IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Vol.-7, Issue-5, May 2019 E-ISSN: 2347-2693

Refine Framework of Information Systems Audits in Indian Context

D M Chudasama[1], L. K. Sharma[2*], N. C. Sonlanki[3], Priyanka Sharma[4]

[1, 4]Raksha Shakti University, Ahmedabad
[2, 3]ICMR – National Institute of Occupational Health, Ahmedabad

[*]*Corresponding Author lksharmain@gmail.com, Tel.: +91-79-2268-8749*

DOI: https://doi.org/10.26438/ijcse/v7i5.331345 | Available online at: www.ijcseonline.org

Accepted: 18/May/2019, Published: 31/May/2019

***Abstract*—** The information system audit is an important review process for any organization. Information system audit is essential to identify any venerability in information technology infrastructure. In this work, information system audit process was studied in Indian context and proposed a refine framework for the information system audit process to overcome the deficit in present auditing process. The proposed framework covers important aspect of information system audit such as security environment, website security auditing, software code security, network security, physical security, organization and administration aspects etc. Further, a case study on information security audit in the small a small business enterprise was performed. The systematic review and the report of audit process are reported based on the case study. Finally, some sensitive managerial issues and findings of an awareness survey of information security were presented.

***Keywords*—** Information security management, information system security audit, data framework and applied model

I. INTRODUCTION

Information Organizations embrace reviews for some reasons. A review can support the venture guarantee compelling activities and validate its consistence with managerial and legitimate guidelines. It can affirm the board that the business is working great and is set up to address potential difficulties. Most significantly, it may guarantee partners about the money related, operational and moral prosperity of the association. Information systems (IS) reviews bolster each one of those results, with an extraordinary spotlight on the data and related frameworks where upon most organizations and open foundations depend for upper hand [1][2][3].

Accomplishment of the numerous advantages that can collect to a powerful review relies upon appropriate and careful arrangement of the review committee. The extension and the goal of the review must be comprehended and acknowledged by both the examiner and the territory being evaluated. When the reason for the review is obviously characterized, the review plan can be made, which will epitomize the concurred degree, goals and methodology expected to acquire proof that is important, dependable and adequate to make and bolster review determinations and sentiments [4][5][6].

A significant segment of the review plan is the review program, otherwise called work program. The review program is regularly used to archive the particular methods and steps that will be utilized to test and confirm control adequacy. The nature of the review program significantly affects the consistency and nature of the review results, so it is basic that IS auditors see how to create far-reaching review programs [7].

The paper is organized as follows. Next section the refine framework for the information system is proposed. In the section 3, a case study is reported. The recommendation is highlighted in the section 4. Finally, the work is concluded in the section 5.

II. REFINE FRAMEWORK FOR ISA

In this section, the refine framework for information system information is described.

A. Security Environment

1) Accountability Framework

If departments are to implement programs that are efficient and effective, they must be able to administer them within their particular mandates and according to their priorities, budgets, and organizational cultures and environments. The policy recognizes this by defining broad requirements to ensure a certain level of security within a department or government as a whole, while allowing the discretion needed to respond to financial needs and other conditions [7].

2) The Security Model

The Security Policy and Operational Standards describe a departmental security program model having the components such as Organizational structure, Administrative procedures

and Three (3) sub-systems: Physical Security, Information Technology Security, and Personnel Security.

Therefore, where responsibility for the various sub-systems is assigned to different organizational units, or where it is decentralized, the sub-systems should be structured to support cooperative planning, management and administration [7].

3) The Information Technology Security (ITS) Model

ITS is often described as the protection from threats using an integrated set of safeguards designed to ensure the confidentiality, integrity and availability of information electronically stored, processed or transmitted [7].

The Operational Standards describe an ITS model with the following components:

- Organizing and administering
- Personnel security
- Physical security
- Hardware security
- Software security
- Communications security
- Operations security

The effectiveness and efficiency of the ITS program depend upon the performance of each of these elements. Therefore, wherever responsibility for the assorted ITS parts is allotted to completely different structure units (for example, to an IT Security unit and a communication-electronic security (COMSEC) unit) or where it is decentralized, the elements should be structured to support cooperative planning, management and administration [7].

ITS is most effective when it is accepted as just one of the many important requirements that system developers and maintainers need to consider. ITS should not be an "add-on". It should be viewed as an integral component of any given IT infrastructure. When properly managed, it provides system and data owners with a return on investment [7].

4) Risk Management Framework

Conducting a threat risk assessment is the fundamental principle in assessing the need for adequate security measures to protect sensitive information technology assets. The Security policy requires departments to assess threats and risks to that sensitive info and assets are exposed, choose risk-avoidance choices, implement cost-efficient safeguards, and develop contingency and business start plans. A department's IT system development life cycle methodology should include the appropriate steps for [7]:

- Coordination of security plans and implementation
- Application of security risk management techniques throughout the life cycle and
- Approval, selection and implementation of appropriate safeguards.

Conducting the Audit: Audit Objectives, Criteria and Detailed Criteria/Audit Procedures Auditors may wish to add, modify or delete the specific objectives, criteria and detailed criteria in order to tailor the audit process to their organization [7].

Organizing and Administering IS: Ensure that an IS management structure is in place and meets the needs of the department. Ensure that IS safeguards are implemented, maintained, monitored and adjusted, within a risk management environment. Ensure that the information technology (IT) resources are appropriately managed. Ensure that IS equipment is appropriately managed, repaired, maintained and disposed. Ensure that cryptographic material is appropriately managed, repaired, maintained and disposed. Ensure that departmental IS undergoes regular monitoring and review [7].

Personnel Security: Ensure that personnel having access to IT systems/networks/ applications that process, transmit or store sensitive information are appropriately screened before being given access and are aware of their security-related responsibilities [7].

Physical Security: Ensure that IT is developed and maintained with consideration given to its physical and environmental security requirements [7].

Hardware Security: Ensure that IT is developed and maintained with consideration given to its hardware security requirements.

Software Security: Ensure that IT is developed and maintained with consideration given to its software security requirements.

Communications Security: Ensure that IT is developed and maintained with consideration given to its general communications security requirements. Ensure that networks and network applications are developed and maintained with consideration given to their security requirements. Ensure that IT is developed and maintained with consideration given to electronic authorization and authentication (EAA) security requirements. Ensure that IT is developed and maintained with consideration given to emanations security requirements.

Operations Security: Ensure that ITS operations are in place and meet the needs of the department [7].

B. Website Security Auditing

1) Update your scripts and applications

It provides audit website and gets the website to develop the framework and all your script and applications word press and plugins are up-to-date and current. Audits out-of-date contact us page, a vendor's system module may be explored. Also, find out vulnerabilities in the client side category page.

It can be performed by using the website https://builtwith.com/ and tool wire shark [8].

2) Check your domain and IP are clean

Audit to see if domain and IP are clean and not blacklisted. MxToolbox is a good tool for quick checks. As long as information processing blacklists usually aren't ruled by one supply, it will be required to contact a few places in order to have the blacklist removed [8].

3) Use strong passwords

Audit is to see across if the whole organization is using strong passwords or not. For individual user account, other users' accounts, hosting dashboard and FTP access — all of them are required to be secure. During the audit, it finds out if people used passwords like a pet name, Birth date and spouse names etc. It is suggested to make the strong and difficult password [8].

4) Deleted user accounts

During the audit process, there is verification of deleted user account and the login credentials are not to be shared. It is best practice to produce new logins for new users [8].

5) Add an SSL

The checking of SSL is in place or not is required during the audit. An SSL can give data between site visitor's browsers and website. An SSL has user logins and do in fact store sensitive user data. Generally, an SSL just used for e-commerce website, but now use for all websites [8].

6) Use SSH

The SSH protocol (also cited as Secure Shell) may be a methodology for secure remote login from one laptop to a different. It gives various choices for sturdy authentication, and it protects the communications security and integrity with sturdy cryptography. Ensure that secure various to the non-protected login protocols (such as Telnet, login) and insecure file transfer ways (such as FTP). The verification of SSH is required during the audit process when user uses FTP etc. [8].

7) Run a security scan

The security scan is also important during the audit. Security scan of the website can be performed for known malware, blacklisting status, website errors and out-of-date software [8].

8) Malware infection

Generally, common threat, malware, is an overarching term that covers viruses, worms, Trojan horses, ransomware, spyware and more. Malware can remove all of the information, steal customer information, infect your visitors — the probability is nearly endless [8]. The malware infection checking is also recommended during the information system audit process.

9) Distributed Denial of Service (DDoS)

A DDoS attack will bring down the website by a huge flood with an automated traffic. In addition, every minute web site is down, it can cause losing consumer and sales [8].

10) Brute force

This is where a connection is established to an application cycle passing each doable positive identification combination until it finds one that works. Here, hackers can access the system, steal sensitive data, and do pretty much whatever they want [8].

11) Injection

A hacker sends malicious data as part of a command or query that tricks the site into doing something it could not, such as giving the hacker your entire customer database [8].

12) 12) Cross-site scripting

Generally, abbreviated as XSS, cross-site scripting sends user-supplied data to a web browser without validating it first. Hackers use these flaws to hijack users' fault from the positioning or damage it, costing the site owner to lose business [8].

13) Zero-day

This is an associate degree attack to identify if new vulnerability is discovered, before a patch is created out there. While these are never to predict, you will invest in a Website Application Firewall (WAF) that will virtually patch site within a short time of a zero-day attack being disclosed [8].

C. Software Code and Security Audit

Software Audit - Amid reviews numerous approaches to "review" a product application. Extremely the most fundamental kind of programming review looks at how the product is practically arranged, incorporated or used in an association. This sort of audit procedure will be finished either by interior IT, an outside firm or a free arrangement supplier – regularly as an initial phase in a greater advancement venture. Nevertheless, the stakes are a lot higher in three different classes of programming review – with the main sort regularly imparting certainty and the other two, tension [9].

Software Quality Assurance Audit – Starting with the product review is a piece of the product quality affirmation (QA) process. Just of a QA review is regularly – to better the product. For the product investigation – just as code, system, yield report, information, test information and media - and associated the product improvement association might be approached to direct the product QA review. The objective is to evaluate the specialized quality, structure and capacity with the point of improving perspectives, for example, usability, dependability, security and execution [9].

Software Compliance Audit – This sort of reviews are constantly led by a body outside of the organization, for

example, an industry or government controller. In a consistence review, an association is required to permit the evaluator survey their product applications for consistence with set particulars, measures, codes, controls and commanded methods. When they finished reviewing it is persistently recertify the product is agreeable, ordinarily on a yearly premise [9].

Software Licensing Audit – Auditor Checks Software Asset Management or Risk Management practices to condition where the product is conveyed and how it is utilized. A permit review might be required for greater assurance or discover cost investment funds. The review may check execute programming copyright securities. It will be requested by the courts as a major aspect of a lawful question. It is normally required by hazard chiefs who request to see the association's dimension of showcase from proceeding with utilization of the product [9].

Software Audit Team – However, a group to finish a product review and it requires the dynamic interest of the association. The inward Sponsor or Initiator sets up the requirement for the product review, the best possible members, their motivation and degree, assessment criteria and detailing components. The Lead Auditor is frequently an out of entryways analyst free from inclination and impact who will fabricate target assessments. This individual leads the independent evaluating group that truly directs the product survey in accordance with review goals. At last, the individual in charge of regulatory errands, for example, archiving activity things, choices, proposals and reports is known as the Recorder. At the point when the product review is finished, the inspected association executes remedial activities and proposals [9].

Software Audit Tools – Selecting the correct device for the activity cannot be downplayed. A large number of them programming review apparatuses will create diverse perspectives on an association's application and design. Acclimate that the review group incorporates a specialist in utilizing the device of decision, and that it will return adequate information to decide suitable activities. For instance, programming's consistence with application security can be reviewed utilizing an assortment of static investigation and dynamic examination instruments that break down an application and score its conformance with security benchmarks, rules and best practices. In conclusion, the product-reviewing instrument should report its discoveries as a feature of a benchmarking procedure for future reviews by the review group [9].

Get ready for a product Audit – odds are high that most IT associations are liable for some type of programming review. The way to enduring the procedure is associated. For enterprises that are ill equipped, any product review will turn into an excruciating, expanded exercise requiring numerable worker hours. Planning for potential reviews ahead of time will maintain a strategic distance from amazement costs that could affect gains. As precedents: yearly programming consistence reviews are a typical event in exceedingly directed ventures [9].

D. Network Security Audit

A system appraisal survey of organization's IT foundation to evaluate the profitability and association of its execution, the executives and procedures. Utilizing this information, a pro will create an inside and out report back to help you see the power of your framework and grant you to shape extra well-perused business determinations and pick the best answers for your organization [10][11].

They may find network inefficiencies and errors - System reviews centre on more than security issues. They conjointly investigate for strength blunders, for example, bottlenecks. At the point when arrange issues like these wet blankets up on you, they can regularly convey your business to a halt - and when they're tackled, they can result in an inundation of multiplied messages. That is the reason for completing a prior system review, which might be a reasonable strategy [10][11].

They can discover hardware issues - Equipment, similar to servers and workstations, will keep going for quite a long time. They can flop, notwithstanding, in a moment. That can put your activities on hold, which may result in postponements in satisfying requests, gesture based communication new buyers and diverse significant errands. With a business arrange a review, equipment assessments uncover issues before they become issues [10][11].

They could uncover security vulnerabilities - Security is significant currently of shared information, stockpiling and information. For most firms, the primary felt rings a bell at the notice of systematic reviews. Amid these assessments, any discovered vulnerabilities are noted. Getting these dangers offers significant returns by anticipating the loss of touchy learning, just as the potential aftermath of the burglary of such data [10][11].

They offer recommendations and Solutions- Reviews for your organization's system more often than not encapsulate a posting of proposals, which detail any revealed issues, for example, arrange blunders, old equipment or security vulnerabilities. As a rule, your review supplier can convey the vital patches, just as substitution gear to restore your system to ideal execution and assurance [10][11].

They can help lessen its Workload- Crafted by IT gatherings, particularly for small and average sized organizations, can be considerable. For IT representatives, it's a test to review your system on a set timetable. Employing an outsider to direct a system review guarantees your system is checked consistently, just as examined by a group that knows about system issues and cures[10][11].

Underused or abused assets: Many organizations include assets inside their framework that they keep on paying for however scarcely used. These projects squander region and may devour a prominent bit of organization reserves. When you find the careful assets that your organization under uses — just as the ones that your business may depend on too vigorously — you can reallocate as needs be[10][11].

- Congested transmission capacity: Have you seen your system fundamentally slacking in the previous couple of months, particularly when spilling recordings or opening vast projects? Not exclusively is engorged data measure irritating, yet it can likewise diminish organization's profitability and resulting income. System evaluations will alarm you to bottlenecks and locate the most ideal approach to cure the circumstance [10][11].
- Poor arranges setup: Sometimes a system stoppage can be brought about by poor system design. A review will reveal wasteful setups and help you confirm the best approach to run your system extra swimmingly. On the off chance that you propose to extend your system or develop your business right away, an appraisal can likewise enable you to design and guarantee that your framework is set up to deal with your future development [10][11].
- Security gaps: Numerous organizations today are running their systems utilizing obsolete security programming — a serious issue in the realm of information breaks. Security appraisals will discover out of date safety efforts still as various evident security vulnerabilities that may undermine the security of your insight and debilitate your framework's activity. With aggressors revealing new ways consistently to undermine arrange security, you might be astounded to discover new security gaps regardless of whether nothing includes changing inside your framework since your last review[10][11].
- Already-bargained security: Unfortunately, security can be undermined even in the most determined organizations, and you might not have even understood that your system has just been broken. A security review will find infections, malware or information breaks and help you choose the best game-plan for your business in case of a functioning risk [10][11].
- Lack of guideline or arrangement consistence: Today, a few organizations zone unit sure by government laws that layout what safety efforts got the chance to be taken to shield information. A review will help you check whether you suit these laws and, if not, what steps you'll have to take. Regardless of whether you're not bound by government laws, you may have organization arrangements concerning representative logins, passwords, messages and other delicate regions. A review will anyway confirm you and your staff territory unit yielding with these approaches [10][11].

E. Physical Security Audit

The physical security audit begins to pursue these four stages:

1. Look at the physical format of the office [12][13]

- Does the format make spots to stow away?
- Is there enough lighting to enlighten key regions?
- Is arranging, making spots to stow away or giving rooftop has gotten to?

2. Note the number and area of all passages [12][13]

- Do representatives and guests experience a solitary security checkpoint, or are there different passages?
- Are entryways, doors, lifts, and different focuses verified utilizing electronic access control innovation?
- Are the windows shut and bolted or generally verified?
- Are all passages enlightened?

3. Consider the utilization of security protects [12][13]

- Does the association as of now utilize watches?
- If this is true, square measure they used viably to directly access, fabricate adjusts, and react to security episodes?
- If not, would include security protects be a decent alternative for improving security?

4. Research the adequacy of the office's ebb and flow physical security innovation.

- What accreditations are required for accessing the office? Are workers utilizing the entrance control framework as expected?
- How is guest the executives taken care of? Amid a security occurrence, would the association have knowledge in which guests are right now on location or were amid a specific time?
- When workers quit or are terminated, the end result of their keys or access cards?
- If the association utilizes PIN codes for secure access, how regularly would they say they are changed?
- Are the offices and the structure's edges enough secured by observation cameras?
- Do outside cameras give usable film, both day and night?
- Do cameras verify passages, stairwells, and other key territories?
- Are cameras observed? To what extent does the client hold the recording?
- During a security episode, how are security faculty told of the unapproved movement? Is the present conventional/framework empowering a fast and successful reaction?
- If security holes exist, would it be more financially savvy to include cameras or different innovations, put resources into security protects, or a mix of the abovementioned? [12][13].
- Do you by and large lead a full review with each new or returning client? What parts does one request once leading a security review? [12][13].

F. Physical Security Assessment

A thorough physical audit and investigation of all security frameworks, controls, and their parameters in a specific open/private property, resource or an association are called physical security appraisal. By and large, it's the joint strategy for directing escalated review and investigating the review results addressing the entire physical security instrument of a particular office [12][13].

Physical Security Assessment Scope: It is a well-characterized process regularly received for the consistence of prerequisites from numerous administrative specialists and standard associations. A wide range of physical security frameworks put in for a chose establishment or work environment security square measure analysed profoundly though the leading physical security appraisal [12][13].
Significance of Physical Security Audit : There are numerous sorts of normal just as human started dangers to the assets, resources, touchy data and business mysteries that can result in either incomplete or complete obliteration of an individual or an association. Those dangers strike either through IT organize or through physical interruption [12][13].

Interruption into IT assets is way simpler, if a programmer can physically barge in into your offices. In this way, the physical security frameworks should be 100% dynamic, viable and ready all the time that can be accomplished by executing incessant physical security reviews. Security reviews will help you understand defects and inadequacies inside the security frameworks all together that you'll have the capacity to just determine them to them solid and tough. A strong security framework is essential to protect your advantages and business associated key data [12][13].

Serious Problems Physical Security Audits Can Uncover: Physical security reviews will reveal different issues identified with the association or work environment security. A hearty security framework may incorporate various security controls, for example, human gatekeepers, physical locks, keying locks, wall, CCTV framework, lighting, alert frameworks, merchandise development controls and numerous others. Furthermore, physical security review discovers the wellbeing holes related to partner existing security arrangement of the association square measure revealed with the help of visual audit and operational exercises. The primary issues revealed by the physical security review include [12][13]:

- Lack of legitimate follow up for the security approach by higher administration to execute it in evident spirits [12][13].
- Very poor dimension of inspiration, supervision and observing over the human security protects procured from the outsider temporary workers, which lead to inappropriate adherence to security arrangement methodology [12][13].
- Low dimension of insurance and care by representatives about the significant resources of the organization, for example, PCs, furniture, office gear, workstations and others [12][13].
- Both the representatives and the security staff are not very much aware/prepared about the security arrangement and methods while getting to resources, working with resources and leaving the organization [12][13].
- Proper wearing the organization recognizable proof identifications is another issue found in physical security review. Numerous outsider contractual workers and representatives don't wear identifications constantly; or the photos of identification holder on those identifications are unrecognizable [12][13].
  Poor command over the guests of the organization or its representatives is another serious issue found in security reviews. Either numerous labourers escort their visitors with them or they do not construct the correct passages inside the explorer registers [12][13].
- Security screening of the workers of an outsider temporary worker is another exceptionally basic issue found in the physical security review. Numerous representatives working as contractual workers are not completely screened in typical circumstances [12][13].
- The absence of secure taking care of and development of reports inside the organization and outside the organization premises is another basic issue for the most part found in security reviews [6][7].
- Skilfully observing of electronic security framework is another issue because of untalented staff that work them [12][13].
- The customary testing, upkeep and observing of the security hardware at all focuses are not led according to characterized strategy [12][13].
- Inadequate lighting inside and outside the structure, patio or dividers is another significant issue usually featured by the security reviews [12][13].
- Intrusion recognition frameworks, fire alert frameworks, CCTV observe frameworks and others are not appropriately tried according to strategy to keep them 100% employable [12][13].

Key Points to consider in Physical Security Audit posting

There is a unit of few noteworthy classes that should be contemplated inside the physical security review posting. Every class ought to be additionally extended for its sub focuses on the types of the polls. A portion of those significant classes in the workplace security check list is given beneath [12][13].

- Management strategy
- Physical Security strategy
- Risk evaluation
- Access control
- Staff security
- Data/data security
- Emergency correspondence
- Rapid Response

- Technology audit

G. Organization and administration

1) Characterize the extent of a review

The primary thing you have to do is to set up the extent of your review. Regardless of whether you check the general condition of security in your association or complete a specific system security review, outsider security review, or some other, you have to realize what you should take a gander at and what you should skip [14]. So as to do this, you have to draw a security border – a limit around the entirety of your significant resources. This limit should be as little as feasible and exemplify every profitable in addition to that you simply have which needs security. You should be constrained to review everything inside this limit and wouldn't bit something outside it [14]

The best gratitude to layout security border is to frame a stock of every profitable resource that your organization has. This can be genuinely troublesome, because of partnerships as a rule discard things like carefully inner documentation, specifying, for instance, different corporate strategies and techniques, since it seems to have an incentive for the potential culprit. Notwithstanding, such data is significant for the organization itself, in light of the fact that on the off chance that those archives are ever lost or devastated (for instance, on account of equipment disappointment or worker botch), it will take some time and cash to reproduce them.

2) Characterize the dangers your information faces

When you diagram your security border, you have to make a rundown of dangers your information faces. The hardest part is to strike a correct harmony between how remote a risk is and how much effect it would have on your primary concern in the event that it ever occurs. For instance, if a cataclysmic event, for example, a sea tempest, is moderately uncommon, yet can be annihilated as far as accounts; it might in any case be incorporated into the rundown [14].

All and all, the most widely recognized dangers that you presumably ought to consider including, are the accompanying:

- Natural calamities and physical breaks – as referenced above, while this is something that happens infrequently, results of such a risk can be decimating, subsequently, you most likely need controls set up in the event of any unforeseen issue [14].
- Malware and hacking assaults – outside hacking assaults are one of the greatest dangers to information security out there and ought to dependably be considered [14].
- Ransomware – this kind of malware collected ubiquity in most recent years. In case you are working to help, instruct or funds, you most likely should keep an eye out for it [14].
- Denial of administration assaults – the ascent of IoT gadgets saw a sensational ascent in botnets. Forswearing of administration assaults is currently more far reaching and more hazardous than any time in recent memory. On the off chance that your business relies upon continuous system administration, you should investigate including those [14].
- Malicious insiders – this is a risk that few out of every odd organization considers, yet every organization faces. Both your very own staff and outsider sellers with access to your data will basically spill it or abuse it, and you wouldn't most likely distinguish it. In this manner, it's ideal to be arranged and incorporates it into your own risk list. Be that as it may, previously, we'd prescribe you peruse the correlation of risk perception arrangements [14]
- Inadvertent insiders – not all insider assaults are done out of vindictive purpose. The worker committing a legitimate error and releasing your information incidentally, is something that turned into very normal in our associated world. Unquestionably a danger to consider [14]
- Phishing and social building – as a general rule a programmer will attempt to gain admittance to your system by focusing on your workers with social designing methods, for all intents and purposes making them surrender their certifications intentionally. This is certainly something that you ought to be prepared for [14].

3) Compute the dangers

When you built up the rundown of potential dangers that your data could confront, you have to survey the danger of every one of those dangers terminating. Such hazard evaluation can help you place a tag on each risk and grade appropriately once it includes executing new security controls. So as to do this, you have to take a gander at the accompanying things [14]:

- Your past experience – regardless of whether you have experienced a particular risk or not may affect the likelihood of you experiencing it later on. On the off chance that your organization was an objective of hacking or forswearing of administration assault, there is a decent possibility it will happen once more [14].
- General Cyber security scene – take a gander at the present patterns in digital security. What dangers are winding up progressively famous and visit? What are new and rising dangers? What security arrangements are ending up progressively well known? [14]
- State of the business – take a gander at the experience of your immediate challenge, just as dangers your industry faces. For instance, in the event that you work in social insurance or training, you will all the more often face insider assaults, phishing assaults, and ransomware, while retail may confront disavowal of administration assaults and other malware all the more every now and again [14].

4) Gadget the important controls

When you set up the dangers identified with each risk, you're up to the last advance – making IT security review agenda of controls that you have to actualize. Inspect controls that are set up and conceiving an approach to improve them, or actualize forms that are absent [14].

The most well-known safety efforts that it could be considered which include:

a) Physical server security

In the event that you claim your own servers, you should tie down a physical access to them. Obviously, this is frequently not a take on the off chance that you simply deal with server territory from a data focus. In the meantime, any IoT gadgets being used in your organization ought to have all their default passwords changed, and physical access to them altogether verified so as to anticipate any hacking endeavors [14].

b) Equipment Security

Physical Attacks: The primary concern that separates equipment, assaults from programming assaults is the physicality of the assault finished with equipment devices. This increases current standards for equipment assaults in light of the fact that any assailant that needs to play out an assault on the equipment needs broad information of the equipment, dissimilar to the product assaults that should be possible by simply downloading a powerlessness instrument on the web to perform assaults [16]. For the most part, the equipment wants to monitor a mystery in this way the mystery is implanted in a very substantial [16].

Assault Vectors: The equipment that would be utilized to ensure the mystery would be created by somebody in a plant. The manufactory can either program the key onto the equipment or send the equipment to the corporate with memory for peruse access in one section and compose access in another part so the organization can program the equipment and devastate the compose segment to abstain from revising. This methodology can't be utilized for all equipment. Look at the workers and their methods and finish up whether the research center is trusted or not [16].

Inventory network: After the equipment has been made, it will be delivered to stores that will offer it or it is transported to the purchasers from the store. Amid delivery it could be blocked by the aggressors and messed with, at that point re-bundled without the learning of the store or the customers. Additionally, a few assaults can be performed on purpose of offer terminals when some insider (representatives) approaches the terminals and messed with it in the distribution center [16].

Mishaps: there is a great deal of memory based gadgets (for example USB Keys, Digital picture outlines) which may contain malware in them unintentionally, which could influence the arrangement of the client. The organization that made this equipment may not know about the malware on the gadget [16].

c) The Circuit assaults

- Discovery Testing: To play out this assault, the aggressor sends a contribution to the circuit and gets a yield. In view of the info and yield conduct, the assailant will choose what sort of calculation to utilize [16].
- Physical Probing: To play out this assault the assailant sticks a test onto the chip itself and peruses information off the chip. Inside a circuit, there is a wire that interface parts to one another called the transport and the transport is the place the data would be perused as the information is moving around in the transport. The information can even be perused off the memory area in the circuit. The test will have an accommodation accuracy and its Associate in nursing obtrusive approach. A great deal of circuits is driven by a clock, and if the aggressor can hinder the clock it gives a ton of time to the assailant to peruse the voltage of the circuit [16].
- Figuring out: To play out this aggressor, the assailant must obtain the keen card and physically uncover the circuit. The savvy card is produced with various layers and each layer is evacuated until the physical circuit is uncovered [16].
- Issue Generation: Some innovations fizzle [16].
- Side Channel Analysis: To play out this assault, the assailants utilize the equipment typically; however, makes touchy proportion of specific things and depending on the estimations done, the aggressor can gather insider facts [16].

d) Counter Measures

- Muddle information (Scramble, encode) on transports [16].
- Muddle the ASICS design, 3D stacking [16].
- Metal work over the circuit (if the circuit is examined, it causes a short and the memory resets) [16].
- Side Channel: physical shields, non-concurrent circuits. Additionally, a diminishing in the signs from the circuits of the equipment like the commotion or include fake clamor or low the circuit's capacity [16].

III. CASE STUDY – A SMALL BUSINESS ENTERPRISE AUDITS

Small organizations ordinarily have some trademark security issues, and they generally have little spending plans accessible for security changes. That does not mean, in any case, that private companies can't or ought not to matter similar standards of hazard investigation and security utilized by vast partnerships, scaled to their necessities and the assets accessible [9]. In this section, the information security audit performed in small business enterprises is shown. Table 1 is showing the major IT infrastructure at the organization.

Audit of the Mac

Evaluating a Mac Pro is more troublesome for most heads than examining a PC, because of a similar shortage of both robotized apparatuses and best practices archives, agendas, and other such instruments. The agenda with Daniel Deal's

astounding examination in his "Macintosh OS X 10.10: Security Analysis and Recommendations was explored. The agenda was composed as manner so answers ought to be "Yes" [15]. The questioner is shown in Table 2.

Table 1. IT infrastructure available at organization

Computer Name/ Description	Computer/Device Role
"Big Mac": Mac Pro Desktop Computer. Running Mac OS X(10.2.1).	Owner's primary personal computer. Used for email and electronic order storage, as well as Business financial records.
"The PC": Gray-box PC. Running Microsoft Windows XP Professional.	Used for personal use and for editing the website. No customer data.
"Staging": Old Compaq Desktop Computer runs Mandrake Linux 8.5	Used as a staging server for the0Website. No customer data.
"MacBook": MacBook Laptop Computer runs Mac OS 9.2	• Inventory database • Credit card authorization • All sales functions when on the road
Printer: Hewlett- Packard LaserJet 4Mwith JetDirect card.	• Printing, both paper work and package labels
Router: D-Link router/firewall appliance	• Wired/Wireless Router (802.11G) • Firewall • DHCP Server

Table 2. Mac PC regarding questioner

Item General Items (not Mac Pro-specific)	Yes	No
Is the computer backed up regularly?		X
Is the admin group restricted in membership?	X	
Is an actual login required (disable auto-login) Are there individual, named usernames for all employees? Is display of all usernames restricted?	X X	X
Is password strength appropriate?	X	
Is a personal firewall configured?		X
Is an antivirus program installed and properly configured?	X	
Is the physical case locked and secured?		X
Is theft-prevention software installed (Mac Phone Home in this case)?		X
Is the computer connected through a surge protector or UPS?	X	
Is a locking screensaver configured?		X
Mac - specific items		
Is the OS installed on a UFS volume, rather than HFS+?		X
Is an Open Firmware Password created and set?		X
Is access to Net Info restricted?		X
Is the root account still disabled?	X	
Is the system configured for at least weekly Software Updates?	X	

Audit of the PC

The PC is utilized in the Business just to run a solitary bit of programming: the Indian Postal Service's Shipping Assistant. This product enables the Business to print shipping marks for requests that as of now have the postal scanner tag on them, and to empower bundle following for Priority Mail bundles at no extra expense. The loss of Availability of this machine would be terrible, yet it would not be an emergency [15].

Table 3. PC related questioner

Item General Items(not Windows-specific)	Yes	No
Is the computer backed up regularly?		X
Is the admin group restricted in membership?	X	
Is an actual login required (disable auto-login)	X	
Are there individual, named usernames for all employees? Is display of all usernames restricted?	 X	X
Is password strength appropriate? Is a personal firewall configured?	X	 X
Is an antivirus program installed and properly configured? Is the physical case locked and secured?	X	 X
Is theft-prevention software installed (PC Phone Home in this case)?		X
Is the computer connected through a surge protector or UPS?	X	
Is a locking screensaver configured?	X	
Windows Items		
Is the Guest account disabled?		X
Is the Administrator account renamed?		X
Is there a login warning message?		X
Are all drives NTFS? Is the system currently patched to appropriate levels?	X X	
Is the system set for Automatic Updates and to ask the user if he/she wishes to install updates?	X	
Is a BIOS password set?		X

Audit of the MacBook

Applications which, rather than running locally in Mac OS X, keep running in the Classic similarity condition don't approach the inside modem. One such model is Mac Authorize, an application for handling Visa exchanges. Macintosh Authorize requires an accessible modem for reaching the money related systems, and keeping in mind that it generally works fine in Classic, the failure to utilize the interior modem represents an issue [15].

Table 4. MacBook regarding questioner

Item General Items (not Mac-specific)	Yes	No
Is the computer backed up regularly?		X
Is the admin group restricted in membership?	X	
Is an actual login required (disable auto-login)		X
Are there individual, named usernames for all employees? Is display of all usernames restricted?	X	X
Is password strength appropriate? Is a personal firewall configured?	X	 X
Is an antivirus program installed and properly configured?	X	
Is the physical case locked? Is the laptop physically secured?	N/A	N/A X
Is theft-prevention software installed (Mac Phone Home in this case)?		X
Is the computer connected through a surge protector or UPS?	X	
Is a locking screensaver configured?		X
Mac-specific items Is an Open Firmware Password created and set? Is the system configured for at least weekly Software Updates?	 X	 X

Audit of the Router Appliance

The router apparatus is a D-Link 624 Air in addition to Extreme link modem router. It has four standard turned pair Ethernet ports, and fills in as a 802.11b/g remote router, too. It is moreover a firewall machine and a DHCP/NAT server, too. It is arranged to run NAT, with all LAN customers getting private range IP addresses. On the WAN side, it acquires a dynamic IP address from the link modem organize supplier [9].In spite of the fact that it's anything but an ideal fit, I utilized the framework for "Getting the Most Security out of the Linksys Cable/DSL Router made by Earl Char scratch as my beginning stage. The reason I utilized this record is that the D-Link and the Linksys switches are comparable to in structure and capacity. I basically needed to include reviewing the remote segments that the Linksys needs [9]. Table 5 shows the parameter of router appliance.

Table 5. Router Appliance related parameter

Item	Yes	No
Has the administrator password been changed?	X	
Are ICMP ping requests blocked?		X
Is Remote Management disabled?	X	
Is Remote Upgrade disabled?	X	
Is IP address filtering enabled and functioning?		X
Is IP service filtering enabled and functioning?		X
Is MAC address filtering enabled and working? Is Virtual Server disabled?	 X	X
Are unwanted ports shut down to keep them from serving as a	X	
Starting point of an attack? Is logging configured and working?	 X	
Is the appliance plugged into a surge protector?	X	
Is the firewall set to default Deny all connections from the Internet to the LAN?	X	
Is the router set to obtain a dynamic IP address from the ISP, rather than a static one (if available)? Has the wireless SSID been changed from “default”?	X 	 X
Has the wireless channel been changed from the default value? Is the 128-bit WEP (Wired Equivalent Privacy) protocol enabled?	X 	 X

The Threat was explored and it is reported on the Table 6.

IV. ORGANIZED RECOMMENDATION LIST PRESENTED TO BUSINESS OWNER

1. Back up all the Business' significant information. This is a piece of industry best practices for any information that the association thinks about, as it enormously decreases the effect to data accessibility from equipment disappointments, infections, wafers, and different incidental causes. This tends, nonetheless, to "get lost in an outright flood" in home and private companies, as this is a hazard that seems minor until it "chomps you" [15].
2. Chronicle old information. Figure out what old information ought to be chronicled, document it to CD- ROM or other media, check the chronicles, and put the media in a flame resistant sheltered or safe-store box. At that point expel the documented information from the PCs. This not just decreases the effect of privacy and accessibility hazards by a colossal edge, yet it likewise lessens the effect of respectability chances (the can go look into old information on the off chance that she needs it, and realize that it has not changed). A worry has as of late been raised with respect to the life span of DVD-ROM media, in any case, so the proprietor must know about this [15].
3. Solidify PC frameworks and the system as per best practices. I have reported the framework reviews and explicit proposals for every PC and the switch in table 2 through five [15].
4. Secure stock and paper records with a flame resistant lockbox or identical. The stock and paper records were powerless against both flame and break-ins, and they were simply staying there on the rack. While both of these dangers were low probability, the effect of at the same time losing the stock and earlier years' business records would be high. A sufficiently expansive flame resistant lockbox for the stock, be that as it may, was not practical, and the Business proprietor decided not to execute this proposal [15].
5. Physical barrier inside and out for the PCs. The PCs are in a stay with a bolted entryway, yet with windows. There are industry-standard links produced for verifying PCs and the instances of the majority of the Business' PCs previously had specialties to acknowledge them [15] .
6. Make a half-page structure for telephone requests and spot duplicates close to all Business telephones. This structure, imprinted on hued paper, should help avert telephone orders from being lost in the general commotion. A duplicate has been replicated underneath [15].
7. Value a halon-based flame control framework. This, as anyone might expect, swung out to way out of the Business' value extend, yet we needed to assess alternatives. These frameworks, normally found in expert evaluation server farms, can put fires out without the risk to PCs spoken to by water [15].

Table 6. The Threat report

Threat	Aspect (C-I-A)	Impact (H-M-L)	Likelihood (H-M-L)	Risk (H-M-L)	Response & Recommendation: Accept, Mitigate, or Transfer[66]
Mac hardware problem	I,A	H	L	H	Mitigate: • Back up data • Archive old customer data Transfer: Data recovery clause in business insurance
PC hardware problem	I,A	L	M	L	Mitigate: • Nocustomer data on PC • Backup system
Staging hardware problem or virus	I,A	L	M	L	Accept
Mac Pro virus	IA	H	L	H	Mitigate: • Harden the system • Keep antivirus software up to date • Back up data • Archive old customer data Transfer: Data recovery clause in business insurance
PC virus	I,A	L	L	L	Mitigate: • Harden the system • Keep antivirus software up to date • No customer data on PC
Computers stolen in a break-in	A,C	H	L	H	Mitigate: • Physical security measures already in place • Add cables to physically secure computers • Back up data to safe location • Archive old customer data & remove it from computers. • Install Mac Phone Home & PC Phone Home Transfer: Business insurance.
Cracker "0wn1ng" Big Mac	CIA	H	L	H	Mitigate: • Harden the system • Back up data • Archive old customer data & remove it from Big Mac
Cracker "0wn1ng" PC	CIA	M	M	M	Mitigate: • Harden the system • No customer data on PC

Electrical surge due to lightning or other cause	IA	H	L	H	Mitigate: • Back up data • Use UPS's Transfer: • Business insurance covers replacing dead computers • Data recovery clause in business insurance
MacBook lost or stolen while traveling.	CA	H	M	H	Mitigate: • Back up data • Archive old customer data & remove it from MacBook. • Install Mac Phone Home Transfer: Business insurance.
Fire in office	A	H	L	H	Mitigate: • Back up data to safe location • Smoke alarms & fire extinguishers • PriceaHalonfirecontrol system Transfer: Business insurance.
A cracker steals order information from the web server before it gets to the Business.	CIA	H	M	M	Mitigate: • File/directory security setup well on web server • Orders never emailed with credit card numbers Transfer: Liability clause in business insurance.
Cracker intercepts customer information over cord less phones	C	H	L	M	Transfer: Liability clause in business insurance.
Owner accidentally deletes old order files (human error)	IA	L	L	L	Mitigate: • Archive old customer data • Back up data
Cracker intercepts data over wireless network	C	H	L	M	Mitigate: Add WEP Transfer: Liability clause in business insurance.
Order information is stolen from the Big Mac or the MacBook by an employee and used for identity theft	CIA	H	L	M	Mitigate : • Few, well-screened employees • Employees normally working under direct supervision Transfer: Liability clause in Business insurance.

A customer list (names and addresses) is printed by an employee and given to a competitor	C	M	L	L	Mitigate: • Few, well-screened employees • Employees normally working under direct supervision Transfer: Liability clause in Business insurance.
Business is slandered by a competitor or former customer	I	M	L	L	Mitigate: Good communication With vendors and customers Otherwise, Accept.
Orders go out late and customers are angered, taking Business elsewhere.	IA	H	L	M	Mitigate: Owner works hard to set expectations properly and to get orders out on time. Otherwise, Accept.
A phone order is lost and never found, or found too late.	IA	H	M-H*	H	Mitigate: Create half-page form, place near all Business phones. Form is placed directly on Orders Clipboard when filled out.
An item advertised Becomes no longer available to Business.	IA	M	M*	M	Mitigate: Good communication with vendors and customers
Misc. fixtures & equipment destroyed or damaged in fire or stolen in break-in	IA	M	L	M	Mitigate: Physical security measures already in place Transfer: Business insurance.
Owner gets sick and is in hospital for a week	A	M	M*	M	Mitigate: • Owner taking care of herself in terms of health. • Hus0b6aEn4d learning technical Details. Transfer: Investigate disability insurance.
Owner or staff is given and passes on bad information about stock	I	L	L	M	Mitigate: Owner reads and studies widely in the field, and staff defer to her on customers' technical questions.
Paper records stolen in break-in	CA	H	L	H	Mitigate: • Physical security measures already in place • Lock all paper archives in a sturdy cabinet (preferably a fireproof safe).
Stock stolen in break- in	A	H	L	H	Mitigate: • Physical security measures already in place • Lock stock in locking file cabinets. Transfer: Business insurance.

Stock, paper records destroyed by fire in garage	A	H	L	H	Mitigate: • Smoke alarms & fire extinguishers • Price a Halon fire control system Transfer: Business insurance. Accept: • Increased vulnerability to credit card charge backs • Replacement stock will take a week or more to arrive.

Stock, paper records destroyed by flood in garage	A	H	L	H	Transfer: Business insurance. Accept: Increased vulnerability to credit card charge backs Replacement stock will take a week or more to arrive.
Website becomes unavailable due to hosting firm going out of business.	A	H	L	M	Mitigate: Complete copy of site on staging 0s6eErv4er exactly as it is in Production.
Website becomes unavailable temporarily due to a DOS or other "Internet forces of nature"	A	M	M	M	Mitigate: Keep Business's site as secure as possible. Accept that there are things beyond the Business's control.
Website is defaced by a cracker.	IA	M	L	M	Mitigate: Keep Business's site as secure as possible. Complete copy of site on Staging server exactly as it is in production.
All physical assets destroyed in an Earthquake	A	H	L	L	Transfer: Business insurance.
All physical assets destroyed in an hurricane	A	H	L	L	Transfer: Business insurance.
All physical assets destroyed in an Tornado	A	H	L	L	Transfer: Business insurance.

V. CONCLUSION

A refine framework for information system audit was presented and based on the proposed framework information system audit was performed in the small business enterprise. It can be concluded that the security policies should be discussed and explained by management or the IT department on occasion. The personnel department should also present new staff with these policies during orientation and it would dramatically increase the awareness and understanding of the importance of the policies. Users should be made aware that they must "never" give their passwords to anyone, especially someone they don't know and especially over the phone. Although it is difficult to completely secure 802.11b networks, a few measures can be taken to make it more difficult for would-be attackers. Further, users should be required to use passwords of sufficient length and complexity. The level of security must permit reasonable access, yet protect against threats. Security is a delicate balance among protection, availability and user acceptance. Finally, top management should spearhead the security auditing process, make it a regular ongoing event and follow through recommendations..

REFERENCES

[1] H Botha and J A Boon, "The information Audit: Principle and Guidelines", Libri 53, pp. 23-38, 2003.

[2] Manual of Information Technology Audit, Office of the Comptroller and Auditor General of India, Vol 1 & 2, 2014.

[3] Information security audit (IS audit) - A guideline for IS audits based on IT-Grundschutz - German Federal Office for Information Security 2008 – Version 1.0

[4] National Audit Office of Finland - Auditor General Manual - Finland Registry no. 23/01/2015

[5] Coordinated Audit of Information Technology Security (with Shared Services Canada), Govt of Canada. https://www.canada.ca/en/treasury-board-secretariat/corporate/reports/coordinated-audit-information-technology-security.html [Last access on 14/04/2019]

[6] D M Chudasama, L K Sharma, N C Solanki, Priyanka Sharma , " A Comparative Study of Information Systems Auditing in Indian Context" , IPASJ International Journal of Information Technology (IIJIT) , Volume 7, Issue 4, April 2019 , pp. 020-028.

[7] Coordination for Website security audit [Go daddy-Website Domain Hosting]] https://www.godaddy.com/garage/how-to-do-your-own-website-security-audit/[Last access on 21/04/2019

[8] SSH standard and detailed technical documentation [SSH.com] https://www.ssh.com/ssh/protocol/[Last access on 21/04/2019]

[9] Coordination For Performing software code & security audit [Vera code] https://www.veracode.com/security/software-audit[Last access on 21/04/2019

[10] Coordination for Network Security audit [swissns] https://www.swissns.ch/site/2016/09/5-steps-of-performing-a-network-security-audit/[Last access on 21/04/2019

[11] Coordination for Network Security audit [Consolidated Technology Inc.] https://consoltech.com/blog/business-network-security-audit-say-yes/[Last access on 21/04/2019

[12] Coordination for Physical Security audit [Imgram] https://imaginenext.ingrammicro.com/Trends/November-2017/The-4-Step-Physical-Security-Audit[Last access on 21/04/2019

[13] Coordination for Physical Security audit [kisi blog] [Last access on 22/04/2019] https://www.getkisi.com/blog/physical-security-assessment-problems-it-can-uncover

[14] Coordination for Organization and administration audit [Smart data collective][https://www.smartdatacollective.com/4-easy-steps-conduct-security-audit-company/Last access on 23/04/2019]

[15] Coordination for small business preparing case study audit [Sans Institute] https://www.sans.org/reading-room/whitepapers/casestudies/case-study-risk-audit-small-business-1243 [Last access on 23/04/2019]

[16] Coordination for small business preparing case study audit, Concordia University, https://users.encs.concordia.ca/~clark/courses/1501-6150/scribe/L09b.pdf [Last access on 23/04/2019]

