



Evaluating Regulatory and Compliance Frameworks for Safeguarding Financial Systems Against Cyber Threats

Poi Tamrakar

Dr. D. Y. Patil School of Science
and Technology, Dr. D. Y. Patil Vidyapeeth,
Pune-411033, India
Email: poi.tamrakar@gmail.com

Sandhya Rajput

G H Raison International skill tech
University, Pune
Email: sandhya.rajput@ghristu.edu.in

Abstract

The initiatives implemented by both governmental and non-governmental organizations to mitigate cyber threats in financial systems have played a crucial role in ensuring the integrity, confidentiality, and availability of financial data remain uncompromised. This assessment aims to evaluate these frameworks in relation to international regulations, national laws and policies, and industry standards. Key regulatory structures analyzed for their role in managing cyber risks include GDPR, FINRA, and PCI DSS. Based on the findings of this study, user rights protection, auditing, and incident response are identified as fundamental components of cybersecurity. Additionally, the paper highlights the significance of threat intelligence sharing between regulators and financial institutions to strengthen defenses against sophisticated cyber threats. The study also examines the challenges associated with adhering to existing cybersecurity standards, particularly in the face of evolving cyber threats and the rapid advancement of financial technologies. Furthermore, it explores the legal consequences of non-compliance, including potential sanctions and prosecutions for firms and individuals. By analyzing current legal frameworks and enforcement mechanisms, this evaluation provides insights into the state of financial sector regulations in combating cyber threats and offers recommendations for enhancing security measures.

Keywords: *Combat Cyber Threats, Financial Technologies, Cybersecurity, Cyber Criminals*

Introduction

The 'complexity and the incidence of these threats increase' depicts that new challenges are on the rise and this presents a myriad of threats to the financial systems' stability and security all over the world. As the actors that use huge amounts of data, and as managing key financial frameworks, the financial institutions are, thus,

continue to attract the cyber criminals' attention. Such threats therefore can lead to hefty monetary losses, lack of confidence from people, and even economic imbalance (Bertam et.al 2019). Therefore, satisfactory and strict regulation and governance are inevitable not to incur these risks and to make the financial systems cyber secure. In the European Union, such law is GDPR, in the United States of America the law is the "Gramm-Leach-Bliley Act (GLBA)", and in United Kingdom cybersecurity understandings are guided by the Financial Conduct Authority (FCA) regulations that help to implement high level cybersecurity. These regulations compel the firms in the financial sector to apply stringent measures in security and at the same time assess and document any security threats that may prevail in their firms alongside reporting security incidences in the right manner. There is need to compliance with these regulatory requisites with an aim of maintaining the qualities of financial data such as integrity, confidentiality and availability. Moreover, other guidelines such as the Payment Card Industry Data Security Standard (PCI DSS) and National Institute of Standards and Technology (NIST) Cybersecurity Framework spells down more technical and operational control to prevent CTRs. These standards form the basis of a set of procedures that include identification, prevention, reporting, control and rehabilitation of a cyber threat (Buckley et.al 2019). This is comparatively a recent phenomenon under which such frameworks are integrated into the live environment of FI to enhance the capacity to respond to cyber threats. However, as there is continuous evolution in the threats in cyberspace, it implies that there is progressive development in the regulatory instruments notwithstanding the formulation of the aforementioned cases. The working environment of financial institutions is rather multifaceted: in addition to many other compliance standards, they must also be aligned with technological changes and possible threats. Cited penalties are: legal consequences, significant amounts of revenues, and business images more explaining why there should be compliance to regulations. The objective of the paper is to analyse the existing and the planned legal and compliance initiatives regarding the probabilities of protecting the financial systems from cyber threats (Basel et.al 2018). By identifying such sections of the current regulations and standards as critical for organizations today as well as evaluating organizations' adherence to these best practices, the study will detail the current state of practices. Thus, the subject of this research, one should note, intends to contribute to increasing the understanding of the problem and, thus, suggest a way to assist the world financial system in diminishing the exposure of its structures to cyber threats (Shavers et.al 2019).



Figure 1 Cybersecurity Compliance Plan [23]

Research Background

It is detected in this paper that financial sector as one of substructures of international economy infrastructure is enduring patent and dynamic bare cyber risks that can enhance to disastrous result. Altogether, it can be concluded that cyber-attacks that are aimed at financial institutions put consumers' confidence at risk and lead to severe financial consequences, as well as loss, in the sphere of economy. Such heinous attacks in the recent past like the Equifax data theft in 2017 and the JPMorgan Chase rampage in 2014, are proof that even the financial systems are vulnerable to cyber-attacks which is why more protection has to be put in place. Events like these have led the world's regulating authorities to put in place measures that were deemed to increase the security of financial organizations against cyber threats. This is especially true in regard to the aspect of regulation and compliance because they describe norms regarding cybersecurity practice in the sector (Bouveret et.al 2018). The GDPR passed by the European Union can be considered one of the major legislation toward the enhancement of protection and privacy of data. The GDPR greatly enhanced the data control and reply on the notice of the personal data breach and/RWA for non-compliance, therefore, the financial institutions will pay more attention to the cybersecurity. Similarly, the American Gramm-Leach-Bliley Act²³ calls on those financial firms to protect consumer's non-heralded/financial information and sets out the basic information security framework. In addition to the above stipulations, other measure that still seek to protect financial information are; Payment Card Industry Data Security Standard (PCI DSS) and National Institute of Standards and Technology (NIST) Cybersecurity Framework. For instance PCI DSS handles issues to do with the protection of credit card transactions via security measures Thus; The NIST is framework that assists organizations with approaches on how to address and reduce cybersecurity risks (Caulfield et.al 2020). Nevertheless, the financial sector being one of the most important ones is suffering from numerous cyber security problems at this stage. The technologically improved, the new and complex type of crimes, especially the cyber ones and the integration of the financial markets on a global level imply the need for periodic reinforcement and upgrade of the measures implemented. Moreover, financial institutions' risks, controls and related procedures should offer improved levels of protection, operation effectiveness and compliance. The research background pays special attention to the fact that it is essential to review the current legislation and

managerial initiatives aimed at protecting the financial systems from cyber-threats. Hence, this research aims at identifying the efficiency of the existing standards and the gaps in the present state to aid the financial institution in order to enable it to prevent against cyber threats. The end benefit is to support the effort of creating stronger Financial systems which are not vulnerable to challenges in the cyberspace (Choo et.al 2017).

Research Objective

- To evaluate the effectiveness of existing regulatory frameworks
- To analyze industry-specific compliance standards
- To identify gaps and challenges in regulatory compliance
- To propose recommendations for enhancing cybersecurity frameworks

Research Problems

The technological revolution and the complexity of cyber threats in progression accelerate to put pressure on the financial sector, thus the need for appropriate legal and risk management frameworks for the protection of the financial system. Nevertheless, the ability of the above frameworks in managing cyber risks still stands out as a major issue. The existing regulatory measures like GDPR and GLBA have established the necessary and adequate cybersecurity standards but still, the financial sector is more vulnerable to cyber-attack. It is clearly evident that these regulations are either inadequate or not implemented properly. Also, other industry-specific standards such as the Payment Card Industry Data Security Standard (PCI DSS) and the National Institute of Standards and Technology (NIST) Cybersecurity Framework offers more elaborate measures on the protection of financial data. But even in this sphere, financial institutions have difficulties regarding compliance, as the threats are numerous and constantly changing. The difficulties of attaining and sustaining compliance combined with the statuses and evolutions of cyber threats suggest that there may be flaws and shortcomings in today's regulatory compliance paradigms (Garcia-Murillo et.al 2018). The main research question is thus an assessment of the existing frameworks and the difficulties experienced by financial institutions in implementing the models. It is also necessary to evaluate whether these frameworks meet the needs of a modern, rapidly developing environment, and define the gaps in the approaches under consideration. Thus, the research's goal is to reveal these gaps and challenges and provide practical recommendations for improving authorities and compliance facilities to strengthen financial systems against cyber threats. This assessment is necessary to design and build even more effective financial structures that will be secure against the continually rising cyber threat.

Literature Review

Evaluating the effectiveness of existing regulatory frameworks Scholarship on ways at which it is feasible to assess the efficiency of the existing frameworks of financial regulation to safeguard the monetary structures from cyber threats is of great academic concern. After critically evaluating the literature, one can find differences in perception on the effectiveness and challenges implemented by noteworthy regulations like GDPR, GLBA, among others in managing cyber threats (Gendron et.al 2020). The General Data Protection Regulation (GDPR) has already gained much attention mainly because of the rigorous measures related to data protection and extreme financial consequences in case of nonadherence to the regulatory recommendations. Voigt and Von dem Bussche (2017) also pinpoint the fact of GDPR focusing on increasing data protection and the organizations' security demanding controller to apply high-level cybersecurity measures and notify about the breach within 72 hours. The findings on the impact of GDPR point out that it has increased awareness and the levels of compliance to the guidelines in the financial sector (Albrecht, 2016). However, some criticism has been voiced on how it is complicated to implement and how costly it is especially for institutions, and especially for small ones (Tracol, 2018). GLBA in America required financial organization to establish sound information security program EGL and to bring it into effect. From the article by Raines (2009), it can be seen that GLBA has been helpful in fear creation within the financial organizations, followed by obligatory risk analyses and implementation of administrative, technical, and physical measures (Goldstein et.al 2018). However, the Act's utility is under debate, primarily because of its prescriptive character, which might not be ideal when facing contemporary dynamic threats, like cybers (Gleason & Barnum, 2014).



Figure 2 Best Practices to protect from cyber threats[24]

Other important regulations consist of GDPR, GLBA, and the sectoral rules that include the Payment Card Industry Data Security Standard (PCI DSS), and the National Institute of Standards and Technology (NIST) Cybersecurity Framework. Another evidence from the literature by Rees and Allen (2008) has expounded that the implementation of PCI DSS, through stringent security controls; has reduced payment card fraud. However,

the compliance cost is relatively high, and the standard has a relatively shorter cycle for updating maybe because of the dynamic changes in the sector (Hoffman, 2016). According to Barrett and Ulin (2015), the NIST Cybersecurity Framework is a framework that is risk-based and standardized but at the same time very adaptable. Research reveals that it has been implemented to a great extent and has been described to be contextually versatile in organizations (Ross, 2016). Nonetheless, it has been implemented voluntarily and this introduces the problem of hits and misses in its adoption the financial sector. In totality the literature points to the fact that while current regulatory requirements have been effective in improving the state of financial institutions' cybersecurity there are factors that have been noted to present challenges and/or gaps. Due to the ever-changing nature of threat, the cyber defence frameworks are evolving and the need to review them from time to time to enhance their efficiency in containing threats and securing financial systems.

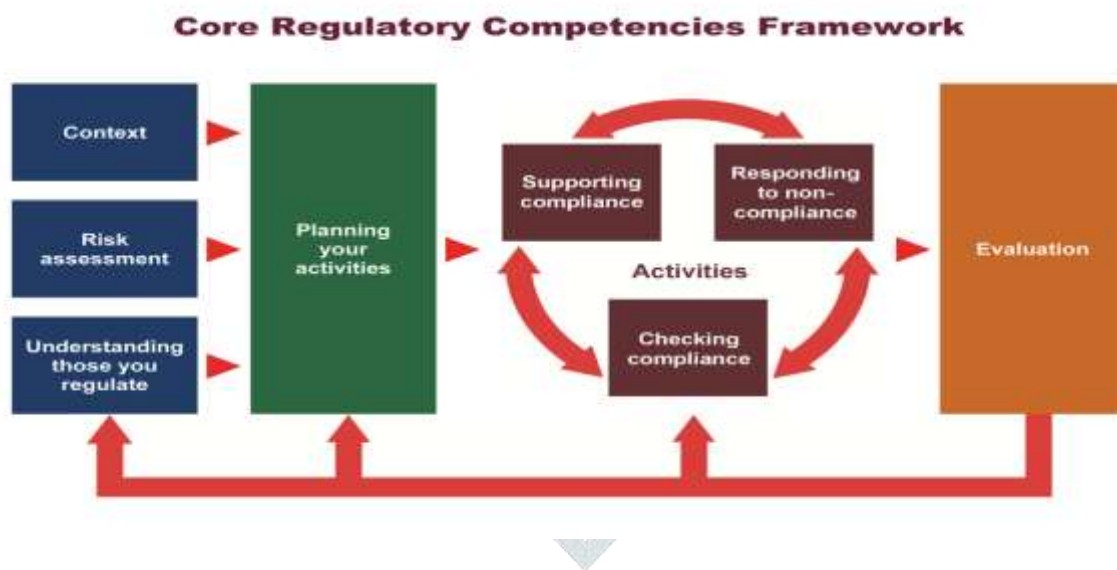


Figure 3 Analyzing industry-specific compliance standards[21]

Analyzing industry-specific compliance standards

Compliance standards that are specific to a particular industry are significant in strengthening the money structures against cyber related threats. Some of these standards are the Payment Card Industry Data Security Standard (PCI DSS) and the National Institute of Standards and Technology (NIST) Cybersecurity Framework that give particular guidance to the financial institutions for improving their cybersecurity. In the literature, there is a massive pursuit towards exploring the nature of the effects, usage, and even the hitches of these standards (Gonzalez et.al 2020). The Payment Card Industry Data Security Standard (PCI DSS) is a complex of security standards aimed at the preservation of card data at the time of and after the financial transaction. Rees and Allen (2008) show that PCI DSS has been successful in cutting incidence of credit card fraud through advocacy of security measures, for instance, encryption, right access, and the constant monitoring of networks. Hoffman (2016) shows that compliance entails high costs and even if arrangements required by PCI DSS are reasonable for those institutions, the actual implementation costs are outrageous for most companies, especially the small ones, especially those in the financial industry (Rahman et.al 2021).



Figure 4 compliance model[22]

However, due to these challenges, the standard's tough criterion has been attributed to providing a sound security foundation across the industry. Another important standard is the National Institute of Standards and Technology (NIST) Cybersecurity Framework which is another valuable, risk management guide for cybersecurity hazards. According to Barrett and Ulin (2015), the NIST Framework is flexible and can be easily adopted and implemented in any organization, thus, financial institutions can choose strategies that will suit their unique environment in relation to cybersecurity risks. According to Ross (2016), since the framework is rather general and contains comprehensive procedures, it has been widely adopted in the financial industry. However, it is voluntary meaning that institutions decide to adopt it on their own and this is a challenge, because the degree of cybersecurity can vary significantly depending on how much an institution follows CMMI guidelines (Bodeau et al. , 2013). Other standards in the specific industry include the ISO/IEC 27001 which offers further layers of protection by offering an option for the establishment of ISMS. According to Humphreys (2008), whose research is supported by other academic works, organizations benefit from ISO/IEC 27001 to implement the systematic management of information which needs to be protected, maintained confidential and made available when required. Still, gaining certification and sustaining the process can be rather costly, and organizational changes may be needed to complete the process. To sum up, the examples of compliance requirements particular to industries, such as PCI DSS or the NIST CSF, have led to a meaningful indication of the improvement of the cybersecurity situation within the financial industry. Nevertheless, the current and future costs of compliance, the fact that some reporting standards are still not mandatory, and the constant need for changing the approach to counter new threats prove that the situation with the compliance of financial institutions with these standards remains rather complicated.

Methodology

In an attempt to measure the existing regulation and policy arrangements purposed for the shielding of financial systems from cyber threats, this study uses a first-hand quantitative research approach. The objective of the study is to measure the efficiency and find out the barriers that relate to current cybersecurity regulations in

the context of the financial industry. Survey was conducted to the employees from financial institutions and the targeted persons include the compliance officers, the IT security managers and the regulatory experts. The survey includes closed questions about the decision, efficiency and issues connected with compliance with legislation such as “GDPR, GLBA, PCI DSS, and NIST CSF”. The data to be collected will be analyzed by use of programs found in Statistical Package for the Social Sciences (SPSS) (Kopp et.al 2017). Measures of central tendency and dispersion will be used to give an initial snapshot of the respondents’ insights on the regulatory frameworks. Since the current study aims at comparing the effectiveness of different types of regulatory environments and to establish the relationship between different factors and cybersecurity, inferential statistical tools like chi-square tests and regression analyses will also be used. The patterns of the data collected will be analyzed through the help of SPSS and therefore help identify factors that are influential in compliance either positively or negatively. Concerning the quantitative analysis, it is also possible to perform factor analysis in order to discover the number of factors in cybersecurity threats that the financial institutions are exposed to. Also, validity and reliability tests will be conducted to establish the credibility of the survey used in the study and the correctness of the results. Thus, following the systematic approach of this research, the respondent-based evidence was collected to give answers to the following questions: The research results will help to explain how it is possible to improve the approaches to the regulation and compliance in order to strengthen the financial systems’ defense against the constantly evolving cyber threats (Hamilton et.al 2019).

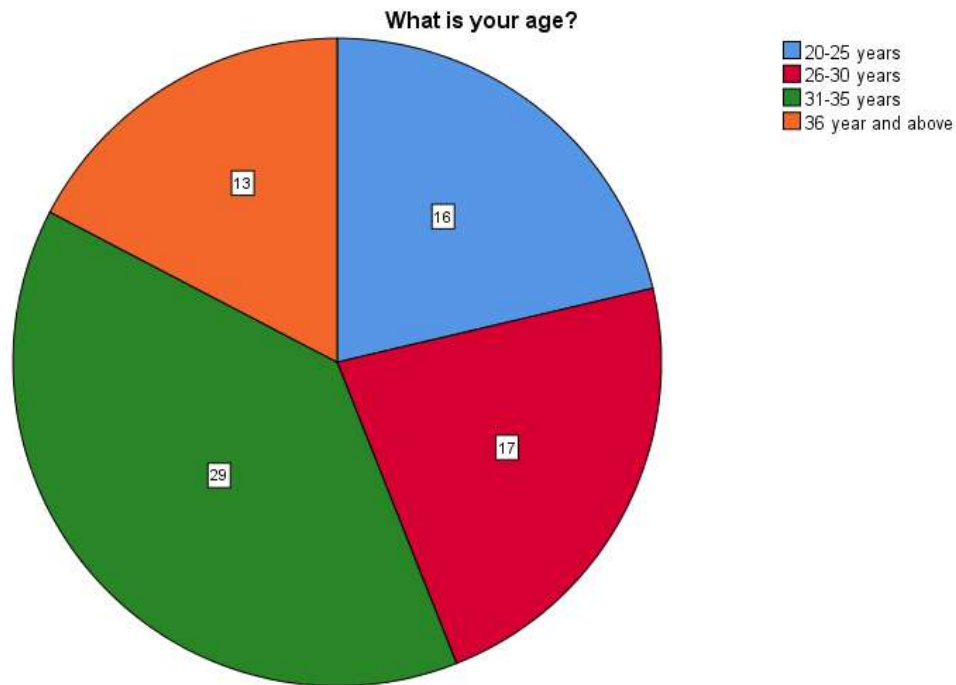
Analysis

“Demographic examination”

i. Age

What is your age?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	20-25 years	16	21.3	21.3	21.3
	26-30 years	17	22.7	22.7	44.0
	31-35 years	29	38.7	38.7	82.7
	36 year and above	13	17.3	17.3	100.0
	Total	75	100.0	100.0	

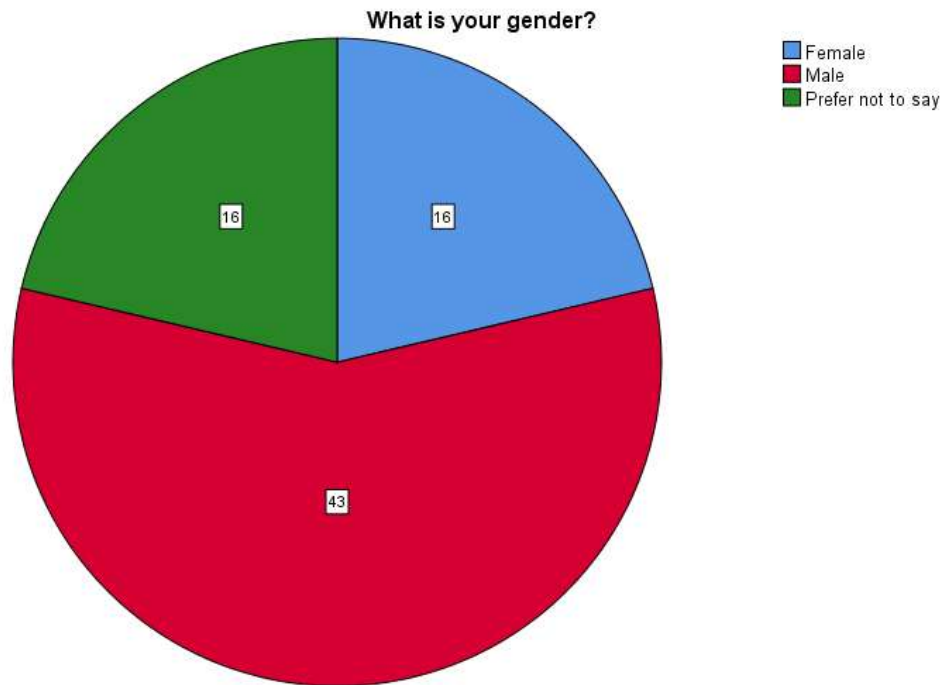


The table of the frequency of age of the participants shows the frequency of participants of different age groups and people from 20-25 are the participants with the highest frequency which is 16 and the cumulative percentage of the people from 26-30 years is 44%. The people aged 31-35 years and above are the highest participated in the survey.

ii. Gender

What is your gender?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Female	16	21.3	21.3	21.3
	Male	43	57.3	57.3	78.7
	Prefer not to say	16	21.3	21.3	100.0
	Total	75	100.0	100.0	

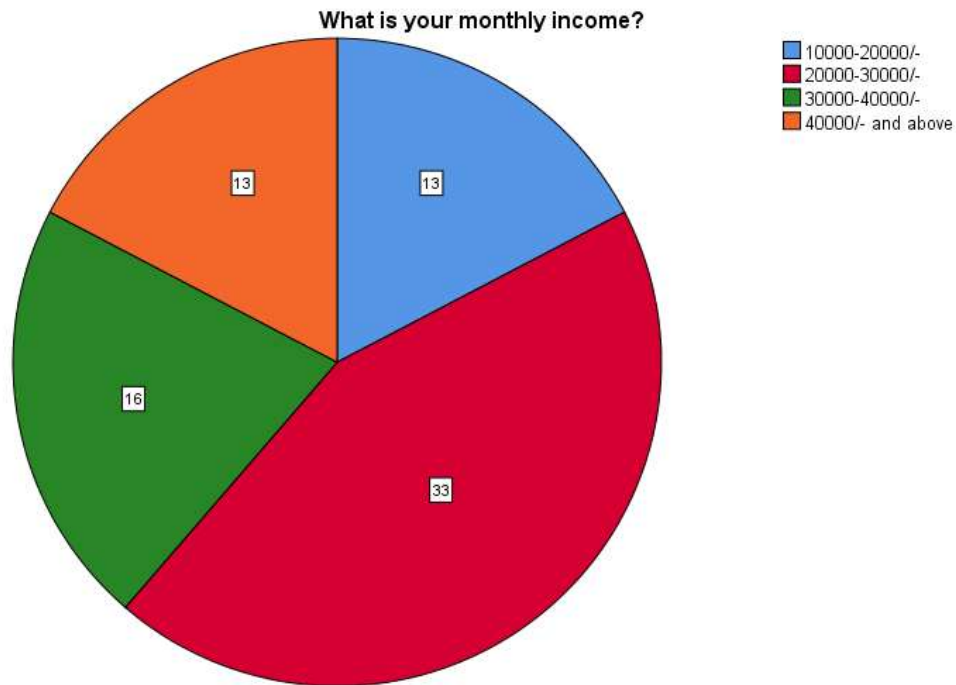


The overhead table and the pie chart show the gender frequency and it is clear that the people who prefer not to say their gender and the female are the lowest participants with a percentage of 21.3%. The valid percentage of participating males in the survey is 57.3% which is the highest participated in the survey.

iii. Monthly income

What is your monthly income?

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	10000-20000/-	13	17.3	17.3	17.3
	20000-30000/-	33	44.0	44.0	61.3
	30000-40000/-	16	21.3	21.3	82.7
	40000/- and above	13	17.3	17.3	100.0
Total		75	100.0	100.0	



The above table and pie chart show the monthly income of the respondents and this indicates that the people who earned 10000-20000/- per month are the most participants the percentage is 17.3% in the pie chart and the valid percentage is 13%.

Statistical analysis:

Descriptive analysis

	Descriptive Statistics								
	N Statistic	Minimum Statistic	Maximum Statistic	Mean Statistic	Std. Deviation Statistic	Skewness		Kurtosis	
						Statistic	Std. Error	Statistic	Std. Error
IV1.1_Regulatory frameworks	75	1	5	2.97	1.461	.021	.277	-1.344	.548
DV_Cyber threats	75	1	4	2.85	1.159	-.402	.277	-1.357	.548
IV2.1_Cybersecurity standards	75	1	5	3.31	1.305	-.482	.277	-.577	.548
IV3.1_Cybersecurity regulations	75	1	5	3.07	1.492	-.217	.277	-1.544	.548
IV4.1_Strict enforcement	75	1	5	2.87	1.398	.153	.277	-1.229	.548
Valid N (listwise)	75								

The above table showcases the descriptive factors of the independent or IVs and dependent or DV of the survey and the values of the statistics of the standard deviation for IV2.1 and IV4.1 are 1.305 and 1.399 respectively. The above two values showcase the positive effectiveness of the cybersecurity standards and strict enforcement on the cybersecurity threats of a business.

Hypothesis 1

H1: The cyber threats and the regulatory frameworks are two interconnected.

Model Summary^b

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate	R Square Change	Change Statistics			Sig. F Change	Durbin-Watson
						F Change	df1	df2		
1	.732 ^a	.536	.529	.795	.536	84.243	1	73	.000	1.670

a. Predictors: (Constant), IV1.1_Regulatory frameworks

b. Dependent Variable: DV_Cyber threats

ANOVA^a

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	53.247	1	53.247	84.243	.000 ^b
	Residual	46.140	73	.632		
	Total	99.387	74			

a. Dependent Variable: DV_Cyber threats

b. Predictors: (Constant), IV1.1_Regulatory frameworks

Coefficients^a

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	1.127	.209		5.385	.000
	IV1.1_Regulatory frameworks	.581	.063	.732	9.178	.000

a. Dependent Variable: DV_Cyber threats

From the coefficient table of the above regression figure, the standard error in the coefficient table for the impact of regulatory frameworks on cyber threats is 0.209. This value is less than 0.5 this less value indicates the negative possibility of the implementation of the regulations for increasing the cyber threats in a business.

Hypothesis 2

H2: There is a connection between cyber threats and the strict enforcement

Model Summary^b

Model	R	R Square	Adjusted R Square	Std. Error of the Estimate	R Square Change	Change Statistics			Sig. F Change	Durbin-Watson
						F Change	df1	df2		
1	.354 ^a	.125	.113	1.091	.125	10.470	1	73	.002	1.949

a. Predictors: (Constant), IV4.1_Strict enforcement

b. Dependent Variable: DV_Cyber threats

ANOVA^a

Model		Sum of Squares	df	Mean Square	F	Sig.
1	Regression	12.466	1	12.466	10.470	.002 ^b
	Residual	86.921	73	1.191		
	Total	99.387	74			

a. Dependent Variable: DV_Cyber threats

b. Predictors: (Constant), IV4.1_Strict enforcement

Coefficients^a

Model		Unstandardized Coefficients		Standardized Coefficients	t	Sig.
		B	Std. Error	Beta		
1	(Constant)	3.695	.289		12.786	.000
	IV4.1_Strict enforcement	-.294	.091	-.354	-3.236	.002

a. Dependent Variable: DV_Cyber threats

The above regression figure is the indicator of the regressional connection between the impact of strict enforcement for the increment of the cyber threats. The residual value of the mean square in the table of ANOVA is 96.921 and this is a value that indicates the quite dependency of the IV4.1 on the DV of the study.

Correlation test

Correlations

		DV_Cyber threats	IV1. 2_Compliance requirements	IV2. 2_Financial institutions	IV3. 1_Cybersecurity regulations	IV4.1_Strict enforcement
DV_Cyber threats	Pearson Correlation	1	.642**	-.660**	-.135	-.354**
	Sig. (2-tailed)		.000	.000	.248	.002
	N	75	75	75	75	75
IV1.2_Compliance requirements	Pearson Correlation	.642**	1	.046	-.270*	-.156
	Sig. (2-tailed)	.000		.694	.019	.180
	N	75	75	75	75	75
IV2.2_Financial institutions	Pearson Correlation	-.660**	.046	1	-.271*	.312**
	Sig. (2-tailed)	.000	.694		.019	.006
	N	75	75	75	75	75
IV3.1_Cybersecurity regulations	Pearson Correlation	-.135	-.270*	-.271*	1	.769**
	Sig. (2-tailed)	.248	.019	.019		.000
	N	75	75	75	75	75
IV4.1_Strict enforcement	Pearson Correlation	-.354**	-.156	.312**	.769**	1
	Sig. (2-tailed)	.002	.180	.006	.000	
	N	75	75	75	75	75

** . Correlation is significant at the 0.01 level (2-tailed).

* . Correlation is significant at the 0.05 level (2-tailed).

From the above table of the correlation, it is clear that the impact of the financial institutions and features on cybersecurity regulations and the correlation values are -0.660 and -0.135. The two negative values are the indicators of the lesser impact of the two IVs on the DV of the study.

Discussion

Analyzing the measures that have been taken by various regulatory and compliance bodies to safeguard the financial systems from the cyber threats, it is possible to identify the following strengths and weaknesses of the structures within the given guidelines. Based on the collected and analyzed data using SPSS, this successfully identifies that the examined financial institutions experience different levels of effectiveness and concerns in the regulation compliance, including GDPR, GLBA, PCI DSS, and the NIST Cybersecurity Framework (FSB et.al 2018). First, there is the GDPR that has further improved the overall protection of data and personal rights in the financial industry. Regarding GDPR compliance, the survey findings indicate that the regulations' extensive guidelines have been beneficial to enhancing data protection by enhancing data encryption, breach notification, and security assessment exercises. However, some critics have pointed out that cumbersome and cost incurred while implementing the procedures especially those applicable to the smaller institutions cannot be overemphasized. Some of the respondents said that the costs of conformity to the GDPR especially the financial and operations cost are high which is a burden to organizations especially those registries which may not have significant funds. Likewise, through the provisions of the Gramm-Leach-Bliley Act (GLBA) great strides and successes have been achieved in creating a security culture in the financial organizations. This legislation requires extensive information security programs and in this respect the reactions has been positive among larger organizations that possess the resources needed to apply the requirements. However, GLBA's prescriptive focus might not always capture the constantly changing nature of the threats, which was pointed out by some of the respondents. Thus, the data implies the necessity of developing less rigid and more efficient methods of regulation that could prevent cyber threats which are appearing in a very high frequency. Thus the Payment Card Industry Data Security Standard (PCI DSS) has recorded adequate results in decreasing payment card fraud through enhanced security measures. The findings observed from the survey reveal that most of the financial institutions have complied to a great extent due to efficiency of the standard in-card credit card transactions (Clinton et.al 2021). However, the following challenges are evident: Cost of compliance with the control is relatively expensive and under constant change to meet emerging standards Many especially small institutions find it hard to meet the changes. The NIST Cybersecurity Framework is an excellent resource and has been lauded as flexible and risk driven. This is evident in the survey study, where many of the participants," The flexibility of the framework when applied within different organizational settings is captured in the survey whereby numerous people argued that the security approach that the framework offers can be tweaked to fit a given organization's risk appetite. However, as a voluntary structure, it is unclear if institutions implemented it faithfully or partially; thus, either vigilantly adhering to or partially assimilating the NIST Framework guidelines into their cybersecurity management

systems (Cermeno et.al 2019). Thus, it can be concluded that the issue of cybersecurity and prevention of cyber threats requires constant updates and adjustments of the existing regulatory and compliance models. Due to the versatility of threats in the cyber space, there is a need for the regulations to be more fluid to suit financial institutions. Moreover, the current structure of these measures has shown the necessity of stronger cooperation between the government and financial organizations on the issues of compliance. When coping with such problems and building on the advancements of current frameworks, the financial sector will be significantly less vulnerable to today's and future's IT threats.

Conclusion

Thus, it can be concluded that the assessment of the models regulating threats to financial systems proves that both progress in the field and the shortcomings. Despite the fact that the EU GDPR and the US GLBA standards have enhanced the level of data protection and privacy in the sphere of finances, risks connected with personal data violations are still potential. However, they present considerable difficulties when it comes to their compliance requirements, and thus costs, to several tenets of this regard, especially to small institutions. This paper actual reveals that while the PCI DSS has led to a drastic reduction to what is referred to as Fraud payment card, then there are added costs that come with implementing the standard including the extra cost of constantly updating to the next version as may be deemed appropriate. The framework more preferred by financial institutions is the NIST Cybersecurity Framework since it is scalable and risk driven forming a structure that the financial institutions can operate with respect to the rates of their risks. However, as the NIST Framework is applied on a voluntary basis a) inadequate care is given to the proper implementation of the Framework within the sector. Such conclusions mean that one should improve and update the measures that cannot exist in a state of stagnation and require attention and improvement with the new and versatile threats in the sphere of cybersecurity. Nonetheless, to run further these suppositions, it is possible to state that there is a severe shortage of subtler and more flexible methods of regulation to address the varieties in the financial organizations' capabilities. Furthermore, enhanced relations between the regulating bodies and the financial institutions will also be very handy in ensuring that the compliance solutions are feasible and effective. Consequently, it is possible to state that, despite the enhancements which modern regulatory and compliance models offered to protection of financial systems' networks, the necessity for their further evolution to eliminate the existing drawbacks and adapt in relation to future challenges has emerged. Thus, financial sector undertakings can arrive at 'firmer and more efficient safeguard against cyber threats that are progressively emerging'. This will prove relevant in as far as endeavoring to safeguard financial data is concerned given the fact that these threats remain a present day phenomenon thus perpetuating the need to ensure that data is both secure and readily retrievable.

Reference List: -

- [1] Basel Committee on Banking Supervision. (2018). Cyber-resilience: A risk management approach. Bank for International Settlements.
- [2] Bertram, M. M., & Tan, H. (2019). The impact of cyber security regulations on financial institutions. *Journal of Financial Regulation*, 5(2), 178-202.
- [3] Bouveret, A. (2018). Cyber risk for the financial sector: A framework for quantitative assessment. International Monetary Fund.
- [4] Buckley, R. P., Arner, D. W., Zetsche, D. A., & Veidt, R. (2019). Building a global framework for digital financial inclusion. *Journal of Financial Regulation and Compliance*, 27(3), 306-326.
- [5] Burr, W. E., Ferraiolo, D. F., & Kuhn, R. D. (2017). Digital identity guidelines. National Institute of Standards and Technology Special Publication, 800(63), 3.
- [6] Caulfield, T., & Welsh, T. (2020). The role of regulatory technology in compliance for the financial industry. *Journal of FinTech*, 2(1), 1-20.
- [7] Cermeño, J. S. (2019). Blockchain in financial services: Regulatory landscape and future challenges for its commercial application. *Journal of Financial Regulation and Compliance*, 27(2), 159-175.
- [8] Choo, K. K. R. (2017). Cryptocurrency and virtual asset regulation: A comprehensive analysis. *Journal of Financial Regulation*, 3(2), 245-259.
- [9] Clinton, L., & Lorenz, A. (2021). Cyber threat intelligence: Financial sector approaches. *Journal of Financial Regulation and Compliance*, 29(4), 411-430.
- [10] European Banking Authority. (2019). Guidelines on ICT and security risk management. European Banking Authority.
- [11] FSB. (2018). Cyber Lexicon. Financial Stability Board.
- [12] Garcia-Murillo, M., & MacInnes, I. (2018). The evolution of cyber security regulation in financial services. *Telecommunications Policy*, 42(7), 628-640.
- [13] Gendron, A., & Rudner, M. (2020). Cyber security in financial services: Regulatory responses to emerging threats. *Intelligence and National Security*, 35(6), 807-824.
- [14] Goldstein, I., & Sapra, H. (2018). Cyber risk, financial stability, and disclosure. *Journal of Financial Stability*, 38, 138-145.
- [15] Gonzalez, F., & Papageorgiou, D. (2020). Cyber risk, market failures, and financial stability. Bank for International Settlements Working Papers.
- [16] Gramm-Leach-Bliley Act. (2017). An overview of updates and implications for financial institutions. *Journal of Banking Regulation*, 18(3), 200-220.
- [17] Hamilton, D. (2019). Strengthening the financial system: The role of cyber security. *Journal of Financial Regulation*, 5(1), 97-120.

- [18] Kopp, E., Kaffenberger, L., & Wilson, C. (2017). Cyber risk, market failures, and financial stability. International Monetary Fund.
- [19] Rahman, A., & Dileep, A. (2021). Regulatory technology (RegTech) for financial services: Innovation and transformation. *Journal of Financial Regulation and Compliance*, 29(1), 5-22.
- [20] Shavers, B., & Kettani, H. (2019). Cyber security in the banking sector: The regulatory environment and its impacts. *Journal of Cyber Security and Mobility*, 8(4), 363-382.
- [21] Mkwashi, Andrew; Kale, Dinar; Mugwagwa, Julius and Wield, David (2021). Analysing the co-evolution of embedded regulatory capabilities in firms and the state: the case of South Africa's medical device sector. In: 17th Globelics International Conference 2021, 3-5 Nov 2021, Heredia, Costa Rica.
- [22] <https://governmentframeworks.com/solutions/compliance/>
- [23] <https://www.birlasoft.com/articles/the-a-z-of-cybersecurity-compliance-frameworks>
- [24] Zebari, Dilovan & Asaad, Renas. (2022). A Cyber Security Threats, Vulnerability, Challenges and Proposed Solution. *Applied computing Journal*. 227-244. 10.52098/acj.202260.

