Project submitted in partial fulfillment for
the Degree of B. Tech in Information
Technology
under Maulana Abul Kalam Azad

# INFORMATION SECURITY AUDIT

**By**

Samreen Haider (11700214061)

**Under the Supervision of:**

Ms. Shyonee Roy, Manager-One Cyber, PwC

DEPARTMENT OF INFORMATION TECHNOLOGY,
RCC INSTITUTE OF INFORMATION TECHNOLOGY,
CANAL SOUTH ROAD, BELIAGHATA, KOLKATA –
700015,
May 2018

# DECLARATION

I hereby declare that the work entitled **“ Information Security Audit “** submitted to my college **RCC INSTITUTE OF INFORMATION TECHNOLOGY**, is a record of an original work done by me under the guidance of **Ms. Shyonee Roy, Manager-One Cyber, PwC.** And this work is submitted in the partial fulfillment of the requirements for the award of the degree of Bachelor of Technology in Information Technology. This work has not been submitted to any other University or Institute for the award of any degree or diploma.

**-------------------------------**

**Samreen Haider**

# CERTIFICATE OF APPROVAL

The project report titled "Information Security Audit" prepared by Samreen Haider is hereby approved and certified as a creditable study in technological subjects performed in a way sufficient for its acceptance for partial fulfilment of the degree for which it is submitted.

It is to be understood that by this approval, the undersigned do not, necessarily endorse or approve any statement made, opinion expressed or conclusion drawn therein, but approve the project only for the purpose for which it is submitted.

**-------------------------------------**

**[Head of the Department]**

# ACKNOWLEDGEMENT

I express my deep sense of gratitude to my respected Manager Ms. Shyonee Roy for her valuable help and guidance, I am thankful to her for the encouragement she has given me in completing the project.

I am also thankful to the faculty and staff members of our department for their kind cooperation and help.

Lastly, I would like to thank my colleagues and my parents for their constant moral support and encouragement which helped me in the successful completion of my apprenticeship at PwC.

----------------------------
Samreen Haider

# ABSTRACT

The rapid and dramatic advances in information technology (IT) in recent years have without question generated tremendous benefits. At the same time, information technology has created significant, unprecedented risks to government and to entities operations. So, computer security has become much more important as all levels of government and entities utilize information systems security measures to avoid data tampering, fraud, disruptions in critical operations, and inappropriate disclosure of sensitive information. Obviously, uses of computer security become essential in minimizing the risk of malicious attacks from individuals and groups, considering that there are many current computer systems with only limited security precautions in place.

As we already know financial audits are the most common examinations that a business manager encountered and examine the financial records and how those records are used. They may even be familiar with physical security audits. However, they are unlikely to be acquainted with information security audits; that is an audit of how the confidentiality, availability and integrity of an organization's information are assured. Any way, if not, they should be, especially that an information security audit is one of the best ways to determine the security of an organization's information without incurring the cost and other associated damages of a security incident.

# Contents

# 1. INTRODUCTION

Security audits are part of the ongoing process of defining and maintaining effective security policies, which involves everyone who uses any computer resources throughout the organization. Given the dynamic nature of computer configurations and information storage, some managers may wonder if there is truly any way to check the security ledgers. Security audits provide such a tool, a fair and measurable way to examine how secure is an information environment. Because a policy is typically published, and because it represents executive decision, it may be just what is needed to convince that potential client, merger partner or investor is really exactly who he pretend to be. Increasingly companies are requesting proof of sufficient levels of security from the parties they link to do business with. They are concerned primarily with how security policy is actually used, that’s way the secure policy is a way to start. A security audit is essentially an assessment of how effectively the organization's security policy is being implemented. Of course, this assumes that the organization has a security policy in place which, unfortunately, is not always the case. Despite all of this it is possible to find organizations where a written security policy does not exist yet. The security audit should seek to measure security policy compliance and recommend solutions to deficiencies in compliance. The policy should also be subject to scrutiny.

## 1.1 The Auditing process

Auditors use a set of specific audit techniques and procedures such as observation, interviews, questionnaires, collecting and studying internal regulations and relevant analyses and statistical comparisons, etc. The evidences can be obtained by combining the techniques direct observations, interviews, questioning, examination, and sampling. At the beginning, the aim of the auditors is to conduct an entry briefing where they outline the scope of the audit and what they are going to accomplish. The auditors should be thorough and fair, applying consistent standards and procedures throughout the audit. During the auditing process, they will collect data about the physical security of computer assets and They may perform network vulnerability assessments, operating system and application security assessments, access controls assessment, and other evaluations. Throughout this process, the auditors should follow their checklists, but also keep eyes open for unexpected problems. They should look beyond any preconceived notions or expectations of what they should find and see what is actually there. After the audit is complete, the auditors will conduct an outgoing briefing, ensuring that management is aware of any problems that need immediate correction. Questions from management are answered in a general manner so as not to create a false impression of the audit's outcome. At this point of time it should be stressed that the auditors may not be in a position to provide definite answers. Any final answers will be provided following the final analysis of the audit process. The next step for auditors is to comb their checklist and analyze their discovery through vulnerability assessment tools. There should be an initial meeting to help focus the outcome of the audit results. During this meeting, the auditors can identify problem areas and their possible solutions. The audit report must be simple and direct, containing concrete findings with measurable ways to correct the discovered deficiencies. The audit report can follow a general format of executive summary, detailed findings and supporting data, such as scan reports as report appendices. Next, the auditors can provide detailed report based on audit checklists. The audit findings should be organized in a simple and logical manner in a one-page worksheets for each discovered problem. This worksheet outlines the problem, its implications, and how it can be corrected. The final step for the audit staff is to prepare the report as speedily as accuracy reacting to the problems discovered during the audit. Depending on company policy, auditors should be ready to guide the audit organization staff in correcting deficiencies and help them measure the success of these efforts.

In an external audit, a customer audits the vendor/supplier to verify integrity of transactions, internal controls, compliance or the entire relation. In other words, the business audits its supplier or customer or vice versa. The goal is to ensure the expected level of performance as mutually agreed upon in their contracts. In external audits we perform VRM and ITGC.

## 2. ISO Audit

An ISO Audit is basic terms means checking to ensure you are *actually* doing what you *say* you are doing. Audits can (and sometimes must) be conducted against any of the ISO standards, including ISO 9001, ISO 14001, OH&S 18001, AS9100, ISO 13485, TS 16969, ISO 27001.

There are 3 main types of ISO audit:

1. First Party Audit – also known as an internal audit. These audits are usually conducted internally by your own staff (that are trained to carry out internal audits), or they can be carried out by an external company on your behalf if you do not have the internal resources.
2. Second Party Audit – also known as a supplier audit. These audits are usually carried out by lead auditors with your organization, and are designed to ensure that the companies that supply products/services to you are doing what they say they are doing. Again, these audits can be carried out by an external company if you do not have the internal resources.
3. Third Party Audit – also know as a certification audit. These audits are always carried out by a Certification Body auditor. These audits are for the purpose of gaining certification to the relevant ISO standard by an approved body.

During an ISO audit we:

- verify that the management system is in compliance with the relevant ISO standard.
- check to ensure that the actions taken to meet the quality objectives of the organization are suitable.
- verify that any problems within the management system have been addressed.
- look for any improvements that can be made to the system.

# 3. VRM

A vendor risk review (risk assessment) helps you understand the risks that exist when using a vendor's product or service. Performing a risk review is especially critical when the vendor will be handling a core business function, will have access to customer data, or will be interacting with your customers. Assess the adequacy of administrative, technical and physical controls that support the security and protection of client data at offshore vendor locations.

**VRM review goals:**

Vendor risk reviews are not only critical when bringing on a new vendor but are also needed to ensure that the vendor is maintaining expected quality standards without causing any risks to the company, investors or your customers.

The goals of a risk review are to:

•Identify any risks the vendor will pose

•Evaluate if the vendor is able to eliminate those risks

•Monitor the risks that cannot be eliminated

•Assess the extent that any outstanding risks may bring to the company

•Determine if your company is willing to accept those risks.

VRM should be performed in the following way:

**Initial Risk Review**

Risk reviews should be introduced to vendors during the Request For Proposal (RFP) process. Depending on your current RFP process, you may be able to embed your risk review assessment into the RFP.

**Ongoing Risk Reviews**

The best time to perform the risk review is 180 days prior to the renewal notification notice. This normally gives ample time to identify any changes to the vendor's risk level and lets your company respond appropriately.

## 3.1 Vendor Risk Management (VRM) – Controls Review

We perform the cyber security risk assessment for Data / Delivery Center on behalf of client. We will use a risk-based approach in determining the sample size and in-scope systems selected for our controls review. Our assessment will cover the following security domains:

**Physical Security**, for vendor Data Centers via onsite inspection and interviews. Our assessment will include the following key controls:

●Physical access controls

●Physical environmental protection systems

●Security management

●Asset protection

●Personnel security

**Security Management**, which include the following key controls:

●Information security policy and procedures

●Risk assessment process

●Compliance to regulatory requirements

●Management reporting process

●Cyber security strategy

**Human Resources Security**, which includes the following key controls:

●Documented and agreed responsibilities.

●documented job descriptions, perform appropriate background checks and screenings of employees, provide sufficient training in job function and security awareness, and obtain employee agreements covering confidentiality, non-disclosure, and authorized usage.

**Asset Management**, which include the following key controls:

●Accountability and inventory -accurate inventory of assets and ownership of all assets.

●Classification -Mechanisms to classify assets based on business impact, Labeling -Mechanisms to label assets that don't readily identify the owner and nature of information.

●Handling -Handling standards, including introduction, transfer, removal, and disposal of all assets are based on asset classification.

**Communication and Connectivity –Network Management**, which include the following key controls:

●Robust controls over communication network to safeguard data

●Access to network devices through

●Logging and monitoring remote access

●Encryption Mechanisms

**Identity and Access Management**, which includes the following key controls:

●Identity management –access entitlement

●User access administration process

●Authentication and authorization controls

●Access Control management

●Privileged account management

**Media Management**, which include the following key control:

●Media Removal ad Usage

●File Transfers and Media Handling

●Instant Messaging and Email

**Security Awareness and Training**, which include the following key control:

●Security training

**Data Integrity and Encryption**, which include the following key control:

●Data transmission and transaction controls

●Data encryption while in transit/ rest

●Key Management Procedures

# 4. Information Technology General Controls (ITGC)

"To provide an organization **high level of assurance** that the controls are operating **effectively** by

**ensuring security**, **confidentiality**, **availability** and **integrity** of **corporate data**"

## 4.1 ITGC Controls

**IT general controls** (ITGC) are controls that apply to all systems components, processes, and data for a given organization on information technology (IT) environment. The objectives of ITGCs are to ensure the proper development and implementation of applications, as well as the integrity of programs, data files, and computer operations.

The most common ITGCs:

- Logical access controls over infrastructure, applications, and data.
- System development life cycle controls.
- Program change management controls.
- Data center physical security controls.
- System and data backup and recovery controls.
- Computer operation controls.
- BCP/DR controls.

# 5.Conclusion

By and large the two concepts of application security and segregation of duties are both in many ways connected and they both have the same goal, to protect the integrity of the companies' data and to prevent fraud. For application security it has to do with preventing unauthorized access to hardware and software through having proper security measures both physical and electronic in place. With segregation of duties it is primarily a physical review of individuals' access to the systems and processing and ensuring that there are no overlaps that could lead to fraud. The following should be taken into consideration for better audit results.

- **Confidentiality** refers to limiting information access and disclosure to authorized users and preventing access by or disclosure to unauthorized users
- **Integrity** refers to the trustworthiness of information assets, that data have not been changed inappropriately, whether by accident or deliberately

- **Availability** is a requirement intended to assure that systems work promptly and service is not denied to authorized users