An Evidence Gathering Framework for Auditing Policy Compliance

Configuration Manual

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……………………………………………………………………….………

Lecturer: ……Mr. Vikas Sahni…………………………………………………………………….………

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

Project Title: An Evidence Gathering Framework for auditing Policy Compliance

Word Count: ……1564…………………………… **Page Count:** …………8…………………**.**

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
Student ID: 19217242

1 Framework and guidelines

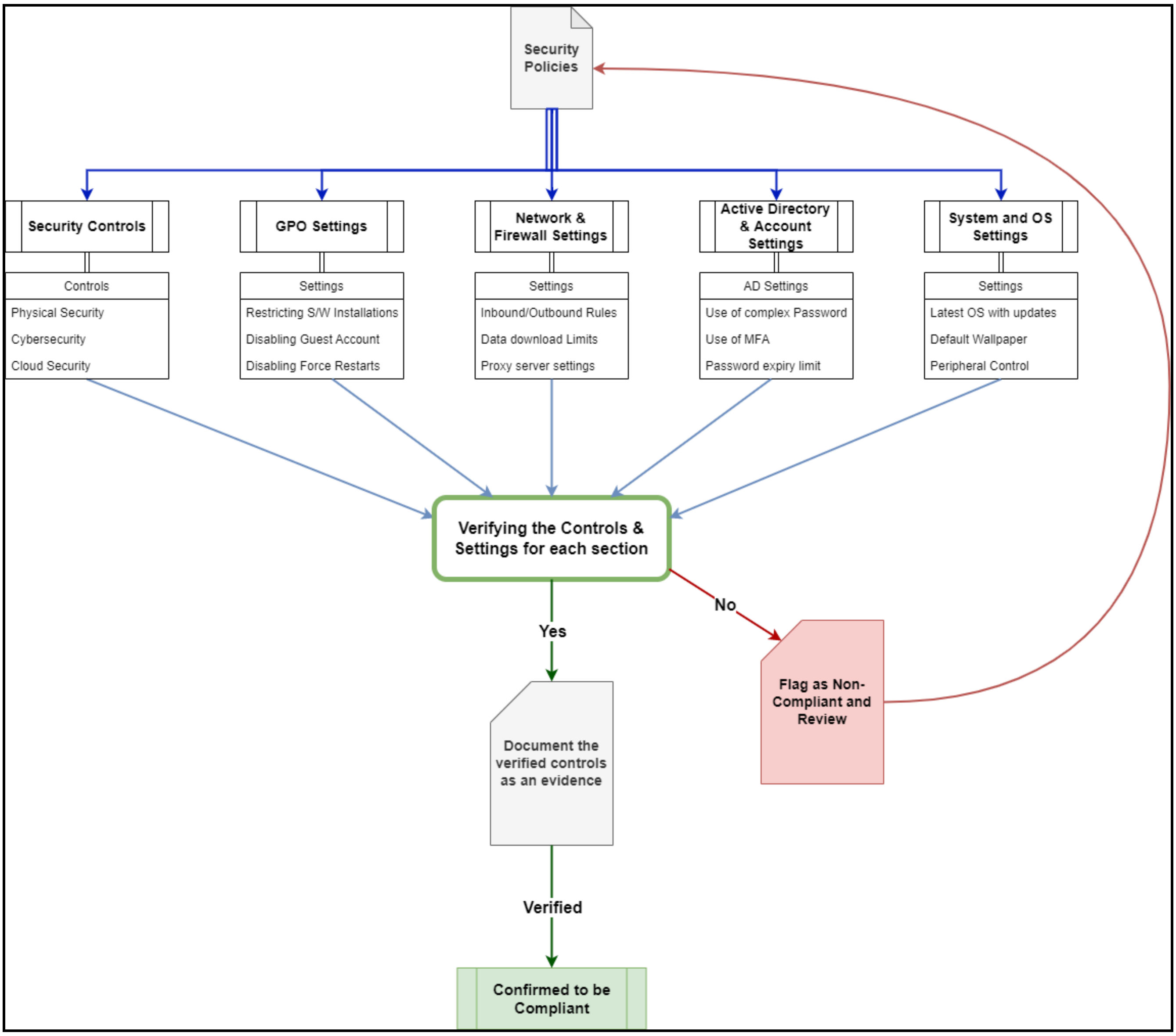

Fig 1: Framework Design

Guidelines for using the framework:

Evidence gathering is the process of verifying and documenting the security controls and settings implemented in the IT Infrastructure as per the adopted Security Policies and ensuring that the settings and controls matches the parameters as mentioned in the security policies and is compliant.

Below guidelines shows how the framework can be used for evidence gathering, verification and documentation. To easily understand the guidelines, the below steps describe how the framework can be used in terms of gathering the evidence based on an adopted security policy. For example, if Password Policy is under review and the controls needs to be verified, below is the process:

1. As per the Password Policy, there are basic parameters which are mentioned in the password policy which are Password complexity, minimum password length, password age, account lockout threshold.

2. In an organizational infrastructure, these settings are implemented through a GPO (Group Policy Object) which is deployed through a Domain Controller (DC), also known as AD server, which hosts the Active Directory for the organization.

3. To verify the controls, it needs to be checked if the settings mentioned in the security policies are correctly implemented through the GPO or not. To do this, the DC server needs to be accessed from where the GPO is deployed. The GPO can be a basic Default Domain Policy, or it can be separate GPO which can be named as Password Policy GPO.

4. Once in the DC server, search for the GPO and go deep down inside the GPO where the controls are implemented. In the case of Password Policy, all of these controls are implemented through a feature called "Policies" which is a part of Computer Configuration tab.

5. Under the Computer Configuration tab, go to the source of the GPO where the parameters are defined, which can be found at: **Computer configuration-> Policies-> Windows Settings->Security Settings -> Account Policies -> Password Policy** [1]

6. This source of the settings will define the controls implemented by the team; these controls can then be verified against the security policies. For example, if the policy defines that the maximum password age must be 45 days, the same settings must be defined in the GPO, if minimum length must be 8 characters, the same control must be defined in the GPO, and so on.

7. As these controls are verified, the auditor can document these setting in the report or a screen capture can be taken to document it as a proof of implementation. Once the security settings are verified, the settings can be deemed as compliant with the security policy adopted.

[1] https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/get-started/virtual-dc/active-directory-domain-services-overview

8. If there are any controls missing, the auditor can flag that specific setting as non-compliant and raise it with the IT or Admin team for review and re-implementation.

The primary aim of Evidence Gathering is to go to the source of any implemented controls or setting and verify it against the security policy adopted to make sure that the controls are correctly implemented or not.

The above steps explained with respect to Password Policy, can be replicated to be used for any other adopted Security Policies or security controls which needs to be verified using the framework.

2 Monthly Internship Activity Report

October 2021 Internship Activity Report

The Internship Activity Report is a 1-page monthly summary of the activities performed by you and what you have learned during that month. The Internship Activity Report must be signed off by your Company and included in the configuration manual as part of the portfolio submission.

Student Name: __Nachiket Phadnis__ Student number: _19217242_

Company: Spector Information Security Ltd.

Month Commencing: 28th Sept – 28th Oct 2021

Activity Details:

1) Induction – Mandatory Trainings, account setup and tools setup.
2) Certifications – Completed SOPHOS Certified Engineer certification for Firewall and Endpoint Management.
3) Getting Familiar with the Cybersecurity and Monitoring Tools such NinjaRMM, SOPHOS, Confluence and Webroot.
4) Discussions and introduction to security policies and compliance audits.
5) Finalizing the research domain and adopting the Research Project topic.

Employer comments:

The cybersecurity stack required to protect ourselves and our clients has grown significantly in recent years. Familiarity and training on the different tools can be a challenge for new employees. Nachi has shown a willingness to be trained, certified and familiar as soon as possible whilst providing feedback on possible improvements to ensure their best use is achieved. Nachi has begun reviewing our compliance services offered to clients with a view to systemizing and improving what is a very structured and manual improvement. Nachi has settled in really well to the team and proved very helpful to colleagues in various areas of his expertise.

Student Signature: Nachiket Phadnis Date: 30th October 2021

Industry Supervisor Signature: Gerard Whitehead Date: 30th October 2021

November 2021 Internship Activity Report

The Internship Activity Report is a 1-page monthly summary of the activities performed by you and what you have learned during that month. The Internship Activity Report must be signed off by your Company and included in the configuration manual as part of the portfolio submission.

Student Name: __Nachiket Phadnis__ Student number: _19217242_

Company: Spector Information Security Ltd.

Month Commencing: 29th Oct – 28th Nov 2021

Activity Details:

1) Asset registry and compliance check for all client assets.
2) Policy reviews and migration to Confluence Platform.
3) GPO Management for client devices with Policy creation and enforcing.
4) SOPHOS Compliance checks performed for client assets and incompliant machines disabled and decommissioned.
5) Gathering the topic relevant data, practical implementations and evaluation.

Employer comments:

Nachi has begun the task of systemizing our compliance services by migrating our security policies to the Confluence platform. While migrating, he has suggested multiple improvements on the wording and scope of various policies. Each client requires and up to date asset and risks register and Nachi is reviewing asset registers and ensuring each device under our control meets our minimum standard. Nachi stays up to date with all new threats reported online and has become a key point of contact for clients with security concerns.

Student Signature: Nachiket Phadnis Date: 30th November 2021

Industry Supervisor Signature: Gerard Whitehead Date: 30th November 2021

December 2021 Internship Activity Report

The Internship Activity Report is a 1-page monthly summary of the activities performed by you and what you have learned during that month. The Internship Activity Report must be signed off by your Company and included in the configuration manual as part of the portfolio submission.

Student Name: __Nachiket Phadnis__ Student number: _19217242_

Company: Spector Information Security Ltd.

Month Commencing: 29th Nov – 28th Dec 2021

Activity Details:

1) Onboarding and audit for client infrastructure.
2) Adoption and implementation of security policies for clients.
3) Risk Assessment and Mitigation Plan for clients.
4) Creation and updating of IT Security Posture for clients.
5) Creation of the Research project report with the relevant information gathered through the industry internship and implementation.

Employer comments:

Nachi is helping align our onboarding and offboarding processes to ensure accurate and up to date asset registers at all times. He is now reviewing individual clients to update the asset register, creating mitigation plans for areas deemed at risk and in need of attention. Nachi has been key in working on the recent Log4j exploit to ensure the necessary measures are in place across all clients and communicating directly to ensure they know they are secure. Nachi is now a key person in the team already who completes any task given to a standard above what was expected to begin with.

Student Signature: Nachiket Phadnis Date: 30th December 2021

Industry Supervisor Signature: Gerard Whitehead Date: 30th December 2021