# Final Report

# Project: Vendor Security Risk Assessment

Submitted by

Kashif Manzoor
Graduate Student, Computer Science
manzoor2@uiuc.edu

# Table of Contents

# Overview

## IT – the first class citizen of every business

Information Technology (IT) has grown from being used amongst the exclusive 'Fortune 50' to being as ubiquitous as the trusted telephone. IT has assumed an extremely important role in almost every company today. More and more businesses rely on IT to support not only their day to day operations but also for market trend analysis, customer targeting and for strategic future planning. From Payroll management to Market trend analysis – companies are realizing that IT, in almost every aspect of their business, has a role to play. But all this isn't without a price. IT is not without its perils. As reliance on IT has grown, so has its misuse. Since IT is, arguably, one of the most important aspects of majority of businesses – it has also become a single point of failure. Companies are faced with the challenge of  not only figuring out how they can use IT to help them increase the bottom line, but also on how to safeguard their IT infrastructure from outside attacks. The intentional and unintentional misuse and attacks on company's IT infrastructure can bring the company to its knees.

In today's paperless environment the most important asset of a company is the information it posses – and the IT infrastructure is the guardian of this valuable asset. It is therefore, imperative that a company does everything in its power to maintain, manage and properly safeguard its IT infrastructure.

## IT Spending Dilemma

Despite the importance of IT – companies can not go overboard with the IT spending. After all, for most of the companies IT is not their business – instead IT is there as an operational aide to their main business. For example General Motors may have a huge IT infrastructure but their main business is making automobiles not IT. With the recent financial scandals (e.g. Enron, WorldCom etc.) the USA govt. has brought about several legislations that have forced the companies to reform their financial practices. "Sarbanes-Oxley Act of 2002" (SOX) being one such legislation. Although SOX does not mandate the use of computer systems for compliance or financial reporting, yet the need is clear and the IT frameworks are responding by including sections that are specifically targeted to ease the compliance. While, in general, this should be considered a good thing – but in some cases this may turn out to be shooting a fly with a canon. This compounds the problem of deciding how much to spend on IT. On one hand there are forces that would tend to favor a huge IT budget (e.g. compliance with SOX etc.), and on the other hand there are the market realities which require cost cuts.

## IT Outsourcing

Some forward thinking companies like, General Electric (GE) foresaw this problem decades ago – and started IT outsourcing, mainly to offshore software development companies. Under this strategy GE could get their software developed much cheaper. This software would then strengthen their IT infrastructure without substantially increasing their IT spending.

Despite the recent legislation the IT outsourcing trend has not slowed down. But there is a dilemma that companies have to face. For a  USA based company it makes sense to invest in implementations of frameworks and standards like COSO, COBIT etc. primarily since it aids them with SOX (and other legislation/requirements) compliance. But what about the offshore companies to which the IT work has been outsourced. Should the USA based companies (the *customer*) also require these *vendors* to comply with COBIT? If the compliance is made a condition of outsourcing then surely the offshore companies will have to invest in compliance frameworks and the cost incurred on doing so will eventually be transferred to the customers – thus raising the cost of IT.

Taking a deeper look at COBIT may evoke the following statement: Requiring the offshore companies to comply with COBIT may well be like shooting a fly with a canon. Take for example the first COBIT control “Define a strategic IT plan”. Whether the offshore company has a strategic IT plan or not should not have much bearing on the quality of software that they produce. Similarly the last control “Provide for independent audit” should not be a concern either.

This does not mean that the customer should not expect the offshore company to comply with any standard. What is required is an optimum set of best practices that only target the interface between the customer and the offshore center. By interface I mean not only the network connectivity interface (i.e. how the offshore center will be given online access to the customer’s network – if need be) but also interface during other direct or indirect interaction between the customer and the offshore company. I believe that ISO 17799 may be better suited under such circumstances.

In this document I present guidelines and checklist for conducting an IT security risk assessment of an offshore company. The idea is that a USA based company (the *customer*) can use this document to conduct a security audit of an offshore company (the *vendor*) which the customer intends on outsourcing the IT work to. This document not only includes an audit checklist for the customers against which the audit can be conducted, but also includes some guidelines for the vendors for implementing the checklist.

# IT Standards and Models

There are several IT standard frameworks that address the IT security, risk and vulnerability. Most of these frameworks and standards are a useful juxtaposition of industry's best practices. Three most popular and widely used frameworks include:

- COBIT
- ITIL
- ISO 17799

Although all these frameworks address the IT security, risk and control issues; their, intricate details do differ.

## COBIT

The **Control Objectives for Information and related Technology** (**COBIT**) is a comprehensive framework for control over IT that fits with and supports the **Committee of Sponsoring Organizations of the Treadway Commission** (**COSO**) *Internal Control—Integrated Framework*, the widely accepted control framework for enterprise governance and risk management.

COBIT's process model is logically divided into four domains namely: *Plan and Organize*, *Acquire and Implement*, *Deliver and Support* and *Monitor and Evaluate*. COBIT has 34 generic processes that are spread across these four domains. COBIT takes its inspiration from CMMI maturity levels. It evaluates the IT maturity of a company by placing it into one of the five maturity levels namely: Non-Existent, Initial/Ad hoc, Repeatable, Defined, Managed and Measurable, Optimized.

In summary COBIT encompasses industry's best practices and consolidates all the contemporary IT standards. It is, therefore, 100% compliant with ISO 17799. Details of COBIT are beyond the scope of this document. Interested readers should see reference [1] for details.

## ITIL

The **Information Technology Infrastructure Library** (**ITIL**) is a framework of best practices that promote quality computing services in the Information technology (IT) sector. ITIL addresses the organizational structure and skill requirements for an IT organization by presenting a comprehensive set of management procedures with which an organization can manage its IT operations. In specific ITIL evaluates the following areas: Service Desk, Incident Management, Problem Management, Release Management, Configuration Management, Change Management. ITIL also follows the concept of maturity levels however its names and numbers of the levels differ from that of COBIT and CMMI. ITIL web site provides an online self assessment utility that can be downloaded from [3]. Details of ITIL are beyond the scope of this document. Interested readers should see reference [2] and [3] for details.

## ISO 17799

This document is not intended as a primer of ISO 17799. For readers who are not fully aware of ISO 17799 we give a brief introduction to ISO 17799 below. For the purpose of this document this brief introduction, should suffice.

By following this document the readers may not be able to go out and achieve ISO 17799 certification (although this document will help in that direction) – but the real intention of this document is to act as a yardstick through which a company can evaluate its offshore vendors' security practices.

ISO 17799 is used as a generic umbrella term that covers both the ISO 17799 and ISO 27001 standards. ISO 17799 specifies 10 mains sections that include a total of 36 control objectives. The 36 control objectives suggest hundreds of specific controls. All of these collectively form ISO 17799.

ISO 27001 is the new name for BS7799-2. BS7799-2 was the British Standard Specification for Information Security Management Systems. It has been superseded by ISO 27001:2005.

ISO 17799 may be considered as a set of controls that a company must place and address to ensure its IT security. Whereas ISO 27001 provides guidelines on how to go about implementing the security controls suggested in ISO 17799. Companies that wish to achieve ISO 17799 certification will usually use both ISO 17799 and ISO 27001 standards to achieve the prized certification.

Simply put, ISO 17799 tells you what you must address and implement and ISO 27001 tells you how to implement it.

## Why not require the vendors to simply get ISO 17799 certified

The obvious question that may come to the mind of many readers would be: "*Since this document is based on ISO 17799 why do we need to bother with this why not simply require the vendors to be ISO 17799 certified*".

It is true that this document gets its inspiration from ISO 17799 but the document is written in the context of offshore software companies. It therefore cuts on some of the ISO controls which are not very relevant to our context, and adds some additional concrete controls that are more applicable to our context. In other words this document takes in a comprehensive standard like ISO 17799 crops it and scales it and makes it more specific to our context.

ISO 17799 toolkit costs around 1200 USD, and this is just the beginning. The ISO consultants will cost an additional several thousand dollars – since to make sense out of these fairly generic documents one needs expert advice. It doesn't stop here; the ISO audit itself puts a dent in your pocket. After all these expenses, a seemingly simple certification, will suddenly seem to carry a huge financial baggage. The vendor will probably transfer this expense (at least a part of it) to the Customer. In our opinion the excess financial baggage associated with ISO certification will prove to be a big deterrent.

## Why Choose ISO 17799 over COBIT and ITIL?

Just by looking at the names of these standards, without actually going into their details, one could get a fairly good idea as to the intention of these standards. COBIT - **Control Objectives for Information and related Technology –** intends on proposing controls that can help a company better *control* their IT infrastructure. ITIL - **Information Technology Infrastructure Library** – intends on addressing the issue of how an IT company can better *manage* its IT operations. Both of these standards would cover more than juts the security aspects of IT. They would cover things like Software Configuration Management, Software Release Management etc. things that would help the IT company to deliver software. ISO on the other hand has different standards that cover all which COBIT and ITIL cover in a single standard. For example ISO 9001:2000 is a comprehensive standard that addresses the product (including software) development capabilities of a company. ISO 17799 specifically addresses the IT security aspect. In this sense ISO 17799 is a much smaller but more security focused standard as compared to COBIT and ITIL. It is for this reason that we have based our IT risk assessment on ISO 17799.

# Security Risk Assessment

To perform security risk assessment we have developed a security risk audit checklist. This checklist has been mainly inspired by ISO 17799 and Protiviti's Technology Risk assessment methodology [5].

The security audit checklist is divided into 9 sections (note that this division is different from the section division used in ISO 17799) – each of which is further divided into sub-sections. The complete audit checklist along with its explanation is given in Appendix A.

The checklist in Appendix A is, by no means, exhaustive. ISO 17799 contains several hundreds of security controls all of which can potentially be added to the checklist. We have tried to customize the checklist such that it is not overwhelming to follow and at the same time addresses majority of security risks.

The audit checklist contains specific questions/Audit items which will be asked to the vendor. For each of the items in the checklist the vendor can reply *Yes, No* or *Not Applicable (N/A)*. Each *Yes* response must be further qualified by one of the following:

a. Planned / just started,
b. Partially completed,
c. Fully implemented.

Each item in the checklist is assigned a severity level and each possible response is assigned a weight. These assignments are made by the customer and are based on the customer's perspective. The response can then be quantified using these weights and severity levels, thus producing an overall risk score. Since weight/severity level assignments are particular to each customer we have not taken the liberty of assigning them to the checklist items. We believe that each customer will come up with their own weights based on their culture and their own perception of security risk. We do however show some sample weights and risk score calculations (given in Appendix B).

## General To-Dos

Although each of the checklist item would require the vendor to implement it in specific way (as shown in Appendix A) but there are some general controls that the vendor must have in place. These controls will act as prerequisites to most of the items in the checklist. These general controls are given below:

- **Creation of Security Policy**
  The vendor must have a documented security policy. This policy should have concrete guidelines and rules that the company must follow. Several of the items in the Audit checklist require specific sections to be added to this policy. This should give the readers a good idea on what to include in the policy. The vendor must not make an overwhelming policy – spanning several hundreds of pages. Since this way the vendor runs the risk of making a policy that no one will read. Although the size of the policy varies from company to company but a good policy should be brief, to the point and should only address the relevant issues. The items in the policy would usually follow the template given in Appendix C. Readers may wish to look at some of the policies that University of Illinois follows. Some of these policies can be found

at the following URL: http://www.vpaa.uillinois.edu/policies/. The policies specific to IT can be found at: http://www.cio.uiuc.edu/policies.html. The policies that relate specifically to Internet and email can be found at: http://www.fs.uiuc.edu/cam/CAM/viii/viii-1.1.html

All these policies act as a good guideline on how a vendor should create their security policies. Note that the actual policy will depend on the vendor's nature of business, size, posed security risk etc. But the above URLs present a good starting point. The email policy item given in the Appendix C is improvised from the URLs given above. At minimum, a good policy document must contain policies pertaining to the following

- Data Ownership and Classification (data must be classified as secure, confidential, public etc.).
- Password Management.
- Account Creation and Removal.
- Third Party Connections to the network.
- Modem Usage.
- Business Continuity Program (e.g. Disaster Recover Plan).
- Incident Response.
- Confidentiality Agreement.
- Data Protection.
- Internet Usage.
- Email Usage.
- Chat and Instant Messaging Usage.
- Network protection and management.
- Laptop usage.
- etc…

- **Appointment of a Security Officer**

  A designated security officer must be appointed by the vendor. The security officer will primarily be responsible for the following:

  - Employee training.
  - Security policies creation, management and continuous update.
  - Internal security audits.
  - Security violation escalation and closure.
  - Single point of contact for any security related questions.
  - Managing and conducting Security Council's meetings.

- **Creation of Security Council**

  A security council must be set up. This council should have the following members:

  - Security officer.
  - Senior management representatives.
  - Representatives from all departments/groups of the company e.g. administrative group, software development group, Quality Assurance group etc.

  The Security Council will have the following responsibilities:

  - Conduct regular meetings.
  - Conduct internal security audits.
  - Follow up on the security violations.
  - Disseminate security awareness and knowledge amongst their respective group members.
  - Escalate any concerns of their groups.

- Contribute towards the creation, maintenance and update of security policies.

# Case Studies

Security risk assessment is considered a cardinal and a continuous activity by all the security conscious companies. IT security is not a matter of choice anymore; it has become a legal requirement in many countries and across many industry segments. Several companies in USA specialize in conducting security audits. Protiviti [4] is one such company. Protiviti uses external penetration testing to assess their customer's network and server security (these refer to *Network Security* and *System Security* sections of our audit checklist in Appendix A). Their experience has shown that even the simplest of testing reveals serious loop holes. The specifics of Protiviti's network penetration testing are given below:

Protiviti connects to the internet and performs the following activities in an attempt to break into their customer's network, this uncovering the vulnerabilities:

**Nmap** is used to discover open ports, services and operating system types on the target systems. Knowing the operating system type of the target system can help exploit operating system specific vulnerabilities.

**Ethereal** is used as network traffic sniffer. This tool can identify operating system and can also identify version and specific details of web servers and other server applications. (In our audit checklist we have added an item to specifically address network sniffers e.g. using switches in the network can stop the sniffers from sniffing. See Appendix A section: *Event Management and Intrusion Detection*)

**Telnet** client is used to telnet to severs. If a telnet is successful then attempts are made to logon to the server and once in lot of damage can be done.

**Nessus** – is used to scan all the ports and check for any open port. Once an open port has been found the tool then attempts to exploit the service running on that port using its knowledge database. In Appendix A we have included item to make sure that all unnecessary ports (including Telnet) be blocked to counter such attacks.

**Pwdump4** – is used to obtain the user login names and encrypted passwords from a Windows server. Once this information is obtained it can be passed on to
**John the ripper** (a password cracking tool). This tool takes in the pwdump4 login/password file as input and performs dictionary and brute force attacks to decrypt the passwords. This decryption is done offline and with sufficient computing power the passwords can be decrypted in a short time.

All the above tools are freeware and can be downloaded by any one. They are automated and do not have much of a learning curve. According to Protiviti's findings even the simplest of these tools are successful in finding several vulnerabilities.

## Related Topics

In preparing this document we utilized several sources of information. While the information provided in [6], [7] and [8] were the primary reference; [9] inspired us to include the items pertaining to Disaster Recovery. Reference [10] was extremely helpful in identifying contents of a policy and in coming up with a sample template for a policy (Appendix C).

# Conclusion

IT Security has become an important consideration. Unfortunately companies usually have a tight budget to implement the necessary security controls. Despite its importance, being secure is not the primary business of a company (except of security auditing companies and consultancies); therefore companies are not willing to spend large amount of money on security if this means a dent in the bottom line.

Having too many standards simply aggravates the situation. Even if a company picks up one of these standards and decides to follow it and roll it out – it can still find the standard overwhelming as most of the standards have hundreds of controls and practices that the company must instill in its culture. Even if a company overcomes these deterrents it still needs to evaluate the value added by rolling out these standards.

Despite the importance of security the fact remains that companies usually do not treat this as high priority unless there is either a big incentive for doing it (e.g. high profit) or a liability for not doing it (e.g. mandatory government compliance). USA legislations (like SOX, HIPAA) have proven to be a hanging sword for the related companies. This has forced such companies to implement IT security standards. However these regulations only apply to local USA companies and their subsidiaries. Such legislations are not present in the rest of the world and hence companies outside USA may not have enough of an incentive to undertake aggressive overwhelming security standards. The economic pressure dictates that USA companies must outsource and conduct business with foreign companies. What is required is for these foreign companies to follow a customized, low cost and simple security standard which is fully tailored towards their specific needs.

USA companies need only worry about evaluating the risk of doing business with such companies in the context of what affects them. The security risk assessment checklist presented in this document is one such light weight standard. This standard aims at ensuring that a USA based company that outsource its Software Development to a foreign company, can evaluate the foreign software company against this checklist and be assured that the vendor can be entrusted with their data and their software development tasks.

The underlying theme of the assessment checklist presented in this document is *development of a security conscious culture* at vendor. Despite all the checks and balance a determined individuals may cause serious damage to a company – no standard and regulation can stand in his way. However by changing the culture of a company and making sure that security is engrained in the culture a company stands a better chance of keeping itself secure. This is the aim of our assessment checklist. It is light weight, concise and easy to implement. We believe that a vendor may not need any outside consultant or auditor to help them implement it. All it needs is a committed management who are sincere in improving the security of their company.

# Appendix A: Security Risk Assessment Checklist

This appendix presents the Security Risk Assessment checklist. We have made every attempt to make each of the items self-explanatory and unambiguous. The checklist is divided into nine sections, some of these sections are further divided into few sub-sections. This appendix is followed by Appendix B, which gives a sample risk score calculation of one of the sections of the checklist. Accompanying this document is an EXCEL sheet that fully implements this checklist and has embedded formulae to calculate the risk score.

## 1. ORGANIZATION

This section analyses the organization in general. For a vendor to have a security focus there must be evidence that security is one of the priorities of the vendor organization. For starters the vendor must have a clear well written security policy in place. The policy should set the ground rules which all the company must abide by. The policy should act as a 'security bible' for the organization.

Having a policy is not enough there must be individuals dedicated to ensuring that the policy is kept up-to-date and that it is being abided by. The policy must be a dynamic and live document that must be reviewed and updated frequently. This requires that there must be individuals responsible for the management of the policy. Additionally no policy, no matter how well written can be free of ambiguities. There must be individuals to whom an employee can turn to in case he requires clarification of the policy.

Based on the above observations the following checklist must be implemented by the vendor.

| **ORGANIZATION** | **Response** | **"Yes" Details** | **Severity** | **Risk Score** |
|---|---|---|---|---|
| **SECURITY POLICY** | **YES.**<br>**NO.**<br>**N/A.** | **Planned / just started.**<br>**Partially completed.**<br>**Fully implemented.** | **High.**<br>**Medium.**<br>**Low.** | **Calculated** |
| Have the Information Security Policies been issued to all employees, including third party personnel and contractors? | | | | |
| Have all employees formally acknowledged adherence to the Information Security Policies? | | | | |

| | | | | |
|---|---|---|---|---|
| Are employees required to annually re-acknowledge compliance with the Information Security Policies? | | | | |
| How and when do you perform internal audits to measure compliance with the Information Security Policies? | | | | |
| How frequently do you perform periodic reviews to update security policies and guidelines for relevancy and emerging topics? | | | | |
| Are controls in place to restrict your ability to transmit customer data to unauthorized personnel outside your company? | | | | |
| Has an organizational policy on copyright compliance been implemented and communicated to all users? | | | | |
| Do you have a policy that prohibits generic logon account and do you follow the policy? | | | | |
| Are all the following subject to data confidentiality agreements?<br>* Permanent employees<br>* Contractors / temporary staff<br>* 3rd Party service providers | | | | |
| Has your business issued an E-mail Usage Policy? | | | | |
| Do you take action against users who use e-mail in contradiction to the E-mail Usage Policy? | | | | |
| Has your business issued an Internet Policy? (e.g. only access the Internet for legitimate work-related purposes, no downloading of games, etc.) | | | | |
| Are all users required to sign an internet usage and responsibility agreement that acknowledges compliance with the stated Internet Policy? | | | | |
| Are there comprehensive documentation standards for IT development and operational controls? | | | | |
| Is there a clear desk policy? | | | | |
| **SECURITY OFFICER & ORGANIZATION** | | | | |
| Do you have a full-time Information Security Officer? | | | | |
| Have roles and responsibilities for protecting assets and implementing security measures been explicitly defined and communicated to all the department/groups? | | | | |
| Has a formal risk analysis process been implemented to assist management in identifying security threats? | | | | |

## 2. EMPLOYEES SECURITY FOCUS

Policy is at a much higher level. To execute the policy there must be concrete processes and procedures that a company must follow. A company can have several processes and procedures that will stem out of their security policy but from our perspective the most important are the ones that pertain to employee empowerment. A vendor may have an excellent policy but unless steps are taken to actively get the buy in from the employees these policies are useless. Having processes in place that will actively give the employee the right security focus is an important aspect of the security audit. Based on this the checklist has been devised.

| **EMPLOYEE SECURITY FOCUS** | **Response** | **"Yes" Details** | **Severity** | **Risk Score** |
|---|---|---|---|---|
| **AWARENESS & TRAINING** | **YES.<br>NO.<br>N/A.** | **Planned / just started.<br>Partially completed.<br>Fully implemented.** | **High.<br>Medium.<br>Low.** | **Calculated** |
| Has a formal, on-going Security Training program been implemented? | | | | |
| Have you implemented a process to measure the Effectiveness of Security Training? | | | | |
| Does the on-going Security Awareness program include instructing users on how to detect and avoid 'social engineering' attacks as well as competitive intelligence probes? | | | | |
| Have users been educated on how to report suspected security violations or vulnerabilities? | | | | |
| Do regular bulletins sent to employees alerting them to risks and vulnerabilities involved in computing, including basic tasks such as backup, anti-virus scanning and choosing strong passwords? | | | | |
| Is there a process to communicate security policy and guideline changes to employees? | | | | |
| Is the importance of Information Security visible throughout the organization (e.g. security discussions in company meetings, security award, posters etc.)? | | | | |
| Do you notify employees that customer sensitive data cannot be loaded on personal PC's? | | | | |

| | | | | |
|---|---|---|---|---|
| Are users of systems containing sensitive information made aware of legal and company obligations associated with the use of the application? (e.g. through Logon Banner) | | | | |
| Have employees been instructed to challenge strangers or unescorted visitors in non-public areas? | | | | |
| Are there periodic spot-checks of users' workspaces to monitor compliance with the information protection program. | | | | |
| **RECRUITMENT PROCESS / NEW EMPLOYEE IT ORIENTATION** | | | | |
| Are new hire workers (including contractors & third party personnel) subjected to a history and background check? (e.g. References, police records, etc.) | | | | |
| Do workers receive introductory awareness security training? | | | | |
| **EMPLOYEE EXIT / TRANSFER** | | | | |
| Does Human Resources (HR) department provide system administrators with a list of:<br>* workers transferring departments<br>* workers leaving the company | | | | |
| Is there a process to notify system administrators when workers leave the business? | | | | |
| Are exit interviews conducted to recover property given to workers?<br>For Example:<br>a) Company property (badges, company credit cards etc).<br>b) Tools of the job (laptops, mobile phones, pagers, remote dial-in access cards, modems etc.). | | | | |
| Is there an emergency program for immediate removal of employee's system access when the departing employee is identified as disgruntled or high risk? | | | | |
| Are access / exit controls employed in your facility? | | | | |
| When employees leave, do you 1) check to see if they have sponsored accounts or badges for guests and 2) question them on continued need AND 3) assign new sponsors? | | | | |

## 3. CHANGE MANAGEMENT

Change is a natural process and a vendor must make sure that changes occur in a controlled manner. Changes can be of several types but we restrict ourselves to the changes that apply to the vendor’s ability to develop and deliver the software. For example upgrading the computers either the hardware upgrade or the software upgrade is of extreme importance. Similarly changing the physical security system is also important. Changes should not be at an individual's whim neither should they be carried out arbitrarily. Instead changes should be approved and should be planned. A vendor must show proof that the changes happen in a planned and approved manner. The checklist below attempts at verifying vendor's capability to handle changes properly and in orderly fashion.

| **CHANGE MANAGEMENT** | **Response** | **"Yes" Details** | **Severity** | **Risk Score** |
|---|---|---|---|---|
| **CHANGE MANAGEMENT** | **YES.<br>NO.<br>N/A.** | **Planned / just started.<br>Partially completed.<br>Fully implemented.** | **High.<br>Medium.<br>Low.** | **Calculated** |
| Do you have documented change control procedures to manage all modifications to the development environment (software, hardware, network)? | | | | |
| Is change control preformed on a regular basis? | | | | |
| Is Physical Security (e.g. power control, locks, badges, entrance cards) part of your change control process? | | | | |
| Are Changes approved in change control documented and stored in a publicly accessible format? | | | | |
| Does the customer sign off on changes affecting them? | | | | |
| Is there a documented procedure for performing emergency changes outside the change control process? | | | | |

## 4. NETWORK SECURITY

Securing the network is an extremely important aspect of any company's security portfolio. While a construction company must also secure its network against hackers but for a software development firm a hacker can literally wipe off all the company's asset – since most part of company's assets are in soft form stored on computers.

There are several hardware and software solutions available that will help secure the network. In particular a vendor must address the controls given in the checklist below:

| NETWORK SECURITY | Response | "Yes" Details | Severity | Risk Score |
|---|---|---|---|---|
| **ROUTER / FIREWALL** | **YES.<br>NO.<br>N/A.** | **Planned / just started.<br>Partially completed.<br>Fully implemented.** | **High.<br>Medium.<br>Low.** | **Calculated** |
| Do you maintain a current network diagram and who owns and maintains it? | | | | |
| Has, at minimum, stateful firewalls been deployed at all external connections (e.g., Internet)? Give type of firewall currently used. If no, list the type of security mechanism used (e.g., router with ACL's) | | | | |
| Is the firewall(s) configured with a policy that all services are denied unless expressly permitted? | | | | |
| Do you have a process/criteria to evaluate the risk of protocols/ports before implementing them on the firewalls? | | | | |
| Is outgoing traffic directed to external proxy servers? If so, are these proxy servers resident on a DMZ? | | | | |
| Are all services forbidden except when specifically requested? | | | | |
| Is logging enabled on all firewalls, routers, and proxy servers? Is a process in place to review the logs regularly? | | | | |
| Are the firewall(s) and/or the proxy server(s) configured on a hardened platform, with limited functionality (e.g., all unnecessary applications removed)? | | | | |
| Is access to all firewalls, routers, and proxy servers restricted to only those people who need to manage these devices? | | | | |
| Do administrators remotely access the routers and/or firewalls? If So are they securely authenticated by using one-time passwords or encrypted login sessions? | | | | |
| Is there a process in place to ensure that all the routers/firewalls have the latest software and that they are patched regularly with the latest security updates from their respective vendors? | | | | |
| **VPN - REMOTE USER CONNECTIVITY** | | | | |
| For computers used for VPN remote access, have you implemented a Personal Firewall? | | | | |
| Do you only allow VPN access to computers that implement Antivirus Software and Personal Firewall? | | | | |

| | | | | |
|---|---|---|---|---|
| Do you have a process in place in order to cancel anyone's VPN access rights as soon as their project is completed or their reason for having the VPN is invalidated? | | | | |

## 5. APPLICATION SECURITY

Since our focus is on the vendor’s ability to develop and deliver high quality software it would not make much sense if the vendor is well secured but the software they develop has security holes in them. We must ensure that vendor’s employees understand that any software that they develop must have security as its basic requirement. Additionally during the course of software development the vendor may be given access to customer’s sensitive data we must make sure that this data is properly handled and secured. This results in the following audit items that the vendor must address:

| **APPLICATION SECURITY** | **Response** | **"Yes" Details** | **Severity** | **Risk Score** |
|---|---|---|---|---|
| **SECURITY IN APPLICATION DEVELOPMENT** | **YES.<br>NO.<br>N/A.** | **Planned / just started.<br>Partially completed.<br>Fully implemented.** | **High.<br>Medium.<br>Low.** | **Calculated** |
| Does your system development methodology address information security during the discovery and development phase? | | | | |
| Do you perform a security code review during each phase of development? | | | | |
| Are there separate environments for each customer for development and testing of systems? | | | | |
| Are all the software developers working on the software given orientation in security requirements of the customer before they start work on the project. | | | | |
| Are all developed software tested for virus by running anti-virus on them before delivering them to the customer? | | | | |
| **DATA SECURITY** | | | | |
| Are backups of business critical data done regularly (at least weekly)? | | | | |
| Do you have an on-line mechanism to verify that all backups complete successfully? | | | | |
| Do you periodically restore information from backup tapes to ensure data integrity? | | | | |

| | | | | |
|---|---|---|---|---|
| Are backup tapes kept in an environmentally controlled and secured area? | | | | |
| Do you store tapes off-site? If yes, how is access to the tapes protected at the site? | | | | |
| Are back up tapes stored in location with physical access control? | | | | |
| Is there a regular audit conducted to account for all the backup tapes. | | | | |
| Are backup tapes ever destroyed if yes then what procedure is used to destroy them. | | | | |
| **DATA CLASSIFICATION** | | | | |
| Does all critical business data have an owner? | | | | |
| Is critical information classified according to a classification guideline (e.g. secure, confidential, public etc.)? | | | | |
| Does access to sensitive customer data have to be authorized by the owners of the data? | | | | |

## 6. SYSTEM SECURITY

Computer Servers form the backbone of a vendor's IT infrastructure. Any damage to the servers can create havoc. When a vendor's network has been compromised it is usually the servers that are the prime targets. The vendor must address the following items in the checklist given below:

| SYSTEM SECURITY | Response | "Yes" Details | Severity | Risk Score |
|---|---|---|---|---|
| **SERVER VULNERABILITY & HARDENING** | YES.<br>NO.<br>N/A. | Planned / just started.<br>Partially completed.<br>Fully implemented. | High.<br>Medium.<br>Low. | Calculated |
| Is there a process to proactively obtain the latest security patches and updates? | | | | |
| Do you have a process to identify network, application and OS based systems vulnerabilities? | | | | |
| Do you use automated tools to assess system vulnerabilities? | | | | |
| Does your internal audit simulate outside attacks or do you hire external consultants to simulate attacks on your system to uncover its susceptibility. | | | | |
| Have all business critical systems used in customer software development been analyzed for their security risks? | | | | |
| Do you have a security checklist for each OS deployed at your company? | | | | |
| Do you regularly perform audits (Internal or external) against your security checklists? | | | | |
| Are your system security checklists updated on a regular basis? | | | | |
| Are super user privileges regulated on systems in a written policy? | | | | |
| Are applications regulated from running as a super user privilege? | | | | |
| Do you require logon banners on systems? | | | | |
| Are users with super user privileges reviewed and revised on a regular basis? | | | | |
| Do you have Anti-Virus software running on all of your Microsoft Platforms (Servers, Workstations, PC's and Laptops)? | | | | |
| Have you rolled out Anti-Virus Software to all of your email servers? | | | | |

| | | | | |
|---|---|---|---|---|
| Are all your Email servers configured to check all the incoming and outgoing emails for viruses, spam, trojan horses and other threats? | | | | |
| Do you have a procedure to ensure that all the servers, user machines and laptops are configured to automatically install the latest Virus Definition Files? | | | | |
| Do you have a mechanism in place to check all FTP inbound and outbound file transfers for viruses? | | | | |

## 7. IDENTITY MANAGEMENT

Securing hardware and software means that only the authorized users be given access to them. This is usually done by giving each authorized user a user account with suitable privileges. The account has an associated login name, password and access rights. The user must use his login name and password to log into his account, after which what he can and cannot do, will depend on his user rights. The vendor must have a good process in place that will ensure proper management of the user accounts. The following items must be addressed by the vendor:

| **IDENTITY MANAGEMENT** | **Response** | **"Yes" Details** | **Severity** | **Risk Score** |
|---|---|---|---|---|
| **ACCOUNT MANAGEMENT (USER & HIGH PRIVILEGE ACCOUNTS)** | **YES.<br>NO.<br>N/A.** | **Planned / just started.<br>Partially completed.<br>Fully implemented.** | **High.<br>Medium.<br>Low.** | **Calculated** |
| Is each customer account owned or sponsored by the customer? | | | | |
| Does each account prohibit concurrent access (e.g. User cannot be logged in from two different machines)? | | | | |
| Are all user accounts deleted on the users' departure date? | | | | |
| Does the system disable user accounts after a period of inactivity? | | | | |
| Do you periodically reconcile system accounts to existing users? | | | | |
| Does the system lock user accounts after a number of failed attempts to login? | | | | |
| Do you have a consistent userid for a single person in all platforms & instances? | | | | |
| Are privileged accounts set up for emergency problem resolution fully logged and subjected to regular reviews? | | | | |
| Do you have a policy on privileged accounts? | | | | |

| | | | | |
|---|---|---|---|---|
| Do you have a compiled list of personnel with root or admin privileges? | | | | |
| Do you disable all the default account in all your server applications (e.g. Oracle's default DBA account and Oracle's default scott-tiger account, Windows default remote assistant accounts etc.)? | | | | |
| **PASSWORD MANAGEMENT AND AUTHENTICATION** | | | | |
| Are users forced to change their passwords at first sign-on? | | | | |
| Do passwords expire periodically (e.g. every XX days)? | | | | |
| Are users prohibited from frequently re-using passwords (e.g. password can not be reused with in six months)? | | | | |
| Do you periodically run password cracking software to identify weak passwords? | | | | |
| Do you have a process which notifies employees with weak passwords and forces a change? | | | | |
| Do you conduct internal audits to identify weak password using social engineering (e.g. password of a user is based on his son's name or the first word of the poster on his desk etc.)? | | | | |

## 8. EVENT MANAGEMENT

Event is defined as an occurrence of some thing. Although there is no negative connotation associated with events themselves but in the context of IT security the term *events* is usually used to refer to something that is undesirable and has negative repercussions. Vendor must have procedures in place to safeguard himself from any undesirable events. At a minimum the following items must be addresses

| **EVENT MANAGEMENT** | **Response** | **"Yes" Details** | **Severity** | **Risk Score** |
|---|---|---|---|---|
| **EVENT MONITORING & INTRUSION DETECTION** | **YES.<br>NO.<br>N/A.** | **Planned / just started.<br>Partially completed.<br>Fully implemented.** | **High.<br>Medium.<br>Low.** | **Calculated** |
| Is security auditing enabled on business critical systems (e.g. all servers configured to log any unsuccessful login attempt etc.)? | | | | |

| | | | | |
|---|---|---|---|---|
| Do you have a process to review security audit logs in a timely, consistent manner and act upon any threats identified by these reviews? | | | | |
| Is there an automated alerting/notification process that is initiated when defined security thresholds are exceeded? | | | | |
| Are you using network based Intrusion Detection (IDS) products on interconnections (e.g., Internet, web-hosting platforms, and 3rd party connections)? | | | | |
| Do you periodically perform network penetration studies either using internal audits or through external consultants? | | | | |
| Is your business critical networks configured with Switches so that sniffer software is ineffective? | | | | |
| Is the intrusion detection system's network placement frequently reviewed to ensure appropriate coverage? | | | | |
| **INCIDENT RESPONSE** | | | | |
| Is there a process for users to report to IT when they have identified a potential virus on their system? | | | | |
| Do you have a documented Security Incident Response procedure? | | | | |
| Have you communicated the Security Incident Response procedure to all employees? | | | | |
| Do you conduct drills to verify the readiness of the company to any security incident? | | | | |
| **DISASTER RECOVERY** | | | | |
| Are there business mandated formal written Disaster Recovery Plans (DRPs) covering the partial or full loss of Servers, Critical Applications, Physical facilities? | | | | |
| Are there disaster recovery facilities for critical systems located in a geographically independent area? | | | | |
| Have employees been trained on and are DRPs tested and updated on at least an annual basis? | | | | |
| Is there an owner responsible for devising and maintaining the DRPs? | | | | |
| Have DRPs been reviewed and approved at the managerial level (e.g. by CIO)? | | | | |
| Have you identified “business critical” individuals to your business (i.e. how would you cope if 'x' left?)? | | | | |
| Has a business impact analysis been conducted on all customer applications and systems? | | | | |

| | | | | |
|---|---|---|---|---|
| Have you identified and documented your business critical applications and applied Business Impact Analysis? | | | | |
| Are training sessions conducted for all relevant personnel on backup, recovery, and contingency operating procedures? | | | | |

## 9. ASSET SECURITY

We have all heard of horror stories of employees' company laptops being stolen. Laptops contain sensitive data, and if they get stolen this could have huge liability for the company. The vendor must ensure that he has controls in place to safeguard himself against such incidents. Security, both physical and otherwise, should be of utmost importance to the vendor. In specific the vendor must address the following

| **ASSET SECURITY** | **Response** | **"Yes" Details** | **Severity** | **Risk Score** |
|---|---|---|---|---|
| **LAPTOP SECURITY** | **YES.**<br>**NO.**<br>**N/A.** | **Planned / just started.**<br>**Partially completed.**<br>**Fully implemented.** | **High.**<br>**Medium.**<br>**Low.** | **Calculated** |
| Are all laptops required to be physically secured (e.g. cable lock) at all times? | | | | |
| Are users instructed to perform back ups on a regular basis on all laptops containing business and customer critical data? | | | | |
| Is there a process to ensure that business and customer critical data is encrypted? | | | | |
| Are employees who travel with laptops provided with theft prevention devices? | | | | |
| **PHYSICAL SECURITY (BUILDINGS & CLIENT MACHINES)** | | | | |
| Are ID badges issued to all working personnel (Permanent, contractor, agency temps, and visitors)? | | | | |
| Are personnel required to display their ID badges? | | | | |
| Do ID badges have to be periodically renewed? (e.g. every 12 months) | | | | |
| Do you have visitor control procedures (i.e. are they logged in and out, and are they escorted within computer areas)? | | | | |
| Are fire detection / suppression systems required in your buildings? | | | | |

| | | | | |
|---|---|---|---|---|
| Are your premises protected by intrusion detection systems e.g. CCTV? | | | | |
| Do you require security guards on all of your sites keeping business and customer critical data? | | | | |
| Do guards at entrances / exits randomly conduct spot checks to prevent unauthorized items from entering / leaving the building? | | | | |
| Are physical security breaches logged and investigated? | | | | |
| Are there random out of hours security inspections of the work place? | | | | |
| Are results of security inspections of the work place reported to senior management? | | | | |
| Is there a preventive maintenance program in effect for all environmental and protection systems? | | | | |
| **PHYSICAL SECURITY (SERVER ROOMS)** | | | | |
| Are firewalls kept in physically secure areas? | | | | |
| Is there a process to restrict access to computer centers only to people who have a business need? | | | | |
| Do you periodically review the list of people who have access to the computer center? | | | | |
| Do outside signs and building directories avoid making reference to computer centers or their locations? | | | | |
| Are servers kept in protected areas with restricted access? | | | | |
| Are there established guidelines detailing what security is needed in areas where servers are (e.g. access control logs)? | | | | |
| **ASSET INVENTORY** | | | | |
| Do you have documented procedures for removing equipment from your facility? | | | | |
| Do you have an inventory of authorized modems and their phone numbers, and are these inventories regularly reviewed? | | | | |
| Is there a process in place to ensure that inventory for all computer equipment is maintained for accuracy and currency? | | | | |
| Do you have methods for the secure disposal of unwanted equipment and documents? | | | | |
| **SOFTWARE MANAGEMENT** | | | | |
| Is there a process to ensure software inventory is maintained for accuracy and currency? | | | | |
| Is license documentation physically available for review? | | | | |
| Are procedures in place to manage software license compliance? | | | | |

| | | | | |
|---|---|---|---|---|
| Are new employees trained on the appropriate uses of company software? | | | | |
| Is an authorized software list maintained and users made aware of the fact that they can only install those applications that are included in this list? | | | | |
| Are employees prohibited from installing unauthorized and pirated software on their desktop and laptop computers? | | | | |

## Appendix B: Sample Security Risk Calculation

In Appendix A we gave a comprehensive audit checklist, but we refrained from recommending any risk score calculation method. In this section we present sample risk score calculations. Readers should note that the risk score is sensitive to the severity level assigned to each item and the weights of each of the severity levels and possible responses. We expect that each company will have their own values for these variables. In this section we shall how the risk score can be calculated. The general calculation method would remain the same irrespective of the chosen weights and severity level.

The following steps were followed for risk score calculations:

- Decide the severity of each item. This represents how important it is for the vendor to implement the particular control, e.g. having firewall installed may have a “Very high” severity whereas having a backup electric generator may have “Low” severity. Since not having a firewall will most certainly compromise the vendor’s network and data whereas not having a backup electric generator will only mean few hours of lost time. In short the severity level of an item indicates its relative importance.
- Decide which numerical value should be assigned to each of the severity levels. We are using the following values:
    - Very High:4,
    - High:3,
    - Medium:2,
    - Low:1.
- If the response to the item is “Yes”, give the “Yes” Details. This could take up any of the given three values: “Planned/just started”, “Partially completed” and “Fully implemented”.
- The final risk score for an item is calculated as given below:
  If the Response is “No” then the risk score is determined by the Severity level as given below:
        - If Severity is “Very High” then the risk is 4.
        - If Severity is “High” then the risk is 3
        - If Severity is “Medium” then the risk is 2
        - If Severity is “Low” then the risk is 1.

  If the Response is “Yes” then the risk score is determined by both the severity level and the “Yes Details” as given below:

  If Severity is “Very High” then the risk is 4 * (“Yes Details” weight).
  If Severity is “High” then the risk is 3 * (“Yes Details” weight).
  If Severity is “Medium” then the risk is 2 * (“Yes Details” weight).
  If Severity is “Low” then the risk is 1 * (“Yes Details” weight).

  Where “Yes Details” weights are given below

"Planned/just started": weight 0.5
"Partially completed": weight 0.25
"Fully implemented": weight 0.

Attached with this document is an EXCEL sheet that incorporates all the above calculations and automatically calculates the risk score as you fill in the values in the checklist. Sample calculations for the "Organization" section are given below (Note that the "Risk Upper limit" is the maximum risk posed by an item, this is used to calculate the %age risk abated by the vendor):

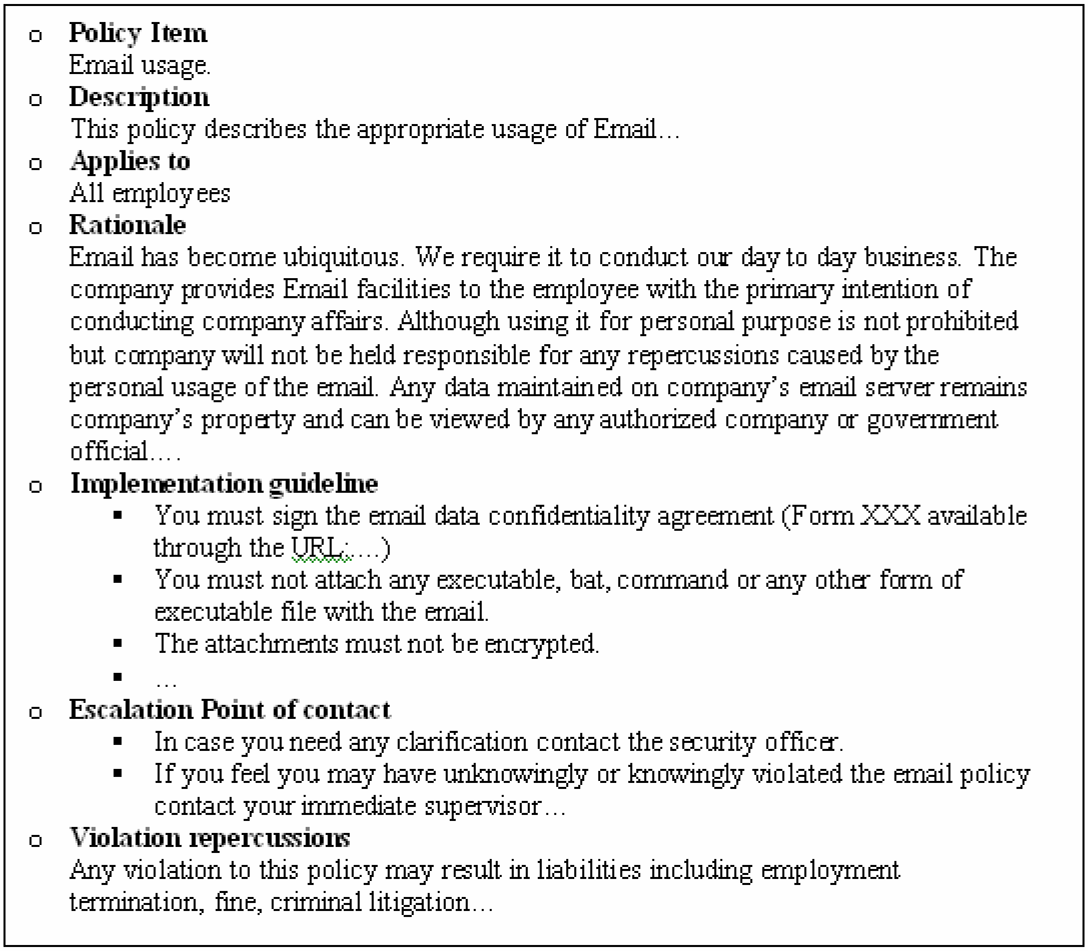
| **ORGANIZATION** | **Response** | **"Yes" Details** | **Severity** | **Risk Score** | |
|---|---|---|---|---|---|
| **SECURITY POLICY** | **YES.<br>NO.<br>N/A.** | **Planned / just started.<br>Partially completed.<br>Fully implemented.** | **High.<br>Medium.<br>Low.** | **Calculated** | **Risk Upper limit** |
| Have the Information Security Policies been issued to all employees, including third party personnel and contractors? | Yes | Planned / just started | Very High | 2 | 4 |
| Have all employees formally acknowledged adherence to the Information Security Policies? | Yes | Partially completed | Very High | 1 | 4 |
| Are employees required to annually re-acknowledge compliance with the Information Security Policies? | Yes | Fully implemented | Very High | 0 | 4 |
| How and when do you perform internal audits to measure compliance with the Information Security Policies? | Yes | Planned / just started | High | 1.5 | 3 |
| How frequently do you perform periodic reviews to update security policies and guidelines for relevancy and emerging topics? | Yes | Partially completed | High | 0.75 | 3 |
| Are controls in place to restrict your ability to transmit customer data to unauthorized personnel outside your company? | Yes | Fully implemented | High | 0 | 3 |
| Has an organizational policy on copyright compliance been implemented and communicated to all users? | Yes | Planned / just started | Medium | 1 | 2 |
| Do you have a policy that prohibits generic logon account and do you follow the policy? | Yes | Partially completed | Medium | 0.5 | 2 |
| Are all of the following subject to data confidentiality agreements?<br>* Permanent employees<br>* Contractors / temporary staff<br>* 3rd Party service providers | Yes | Fully implemented | Medium | 0 | 2 |

| | | | | | |
|---|---|---|---|---|---|
| Has your business issued an E-mail Usage Policy? | Yes | Planned / just started | Low | 0.5 | 1 |
| Do you take action against users who use e-mail in contradiction to the E-mail Usage Policy? | Yes | Partially completed | Low | 0.25 | 1 |
| Has your business issued an Internet Policy? (e.g. only access the Internet for legitimate work-related purposes, no downloading of games, etc.) | Yes | Fully implemented | Low | 0 | 1 |
| Are all users required to sign an internet usage and responsibility agreement that acknowledges compliance with the stated Internet Policy? | No | | Very High | 4 | 4 |
| Are there comprehensive documentation standards for IT development and operational controls? | No | | High | 3 | 3 |
| Is there a clear desk policy? | No | | Medium | 2 | 2 |
| **SECURITY OFFICER & ORGANIZATION** | | | | | 0 |
| Do you have a full-time Information Security Officer? | No | | Low | 1 | 1 |
| Have roles and responsibilities for protecting assets and implementing security measures been explicitly defined and communicated to all the department/groups? | N/A | | Very High | | 0 |
| Has a formal risk analysis process been implemented to assist management in identifying security threats? | Yes | Fully implemented | Low | 0 | 1 |
| **TOTAL** | | | | **17.5** | **41** |

%age risk abated = $1-\sum_{i=1}^{n}(RiskScore)_i \Big/ \sum_{i=1}^{n}(RiskUpperLimit)_i$ = 0.57

# Appendix C: Sample Security Policy Item

The security policy will have several of such items divided amongst relevant sections. Note that the template is only given for illustration purposes, a company will usually have much more 'legally correct' format prepared in consultation with consultants and lawyers.



- **Policy Item**
  Email usage.
- **Description**
  This policy describes the appropriate usage of Email…
- **Applies to**
  All employees
- **Rationale**
  Email has become ubiquitous. We require it to conduct our day to day business. The company provides Email facilities to the employee with the primary intention of conducting company affairs. Although using it for personal purpose is not prohibited but company will not be held responsible for any repercussions caused by the personal usage of the email. Any data maintained on company's email server remains company's property and can be viewed by any authorized company or government official….
- **Implementation guideline**
  - You must sign the email data confidentiality agreement (Form XXX available through the URL:…)
  - You must not attach any executable, bat, command or any other form of executable file with the email.
  - The attachments must not be encrypted.
  - …
- **Escalation Point of contact**
  - In case you need any clarification contact the security officer.
  - If you feel you may have unknowingly or knowingly violated the email policy contact your immediate supervisor…
- **Violation repercussions**
  Any violation to this policy may result in liabilities including employment termination, fine, criminal litigation…

# References

[1] Details of COBIT can be found at ISACA's official website. http://www.isaca.org.

[2] A free version of COBIT 4.0 framework is available at: http://www.isaca.org/Template.cfm?Section=COBIT6&Template=/MembersOnly.cfm&ContentID=23325

[3] Details of ITIL can be found at ITIL's official website: http://www.itil.co.uk.

[4] ITIL Self Assessment URL is given below: http://www.itsmf.com/upload/selfassessment/service_support_assessment.xls

[5] http://www.protiviti.com/

[6] Protiviti's Technology Risk Assessment Framework. http://www.protiviti.com/portal/site/pro-gb/?epi_menuItemID=ac8c16af42dde5489fbfbf10f5ffbfa0&epi_menuID=49d986d63864e321668fc2b2f5ffbfa0&epi_baseMenuID=e436df77853f6a40668fc2b2f5ffbfa0

[7] Jason Weile, (Manager, Systems and Process Assurance, PWC) "Risk Assessment and IT".

[8] Andrew Retrum, (Protiviti), presentation on "Vulnerability Management and External Penetration"

[9] Richard Jaehne, (Director, the Illinois Fire Service Institute) "Emergency Response and Unified Command Systems."

[10] Peter Siegel, (CIO, UIUC) "Enterprise Information Security Issues: The Case of Higher Education Institutions"