An Evidence Gathering Framework for auditing Policy Compliance

MSc Research Project
MSc in Cybersecurity

Nachiket Phadnis
Student ID: 19217242

School of Computing
National College of Ireland

Supervisor: Mr. Vikas Sahni

National College of Ireland

MSc Project Submission Sheet

School of Computing

Student Name: ….Nachiket Phadnis………………………………………………………………

Student ID: …19217242……………………………………………………………………………

Programme: …MSc Cybersecurity……………………………… **Year:** …2021…

Module: …MSc Internship……………………………………………………………….……

Supervisor: …..Mr. Vikas Sahni……………………………………………………………………

Submission Due Date: ……07/01/2022…………………………………………………………………………**.**

Project Title: An Evidence Gathering Framework for auditing Policy Compliance

Word Count: ………80015………………… **Page Count**……20…….……..

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.
ALL internet material must be referenced in the bibliography section. Students are required to use the Referencing Standard specified in the report template. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action.

Signature: ……Nachiket Phadnis………………………………………………………………………

Date: ……03/01/2022………………………………………………………………………………

PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST

Attach a completed copy of this sheet to each project (including multiple copies)	□
Attach a Moodle submission receipt of the online project submission, to each project (including multiple copies).	□
You must ensure that you retain a HARD COPY of the project, both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer.	□

Assignments that are submitted to the Programme Coordinator Office must be placed into the assignment box located outside the office.

Office Use Only	
Signature:	
Date:	
Penalty Applied (if applicable):	

An Evidence Gathering Framework for auditing Policy Compliance

Nachiket Phadnis
19217242

Abstract

In the ever-changing world of cyber threats and attack, establishing a solid security posture for an enterprise and adhering to various standards must be the main priority. The aim of this research project was to close the gap between adherence to security rules and the actual execution of security measures to ensure that these policies are followed. This is accomplished using a suggested EGF, which may be used in conjunction with the compliance audit process to gather evidence of an organization's security settings and controls and record it for review and evaluation.

By conducting an audit and implementing the framework design, the suggested framework was verified against several SMEs and its security posture. This aided in identifying the gaps in the security controls and settings, as well as gathering the information needed to submit them to the appropriate authorities for revisions and implementation. The framework aided in the improvement of the organization's security posture, making it more attentive and prepared to deal with cyber threats and attacks. It also assisted enterprises in closing the gap by adopting a Compliance first strategy via Security Policy Compliance.

1 Introduction

The adherence to numerous compliance laws and regulations, as well as the timely management of risks and the implementation of risk mitigation measures, are all critical components of any organization's reputation. Every organisation that wishes to be considered compliant must demonstrate this through an audit process, which is carried out by external auditors who are experts in the field. (Santos, 2010) What steps may be taken to ensure that a company is better prepared for an audit? In what way can it be certain that the settings and controls have been properly implemented? The best strategy is to be prepared for the audit with all of the documentation and information that the auditors will demand. A suitable framework for the process of evidence gathering is proposed in this research project, which can be used as a comprehensive guide towards the audit process. The guide and the core elements involved in the evidence gathering are investigated in this research project, and a suitable framework is proposed for evidence gathering.

A cyber security audit is an important step in discovering fundamental flaws in any organization’s IT infrastructure. These evaluations assist the company in determining what is on its network, what needs to be secured, and how to increase security if necessary. Auditors want proof that the organization and internal admin teams are doing the correct thing and becoming better. (Majumdar, 2015) Audits aren't meant to put any organization in a tough spot; they're meant to help improve the overall security posture of the organization. However, despite how important cyber security audits are, many businesses are unprepared for them. So, how would an organization be sure to be ready for a cyber security audit so that it goes well and quickly? This is where the Evidence Gathering Framework (hereafter called EGF) can help in gathering all the needed settings and controls and documenting them before the audit.

Researchers have studied multiple frameworks and tools, compare the online available tools (O. M. Al-Matari, 2018), its different features and ease of use but the study did not entail the basics of evidence gathering and how it can be beneficial for getting ready for a compliance audit. Privacy governance frameworks were conceptualized by Swartz et. Al. in their study (P. Swartz, 2019) which helped in building a conceptual unified framework by combining multiple privacy governance frameworks into one. These studies helped in deriving the frameworks for givernance and compliance, but did not provide a basics for evidence gathering. This was due to the limited research which was done in the domain of Evidence Gathering domain under compliance audit. Due to the fact that it was a sub-section of an audit, not a lot of attention was given. Hence, there remains a huge gap in the research, implementation and evaluation of evidence gathering domain.

The risks and chances of being a non-compliant or vulnerable business is the most dangerous thing for an organization to be in these troubled times with the increase of cyber-attacks. (Nader Sohrabi Safa, 2016) As I have interacted with some clients, senior executives of some of the companies, I have seen quite a careless attitude towards the adaptation of policies and verification of the security controls. This little ignorance can ultimately cost a fortune to the company in the long run. This mindset of any organization towards the compliance audit and its application, posture and assistance provides a big gap which needs to be studied and researched on (B. R. Aditya, 2018). The cost of an organization being "Non-Compliant" is pretty huge, starting from hefty fines, lawsuits and ultimately the effect on its reputation and the customers' trust in it. For adopting the "Compliance First" approach, an organization needs to be ready to tackle the audit and come out with the correct posture. This can help organizations to adopt a better security practice and ultimately help in avoiding risky cyber attacks and data breaches. With the help of Evidence Gathering, this research aims to see if it can help to improve the security posture of an organization through a "Compliance First" approach.

This report provides the different sections through which the research was carried out in a sophisticated manner. Section 2 provides an outline over the related work which has been done in the related field of research. Section 3 includes the Methodology which was adopted in conducting this specific type of research and the different steps included in methodology to define the inferences of the study. Section 4 provides the proposed framework for evidence gathering which can be used as an added guide in the audit process. Section 5 and Section 6 covers the Implementation and Evaluation of the said framework against the exploratory methodological approach. Finally, the conclusions were discussed and any prospect of future work was provided in the final part of the report which is the Section 7.

2 Related Work

One of the most crucial parts of a mature risk management system is the collection of evidence to support your present activities. A compliant organization must be able to demonstrate compliance (Puzant Balozian, 2017), and the simplest way to do so is by collecting and preserving documentation of your actions, which can then be used to support your claims during an audit. If this task can be completed before an audit, it will make one's job much easier when dealing with an auditor later on.

2.1 Frameworks and Tools

A discussion of the many technologies available for information systems auditing, as well as the numerous security measures that must be in place, was presented by Al-Matari and Helal. (O. M. Al-Matari, 2018) It is clear that their study was mostly focused on the tools provided rather than on how the tools might be useful for audits; they have not done a thorough investigation into the structure of the tool and its fundamental functionality, nor have they looked into the roadmap that the product follows. Specifically, their work examines the many capabilities that the tools give for an IS audit for cybersecurity, and the results are published online.

In a similar way, Liu, Wang, and Jiao developed a flexible compliance audit policy method for information systems, which was published in the same journal. Due to the fact that it not only expresses audit rules based on periodic time limits, but it also provides fine-grained audit policies via a composite attribute expression, the model is extremely expressive. (Lianzhong Liu, 2010). They offered a security compliance model that was based on the definition and description of security policies that were supplied as a constraint, in addition to the time limitations that were provided. A security database, an operating system, or any application system can benefit from this method, which is easily adaptable to any situation. Policy creation, setup, and administration in a comprehensive security audit platform may all be accomplished through the usage of this paradigm, which is advantageous. The only element that has an impact is that this model requires some type of restriction in order to work properly and offer audit findings more effectively. This has the potential to add complexity, and the framework will be impacted. The model was reliant on the limitations in order to deliver the audit findings, but it does not describe the actual procedure that takes place behind the scenes.

Another system suggested and constructed by Liu, Wang, and Jiao was a security audit system for ensuring compliance in the realm of network security. (Jing Liu, 2012) Its article examined the system architecture and components of a log-based network security audit system for compliance, as well as the concept of compliance auditing in general. Once again, the problem was that the system relies on the system's inputs as well as network records in order to deliver outcomes. In the absence of a fundamental road plan that would allow them to comprehend the process there was no clear and simple framework which could have been easier to be implemented.

Cyber security audits are crucial in detecting and resolving underlying flaws in a company's information technology infrastructure. They are performed by qualified professionals. Following the completion of these evaluations, the business can evaluate what is currently on its network, what needs to be protected, and how to improve network security as a result of the results. If you're doing the right thing and improving your performance, your auditors will be looking for evidence of this. When it comes to the compliance auditing process, evidence collection is crucial and should not be disregarded. (Nadir, 2019)

2.2 Privacy and governance

According to the authors, privacy governance is also an essential component of the compliance audit process. As part of their research, Swartz, Veiga, and Martins constructed a conceptual privacy governance framework. (P. Swartz, 2019) One of the objectives of this research was to provide a conceptual framework for privacy governance. This is done by an evaluation of current privacy governance frameworks and the development of a unified framework that comprises a comprehensive set of privacy components that may assist management in controlling privacy throughout an enterprise. The drawback of this framework is that it is only a conceptual framework that may be used as a reference by any company rather than as a definitive guidance for any organization.

Another group of researchers, G. Drivas, A. Chatzopoulou, L. Maglaras, C. Lambrinoudakis, A. Cook, and H. Janicke, developed a cybersecurity maturity assessment methodology that focuses on conformance with the NIS Directive (G. Drivas, 2020). A framework that is compliant with the NIS Directive focuses on the NIS compliance guide and examines the systems in relation to the NIS guide in order to determine the maturity of the system. An updated Cybersecurity Maturity Assessment Framework (CMAF) was presented in this paper, which has been tailored to meet the goals of the NIS Directive. In addition to being used as a self-assessment tool by operators of essential services and digital service providers, the CMAF may also be used by National Competent Authorities to conduct cybersecurity audits. As part of their future work, they advocated that this paradigm be used for further examination and assessment of diverse systems in many fields.

2.3 Compliance assisted by Machine Learning

Security and compliance audits are time-consuming, expensive, and error-prone for cloud service providers who have a large number of domains to manage. In order to aid in the collection and evaluation of evidence necessary for compliance certification, the majority of existing methodologies make extensive use of formal logic and domain-specific languages. Thakore, Ranchal, Wei, and Ramasamy developed a hybrid strategy to enable such an approach, in which model-based algorithms were paired with machine learning to get the desired outcomes in compliance (U. Thakore, 2019). According to their methodology, model-based reasoning and machine learning was used in conjunction with audit history to learn about the evidence data. Completing the system and framework by including machine learning will inevitably make them more complicated. Their concept intends to eliminate the risks associated with cloud computing in terms of compliance and security.

In their research, Kebande and Ray offered a general Digital forensic based framework for Internet of Things (IoT) in the same way as Thakore, Ranchal, Wei, and Ramasamy proposed a hybrid approach towards cloud security compliance audits (Ray, 2016). DFIF-IoT is a general Digital Forensic Investigation Framework for the Internet of Things (IoT) that is capable of reliably supporting future IoT investigative capabilities, as described by the authors. Aspects of the proposed framework that have been identified as beneficial include: It complies with ISO/IEC 27043: 2015, which is an international standard for information technology, security methods, incident investigation ideas, and incident investigation processes. It should be noted, however, that this framework can only be utilized for Internet of Things devices and systems in an Internet of Things context, and hence cannot be used for compliance audits of information technology systems.

2.4 IT Audits in SMEs

To minimize the spread of hazards and risks within companies, methodologies and procedures for managing IT audits have been developed to address a major issue for big, medium, and small enterprises in terms of IT compliance audits. Using a functional prototype paradigm, Rodriguez, Perez, and Sanchez developed a method for collecting documentation proof of compliance testing for information technology systems (R. E. Rodriguez-Rodriguez, 2018). Their research provided systems auditors with a novel approach to evidence collecting in information technology audits. The testing process may be improved in this way, since the auditor can create a working prototype to govern the information gathered during compliance tests in IT audits. However, the biggest disadvantage is that because their prototype is based on the features of a CAAT tool, it will not be able to deliver the results that are predicted if used independently.

A 'compliance first' strategy encompasses a broad variety of key aspects that must be taken into account in order for an organization to remain compliant. However, if the company is unsure about where to begin, a business tool audit is a good place to start. The 'Compliance first' strategy may assist the organization in developing a compliance-oriented culture inside the organization, so preventing any organization from becoming entangled in the quagmire of noncompliance. (Bulgurcu, 2010)

With the combined references and the approaches, this research project aims to build an EGF which can be helpful and beneficial as an extensive guide for auditors as well as clients for gathering the needed evidence of the system controls before the compliance audit. EGF design will help in guiding the clients as well as the auditors through a definite roadmap to check the policies, controls, compliance and the proofs for the controls in place to chalk out and evaluate the compliance.

3 Research Methodology

Regulation Compliance Audits assist a company in maintaining the greatest possible security posture and in avoiding risks, whether they are from within or outside the business, to its information and infrastructure. In this research project, the primary goal is to propose a Framework Design that can be advantageous for Evidence Gathering and Control Checks, and that can ultimately lead to a "Compliance First" approach to auditing and security in the future.

3.1 Compliance Frameworks and Security Controls

A compliance framework is an organised set of rules that specifies an organization's methods for maintaining compliance with existing regulations, policies, controls, specifications, or legislation. A compliance framework can be defined as follows: Communication processes, risk controls, and governance practises can all be included in such a framework to ensure that the organization's infrastructure is in accordance with the law. Putting in place security measures in accordance with the security policies in place is critical; yet, determining whether or not these controls have been appropriately implemented is a difficulty that many businesses are now facing. According to IBM, human error is the root cause of 95% of cyber-attacks and data breaches. (S. Pahnila, 2007) To close this fundamental gap, the first job for each organization's operations manual should be the implementation of stringent security controls and the verification of those controls. Performing a control verification will ensure that the controls are compliant and easy to audit, and retaining proof of the verification will make it easier to examine any modifications to the controls. Aiming to address this issue, this research project proposes a framework design for the purpose of evidence collecting and verification checks, which will be implemented in the future.

Studying and analysing related frameworks in the realm of compliance auditing is necessary to attain this goal. The associated work assisted in identifying the gaps, developing a strategy, and developing a simplified yet sophisticated framework for the intended use of the framework. Multiple Internationally accepted frameworks like ISO 27001, NIST Framework, GDPR (in the field of Data Protection), PCI DSS were also studied and analysed to understand the basic functionality and flow of a framework design and its different components. Although, researchers in the past have taken a variety of approaches in order to produce various framework designs connected to compliance auditing, the resulting frameworks were complex and included a broad range of operational or implementation issues. More often, compliance goes hand in hand with Risk and Governance, hence it is collectively called as GRC. But, the main objective of this research is to study a specific domain under Compliance – Audits, which is the Evidence Gathering procedure

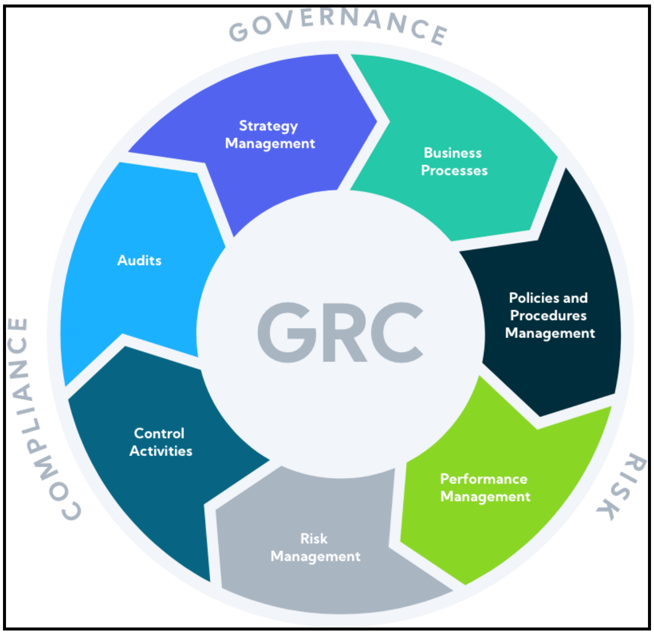

Fig 1: GRC Model [1]

The exploratory research strategy was used in this study in order to investigate, analyse, and design the essential results and conclusions connected to the purpose and the issue in question. This approach was used in order to further study the framework design in a brief manner. This approach will examine the previous research that has been conducted, assemble the pertinent material, evaluate the essential case studies that are connected to the proposed framework design, and develop conclusions based on the evaluation of the case studies and related aspects. In order to support this approach, various research articles, research journals and reports were also sourced from the available repositories such as IEEE to study the relevant details about the framework, related applications and implementation. These studies were mainly based on the framework and its application using machine learning and AI. Thus, making such approaches complex and difficult to understand for the basic group of technical and non-technical individuals.

3.2 Analysis and Assessment:

[1] https://inquisient.com/risk-compliance/

The exploratory research strategy involves looking into previous studies, frameworks, designs and additional information on the relevant issue in order to develop conclusions about the topic at hand. Case studies and the reports provide a comprehensive detail of the issue occurred which can be beneficial for studies and research for future cases. For this reason, the various case studies in the field of data breaches and security attacks were used to further address the gaps, prove the benefits of the proposed framework, and draw the conclusions of this study. Case studies were examined in this manner based on an in-depth examination of the issues that they were written about. With the support of the proposed framework, this research and analysis aided in the identification of gaps and the development of concise solutions to those gaps. The security posture, controls and settings implemented by the client organizations was studied, analysed and assessed with the help of the proposed framework. These assessments and audits were then converted into a case study which helped in the evaluation of the EGF. The case studies helped in finding and curating the gap which was identified, and thus ultimately, the same shall be predicted with the help of Framework design, checking to see if the gap would have been highlighted and how it could have been avoided. To draw the inferences, the case studies were evaluated with the existing assessment procedure against the new procedure which included the use of EGF. The cases were studied in depth along with the different research articles, media stories, root cause analysis reports of different organizations and research groups, specific details were captured, relevant information was used to draw the cause of the issue and the effect of it. Finally, the solution or the approach which would have avoided the respective issue was found out and documented in the case study report.

The evaluation part contains the results of the case study analysis, which included a critical evaluation of the case studies chosen, the identification of the fundamental cause of the problem, and the formulation of mitigation strategies. However, if the recommended framework had been applied during the auditing process, the evidence acquired, or the security measures had been checked, the issue would not have happened as a result of the failure. This is the alternate mitigation procedure that has been added in the Evaluation section once the analysis has been completed.

The Framework Design provided in this research was developed on the basis of a number of research articles, journal papers, and international standards organisation frameworks, among other sources. It is proposed that this framework be used as a later guide towards the procedures or approach that should be used for gathering the necessary proof of the controls that have been placed into an organization's infrastructure. In addition, it illustrates at what stage the controls should be retained as evidence, so that they can be used in an internal or external compliance audit, as well as for re-verification. In addition to auditors, this approach will be valuable to internal executives such as CISOs, ISOs, cybersecurity analysts, risk management teams, and system administrators.

4 Design Specification

The proposed framework works under the Audit domain in Compliance. This simplified framework provides an overview of a critical process which can assure the implementation of the security controls in any organizational infrastructure. Adding this specific guide in the audit process can help in attaining a good security posture for any company.

It does not matter if the full IT System audit is underway or if the audit is being performed for a specific set of controls or for a specific group of policies, this guide can be beneficial to both processes. The main section of this framework is the “Verification” part.

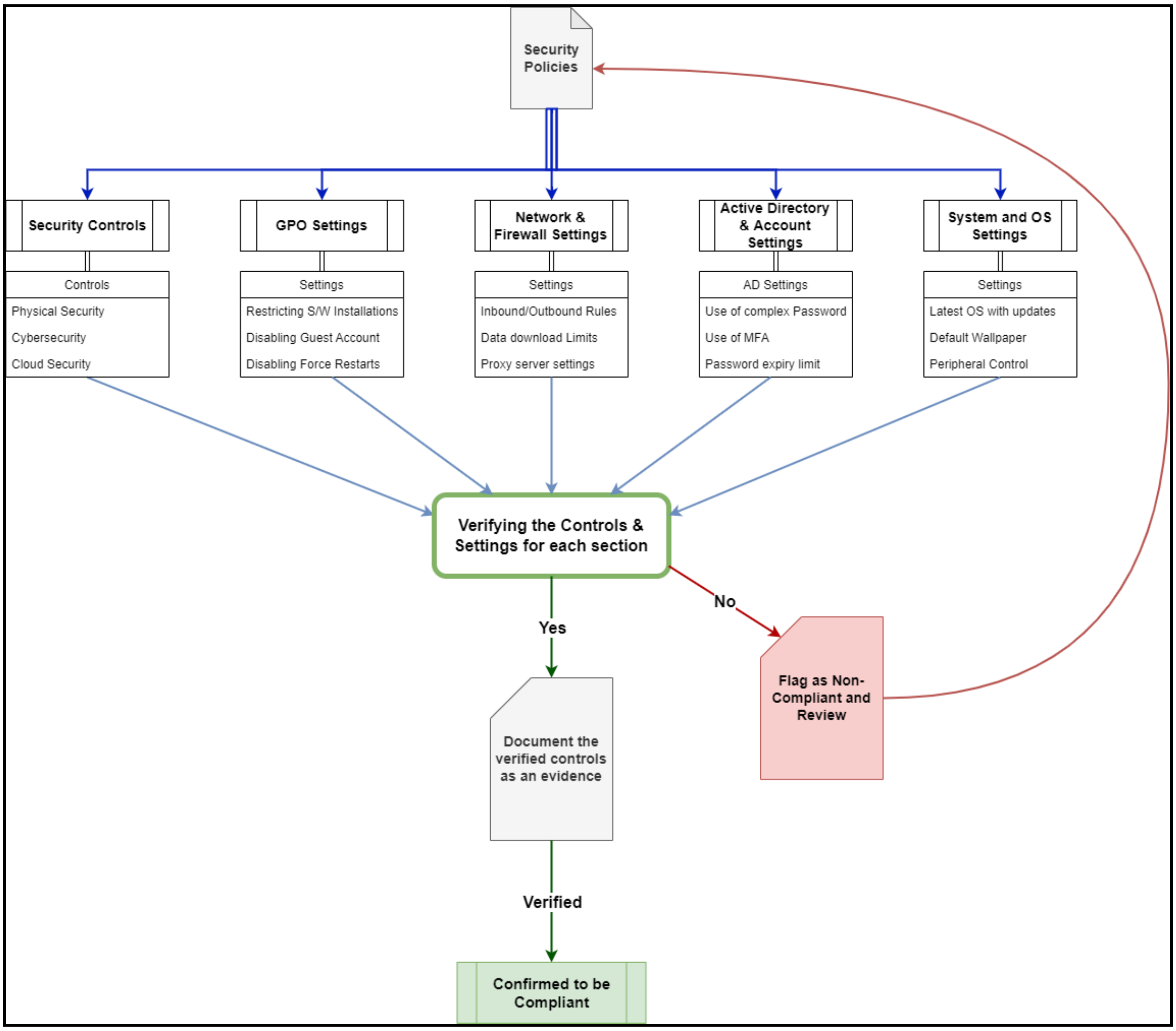

Fig 2: EGF

The different sections of the Framework are as follows:

- **Security Policies**: Security policies provide the primary definition of the controls and settings which needs to be implemented into the infrastructure and to the IT Systems, Accounts, Network, OS etc. Security Policies may contain different policies such as Password Policy, Firewall Policy, Clear Desk Policy, Encryption Policy and so on.
- **Controls and Settings**: Controls and settings define the specific in-depth configurations for each of the Policy in question. For example, if password policy is

considered, the controls will define the minimum password length, password complexity, password expiry and so on.

- **Verification of the Controls**: The most important section of the framework is the verification of the controls. How can we be sure that the controls defined in the Policies and settings have been implemented successfully? – With the help of the evidence of that control. This evidence can be a simple screenshot, or it can be a rule/setting/code in the destination where it is applied.
- **Documentation**: The verified controls need to be documented in the audit report, or can be documented in the Security Policy itself as evidence of the implemented controls for better understanding and easier to access when reviewed or during the compliance audit.

5 Implementation

The proposed framework serves a purpose to be used as an additional guide in the compliance audit process. As this framework is a conceptual proposal, it can be used by auditors and also internal admin teams for evidence gathering and documentation purposes which can be used in future audits or during risk assessment procedure. This framework acts as a guide and does not have any dependency to any other application or software. This can be used as an added guide to the normal audit or assessment process adopted by the organization's internal team or by the external auditing team.

The security policies provide the primary description of controls and settings that needs to be implemented by the organization and also provides and overview of the security controls adopted by the organization to the auditors.

The implemented controls and settings described in the security policies make up the steps or configurations which needs to be done as described in the policies, for example, in case of password policy, the use of complex password, password expiry limit and the minimum characters for the password limit will be set in the AD of the domain controller which the organization is using. These settings are critical and needs to be well implemented.

The verification and evidence gathering part guide the auditor or the internal IT Team to make sure the controls are implemented correctly. For example, as explained above with respect to the password policy controls, the auditor or the IT team must go to the source of the controls which are implemented, in this case the AD on the Domain controller, and must verify the settings by documenting the details and taking a screenshot of the settings to be added in the report as evidence. This ensures the correct implementation and accountability of the settings and security controls. This will be ultimately used in the audit or assessment process and the evidence can be used to review the settings or can simply be stored as a proof of the controls implemented.

Once the controls are verified and are deemed to be correct, the setting and the policy can be flagged as compliant, or can be flagged as non-compliant if the settings to be found not correctly implemented during the verification. This will ensure a strict adherence to the security policies and compliance audit process.

The below diagram shows a basic workflow as described above:

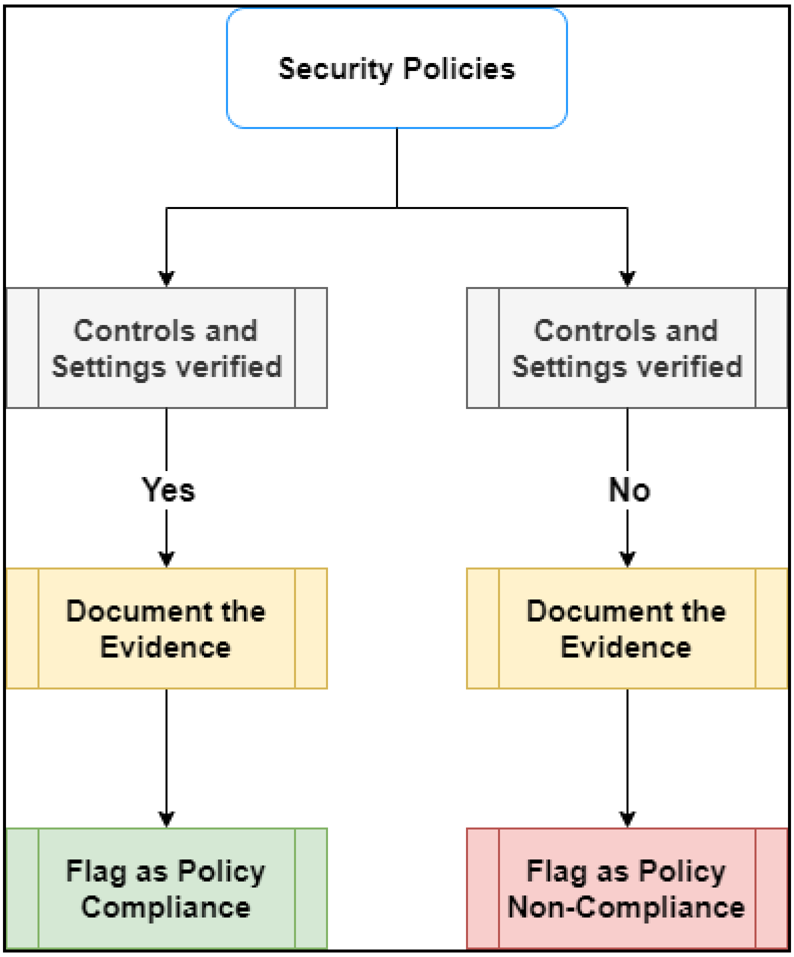
Security Policies
Controls and Settings verified
Controls and Settings verified
Yes
No
Document the Evidence
Document the Evidence
Flag as Policy Compliance
Flag as Policy Non-Compliance

Fig 3: Basic Workflow

6 Evaluation

The proposed framework was used in addition to the standard compliance audit frameworks as a guide. This framework was evaluated against the basic security posture through compliance audit and risk assessment done for some SMEs, the names of which cannot be disclosed because of an NDA in place, during the course of the industry work.

This analysis was done on the security posture of the organization which was already in place and through the course of the audit, the flaws and gaps were identified and documented with the help of the EGF. This process helped in better documenting the proofs of the controls implemented and helped in reporting the same to the clients. This process has been reported as a case study in this report which helped in evaluating the proposed framework.

6.1 Case Study 1:

Basic setup and outline of the organization: The organization is an Ireland Based organization which has its offices in Ireland and Australia. The company has major backbone of infrastructure, which includes around 150 employees, 120 workstations, 12 servers which comprises both cloud and on-premise machines along with BDRs and NAS.

Assessment for the company: An audit and risk assessment were performed for the company wherein the security controls and settings which were implemented by the organization as per the security policies adopted was checked and verified. In earlier audits and assessments, the standard framework such as ISO27001 or NIST. These audits did not prioritize the evidence gathering phase which was important for documentation and accountability within the organization to implement the controls. Hence, in this assessment the EGF was used to check, verify and document the controls which were implemented by the company's IT and Admin Team. The gaps and flaws were identified using the framework and same was reported to the company for review and re-implementation.

Analysis and Gaps Identified: The company had multiple external vendors and suppliers with which it was doing the business. The vendors and suppliers were provided the access to company network with the help of VPN connections and credentials to access the company network. For this, the company had adopted the Third-Party Vendor Access Control Policy, and provided the access to the vendors. A major gap was identified during the course of audit that there was no specific packet filtering and ransomware toolkit installed on the firewall which was used to manage the access to the company network for the vendors. This was urgently highlighted and flagged as non-compliant, documented using the framework and reported to the company. Allowing non-monitored network control to external vendors can lead to a data breach or any external vendor can hack into the internal network using simplest tools available online.

Another flaw identified was non-metered connections over VPN for external vendors. As per the policy adopted, the VPN connections for external vendors shall be metered with a specific connection time-out with an option to re-login for better security and authentication. Through the course of risk assessment and review, it was found out that the VPN connections for externals were not metered and had no time-out settings justified. This gave a huge risk because if an external vendor did not logout or end the session, the session will be kept open without a timeout setting and can be hijacked. This was flagged as non-compliant, documented the proof and was reported to the company for a review and strict implementation.

Mitigation Steps: The audit and the report were discussed with the company's internal IT and Admin Team in the presence of the senior executives. The flaws and gaps were discussed and the mitigation steps were suggested to the company to be implemented.

For the unsecure VPN connection, an IP Packet filtering Firewall was installed to manage the VPN connections of external vendors, with an anti-ransomware toolkit installed in the firewall, which can detect any malicious traffic based on the IP traffic. This secured the VPN connections and access of vendors to the internal company network.

The second step was to monitor the VPN connections which was done by putting a connection timer on the external VPN connections. This timer was set to 7200 seconds (2 hours) as suggested by the company, and the controls were setup for the connection to timeout after 2 hours. Once timed out, it will ask for the credentials of the vendors again to re-login and the connection timer will be reset once the person logs back in. This secured the VPN connection and allowed the IT team to keep track of the authentication of external vendors.

Documentation and Verification: Once these steps were implemented, the framework was used to verify the controls, by taking the screenshot of the configuration of the controls and settings implemented, which was then documented in the audit report. Once the controls were verified, these settings were flagged as compliant in the audit report after review. This helped in improving the security posture of the company and making the connections more secured to be accessed by the external vendors.

6.2 Case Study 2:

Basic setup and outline of the organization: The company is a Health Service provider based in Dublin, which handles various PII, medical records and processes personal data in large quantities related to a person's medical history. The company has an extensive backbone of infrastructure of around 50 employees, 35-40 workstations, various handheld devices, 8 servers which includes both the cloud and on-premise machines and VMs for guest access, BDRs and NAS.

Assessment for the company: Risk assessment and compliance audit was performed for another client during the course of the industry work. In earlier audits and assessments, the standard framework such as ISO27001 or NIST. These audits did not prioritize the evidence gathering phase which was important for documentation and accountability within the organization to implement the controls. The audit was done as per the quarterly risk assessment and compliance audit schedule for the organization and the EGF was also used for doing the assessments. The settings and controls were checked against the security policies adopted by the organization to confirm whether the implemented controls were compliant or not. The company handles various PII, medical records and processes personal data in large quantities related to a person’s medical history. The audit was done in the presence of the company’s internal IT and Admin team for discussion and verification.

Analysis and Gaps Identified: The major gap identified during the audit was the most basic setting which cannot be ignored. The organization adopted the Hardware and OS Policy which defines the use of latest OS with updated security patches for organizational use. In the assessment, it was found out that the company was using obsolete machines with outdated OS Windows 7. Windows 7 has been made obsolete and its support have been discontinued by Microsoft. As this poses a huge security threat of using outdated OS, this issue was directly flagged as non-compliance with the senior executives of the company and was suggested to strictly upgrade all the necessary hardware with the latest OS. This resulted in raising a priority change with the IT and Admin Team for upgrading the OS versions and necessary hardware.

Another flaw identified during the assessment was the periodic Backup and Data Retention system setup. The organization had adopted the Backup and DR Policy for setting up data backups in case of any major cyber-attack. However, the BDR system was connected to the domain of the company, which is non-compliant, with the periodic backup setting was every 6 months which is a very huge gaps between the backups. As per the procedure, the BDR machine/server must never be connected to the internal company network and needs to be connected to a totally separate domain and network for added security. Also, for an organization handling huge amount of PII, the Backup period must be kept to at least every month, or every 6 weeks. Backup periods linger than that can create issues in case of any drive or hardware failure, or data loss due to any cyber-attack. This was also flagged as non-compliant and was raised to the senior executives and IT Team for review and re-implementation.

Mitigation Steps: The audit and the report were discussed with the company’s internal IT and Admin Team in the presence of the senior executives. The flaws and gaps were discussed and the mitigation steps were suggested to the company to be implemented.

For the outdated OS on machines, a critical change request was raised, with all the Outdated OS being upgraded to the latest OS Windows 10, with the latest available security patches and Windows Firewall. All the outdated hardware was replaced with new hardware with better security features, old hardware decommissioned after wiping the contents of it in a safe manner.

For the BDR, the server was disconnected from the company domain, joined to a different local network and domain, re-configured the settings and BDR was enabled again. The period of data backups was change to every 4 weeks from 6 months. This ensured that the latest data is available for retention and during the recovery procedures.

Documentation and Verification: Once these steps were implemented, the framework was used to verify the controls, by taking the screenshot of the configuration of the controls and settings implemented, which was then documented in the audit report. Once the controls were verified, these settings were flagged as compliant in the audit report after review. This helped in improving the security posture of the company and making the connections more secured to be accessed by the external vendors.

In addition to the evaluation and assessment done for the clients, the framework can also be used to review and assess the past cyber attacks to identify the gaps in the system and implementation of security controls. Two of the examples where the framework can be used have been explained below using more case studies:

6.3 Case Study 3: HSE Cyber-attack - May 2021

Issue: In May 2021, HSE, the Health Secretary Executive, which is the National Department of Health, Ireland (Republic of) was attacked with the help of a ransomware, which encrypted thousands of files and led to a major data breach.

How was the attack orchestrated? – The HSE was attacked by a ransomware knows as "Conti", which is a fast-duplicating ransomware and is delivered through a TrickBot Malware. The hackers infiltrated the HSE Network and delivered the payload through the main Network on the machines, thus infecting a huge number of machines in a short span of time. As per the studies shown, at least 700 GB of data was encrypted and stolen by the hackers and published on the dark web.

What caused it? – After the course of attack, a deep investigation was done to find the cause of it, and the root cause was narrowed down to basic settings and controls which were not enforced. The major flaws found were outdated AV Patches, use of obsolete machines and hardware and the absence of Anti-ransomware toolkit on firewalls.

How the Framework can be applied? – As per the security policies adopted, the use of obsolete and outdated machines would have been highlighted during a compliance audit with the help of evidence documented stating that the OS being used is an older version with out-of-date AV patches. This evidence would have enabled the audit team to flag it as non-compliant, forcing the organization to migrate to newer and safer versions of OS and machines for the compliance check to be completed. The next major thing is the absence of Anti-ransomware toolkit on firewalls. The Firewalls must have a basic anomaly based anti-ransomware toolkits installed for traffic filtering, which was missing and not documented as evidence. This led to the fact that it was not highlighted and the network was left vulnerable to such attacks.

6.4 Case Study 4: GE Data Breach – July 2020

Issue: In July 2020, General Electric (GE) experienced a major data leak through one of its business email accounts. Multiple files and confidential data related to employees, personal identifiable information, vendors' information, suppliers' payment details were leaked and stolen from the email account.

How was the attack orchestrated? – During the initial investigation, it was found that, the email account was accessed by an ex-employee who did not have its access revoked after leaving the organization. This was done with the help of an internal system admin who helped the ex-employee in getting the necessary access to the confidential email and steal the data. The ex-employee then forwarded all the data to its personal email id and used it as a leverage for blackmailing the organization.

What caused it? – The thorough investigation found the root cause of the issue which was the negligence of the Admin and IT Team. The account of the ex-employee was found to be still active, accesses still working for the applications. There was no email filter for blocking the emails going to personal email ids outside the organization. These were the basic settings which led to a catastrophic data breach for a reputed organization.

How the Framework can be applied? – The account access would have been revoked automatically if the access threshold was documented and the control was implemented. Also, the password expiry limit can help in limiting the account access for an employee with periodic password changes. The absence of email traffic filter for emails going outside the organization to a personal email id would have been flagged as non-compliant with the help of the evidence documented through the framework. This would have been highlighted in the audit and the organization had to implement the necessary controls.

6.5 Discussion

As per the evaluation done with the two case studies through the assessment and audits for two client organizations, positively shows the change in the security posture of the organization after using the EGF while performing the audit and assessment. The existing process of assessment and audits was done without emphasizing on the evidence gathering process. This led to ignorance of documenting the proofs of the controls and settings which were and which were not implemented. The absence of documentation and proofs also meant that there was no accountability of the actions which needs to be taken or the responsibility of the settings which were missing during the phase of assessments. Due to this, the senior level executives were kept in the dark about the missing controls which were identified during the audit process and as well as the incompliance of the security policies adopted by the organization. This process was changed and with the help of EGF, accountability, implementation and compliance to the security policies was ensured.

It also summarises and educates as to why every organization should adopt a Compliance First model to have the best security posture against any threats. The proposed framework enables the auditors to enforce the respective controls and settings through verification and documentation. The case studies also discuss the mitigation steps undertaken for the settings and controls to be compliant, and how the framework was used to verify and document the settings implemented. The framework also helps the IT and Admin Team to be vigilant and strict about the implementation of security controls, adhere to the security policies, and ultimately help in the organization being compliant, secured and ready in terms of risks and threats.

This framework also fits into the real-world implementation as guide for auditors and risk analysts in addition to the adopted security frameworks. Furthermore, this framework can also be added in some industry based cyber security frameworks to emphasize more on the evidence gathering process for assuring security policy compliance during audits and assessments.

7 Conclusion and Future Work

With the detailed evaluation, it can be concluded that adopting a compliance first approach with the help of evidence gathering will ultimately help an organization to better their security posture and be ready for any threat or attacks. As the evidence gathering domain does not have any extensive research done on it, it is a very good chance of extending this research which can be applied on an organizational level. In earlier researches, there was no basic framework guide which emphasized on the evidence gathering phase in the compliance audit, which affected the implementation of controls due to the missing documentation and proof of the records. This proposed framework hope to bridge the gap and aims to better the security posture of any organization through compliance first approach.

Moreover, I can use this framework guide in assessing and auditing further more client companies during the course of my full-time work as I will be working in the compliance domain itself. Through this, I can assess and create more case studies based on different client organizations which will help me to validate and strengthen the use of the framework on an organization level making it a valuable addition in the standard frameworks which are used.

References

B. R. Aditya, R. F. a. S. S. K., 2018. Requirement and Potential for Modernizing IT Risk Universe in IT Audit Plan. *2nd International Conference on Informatics and Computational Sciences (ICICoS),* pp. 1-5.

Bulgurcu, B. H. C. a. I. B., 2010. Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness.. *Management Information Systems Research Center, University of Minnesota,* 34(3), pp. 523-548.

G. Drivas, A. C. L. M. C. L. A. C. a. H. J., 2020. A NIS Directive Compliant Cybersecurity Maturity Assessment Framework. *IEEE 44th Annual Computers, Software, and Applications Conference (COMPSAC),* pp. 1641-1646.
Jing Liu, X. W. D. J. a. C. W., 2012. Research and design of security audit system for compliance. *International Symposium on Information Technologies in Medicine and Education,* pp. 905-909.

Lianzhong Liu, X. W. a. D. J., 2010. A compliance policy model for security audit. *IEEE International Conference on Information Theory and Information Security,* Issue 10.1109/ICITIS.2010.5689556, pp. 490-493.

Majumdar, S., 2015. Security Compliance Auditing of Identity and Access Management in the Cloud. *IEEE 7th International Conference on Cloud Computing Technology and Science (CloudCom),* pp. 58-65.

Nader Sohrabi Safa, R. V. S. S. F., 2016. Information security policy compliance model in organizations. *Computers & Security,* 56(0167-4048), pp. 70-82.

Nadir, I., 2019. An Auditing Framework for Vulnerability Analysis of IoT System. *IEEE European Symposium on Security and Privacy Workshops (EuroS&PW),* pp. 39-47.

O. M. Al-Matari, I. M. A. H. S. A. M. a. S. E., 2018 . Cybersecurity Tools for IS Auditing. *Sixth International Conference on Enterprise Systems (ES),* Issue 10.1109/ES.2018.00040., pp. 217-223.

P. Swartz, A. D. V. a. N. M., 2019. A conceptual privacy governance framework. *Conference on Information Communications Technology and Society (ICTAS),* pp. 1-6.

Puzant Balozian, D. L., 2017. Review of IS Security Policy Compliance: Toward the Building Blocks of an IS Security Theory. *Association for Computing Machinery,* pp. 11-43.

R. E. Rodriguez-Rodriguez, A. F. Q. V. A. F. S. A. L. a. J. F. P., 2018. Design of an Automation Model for Taking Documentary Evidence of Compliance Tests of the IT Audit. *Congreso Internacional de Innovación y Tendencias en Ingeniería (CONIITI),* pp. 1-5.

Ray, V. R. K. a. I., 2016. A Generic Digital Forensic Investigation Framework for Internet of Things (IoT). *4th International Conference on Future Internet of Things and Cloud (FiCloud),* pp. 356-362.

S. Pahnila, M. S. a. A. M., 2007. Employees' Behavior towards IS Security Policy Compliance. *40th Annual Hawaii International Conference on System Sciences (HICSS'07),* p. 156b.

Santos, T. S. M. P. a. H., 2010. A Security Framework for Audit and Manage Information System Security. *IEEE/WIC/ACM International Conference on Web Intelligence and Intelligent Agent Technology,* pp. 29-32.

U. Thakore, R. R. Y. W. a. H. R., 2019. Combining Learning and Model-Based Reasoning to Reduce Uncertainties in Cloud Security and Compliance Auditing. *38th Symposium on Reliable Distributed Systems (SRDS),* pp. 269-275.

Bubilek, O., 2017. Importance of internal audit and internal control in an organization-case study

M. Florian, S. Paudel and M. Tauber, "Trustworthy evidence gathering mechanism for multilayer cloud compliance," 8th International Conference for Internet Technology and Secured Transactions (ICITST-2013), 2013, pp. 529-530, doi: 10.1109/ICITST.2013.6750257.

Umar Mukhtar Ismail, Shareeful Islam, A unified framework for cloud security transparency and audit, Journal of Information Security and Applications, 2020, Volume 54, https://doi.org/10.1016/j.jisa.2020.102594

Bicaku, A., Tauber, M., & Delsing, J. (2020). Security standard compliance and continuous verification for Industrial Internet of Things, International Journal of Distributed Sensor Networks

Albitar, K., Gerged, A.M., Kikhia, H. and Hussainey, K. (2021), "Auditing in times of social distancing: the effect of COVID-19 on auditing quality", International Journal of Accounting & Information Management, Vol. 29 No. 1, pp. 169-178. https://doi.org/10.1108/IJAIM-08-2020-0128