Towards Cyber Resilience and Readiness: A Framework for Measuring Security Controls' Effectiveness, Efficacy, Efficiency, and Utilization

Author: Renad Alrabea, renadalrubayei@hotmail.com

Abstract

Cyber-attacks statistics and trends are worsening over time, and despite global efforts, there has been significant increase in cyber breaches and their consequences (Boehm, Lewis, Li, Wallance, & Dias, 2022; Brooks, 2022; Sobers, 2022). Security controls play a major role in defending organizations against cyber-attacks and threats. Organizations invest in security controls and spend a lot of time and effort selecting what meets their requirements, deploying it, maintaining it, and utilizing it; trusting that achieving these steps and having the security control in place will mitigate a particular risk and these security controls will always work as intended, by preventing or detecting specific threats. While this is not entirely false, something is missing. To what extent have these security controls' effectiveness been measured? Has the efficacy of these security controls been assessed and validated? Are they efficient enough? And how much are they utilized? This paper will discuss all these questions in detail and will address them by architecting and designing a framework to measure, validate, and assess security controls' effectiveness, efficacy, efficiency, and utilization. The framework includes objective and scope, roles and responsibilities, framework structure and streams, framework mapping with threats and risks, self-assessment with the framework, and framework implementation.

Keywords

Cyber resilience and readiness, cybersecurity framework, measuring security controls, security controls validation, security controls assessment.

1. Introduction

1.1. Security Controls Definition, Objectives, and Types

Security controls are safeguards or countermeasures prescribed for an information system, or an organization designed to protect the confidentiality, integrity, and availability of its information and to meet a set of defined security requirements (NIST, 2016). The primary objective of implementing a security control is to mitigate specific risks behind threats by preventing or detecting them.

For the context of this paper, there are three different types of security controls: preventive, detective, and corrective:

1. Preventive control stops cyber-attacks, aimed at halting cyber intrusions on the wire and at the endpoint.
2. Detective control discovers break-ins, aimed at flagging cyber intrusions on the wire and at the endpoint.
3. Corrective control reverses the impact of cyber-attacks after the occurrence, aimed at remediating irregularities on the wire and at the endpoint following unauthorized or unwanted events.

1.2. Measurement Factors

Measurement Factor	Definition
Effectiveness	The security control will successfully produce the desired and the intended result. It refers to how well the security control will operate in a controlled manner during non-ideal and outstanding situations.
Efficacy	The security control is continuously capable of producing the desired and intended result. It refers to how well the security control will ideally operate during regular situations.
Efficiency	The security control generates a positive Return on Investment (ROI) which is well beyond what have been spent of time, effort, and money. It refers to the value of the security control and how well it is allocated against cyber threats and risks.
Utilization	The features, benefits, and capabilities of the security control are appropriately used, and the security control is utilized to the fullest extent for its intended purpose.

Table 1 – Definitions

1.3. Current Gaps in Measuring Security Controls' Effectiveness, Efficacy, Efficiency, and Utilization

1.3.1. Gaps in Measuring Security Controls' Effectiveness and Efficacy

The security task force, which typically owns the security control are continuously selecting and enabling a specific set of rules, signatures, policies, or filters, assuming that once enabled, all will work as intended by preventing or detecting threats appropriately. However, there is currently no standardized and repeatable way to measure, validate, and assess the actual effectiveness and efficacy of security controls. Typically, and especially during incidents' post-mortem phase, the security task force identifies a failure in the security control while investigating root causes behind cyber incidents where the security control did not operate as expected and intended.

Moreover, measuring and validating security controls' effectiveness and efficacy also results in identifying other issues with security controls, such as misconfigurations, technology limitations, or misstated features or capabilities. There are many root causes for encountering such situations. One of the reasons is that vendors' default configurations and best practices typically look after the performance of the security controls over the security. For example, one of the configuration guides for email security gateway states that if the attachment size is greater than the threshold, the email will be delivered without sandboxing the attachment, which may result in delivering malicious and harmful emails. Another reason is that the security control's rules sometimes do not consider all the possible scenarios. For example, a rule has been enabled in Email Security Gateway solution to block a specific file type by only looking at the file extension and the file header, omitting to recursively investigating the file payload. But what if this file has double extensions, the extension has been renamed and the file has been encrypted, the file has been encoded, compressed into another file type, embedded into another file type, or even renamed, embedded into another file type, encoded, then compressed into another file type, would the enabled rule block this file in all these scenarios? (Wapack, 2022).

1.3.3. Gaps in Measuring Security Controls' Efficiency

Security controls are among the biggest and top investments in cybersecurity program (Debar, 2019). In general, there are always high expectations from executives and leadership on the return on investment. To address this concern, the answer to leadership questions about the value of security controls and return on investment should be quantifiable and meaningful. However, there is currently no standardized and repeatable process to measure and assess security controls' efficiency. Therefore, this could result in having a gap in communicating cybersecurity program requirements, status, or cybersecurity posture to leadership or, possibly, making a wrong investment.

1.3.4. Gaps in Measuring Security Controls' Utilization

With the expanding multitude of security controls which is typically owned by a sole function, in many cases, not all of these security controls are appropriately utilized. Some security controls will be left out with no proper utilization or maintenance. Moreover, there is currently no standardized and repeatable process for measuring and assessing the utilization of security controls. Consequently, these unutilized controls remain unutilized for a prolonged period of time.

1.3.5. Current Available Solutions

There are currently some available solutions in the market for measuring and validating the effectiveness of security controls. Tools like Security Validation for Mandiant, Security Optimization Platform for AttackIQ, Cymulate, and SafeBreach, for example, make an excellent start in simulating and executing attacks to validate whether or not security controls will prevent, detect, or correct these attacks (Moyal, 2022; SafeBreach, 2022; Mandiant, 2022; AttackIQ, 2022). Some of them may even stand in providing one way to measure the effectiveness of security controls. However, they do not entirely address the underlying issue that this paper discusses in other aspects, like having standardized, regularly repeated, and measured exercises to measure security controls' effectiveness, efficacy, efficiency, and utilization.

2. Framework Introduction

2.1. Objectives and Scope

The objective of this framework is to have standardized, scalable, repeatable, and automated processes to measure, validate, and assess security controls' effectiveness, efficacy, efficiency, and utilization to deliver quantifiable, trustworthy, and actionable outcomes. The scope of this framework is any technology or tool that falls under the security control definition.

2.2. Roles and Responsibilities

Typically, there are two different owners for security controls: business and technical. Both owners work on security controls as part of their daily tasks and activities. However, the business owner is the end user of security controls and has the ultimate responsibility of security controls, such as SOC analysts, incident responders, intrusion analysts, threat hunters, penetration testers, and vulnerability assessors. Conversely, the technical owner is responsible for maintaining and administrating all security controls, such as managing security controls upgrades, licenses, appliances, and operational issues.

This framework does not overlap with business and technical owners' roles and responsibilities; rather, it complements both entities by optimizing security controls through measuring, validating, and assessing security controls' effectiveness, efficacy, efficiency, and utilization.

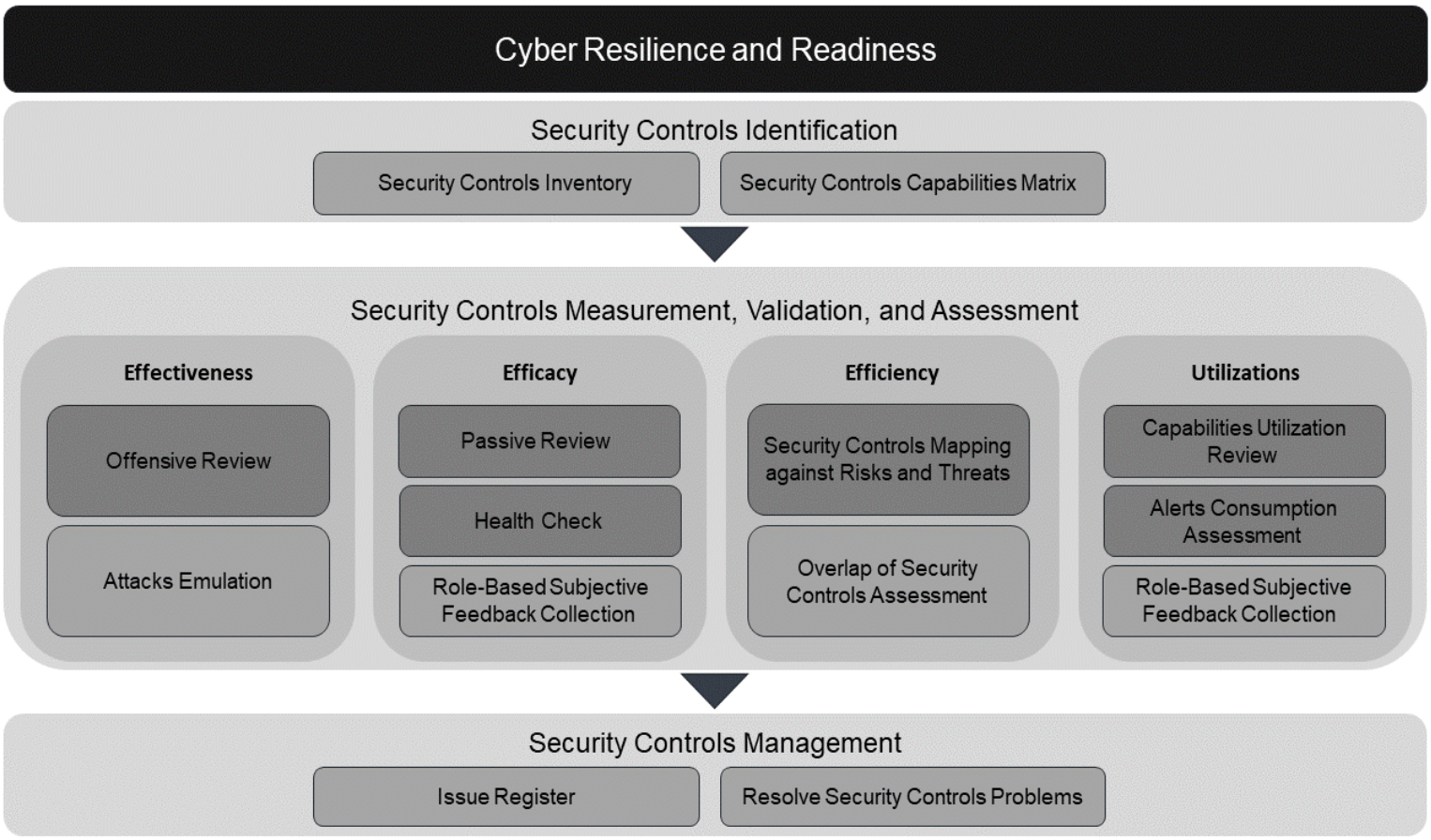
2.3. High-Level Framework Structure

The framework has six main streams, starting with identifying security controls by building and maintaining a comprehensive inventory of all security controls with their capabilities, followed by four measurements and assessments for security controls' effectiveness, efficacy, efficiency, and utilization, and lastly, managing all security controls by maintaining a comprehensive issue register that will be used for tracking and resolving security control related problems.

The framework has been designed following the SMART model. Each stream and activity of the framework follows SMART, which is a guide for setting objectives to ensure better results. (Kim, 2020). SMART stands for:

1. Specific: Targets a specific area.
2. Measurable: Can be quantified to show progress.
3. Achievable: Is attainable and action-oriented.
4. Realistic: Can be achieved using available resources.
5. Time-Based: Define what can be achieved in a given time period.

Graph 1 below illustrates the high-level structure of the framework.



Graph 1 – High-Level Framework Structure

3. Framework Streams

3.1. Security Controls Identification

3.1.1. Security Controls Inventory

This exercise shall be the first activity executed between all other framework streams and activities. Having a comprehensive inventory for all security controls and continuously tracking and updating the inventory is crucial. The comprehensive inventory of security controls will be used as input to the following streams and activities. The inventory shall include for each security control the information listed in Appendix A table 16.

3.1.2. Security Controls Capabilities Matrix

Each security control has many capabilities and features; capability is something that the security control can accomplish. For example, some of EDR capabilities are endpoint isolation, file retrieval from endpoints, applications allowlisting and blocklisting, remote operation on the endpoints, and file sandboxing.
The outcome of this exercise is a matrix for all security controls with their capabilities and features. This matrix will be used as input to some of the following streams and activities, such as capabilities utilization review and offensive review.

3.2. Measuring, Validating, and Assessing Security Controls' Effectiveness

3.2.1. Offensive Review

Testing security controls offensively is the main activity to measure the effectiveness of security controls and to validate whether security controls will prevent, detect, or correct these events or not. An offensive review for security controls includes both red teaming and penetration testing. Penetration testing is designed to discover vulnerabilities and gaps across a specified scope of the network or technology. Red teaming is a realistic attack based on an agreed scenario with a specific goal. Unlike in a penetration test, the red team only needs to find one open door. Once inside, the red team will try to navigate toward a target without being detected or blocked (AON, 2020).

Moreover, for complete measurement and validation of security controls, the selection of attacks and scenarios for penetration testing should cover all the capabilities of the selected security control. However, offensive testing might not be applicable to all security control capabilities. There might be some capabilities that cannot be tested offensively. In this case, the capability should be validated by an alternative test, or the historical logs should be reviewed. If the historical logs have been reviewed, the numbers shall be normalized to be on the same scale as offensive tests for other capabilities. The logs can be exported from the security control itself, depending on the retention period of the security control, or they can be extracted from the SIEM solution; a prerequisite for that is an integration with the SIEM solution. This exercise can also be conducted to measure and validate security controls' effectiveness against a specific attack, risk, or threat, such as a new large-scale vulnerability.

	Offensive Review
Frequency	Annually
Applicability	All Security Controls
Indicator	Key Control Indicator (KCI)
Rationale	- Preventive security controls are expected to prevent attack attempts. To measure the KCI, the prevented attack attempts and the alerted-only attempts, shall be compared to the total number of attempts. However, it should be noted that the alerted-only attack attempts should not be fully considered as it does not cover the whole purpose of the security control. - Detective security controls are expected only to detect attack attempts. To measure the KCI, the alerted attack attempts shall be compared to the total number of attempts. - Corrective security controls are expected to remediate irregularities. To measure the KCI, the remediated irregularities and the alerted-only attempts shall be compared to the total number of attempts. However, it should be noted that the alerted-only attack attempts should not be fully considered as it does not cover the whole purpose of the security control.
Preventive Security Controls Formula	$KCI = \frac{\sum Prevented\ Attempts + \frac{\sum Alerted\ Attempts}{2}}{\sum Attempts} \times 100$
Detective Security Controls Formula	$KCI = \frac{\sum Alerted\ Attempts}{\sum Attempts} \times 100$
Corrective Security Controls Formula	$KCI = \frac{\sum Corrected\ Attempts + \frac{\sum Alerted\ Attempts}{2}}{\sum Attempts} \times 100$
Example	An offensive review for Web Application Firewall (WAF) that covers numerous web attacks has been conducted. The total number of executed attack attempts is 35.WAF blocked 20 attempts, 10 attempts were only alerted, and 5 attempts were not blocked nor alerted. $KCI = \frac{20 + \frac{10}{2}}{35} \times 100 = 71\%$

Table 2 – Offensive Review Measurement

3.2.2. Attacks Emulation

Another way of measuring security controls' effectiveness is the available solutions mentioned in this paper. Each solution has different capabilities and uses different techniques for validating security controls' effectiveness. However, the primary capability of these solutions is executing numerous attacks to validate whether security controls will prevent, detect, or correct these attacks or not. Given that each solution has its way of presenting the result, this activity is not part of the designed formula for measuring security controls' effectiveness.

3.3. Measuring, Validating, and Assessing Security Controls' Efficacy

3.3.1. Passive Review

The outcome of security controls passive review is a detailed report which includes a table with all the discovered gaps, findings, and observations. The table must include for each gap: aspect, impact, recommendation, and criticality (High, Medium, and Low). The passive review should include aspects listed in table 3.

#	**Aspect**	**Description**
1	Configurations Review	Review of all the configurations of the security controls.
2	Prevention / Detection / Correction Rules Review	Review all the policies, filters, use cases, reports, and dashboards.
3	Coverage Review	Review the coverage of the security controls: - Architecture coverage for network-based security controls. - Endpoint coverage for host-based security controls.
4	Permissions Review	Review the assigned permissions and privileges for all users.
5	Alert Fatigue Review	Review the efficacy of the alerts and the percentage of false positive for alerting security controls.

Table 3 – Passive Review

<table>
<tr><th></th><th>Passive Review</th></tr>
<tr><td>Frequency</td><td>Annually</td></tr>
<tr><td>Applicability</td><td>All Security Controls</td></tr>
<tr><td>Indicator</td><td>Efficacy Rate</td></tr>
<tr><td>Rationale</td><td>Failing to meet the efficacy expected rate would indicate gaps in security control deployment and operability status. Thus, security controls are expected to have the highest possible rate in all passive review aspects. To measure the efficacy rate of passive review, the total of the assigned rates for each aspect shall be compared to the total of the highest possible rate for each aspect.</td></tr>
<tr><td>Precomputation</td><td>• There are 5 different aspects of the passive review, and each aspect should be rated from 1 to 3 based on the number of identified gaps:
o 3 - If there is no gap at all in this aspect.
o 2 - If there are some but not major gaps (medium or low gaps).
o 1 - If there are some major gaps in this aspect (high gaps).
• Total of the Highest Possible Rate = Number of Aspects x Highest Rate = $3 \times 5 = 15$.</td></tr>
<tr><td>Formula</td><td>$Efficacy\ Rate = \frac{\sum Rating\ for\ each\ Aspect}{15} \times 100$</td></tr>
<tr><td>Example</td><td>A passive review has been conducted for File Integrity Monitoring (FIM) solution. The report covered many gaps and observations, and a rating has been assigned to each aspect accordingly:
<table>
<tr><th>Aspect</th><th>Rating</th></tr>
<tr><td>Configurations Review</td><td>2</td></tr>
<tr><td>Detection Rules Review</td><td>1</td></tr>
<tr><td>Endpoint Coverage Review</td><td>3</td></tr>
<tr><td>Permissions Review</td><td>2</td></tr>
<tr><td>Alert Fatigue</td><td>1</td></tr>
</table>
$Efficacy\ Rate = \frac{9}{15} \times 100 = 60\%$</td></tr>
</table>

Table 4 – Passive Review Measurement

3.3.2. Health Check

Health checks are usually done by the vendor as part of the support service. It covers the infrastructure for the security control, the performance, and the current specifications for the appliances or virtual servers against the current utilization. The outcome of this exercise is a report with a table of the identified gaps and recommendations from the vendor. For each gap, the table must include: aspect, impact, recommendation, and criticality (High, Medium, and Low).

The health check should include the aspects listed in table 5.

#	Aspect	Description
1	System Resources Review	Review security controls' resources and the current utilization of the resources, including the number of appliances or VMs, Core, Disk Space, CPU, and RAM.
2	Product Version and Hotfixes Review	Review product version and hotfixes.
3	Product Backups and Database Update Review	1. Review backup configurations. 2. Review the configuration of updating the required databases, such as anti-virus and IP blacklist databases.
4	Logging Review	Review the retention period configurations.
5	License Review	Review the licenses, including available and non-available capabilities, resources, and expiration date.
6	System Error Review	Review system errors and alerts.

Table 5 – Health Check

<table>
<tr><th></th><th>Health Check</th></tr>
<tr><td>Frequency</td><td>Annually</td></tr>
<tr><td>Applicability</td><td>Fully Applicable for On-premise and Hybrid Security Controls
Partially Applicable for Cloud and Service Security Controls</td></tr>
<tr><td>Indicator</td><td>Efficacy Rate</td></tr>
<tr><td>Rationale</td><td>Failing to meet the efficacy expected rate would indicate gaps in security control health and maintenance status. Thus, security controls are expected to have the highest possible rate in all health check aspects. To measure the efficacy rate of health check, the total of the assigned rates for each aspect shall be compared to the total of the highest possible rate for each aspect.</td></tr>
<tr><td>Precomputation</td><td>• There are 6 different aspects of the health check, and each aspect should be rated from 1 to 3 based on the number of observed gaps;
o 3 - If there is no gap at all in this aspect.
o 2 - If there are some but not major gaps (medium or low gaps).
o 1 - If there are some major gaps in this aspect (high gaps).
• Total of the Highest Possible Rate = Number of Aspects x Highest Rate = $3 \times 6 = 18$.</td></tr>
<tr><td>Formula</td><td>$Efficacy\ Rate = \frac{\sum Rating\ for\ each\ Aspect}{18} \times 100$</td></tr>
<tr><td>Example</td><td>A health check has been conducted by the vendor for Data Loss Prevention (DLP), and several gaps have been identified. The below rating has been assigned accordingly:
<table>
<tr><th>Aspect</th><th>Rating</th></tr>
<tr><td>System Resources Review</td><td>2</td></tr>
<tr><td>Product Version and Hotfixes Review</td><td>3</td></tr>
<tr><td>Product Backups Review</td><td>1</td></tr>
<tr><td>Logging Review</td><td>3</td></tr>
<tr><td>Licenses Review</td><td>2</td></tr>
<tr><td>System Errors Review</td><td>1</td></tr>
</table>
$Efficacy\ Rate = \frac{12}{18} \times 100 = 66\%$</td></tr>
</table>

Table 6 – Health Check Measurement

3.3.3. Role-Based Subjective Feedback Collection

The objective of role-based subjective feedback collection activity is to add more insight to the assessment and the validation of security controls. As security controls are being used by business and technical owners in their operations and daily activities, they will undoubtedly have valuable feedback. This activity is to collect their feedback and comments on all security controls and consider it in the management stream, which includes a register for all security controls issues with tracking and resolving them.

	Role-Based Subjective Feedback Collection
Frequency	Constantly throughout the year
Applicability	All Security Controls

Table 7 – Role-Based Subjective Feedback Collection

3.3.4. Overall Measurement of Security Controls' Efficacy

The below formula is for the overall measurement of security controls' efficacy:

$$Efficacy\ Rate = \frac{\text{Passive Review\%} + \text{Health Check\%}}{2}$$

3.4. Measuring, Validating, and Assessing Security Controls' Efficiency

3.4.1. Security Controls Mapping against Risks and Threats

Mapping security controls against the organization's cyber threats and risks is the main activity to measure the efficiency of security controls. There are two types of risk assessment: quantitative and qualitative risk assessment. Quantitative risk assessment uses numbers to assess the likelihood and the impact of risks. The process involves calculating metrics, such as annual loss expectancy, to help determine whether a given risk mitigation effort is worth the investment. Risk is the combination of the probability of an event and its consequence. This can be explained as Risk: Likelihood × Impact (Tierney, 2020). Annual loss expectancy (ALE) is a calculation that helps to determine the expected monetary loss for an asset due to a particular risk over a single year. It can be calculated by multiplying the annual rate of occurrence (ARO) by single loss expectancy (SLE), ALE = ARO × SLE. ARO is the probability that a risk will occur in a particular year, and SLE is the expected monetary loss every time a risk occurs (Capital, 2019). Quantitative risk assessment is a prerequisite of this activity as ALE is an input for ROI formula.

	Security Controls Mapping against Risks and Threats
Frequency	Annually and Upon Project Selection
Applicability	All Security Controls
Indicator	Return on Investment (ROI)
Rationale	Security controls are expected to mitigate risks and not cost more than the expected monetary loss for the mitigated risks. To measure the ROI, the total of the expected monetary loss due to the risks that security control mitigates shall be compared to the cost of the investment.
Formula	R1 = ALE for Risk 1, which can be mitigated by the security control. $ROI = \frac{\sum R1, R2, R3, \dots}{Cost\ of\ Investment} \times 100$ (Positive ROI $> 100\%$)
Example	Proxy has mitigated four risks, and the sum of the ALE for these risks is 3M. Proxy deployment and implementation cost is 1M. $ROI = \frac{3000000}{1000000} \times 100 = 300\%$

Table 8 – Security Controls mapping against Risks and Threats Measurement

3.4.2. Overlap of Security Controls Assessment

The input of this exercise is the security controls capabilities matrix developed in the first stream. Some security controls may overlap in their main capabilities, and this exercise aims to identify these instances. After identifying an overlap between security controls, this overlap needs to be assessed and addressed. It could be justified by the purpose of having multiple layers for defense in depth, or it is not needed, or other possible reasons. However, this exercise is not included in the formula for measuring security controls' efficiency.

	Overlap of Security Controls Assessment
Frequency	Annually and Upon Project Selection
Applicability	All Security Controls

Table 9 – Overlap of Security Controls Assessment

3.5. Measuring, Validating, and Assessing Security Controls' Utilization

3.5.1. Capabilities Utilization Review

The input for this exercise is the security controls capabilities matrix from the first stream. After listing all the capabilities for security controls, each capability should be validated against the utilization, whether it is being fully utilized, partially utilized, or not utilized. However, one possible justification for not having a 100% utilization rate is that there might be some capabilities that are not applicable to the organization and cannot be used. This can be justified and handled case by case after calculating the utilization rate.

	Capabilities Utilization Review
Frequency	Annually
Applicability	All Security Controls
Indicator	Utilization Rate
Rationale	Security control capabilities are expected to be utilized to the fullest extent, referenced to threats, risks, and organization requirements context. To measure the capabilities utilization rate, the total assigned values of the utilization shall be compared to the highest possible utilization value (total number of capabilities).
Precomputation	• A value from 0 to 1 should be assigned for each capability based on the utilization status: o 1 - If the capability is fully utilized. o 0.5 – If the capability is partially utilized. o 0 – If the capability is not being utilized.
Formula	$Utilization\ Rate = \frac{\sum Utilization\ Values}{\sum Capabilities} \times 100$
Example	EDR capabilities are 15. The fully utilized ones, as per the assessment, are 6 capabilities, and 2 are partially utilized. $Utilization\ Rate = \frac{7}{15} \times 100 = 46\%$

Table 10 – Capabilities Utilization Review Measurement

3.5.2. Alerts Consumption Assessment

For any detected activity or event, security controls will trigger alerts with the action taken by the security control. The alerts are usually investigated and handled by the business owner, such as SOC analyst or incident responder. Each investigated alert by the analyst will be recorded in a centralized system, such as the Case Management system or the SIEM solution. This is thought of, as a general best practice in security operations. To assess the utilization of security controls by validating the consumption of these alerts, two reports should be obtained. The first report is for all the triggered and generated alerts for the targeted security control, and the second report is for all the created cases that are related to the security control.

	Alerts Consumption Assessment
Frequency	Annually
Applicability	Alerting Security Controls (Security Controls that generate alerts that have to be investigated and analyzed).
Indicator	Utilization Rate
Rationale	Business owners (security task force) are expected to utilize security controls by consuming the generated alerts. To measure the utilization rate of alert consumption, the handled alerts by business owners shall be compared to the total generated alerts. However, sometimes, for security controls that trigger more than one alert for a single event, the number of created cases will only be one for this single event and not for each alert. Therefore, the number of days where the security control has triggered an alert and the number of days where security control-related cases were created shall be compared to measure the utilization rate of alerts consumption.
Formula	$Utilization\ Rate = \frac{\sum Days\ with\ Cases}{\sum Days\ with\ Alerts} \times 100$
Example	Network Intrusion Prevention System (NIPS) has triggered 3000 alerts for the last 6 months. The alerts have been triggered in 150 days (out of 180 days). 200 cases have been created for NIPS in the same time period, and in 140 days, one case at least has been created. $Utilization\ Rate = \frac{140}{150} \times 100 = 93\%$

Table 11 – Alerts Consumption Assessment Measurement

3.5.3. Role-Based Subjective Feedback Collection

Role-based subjective feedback collection activity is the same feedback collection activity used in measuring the efficacy of security controls. The only difference here is that the collected feedback should be for the utilization of the security control, not the efficacy.

3.5.4. Overall Measurement of Security Controls' Utilization

The below formula is for the overall measurement of security controls' utilization for alerting security controls:

$$Utilization\ Rate = \frac{\text{Capabilities Utilization\%} + \text{Alerts Consumption\%}}{2}$$

3.6. Security Controls Management

3.6.1. Issue Register

A centralized tracker or a ticketing system should be used to log and record all security controls problems that have been identified as part of the framework streams and activities and from other activities, such as risk assessments, internal or external audit missions, regulatory compliance, etc. The tracker must be continuously updated and maintained, and it should include the information listed in Appendix A table 17.

3.6.2. Resolve Security Controls Problems

Resolving security control problems includes coordinating, tracking, and following up on all security control issues until closure. Each resolved issue should be retested after resolving it and before the closure to verify that it has been completely fixed. However, there might be some identified issues that cannot be fixed due to technology limitations, time constrains, etc. In this case, the risk behind the problem should be mitigated by compensation controls.

4. Threats and Risks Measurements with the Framework

To have an accurate measurement of the resilience and readiness for a specific threat or risk, the below steps have to be followed:

1. Identify the threat or risk that the organization would like to measure.
2. Identify and list all the tactics and techniques for the specified threat or risk.
3. Identify all the associated security controls that mitigate any tactic or technique for the specified threat or risk.
4. Retrieve effectiveness, efficacy, and utilization measurements for all the associated security control from the last assessment.
    - If the last assessment for the associated security controls is not within a year, the measurement exercises shall be repeated to gather updated data.

- If there is no prior assessment, the measurement exercises shall be performed against the associated security controls to have the percentages for effectiveness, efficacy, and utilization for all the associated security controls.

5. Calculate the average of the percentages for the identified associated security controls for effectiveness, efficacy, and utilization.

Section 6, "Framework Implementation," will illustrate how to implement this in detail.

5. Self-Assessment with the Framework

The maturity model is predefined evolutionary levels that can be used by organizations to identify their current level based on predefined criteria and aim for continuous improvement towards higher levels. For this framework, there are four different levels. Table 12 illustrates these levels with their criteria.

Maturity Level		**Criteria**
0	Non-exist	- None of the framework streams is in place. - Framework streams and activities are not formalized and documented. - The organization has no awareness of security controls measurement, validation, and assessment.
1	Ad-hoc and Partial	- Some of the framework streams are in place and partially defined. - Framework streams and activities are not formalized and documented. - The performed activities of the framework are ad-hoc, irregularly repeated, and sometimes are reactive manner. - The organization has limited awareness of security controls measurement, validation, and assessment.
2	Repeatable, Managed, and Documented	- All framework streams and activities are in place. - Framework streams and activities are approved by management, formalized, managed, and documented. - The performed activities of the framework are regularly repeated. - The organization has full awareness of security controls measurement, validation, and assessment.
3	Optimized and Automated	- All framework streams and activities are in place. - Framework streams and activities are approved by management, formalized, managed, and documented. - The performed activities of the framework are regularly repeated. - The organization has full awareness of security controls measurement, validation, and assessment. - The performed activities are continuously optimized and improved. - Framework streams and activities are partially automated.

Table 12 – Maturity Model

6. Framework Implementation

6.1. Security Control Based

Email Security Gateway (ESG) has been selected to illustrate all measurement activities. Email Security Gateway' effectiveness, efficacy, efficiency, and utilization will be measured, validated, and assessed, assuming that Email Security Gateway is already covered by the first stream for security controls identification.

6.1.1. Email Security Gateway Capabilities

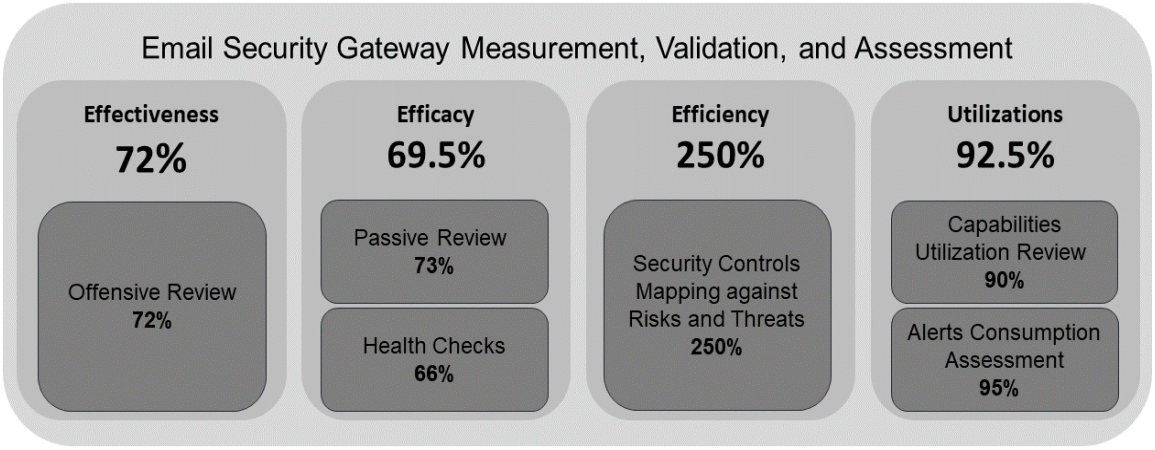
Table 13 shows Email Security Gateway's capabilities.

#	Capability	#	Item
1	Anti-Spam	6	Sender Blocklisting and Allowlisting
2	Anti-Spoof	7	Creation of Custom Rules
3	Anti-Virus	8	Attachment Sandboxing
4	URL Analysis	9	IP Reputation Validation
5	Attachment Blocklisting and Allowlisting	10	Directory Harvest Attack Prevention

Table 13 – Email Security Gateway Capabilities

6.1.2. Email Security Gateway Measurements, Validation, and Assessment

Effectiveness, efficacy, efficiency, and utilization of Email Security Gateway have been measured, validated, and assessed. Appendix B shows and illustrates a detailed walkthrough of each measurement activity. Graph 2 shows the overall measurement result for Email Security Gateway.



Graph 2 – Email Security Gateway Measurements

6.2. Threat Based

Two threats have been selected to illustrate the implementation of the framework with a threat-based approach, Ransomware and data leakage. The steps listed in Section 4, "Threats and Risk Measurements with the Framework," will be applied here.

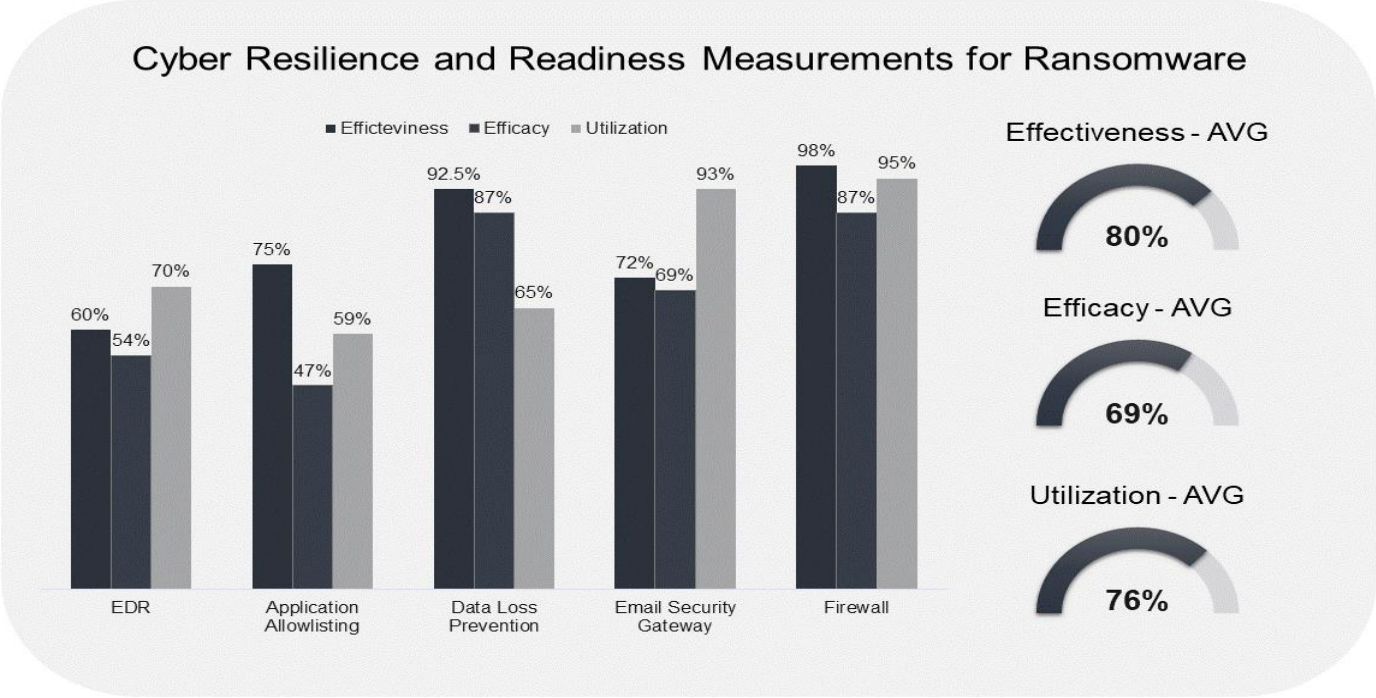
6.2.1. Ransomware

MITRE ATT&CK has been used to identify the tactic for Ransomware, and from that, all the associated security controls that mitigate the tactic have been identified. Table 14 shows the tactic and the mitigations.

#	Tactic ID	Name	Description	Mitigation
1	T1486	Data Encrypted for Impact	Adversaries may destroy data and files on specific systems or in large numbers on a network to interrupt availability to systems, services, and network resources. Data destruction is likely to render stored data irrecoverable by forensic techniques through overwriting files or data on local and remote drives.	- Application Control / Allowlisting (To prevent the execution of unauthorized software). - EDR (To isolate an endpoint to prevent Ransomware from propagating to other endpoints). - Network Segmentation Firewall (To prevent Ransomware from propagating to other endpoints). - Email Security Gateway (To prevent incoming malicious emails). - Data Loss Prevention (To prevent the usage of hard drives such as USB). - Data backup. (One of the mitigation but not a security control).

Table 14 – Ransomware Tactics and Mitigations

After identifying the associated security controls, effectiveness, efficacy, and utilization should be retrieved from the last measurements exercise. If any security control has not been assessed yet or the data is not within a year, it shall be measured and assessed first. Graph 3 shows the measurements of the resilience and readiness for Ransomware. However, the measurements for security controls other than Email Security Gateway are dummy data for illustration purposes only.



Graph 3 – Ransomware Measurements

6.2.2. Data Leakage

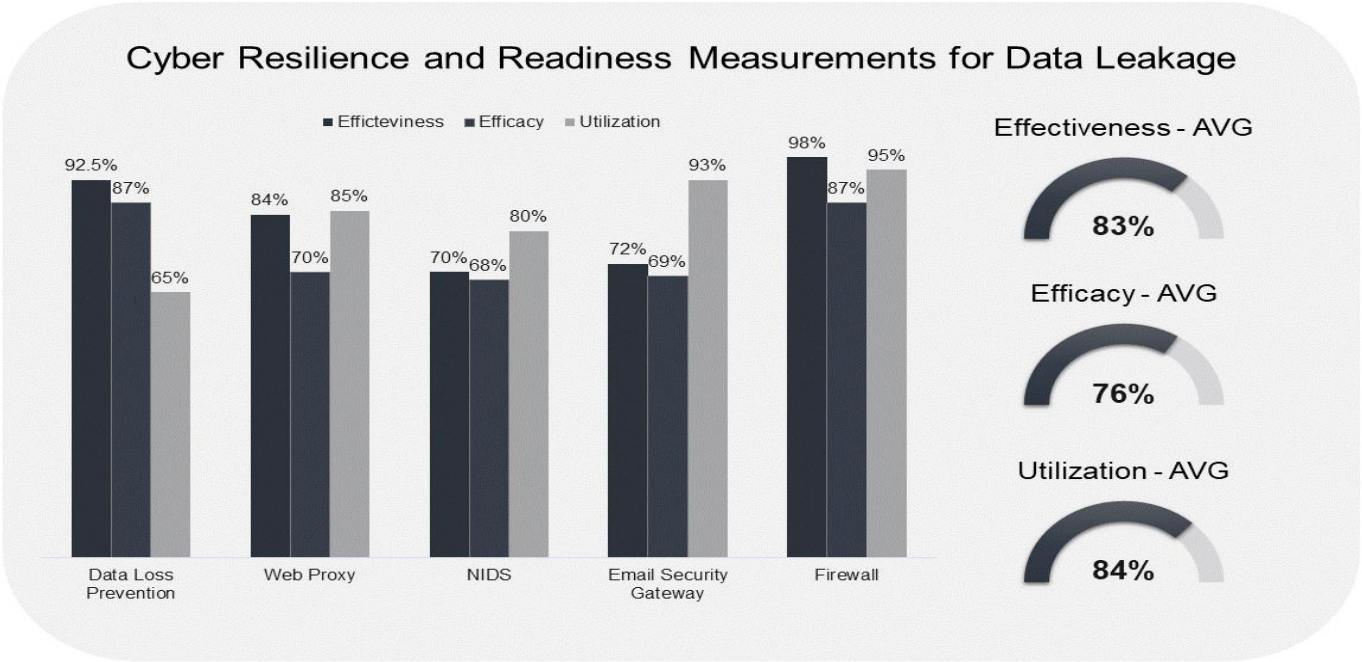
MITRE ATT&CK has been used to identify the tactics for exfiltration, and from that, the associated security controls that mitigate each tactic have been identified. Table 15 shows the tactics and the mitigations.

#	Tactic ID	Name	Description	Mitigation
1	T1020	Automated Exfiltration	Adversaries may exfiltrate data, such as sensitive documents, through the use of automated processing after being gathered during Collection.	- Data Loss Prevention (DLP). - Network Intrusion Detection System (NIDS). - Email Security Gateway (ESG).
2	T1030	Data Transfer Size Limits	An adversary may exfiltrate data in fixed size chunks instead of whole files or limit packet sizes below certain thresholds.	- Network Intrusion Detection System (NIDS). - Data Loss Prevention (DLP).
3	T1048	Exfiltration Over Alternative Protocol	Adversaries may steal data by exfiltrating it over a different protocol than that of the existing command and control channel.	- Network Intrusion Detection System (NIDS). - Data Loss Prevention (DLP). - Firewalls.

#	Tactic ID	Name	Description	Mitigation
4	T1041	Exfiltration Over C2 Channel	Adversaries may steal data by exfiltrating it over an existing command and control channel. Stolen data is encoded into the normal communications.	- Network Intrusion Detection System (NIDS). - Data Loss Prevention (DLP). - Firewalls.
5	T1052	Exfiltration Over Physical Medium	Adversaries may attempt to exfiltrate data via a physical medium, such as a removable drive.	- Data Loss Prevention (DLP).
6	T1567	Exfiltration Over Web Service	Adversaries may use an existing, legitimate external Web service to exfiltrate data rather than their primary command and control channel.	- Data Loss Prevention (DLP). - Web Proxy.

Table 15 – Exfiltration Tactics and Mitigations

After identifying the associated security controls, effectiveness, efficacy, and utilization should be retrieved from the last measurements exercise. The graph below shows the resilience and readiness for data leakage. However, the measurements for security controls other than Email Security Gateway are dummy data for illustration purposes only.



Graph 4 – Data Leakage Measurements

7. Conclusion

Cybersecurity landscape is continuously evolving with ever-changing cyber risks and new cyber threats arising every day. To keep up with the growth of threats and risks, there is always a newly introduced security control to the cybersecurity market with various alleged capabilities that will prevent and detect these threats or risks. This paper aims to empower organizations by realizing the full and actual potential of these security controls. The designed framework has addressed the gaps mentioned across the paper and included different measures the organizations could take to fill these gaps, such as having an ultimate reference for all security controls, having quantifiable responses to questions surrounding security controls' value by measuring, validating, and assessing security controls' effectiveness, efficacy, efficiency, and utilization, managing all issues related to security controls, and more. Furthermore, for an effective cybersecurity strategy, all three pillars of cybersecurity shall be considered: people, process, and technology. Optimizing the technological element: security controls, must be done along with having the proper process and people in place. Future enhancement of the framework will include a process to measure the effectiveness of the two other pillars, process and people.

References

AttackIQ, Inc. (2022, July 29). Real-time cybersecurity readiness. AttackIQ. https://attackiq.com/

Boehm, J., Lewis, C., Li, K., Wallance, D., & Dias, D. (2022, April 20). Cybersecurity trends: Looking over the horizon. McKinsey & Company. https://www.mckinsey.com/business-functions/risk-and-resilience/our-insights/cybersecurity/cybersecurity-trends-looking-over-the-horizon

Brooks, C. (2022, June 6). Alarming Cyber Statistics for Mid-Year 2022 That You Need To Know. Forbes. https://www.forbes.com/sites/chuckbrooks/2022/06/03/alarming-cyber-statistics-for-mid-year-2022-that-you-need-to-know/?sh=3a1c24227864

Debar, H. (2019, February 3). Cybersecurity: high costs for companies. The Conversation. https://theconversation.com/cybersecurity-high-costs-for-companies-110807

eicar. (2006). Download Anti Malware Testfile – Eicar. www.eicar.org. https://www.eicar.org/download-anti-malware-testfile/

Exfiltration, Tactic TA0010 - Enterprise | MITRE ATT&CK®. (2018, October 17). MITRE ATT&CK. https://attack.mitre.org/tactics/TA0010/

Kim, K., (2020, November, 04). MGT514: Security Strategic Planning, Policy, and Leadership. https://www.sans.org/cyber-security-courses/security-strategic-planning-policy-leadership/

Mandiant, (2022). Security Validation. Mandiant. https://www.mandiant.com/advantage/security-validation

MalShare. (2021). MalShare. https://malshare.com

Moyal, M. (2022, June 23). Cymulate - Extended Security Posture Management Platform. Cymulate. https://cymulate.com/

NIST. (2016). security control - Glossary | CSRC. https://csrc.nist.gov/glossary/term/security_control

Penetration Testing or Red Teaming? A Decision Maker's Guide. (2020, October 15). Aon. https://www.aon.com/cyber-solutions/thinking/penetration-testing-or-red-teaming/

PowerArchiver. (1998). PowerArchiver. https://www.powerarchiver.com/

SafeBreach. (2022, August 4). Breach and Attack Simulation Platforms | New Solutions. https://www.safebreach.com/

Sobers, R. (2022). 166 Cybersecurity Statistics and Trends [updated 2022]. VARONIS. https://www.varonis.com/blog/cybersecurity-statistics

Tierney, M. (2020, July 24). Quantitative Risk Analysis: Annual Loss Expectancy. Netwrix. https://blog.netwrix.com/2020/07/24/annual-loss-expectancy-and-quantitative-risk-

analysis/#:%7E:text=Quantitative%20risk%20analysis%20is%20an,effort%20is%20worth%20the%20investment.

U. (2022). urlscan Phishing URL Feed - urlscan.io. URLScan https://urlscan.io/pricing/phishingfeed/

What is Annualized loss expectancy. (2019, May 11). Capital.Com. https://capital.com/annualized-loss-expectancy-definition

Wapack Labs. (2022b, September 18). New Pony Loader Obfuscation Technique via Smoke Loader. Retrieved September 18, 2022, from https://wapacklabs.blogspot.com/2018/04/new-pony-loader-obfuscation-technique.html

Appendix A

#	Item	#	Item
1	Vendor Name.	10	License Type.
2	Product Name.	11	License Expiry Date.
3	Product Version.	12	Assets Type (Appliance, Virtual Machine, or Physical Server. Applicable for On-premise and Hybrid only).
4	Type (Preventive, Detective, or Corrective).	13	Management Interface IP Address and Port (For both Production and DR, if there is a redundancy).
5	Delivery Method (On-premise, Cloud, Hybrid, or Service).	14	Assets OS Type (Applicable for On-premise and Hybrid only).
6	Delivery Type (Application, Website, etc.).	15	Assets OS Version (Applicable for On-premise and Hybrid only. For both Production and DR, if there is a redundancy).
7	Redundant? (Yes, if there is a DR environment for the security control, or No, if there is no DR environment for the security control).	16	Assets IP Addresses (Applicable for On-premise and Hybrid only. For both Production and DR, if there is a redundancy).
8	Business Owner.	17	Assets Hostnames (Applicable for On-premise and Hybrid only. For both Production and DR, if there is a redundancy).
9	Technical Owner.		

Table 16 – Security Controls Inventory

#	Item	#	Item
1	Security Control.	7	Assignee.
2	Description of Issue/Problem.	8	Stream Aspect (Efficiency, Efficacy, Efficiency, or Utilization).
3	Impact.	9	Suggested/Recommended Action.
4	Criticality.	10	Identification Source. (The issue has been identified by which activity?).
5	Reported/Identified Date.	11	Validation Result. (Retest to verify that the issue has been resolved).
6	Status.	12	Closure Date.

Table 17 – Issue Register

Appendix B

1. Measuring Email Security Gateway' Effectiveness

1.1. Offensive Review

Penetration testing has been conducted to validate and assess the effectiveness of Email Security Gateway capabilities. The scenarios in table 18 have been conducted to measure, validate, and assess Email Security Gateway.

#	Capability	Test Scenario	Test Result
1	Anti-Spoof	Historical records for 20 malicious emails have been reviewed and assessed to validate the effectiveness of anti-spoof capability. 18 emails were not spoofed, and 2 emails were spoofed and were not detected by the anti-spoof filter. These numbers have been converted to be on the same scale as other test numbers.	4 Prevented 1 Bypassed
2	Anti-Spam	Historical records for the blocked spam emails and the bypassed emails (these emails were identified using Case Management System as they were reported by users) for the past month have been reviewed to validate the effectiveness of anti-spam capability. 350 spam emails with unique senders were blocked, and 30 spam emails with unique senders were bypassed. These numbers have been converted to be on the same scale as other test numbers.	4 Prevented 1 Bypassed
3	Anti-Virus	An inbound email has been sent with attaching a virus that has been obtained from Eicar.	1 Prevented
4	Anti-Virus	An inbound email has been sent with attaching a compressed virus (.7z file format). Eicar has been used to obtain a virus sample.	1 Prevented
5	Anti-Virus	An inbound email has been sent with attaching a virus that has been embedded in a word document. Eicar has been used for the virus sample.	1 Bypasses
6	Attachment Sandboxing	Three inbound emails have been sent with attaching malware. The hash for Eicar sample is known to anti-virus databases, so it cannot be used here to test sandbox capability as it will be detected by the anti-virus filter first. However, there are many other sources that can be used to obtain malware samples. Malshare has been used for this test. 3 malware samples have been used.	2 Prevented 1 Bypassed
7	Attachment Sandboxing	An inbound email has been sent with encoding the malware and attaching it. Malshare has been used to obtain malware samples, and PowerArchiver has been used to encode the file to uuencode (.uue file extension).	1 Bypasses

#	Capability	Test Scenario	Test Result
8	URL Analysis	Five inbound emails with malicious/phishing URLs have been sent. There are many sources that can be used to obtain malicious URLs. However, for this test, URLScan feeds have been used. The test has been conducted five times with five different URLs.	3 Prevented 2 Bypassed
9	Attachment Blocklisting	An inbound email has been sent with an executable attached (.exe is in the blocked extension for inbound emails).	1 Prevented
10	Attachment Blocklisting	An inbound email has been sent with encoding an executable and attaching it.	1 Bypassed
11	Attachment Blocklisting	An outbound email has been sent with attaching an executable that has been renamed to another file extension.	1 Prevented
12	Sender Blocklisting	The test email has been added to the blocked list, and an inbound email has been sent from the test email.	1 Prevented
13	Creation of Custom Rules	One of the previously created custom rules has been selected to test the effectiveness of creating custom rules. The same defined logic in this rule has been used to send an inbound email. The selected rule has been created to prevent any impersonation attempt against the organization' C-Levels. The rule will block any email that contains in the header the full name of a C-Level and not coming from his actual personal email. Both lists for C-Levels' names and their personal email addresses are predefined in the email security gateway.	1 Prevented
14	IP Reputation Validation	Historical records have been reviewed to validate the effectiveness of this capability. The logs for the terminated connections from the email security gateway have been exported and reviewed with validating the reputation of IP addresses.	1 Prevented
15	Directory Harvest Attack Prevention	The current configuration for this capability is to limit the number of messages per IP address to 20 messages in 15 minutes. A script has been developed to send 21 messages within less than 15 minutes.	1 Prevented

Table 18 – Offensive Testing for ESG

Below is the calculated formula for the offensive review:

$$KCI = \frac{\sum Prevented\ Attempts + \frac{\sum Alerted\ Attempts}{2}}{\sum Attempts} \times 100 = \frac{21}{29} \times 100 = 72\%$$

2. Measuring Email Security Gateway' Efficacy

2.1. Passive Review

The passive review report included table 19 for gaps and observations.

#	Aspect	Gap	Impact	Corrective Action	Criticality
1	Configurations Review	Inbound emails are configured to bypass attachment sandboxing filter if the size of the attachment is greater than 2.5 MB.	Malicious attachments greater than 2.5 MB will bypass sandboxing filter and might be delivered to the end-user.	The configured threshold for this has to be aligned with the configured allowed size of attachments.	High
2	Configurations Review	The current configuration for attachments is blocklisting. Allowlisting should be used.	If blocklisting is used, there is a possibility of missing some unwanted and unneeded extensions.	The allowed extensions should be defined, and all other extensions should be prevented using allowlisting approach.	High
3	Configurations Review	URL analysis is configured to bypass email inspection if the size of the email is greater than 3 MB.	Emails with malicious URLs greater than 3 MB will bypass URL analysis filter and might be delivered to the end-user.	The configured threshold for this has to be aligned with the configured size of the allowed emails.	High
4	Configurations Review	Recipients validation and authentication is not configured.	Not validating the recipients might overwhelm other filters, such as sandbox and URL analysis with unnecessary emails that can be dropped without validation by other filters.	Enable recipients validation and authentication.	High

#	Aspect	Gap	Impact	Corrective Action	Criticality
5	Prevention Rules Review	There are many domains in the whitelist and these domains have not been reviewed recently.	Some domains in the list may no longer be needed to be whitelisted, and whitelisting them will allow them to bypass some security filters.	Adding a domain to senders whitelist shall be done carefully with periodic review for the allowed senders.	Medium
6	Prevention Rules Review	There is a mismatch in the created custom rules between production and DR environments.	As the DR environment is missing some rules, not all the security measures that apply to production will apply to DR.	The developed custom rules should be in both environments.	Medium
7	Permission Review	SOC analysts have insufficient permissions, which limits them from creating and scheduling custom reports.	SOC analysts will not be able to create or schedule custom reports, which can help in their investigations.	SOC analysts should have the right permission.	Low

Table 19 – Passive Review - Gaps

Table 20 shows the assigned rating as per the identified gaps.

Aspect	Rating
Configurations Review	1
Prevention Rules Review	2
Coverage Review	3
Permissions Review	2
Alert Fatigue	3

Table 20 – Passive Review – Rating

Below is the calculated formula for the passive review:

$$Efficacy\ Rate = \frac{\sum Rating\ for\ each\ Aspect}{15} \times 100 = \frac{11}{15} \times 100 = 73\%$$

2.2. Health Check

A health check has been conducted by the vendor for Email Security Gateway, and the report included the gaps and observations in table 21.

#	Aspect	Gap	Impact	Corrective Action	Criticality
1	System Resources Review	There is no high availability in production (HA) as there is only one appliance in production and one in DR environments.	Email Security Gateway is one of the most critical security controls. Not having high availability in production may result in security concerns, operational issues, or business impact.	Production environment should has two appliances for high availability (HA).	High
2	Product Version and Hotfixes Review	The product version is outdated.	The new version has fixed some issues and introduced new features.	Upgrade the product version.	Medium
3	Product Backups Review	Configuration backups are being managed manually.	Having the backup as a manual activity may result in human error.	Schedule a task to automate taking the backups.	High
4	Logging Review	Current storage space is not sufficient to handle the configured retention period.	Some records will be overwritten.	Configure a task to achieve older portions and validate SIEM integration.	Medium
5	System Errors Review	Enable to get NTP time.	Using system local time may result in an inconsistency between other security controls' time.	Check NTP configuration and firewall rules.	Low

Table 21 – Health Check – Gaps

Table 23 shows the assigned rating as per the identified gaps.

Aspect	Rating
System Resources Review	1
Product Version and Hotfixes Review	2
Product Backups Review	1
Logging Review	2
Licenses Review	3
System Errors Review	3

Table 23 – Health Check – Rating

Below is the calculated formula for the health check:

$$Efficacy\ Rate = \frac{\sum Rating\ for\ each\ Aspect}{18} \times 100 = \frac{12}{18} \times 100 = 66\%$$

2.3. Overall Measurement of Security Controls' Efficacy

$$Efficacy\ Rate = \frac{Passive\ Review\% + Health\ Check\%}{2} = \frac{73\% + 66\%}{2} = 69.5\%$$

3. Measuring Email Security Gateway' Efficiency

3.1. Mapping against Risks and Threats

Email Security Solution mitigates three risks: phishing and spoofed emails, malicious software (virus and malware), and data leakage. The ALE for these risks has been obtained from the previously conducted quantitative risk assessment. ALE for all the five threats is 5 Million, and Email Security Gateway costs 2 Million (including product cost, licenses for a year, and support service for a year).

Below is the calculated formula for efficiency:

$$ROI = \frac{\sum R1, R2, R3, \ldots}{Cost\ of\ Investment} \times 100 = \frac{5000000}{2000000} \times 100 = 250\%$$

4. Measuring Email Security Gateway' Utilization

4.1. Capabilities Utilization Review

A utilization review has been conducted, and table 24 shows the utilization status and value for each capability.

#	Capability	Utilization Status	Value	#	Capability	Utilization Status	Value
1	Anti-Spam	Fully Utilized	1	6	Sender Blocklisting and Allowlisting	Fully Utilized	1
2	Anti-Spoof	Partially Utilized	1	7	Creation of Custom Rules	Partially Utilized	0.5
3	Anti-Virus	Fully Utilized	1	8	Attachment Sandboxing	Partially Utilized	1
4	URL Analysis	Fully Utilized	1	9	IP Reputation Validation	Fully Utilized	1
5	Attachment Blocklisting and Allowlisting	Partially Utilized	0.5	10	Directory Harvest Attack Prevention	Fully Utilized	1

Table 24 – Utilization Review

Below is the calculated formula for the utilization review:

$$Utilization\ Rate = \frac{\sum Utilization\ Values}{\sum Capabilities} \times 100 = \frac{9}{10} \times 100 = 90\%$$

4.2. Alerts Consumption Assessment

The alerts for Anti-Virus and Attachment Sandbox filters for the past 6 months have been exported from the SIEM solution. 1500 alerts have been triggered in 165 days. All email analysis cases which are related to these two filters have been exported from Cases Management System, and there are 160 cases that were created in 156 days.

$$Utilization\ Rate = \frac{\sum Days\ with\ Cases}{\sum Days\ with\ Alerts} \times 100 = \frac{156}{165} \times 100 = 95\%$$

4.3. Overall Measurement of Email Security Gateway Utilization

$$Utilization\ Rate = \frac{\text{Capabilities Utilization\%} + \text{Alerts Consumption\%}}{2}$$

$$= \frac{90\% + 95\%}{2} = 92.5\%$$