International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

Unified Management of Cyber Security and Compliance through a Comprehensive Platform

Dr. Nischith. S[1], Dr. Rakesh D[2]

[1]BIMS, University of Mysore, Mysuru, India.
[2]JSS – Centre for Management Studies, JSS Science and Technology University, Mysuru, India.

Abstract:
These days, any information security product or service used in an organization is a stand-alone solution. Examples include information risk management, data security, auditing, and incident management. Since different organizations use different services from different providers, there is currently no single platform or architecture that can address all of an organization's fundamental information security procedures in one easy step. Because of this, businesses must spend a significant amount of money on separate services in order to meet the information security standards that are necessary for their businesses. These dispersed services lead to an increase in physical and manual labor, disorganized processes, and a lack of clarity regarding all information security-related business issues.
To solve these issues, the approach covered in this article combines information security as a service with end-to-end platform/framework to give organizations a single framework for all information security-related organizational aspects. A single service that can handle every information security-related work for the company, including risk assessment, mitigation, vulnerability assessment, incident management, threat analytics, risk response management, and auditing. This will assist the company in spending less money on a wider range of security-related services.

Keywords: Cyber Security, Compliance Management, Threat Detection, ISO 27001, GDPR, PCI DSS, Employee Awareness

Introduction:

Cybersecurity is the defense against cyberattacks of hardware, software, and data on internet-connected devices. In the context of computing, security refers to both physical and cyber security, which are employed by enterprises to guard against illegal access to data centers and other computing systems. Information security, a subset of cyber security, aims to protect the availability, confidentiality, and integrity of data.
In order to maintain corporate intelligence (CIA), organizations must adhere to certain cyber security standards. To do this, they must conduct internal audits, information risk assessments, vulnerability assessments, compliance management, IT audits, and employee education regarding information security.
The method presented in this paper is based on an analysis of the market's current state and the strategies that businesses are employing to ensure information security within their enterprises. The research's conclusions show that all information security products and services that are now used in organizations are stand-alone offerings. Examples of these services include information risk management, auditing, incident management, and data security. Since different organizations use different services from different

providers, there is currently no single platform or architecture that can address all of an organization's fundamental information security procedures in one easy step.

Because of this, businesses must spend a significant amount of money on separate services in order to meet the information security standards that are necessary for their businesses. These dispersed services lead to an increase in physical and manual labor, disorganized processes, and a lack of clarity regarding all information security-related business issues. Because of these standalone services, businesses must pay for each service separately in order to use them. This drives up costs, discourages small and new start-ups from using these services, and leaves them open to attack.

In order to address this issue, this paper proposes a framework and a working model for an information security service that will cover nearly all of the necessary cyber security components for a business, including information risk assessment, compliance management, IT auditing, threat detection, threat analytics, vulnerability assessment, and raising employee awareness of information security. The most significant part of this project is that it will be an automation service that, with very little user intervention, will automate all of the aforementioned cyber security aspects inside of a business using a single platform or service. The project's objective is to offer a variety of affordable cyber security services on a single platform, making it accessible to even small businesses.

Services offered by the System:

This article proposes a service that automates processes using a single platform at a very cheap cost; this sets it apart from other services that are already offered in the market.

The Services offered are as followed -

Risk Assessment:

The system creates a risk assessment matrix and divides the risks into three risk levels: High, Medium, and Low—based on the likelihood and severity of the threats that are found. The risks are broken down into several areas, including financial, external, employee, management, and customer. The system offers solutions to lower the risk level of specific risks [5].

Compliance Auditing:

The software includes PCI DSS and ISO 27001 standard questionnaires for compliance auditing. To automate the procedure, there is a feature that allows you to answer each question. The system will provide actions that can be performed to implement the control if any of the standard's controls are not in compliance.

Vulnerability Assessment:

An open source tool for evaluating a web application's vulnerabilities is offered by the platform. It counts the instances of the vulnerabilities in the particular URL that was mentioned. Every vulnerability has been categorized as high, medium, or low priority.

Threat Detection:

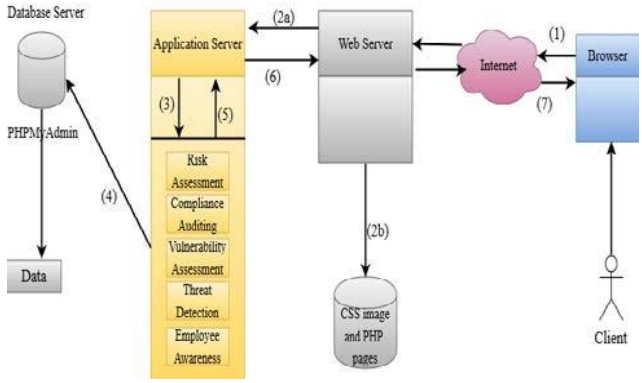
The software has a phishing URL detection feature that assesses whether a given URL is a phishing link. Using several aspects of the connection, we have employed a machine learning method called Support

Vector Machine to identify phishing URLs. This categorization system establishes if a given link is secure to click on.

Employee Awareness:

Any organization's first line of defence is its workforce. Regretfully, they also represent the weakest point in terms of network security. It is the responsibility of a company to enhance the first line of defence by training staff members about cyber security. We have integrated a chatbot with the organization's security team within the platform for the benefit of the staff. They will benefit from having their questions answered by the team about cyber security. In order to inform the staff members on the most recent privacy and data protection legislation, we have also included a GDPR bot in the platform.

Working of the Proposed System:



Working of the proposed system

The above diagram explains seven steps:

- The client connects to the application server, which hosts the applications, and the backend web server, which hosts all the web pages and PHP files needed for database connectivity, while attempting to access services via a web browser.
- The Risk Assessment, Compliance Auditing, Vulnerability Assessment, Threat Detection, and Employee Awareness services are all accessible through the Application Server.
- The database server, which houses the program's logic files and backend data, is referred to by the application server.
- After gaining access to the application data, the application server is accessed again.
- The web server receives pertinent and processed data from the application server.
- Through a web browser, the client receives the processed data from the application server from the web server.

Analysis of the System:

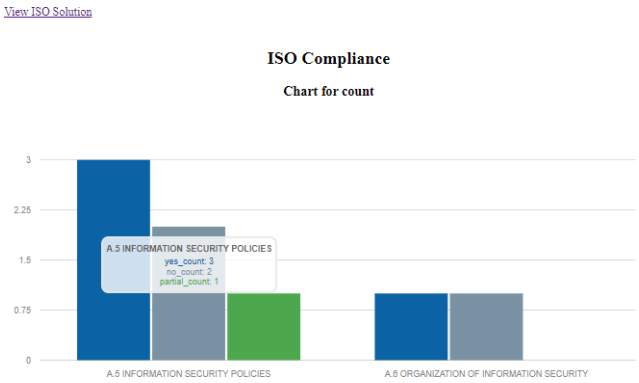
The following describes each of these security requirements/problems for any company and how this article resolves them using these services:

Automated Compliance

The practice of making sure that a group of people are abiding by a specific set of regulations is known as compliance management. While the procedure is what oversees their compliance, these regulations make

reference to the compliance standard and benchmark.

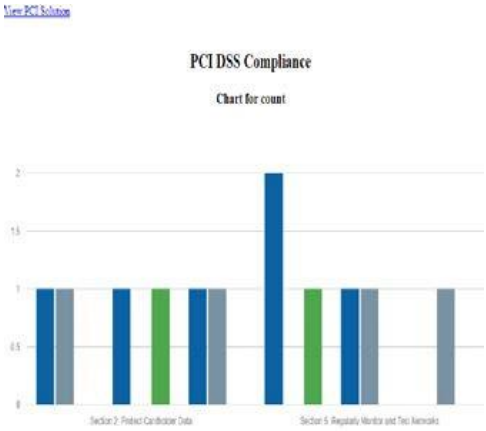
Different approaches may be taken to management compliance. A combination of protocols, guidelines, records, internal and external audits, security measures, and technology enforcement may be used. Currently, compliance with PCI DSS and ISO 27001 standards is being verified in this service[10]. Based on prepared sets of policies for both PCI DSS and ISO 27001, this service creates a report that incorporates the auditor's observations. The established sets of policies assist the auditor in choosing the relevant policies from the available policy sets.



According to the preceding portrayal, noncompliant items are given a way to become compliant by falling under compliance policies; the same is represented below.

Id	Question	Response	Solution
1	Do Security policies exist?	Yes	You are compliant
2	Are all policies approved by management?	Yes	You are compliant
3	Are policies properly communicated to employees?	Yes	You are compliant
4	Are security policies subject to review?	No	The organization must review the security policies time to time. The purpose of the review is to ensure the continued suitability, adequacy and effectiveness of the policies
5	Are the reviews conducted at regular intervals?	No	organizations are required to review the adopted Information Security Policy annually at a minimum
6	Are reviews conducted when circumstances change?	Partially	organizations should review their Information Security Policy on a more frequent basis particularly if significant changes occur within their organization that may have an impact on the effectiveness of the policy
7	Are responsibilities for the protection of individual assets, and for carrying out specific security processes, clearly identified and defined and communicated to the relevant parties?	Yes	You are compliant
8	Are duties and areas of responsibility separated, in order to reduce opportunities for unauthorized modification or misuse of information, or services?	No	This is the solution

Similar to this, a prefabricated policy set for PCI DSS is provided. An auditor verifies this policy set's compliance and generates a graphical report. Based on the amount of terms that are noncompliant, they are then given a solution set.



Threat Analytics and Detection

Threat analytics uses machine learning to anticipate and identify impending risks, offering a means of defending the company against sophisticated attacks [1].

Given that we live in an information age, a vast amount of organizational data is vulnerable to both novel and recurring forms of attack. This service includes a threat detection mechanism that makes use of machine learning to identify potential threats in the future as well as active phishing sites. This helps to keep organizations prepared for attacks in advance and deal with them. [2][3].

Here, a dataset of 41000 records with 32 distinct phishing site features is utilized for detection and prediction. All of these records were evaluated and trained to identify patterns for new phishing attempts.

Vulnerability Assessment and penetration testing:

Penetrating By assessing the system or network using a variety of harmful tactics, penetration testing, also known as pen-testing, is a methodical approach to find security flaws in an application. Hacking into a network or website with the goal of exposing issues and fixing them is undoubtedly a moral course of action[7].

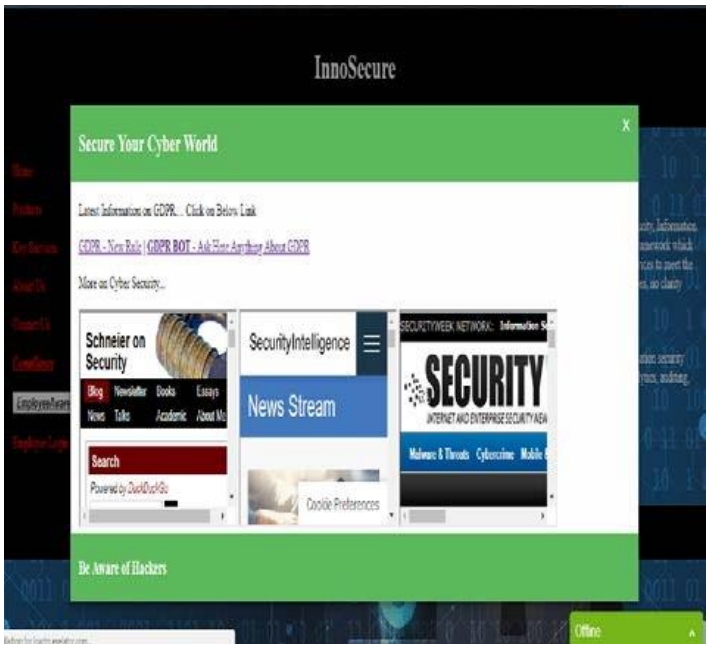
In order to provide this service, we use an open source program that can infiltrate any website and determine whether or not it is susceptible to attacks [8].

A report is prepared based on the tool's results, displaying the results along with the appropriate solutions that are wanted. Each vulnerability is categorized according to its severity, such as high, medium, and low.

Employee Awareness

Sophisticated technology may be the only weapon against a variety of cyber security concerns, such as sophisticated malware. However, employees are usually the biggest source of vulnerability on a daily basis. in order for the employees to be fully informed of their obligations with relation to organizational data [9].

This service provides employees with regular updates about the newest cyber-attacks and dangers. A sample of the service is provided below.



Risk Assessment;

An IT risk assessment is a written evaluation of the potential risks, either natural or man-made, that a business may encounter. These risks are tallied according to how likely it is that they will materialize, and their impact on the operation is then multiplied. One can use this result as a value to determine whether they should disregard the threat or take protective measures to minimize or eradicate it [4].

Here, in this service, risks are classified as High, Medium, or Low depending on how serious they are.

This tool identifies specific hazards based on the observations of the risk assessment team. It then generates a risk assessment matrix that illustrates the risk's severity and likelihood of occurrence. Risks that fall within the Red Zone have a high possibility of happening, and so forth [5]. Below is a snippet of this matrix.

Here, risks are further divided into categories such as management, employee, customer, financial, and external risks. They are then divided into percentages of maximum occurrence in each category based on the likelihood of each risk occurring.

A glimpse of it can be seen below.

Conclusion:

This paper proposes an approach to cyber security for any organization. The organization can use an automated tool to check their IT environment, assess risks, and detect both current and emerging threats. They can also perform vulnerability assessments, employee awareness campaigns, compliance management, and risk assessments. Once all of these assessments are completed based on the requirements, the system offers the appropriate solutions. The key feature that sets this system apart from others is that it is a single, integrated service that offers every cyber security service conceivable that a company could need. This makes the service extremely affordable, enabling even small businesses to take advantage of it.

References:

1. Iffat A. Gheyas and Ali E. Abdallah. Detection and prediction of insider threats to cyber security: a systematic literature review and meta-analysis. Cross Marks 2016.
2. Malek Ben Salem, Shlomo Hershkop and Salvatore J. Stolfo. A Survey of Insider AttackDetection Research. Springer. Insider Attack and Cyber Securitypp 69-90, 2016.
3. Asaf Shabtai, Robert Moskovitch Yuval and Elovici Chanan Glezer. Detection of malicious code by applying machine learning classifiers on static features: A state-of-the- art survey. Information Security Technical Report. Volume 14, Issue 1, February 2009, Pages 16-29.

4. Adrian Munteanu, Alexandru Ioan Cuza University. Information Security Risk Assessment: The Qualitative Versus Quantitative Dilemma. Managing Information in the Digital Economy: Issues & Solutions 227.
5. L. Pan & A. Tomlinson. A Systematic Review Of Information Security Risk Assessment. International Journal Of Safety And Security Eng., Vol. 6, No. 2 (2016) 270–281.
6. Xueni Li, Guanggang Geng, Zhiwei Yan. Phishing detection based on newly registered domains. IEEE International Conference on Big Data,2016.
7. Konstantinos Xynos, Iain Sutherland, Huw Read. Penetration Testing and Vulnerability Assessments: A Professional Approach. International Cyber Resilience conference 2010.
8. Prashant S. Shinde, Shrikant B. Ardhapurkar. Cyber security analysis using vulnerability assessment and penetration testing. Futuristic Trends in Research and Innovation for Social Welfare, IEEE, 06 October 2016.
9. Ling Li, Li Xu, Hong Chen. Cyber Security Awareness and Its Impact on Employee's Behavior. Research and Practical Issues of Enterprise Information Systems. Vienna, Austria, December 13–14, 2016, Proceedings (pp.103-111)
10. Tolga Mataracioglu. Comparison of PCI DSS and ISO/IEC 27001 Standards, ISACA Journal Volume 1, 2016.
11. Ankit Kumar Jain and B. B. Gupta, PHISH-SAFE: URL Features-Based Phishing Detection System Using Machine Learning.