported incidents and analyse the root cause of the problems to prevent them from reoccurring.

6.2.2 Roles & Responsibilities for Outsourcing Providers

Roles and responsibilities for outsourcing providers in information security incident management include, but not limited to, the following:

- Report information security incidents via formal incident reporting procedures promptly.
- Apply corrective actions (or preventive actions) provided by the respective organisations immediately.

Post-outsourcing

In this phase, the ICT outsourcing activities have been completed by outsourcing providers or it has been decided that the outsourced service is to be returned to the organisation. Thus, organisations should prepare for security arrangements for the final delivery of the ICT service. Organisations are responsible to ensure all outsourcing provider's access rights have been removed. In addition, the development system has been recovered back to its normal condition, with all test data being removed permanently. Meanwhile outsourcing providers are responsible to provide training to key personnel within the organisations to ensure that they know how to maintain the ICT service (if applicable).

7.1 Security in Transfer Arrangements

Organisations should prepare for the acceptance of the final ICT service from outsourcing providers. They need to finalise security arrangements for the transfer period. In addition, they should ensure that all assets borrowed and used by the outsourcing provider during the outsourcing project are returned promptly.

7.1.1 Roles & Responsibilities for Organisations

Roles and responsibilities for organisations in transitional security arrangements include, but not limited to, the following:

- Initiate security rules for transferring the outsourced ICT service from outsourcing providers/ organisations' development environment to organisations' live/operational environment.
- Remove outsourcing provider's access (logical and physical) permanently and promptly from development environment (e.g. servers, systems, picture identification badges, keys, etc).
- Verify 'Assets Tracking Form with actual assets returned by outsourcing team to ensure printed information, private data, intellectual property relating to sensitive processes and equipments (i.e. notebooks, servers, external hard disks) belonging to the organisations are returned.
- Ensure that all information, documentation and resources related to the outsourced service have been securely destroyed or returned by the outsourcing provider (as defined in the outsourced agreement).

7

Chapter Contents

7.1.2 Roles & Responsibilities for Outsourcing Providers

Roles and responsibilities for outsourcing providers in transitional security arrangements include, but not limited to, the following:

- Return all assets belonging to organisations and sign the 'Assets Tracking Form'.
- Return physical & logical access (picture identification badges, keys, etc) to organisations (as defined in the outsourced agreement).
- Provide organisations the complete records (e.g. audit logs, reports) those information, documentation and resources related to the outsourced ICT service contract have been properly compiled and handed over to the organisations.

7.2 Training

Outsourcing providers should provide relevant information and training during and after the transition period to organisations. Organisations should work closely with the outsourcing providers and the relationship must be stated clearly in the management contract and also to ensure all documents are documented properly for easy understanding. Human resource management should be planned to ensure the availability of the IT personnel from the development to the deliverable phase. All user manuals and blueprints of the outsourced ICT service developed by outsourcing providers need to be handed to organisations. This is important to ensure future maintenance of the ICT service can be carried out smoothly.

7.2.1 Roles & Responsibilities for Organisations

Roles and responsibilities for organisations in training include, but not limited to, the following:

- Attend trainings conducted by the outsourcing providers.
- Maintain the user manual and blueprints of the ICT service provided by outsourcing providers.

7.2.2 Roles & Responsibilities for Outsourcing Providers

Roles and responsibilities for outsourcing providers in training include, but not limited to, the following:

- Conduct training on the ICT service to organisations.
- Hand over the user manual and blueprint to organisations (refer to 7.1.2).

Appendix A : Key risks in Outsourcing

Negative implications of Outsourcing[10]

The identification and categorisation of key risks is a starting point for preparing the risk assessment of the outsourcing project and should be addressed by organisations to avoid potential difficulties in the outsourcing activities. The list of risk of outsourcing is as follows:

1. Quality Risk
2. Quality of Service
3. Productivity
4. Staff Turn Over
5. Language Skills
6. Failure to deliver business transformation
7. Security
8. Company knowledge
9. Standpoint of labour

1. Quality Risk

Quality risk is the propensity for a product or service to be defective, due to operations-related issues. Quality risk in outsourcing is driven by a list of factors. One such factor is opportunism by suppliers due to misaligned incentives between buyer and supplier, information asymmetry, high asset specificity, or high supplier switching costs. Other factors contributing to quality risk in outsourcing are poor buyer-supplier communication, lack of supplier capabilities/resources/capacity, or buyer-supplier contract enforceability. Two main concepts must be considered when considering observability as it related to quality risks in outsourcing: the concepts of testability and criticality.

Quality fade is the deliberate and secretive reduction in the quality of labour in order to widen profit margins. The downward changes in human capital are subtle but progressive, and usually unnoticeable by the outsourcer/customer. The initial interview meets requirements, however, with

10 http://www.cyfuture.com/outsourcing-problem.htm

Appendixes

Chapter Contents

subsequent support, more and more of the support team are replaced with novice or less experienced workers. Some IT shops will continue to reduce the quality of human capital, under the pressure of drying up labour supply and upward trend of salary, pushing the quality limits. Such practices are hard to detect, as customers may just simply give up seeking help from the help desk. However, the overall customer satisfaction will be reduced greatly over time. Unless the company constantly conducts customer satisfaction surveys, they may eventually be caught in a surprise of customer churn, and when they find out the root cause, it could be too late. In such cases, it can be hard to dispute the legal contract with the outsourcing company, as their staff are now trained in the process and the original staff made redundant. In the end, the company that outsources may find that it is worse off than before it outsourced its workforce.

2. Quality of Service

Quality of service is measured through a service level agreement (SLA) in the outsourcing contract. In poorly defined contracts there is no measure of quality or SLA defined. Even when an SLA exists it may not be to the same level as previously enjoyed. This may be due to the process of implementing proper objective measurement and reporting which is being done for the first time. It may also be lower quality through design to match the lower price.

There are a number of stakeholders who are affected and there is no single view of quality. The CEO may view the lower quality acceptable to meet the business needs at the right price. The retained management team may view quality as slipping compared to what they previously achieved. The end consumer of the service may also receive a change in service that is within agreed SLAs but is still perceived as inadequate. The supplier may view quality in purely meeting the defined SLAs regardless of perception or ability to do better.

Quality in terms of end-user experience is best measured through customer satisfaction questionnaires which are professionally designed to capture an unbiased view of quality. Surveys can be one of research. This allows quality to be tracked over time and also for corrective action to be identified and taken.

3. Productivity

Offshore outsourcing for the purpose of saving cost can often have a negative influence on the real productivity of a company. Rather than investing in technology to improve productivity, companies gain non-real productivity by hiring fewer people locally and outsourcing work to less productive facilities offshore that appear to be more productive simply because the workers are paid less. Sometimes, this can lead to strange contradictions where workers in a developing country using hand tools can appear to be more productive than a U.S. worker using advanced computer controlled machine tools, simply because their salary appears to be less in terms of U.S. dollars.

In contrast, increases in real productivity are the result of more productive tools or methods of operating that make it possible for a worker to do more work. Non-real productivity gains are the result of shifting work to lower paid workers, often without regards to real productivity. The net result of choosing non-real over real productivity gain is that the company falls behind and obsoletes itself overtime rather than making investments in real productivity.

4. Staff turnover

The staff turnover of employee who originally transferred to the outsourcer is a concern for many companies. Turnover is higher under an outsourcer and key company skills may be lost with retention outside of the control of the company. In outsourcing offshore there is an issue of staff.turnover in the outsourcer companies call centers. It is quite normal for such companies to replace its entire workforce each year in a call center. This inhibits the build-up of employee knowledge and keeps quality at a low level.

5. Language skills

In the area of call centres end-user-experience is deemed to be of lower quality when a service is outsourced. This is exacerbated when outsourcing is combined with off-shoring to regions where the first language and culture are different. The questionable quality is particularly evident when call centres that service the public are outsourced and offshored.

The public generally find linguistic features such as accents, word use and phraseology different which may make call center agents difficult to understand. The visual clues that are present in face to face encounters are missing from the call centre interactions and this also may lead to misunderstanding and difficulties. In addition to language and accent differences, a lack of local social and geographic knowledge is often present, leading to misunderstandings or miscommunications.

6. Failure to deliver business transformation

Business transformation promised by outsourcing suppliers often fails to materialise. In a commoditised market where many service providers can offer savings of time and money, smart vendors have promised a second wave of benefits that will improve the client's business outcomes. According to Vinay Couto of Booz & Company "Clients always use the service provider's ability to achieve transformation as a key selection criterion". It's always in the top three and sometimes number one. "White failure is sometimes attributed to vendors overstating their capabilities. Couto points out that clients are sometimes unwilling to invest in transformation once an outsourcing contract is in place.

7. Security

Before outsourcing an organization is responsible for the actions of all their staff and liable for their actions. When these same people are transferred to an outsourcer they may not change desk but their legal status has changed. They no-longer are directly employed or responsible to the organization. This causes legal, security and compliance issues that need to be addressed through the contract between the client and the suppliers. This is one of the most complex areas of outsourcing and requires a specialist third party adviser.

Fraud is a specific security issue that is criminal activity whether it is by employees or the supplier staff. However, it can be disputed that the fraud is more likely when outsourcers are involved, for example credit card theft when there is scope for fraud by credit card cloning. In April 2005, a high-profile case involving the theft of $350,000 from four Citibank customers occurred when call center workers acquired the passwords to customer accounts and transferred the money to their own accounts opened under fictitious names. Citibank did not find out about the problem until the American customers noticed discrepancies with their accounts and notified the bank.

8. Company knowledge

Outsourcing could lead to communication problems with transferred employees. For example, before a transfer the staff has access to broadcast company e-mail that informs them of new products, procedures etc. An outsourcing organization may not have the same e-mail access available to them. To reduce costs, outsourced employees may have new information delivered to them in team meetings.

9. Standpoint of labour

From the standpoint of labour outsourcing may represent a new threat, contributing to rampant worker insecurity, and reflective of the general process of globalisation. While the "outsourcing" process may provide benefits in some form and to some degree it may undermine the ability of labour to resist unwanted changes in the workplace. For example, a corporation may outsource a division of the company to a service provider, that may retain the workforce on worse conditions or discharge them in the short term. The affected workers thus often feel they are being "sold down the river." Outsourcing is thus often criticised for violating the human rights.

Risks of Offshore Outsourcing[11]

Offshore outsourcing is growing per annum, with little evidence of slowing. Indeed, while most enterprises experience initial resistance, most technical issues are readily resolved and geopolitical risk is deemed insignificant after careful evaluation. Even the current political fervour about jobs being moved offshore via outsourcing is not impacting the demand or strategy of IT organizations.

IT organizations will outsource discrete projects/functions offshore (e.g. from application development projects to specific call centre support). Offshore strategies by domestic vendors will shift business from large, integrated outsourcing contracts, but most IT organizations will still develop strategies that focus on pure-play offshore vendors. The top 10 risks of offshore outsourcing are as follows.

1. Cost Reduction Expectations
2. Government Oversight / Regulation
3. Data Security / Protection
4. Lost of Business Knowledge
5. Vendor Failure to Deliver
6. Scope Creep
7. Culture
8. Knowledge Transfer
9. Privacy Risks
10. Business Continuity Risks
11. Exit Strategy Risks

1. Cost Reduction Expectations

The biggest risk with offshore outsourcing has nothing to do with outsourcing - it involves the expectations the internal organization has about how much the savings from offshore will be. Unfortunately, many executives assume that labour arbitrage will yield savings comparable to person-to-person comparison (e.g. a full-time equivalent in India will cost 40% less) without regard for the hidden costs and differences in operating models. In reality, most IT organizations save 15%-25% during the first year; by the third year, cost savings often reach 35%-40% as companies “go up the learning curve” for offshore outsourcing and modify operations to align to an offshore model.

2. Government Oversight/Regulation

Utilities, financial services institutions, and healthcare organizations, among others, face various degrees of government oversight. These IT organizations must ensure that the offshore vendor is sensitive to industry-specific requirements and the vendor’s ability to comply with government regulations and provide sufficient “transparency” showing that it does comply an thus accountable during audits. The issue of transparency is becoming more significant as requirements such as compliance and acts are in place for greater accountability on all corporations.

3. Data Security/Protection

IT organizations evaluating any kind of outsourcing question whether vendors have sufficiently robust security practices and if vendors can meet the security requirements they have internally. While most IT organizations find offshore vendor security practices impressive (often exceeding internal practices), the risk of security breaks or intellectual property protection is inherently raised when working in international business. Privacy concerns must be completely addressed. Although these issues rarely pose major impediments to outsourcing, the requirements must be documented and the methods and integration with vendors defined.

11 searchcio.techtarget.com › Home › CIO News

4. Loss of Business Knowledge

Most IT organizations have business knowledge that resides within the developers of applications. In some cases, this expertise may be a proprietary or competitive advantage. Companies must carefully assess business knowledge and determine if moving it either outside the company or to an offshore location will compromise company practices.

5. Vendor Failure to Deliver

A common oversight for IT organizations is a contingency plan - what happens if the vendor, all best intentions and contracts aside, simply fails to deliver. Although such failures are exceptions, they do occur, even with the superb quality methodologies of offshore vendors. When considering outsourcing, IT organizations should assess the implications of vendor failure (i.e. does failure have significant business performance implications?). High risk or exposure might deter the organization from outsourcing, it might shift the outsourcing strategy (e.g. from a single vendor to multiple vendors), or it might drive the company toward outsourcing (if the vendor has specific skills to reduce risks). The results of risk analysis vary between companies; it is the process of risk analysis that is paramount.

6. Scope Creep

There is no such thing as a fixed-price contract. All outsourcing contracts contain baselines and assumptions. If the actual work varies from estimates, the client will pay the difference. This simple fact has become a major obstacle for IT organizations that are surprised that the price was not “fixed” or that the vendor expects to be paid for incremental scope changes. Most projects change by 10%-15% during the development cycle.

7. Culture

A representative example: although English is one official language in many countries, pronunciation and accents can vary tremendously. Many vendors put call center employees through accent training. In addition, cultural differences include religions, modes of dress, social activities, and even the way a question is answered. Most leading vendors have cultural education programs, but executives should not assume that cultural alignment will be insignificant or trivial.

8. Knowledge transfer

The time and effort to transfer knowledge to the vendor is a cost rarely accounted for by IT organizations. Indeed, we observe that most IT organizations experience a 20% decline in productivity during the first year of an agreement, largely due to time spent transferring both technical and business knowledge to the vendor. Many offshore vendors are deploying video conferencing (avoiding travel) and classroom settings (creating one-to-many transfer) to improve the efficacy of knowledge transfer. In addition, employee turnover often places a burden on the IT organization to provide additional information for new team members.

9 Privacy risks

It should be necessary to identify risks facing organisations if they decide to outsource services which include personally identifiable information. The outsourcing provider is managing organisations’ privacy risk on its behalf, and as such, organisations are responsible for ensuring that those risks are effectively managed.

Examples of privacy risks:

- unauthorised release of personally identifiable information
- inability to provide legitimate access by the data subject to personally identifiable information
- inability to cooperate with Data Privacy Act over complaints of interference with privacy
- inability of the Data Privacy Act to investigate or enforce against outsourcing providers

- inability to guarantee the protection of personally identifiable information in foreign jurisdictions which do not have privacy/data protection laws
- foreign laws which conflict with the Privacy Act applying to organisations or offer less protection for the privacy of personally identifiable information

10. Business continuity risks

The business continuity risks are associated with organisations' ability to recover and/or restore partially or completely interrupted critical services within a predetermined time after a disaster or extended disruption, in the event that its suppliers fail or become dysfunctional, or in the case where the outsourcing provider is internal to the organisation.

Examples of business continuity risks:

- inability to recover within defined requirements
- lack of control over recovery processes/procedures

11. Exit strategy risks

The exit strategy risks are associated with an acquirer's ability to properly manage the outsourced service completion.

Examples of exit strategy risks:

- over-reliance from the acquirer on the outsourcing provider
- loss of relevant organisations capability to bring the service back in-house
- outsourcing agreement with an expensive speedy exit or no defined transition period at the end of the outsourced service

Appendix B : References

[1] ISO/IEC 27001:2005, Information Technology – Security Techniques – Information Security Management Systems, First Edition 2005-10-14.

[2] ISO/IEC 27002:2005, Information Technology – Security Techniques – Code of Practice for Information Security Management, First Edition 2005-06-15.

[3] Guidelines for ICT outsourcing
http://www.bundesrechnungshof.de/publications/booklets-guidance/ictguide.pdf

[4] Managing IT Security When Outsourcing to an IT Service Provider: Guide for Owners and Operators of Critical Infrastructure, Australian Government, May 2007.
http://www.tisn.gov.au/

[5] Good Practice Guide - Outsourcing : Security Governance Framework for IT Managed Service Provision, UK National Infrastructure Security Co-ordination Centre, 2 August 2006.
http://www.cpni.gov.uk/Docs/re-20060802-00524.pdf

[6] NIST 800-35: Guide to Information Technology Security Services
http://csrc.nist.gov/publications/nistpubs/800-35/NIST-SP800-35.pdf

[7] Discussion with Petronas on 18 April 2008.

[8] NIST 800-35: Guide to Information Technology Security Services
http://csrc.nist.gov/publications/nistpubs/800-35/NIST-SP800-35.pdf

[9] Information Security: How to outsource and make use of external services, DTI
http://www.berr.gov.uk/files/file34332.pdf

[10] ISO/IEC 27036 Guidelines for security of outsourcing (Working Draft)

Notes

Guidelines on Information Security in ICT Outsourcing

The objective of this guideline is to discuss important Information Security management issues organisations face when they are considering, or are in the midst of outsourcing their ICT environment to an external service provider. The issues discussed here are mostly related to closing or preventing the "gap" between Information Security Operations and an organisation's business strategy, and how to ensure that the proper identification of, assessment of and action of risky events take place within the outsourced environment. This guideline will provide guidance to organisations in managing and ensuring information security is preserved when choosing to outsource an ICT service to an outsourcing provider.

CyberSecurity Malaysia
Block A, Level 8, Mines Waterfront Business Park
No. 3, Jalan Tasik
The Mines Resort City
43300 Seri Kembangan
Selangor Darul Ehsan
Malaysia
Tel : +603 - 8992 6888 Fax : +603 - 8945 3205
E-mail : info@cybersecurity.my
www.cybersecurity.my

ISBN 978-967-0118-00-0