Cybersecurity And Governance, Risk And Compliance (GRC)

By: Ishwor Thapa Chhetri
Cihe21221@student.cihe.edu.au

Abstract

When it comes to *cybersecurity*, different frameworks, best practices, and standards are used by organization. And these *governance* documents are most often chosen in accordance with corporate governance requirements or legislative requirements. Controls, cyber breaches history and finances are typically prescribed in governance documents, including technical controls, administrative controls, and physical controls. There are also a number of documents that describe specific capabilities that businesses must develop to secure their cyberspace.[i] So, from threats to SQL Injection Attacks to Cloud computing, Load balancing and Internet of things that needs cyber protection and the framework that GRC provides for it are all needs to be included with *GRC framework* while informing about the GRC business benefit to organisation. Thus, the results in this paper should be understanding and evaluating *IT GRC* implementation to reduce mismanagement and risk and ensure adherance in organizations and it can be only achieved by mitigating outside risks like cyber and network attacks by using means of Application Security, Internet of Things Security, Network Security, Infrastructure security and limiting access to sensitive information, showing the, *interrelation of GRC with Cyber security*

Key terms

Data Governance, IT GRC frameworks, Cyber security in IT industry, Cyber capabilities, Cyber vulnerabilities, interrelation of GRC with Cyber security.

Introduction

In an enterprise-wide GRC program, Cyber security needs to be included as part of every business decision. Cybersecurity is an action to prevent or detect theft and electronic attempt to damage data and to helps organizations to identify and reduce cybersecurity risks, protect their systems and data, and respond to cyber incidents. Cybersecurity, or information security governance, risk, and compliance (GRC) as it's sometimes called, refers to policies, processes, and procedures related to protecting an organization's systems and data against cyber risks. As the concept of governance encompasses the set of processes that are implemented and controlled by directors and reflect in the structure and management of the organizations to achieve goals while risk management relies on achieving said goals under any uncertainty while predicting and managing such risks, moreover compliance focuses on sticking to boundaries of company and law itself. In order to fulfill their role of protecting the organization, Governance, Risk and Compliance officers must be aware of cybersecurity and understand its various components and how they are interrelated. For example, GRC officers must be familiar with the organization's risk appetite, its risk management process, the cybersecurity regulatory framework and its associated policies.

Regardless of the size and the area of activity the basic principle of GRC applies to any organisations varying on the information, processes and people.

Literature Review

So, like most aspects of information security, governance, risk, and compliance (GRC) can be broken down into smaller parts that can be more easily understood. It all starts with a threat, then moves on to mitigation, and finally prevention. The purpose of GRC is to identify, assess, prioritize, monitor, and control risks to your information security program. Our ability to identify, assess, monitor, prioritize and respond to cyber threats is also heavily influenced in cybersecurity by our addressing to governance, risk and compliance (GRC). It's this framework that adheres and allows to adhere with regulatory requirements such as Health Insurance Portability and Accountability Act (HIPAA) as well as the Payment Card Industry Data Security Standard (PCI DSS) and it's the foundation for the entire cybersecurity program.

Cybersecurity is a critical element of information security, but it’s also a broad and complex topic. Cybersecurity and governance, risk and compliance have always been closely related. The more we rely on technology to do our jobs, the more we rely on it to protect our data and networks. This relationship between the two is critical to the future of business, both in terms of protecting information and ensuring safety. At the same time, there is a lot of confusion about how to approach cyber security, how to effectively manage risk, and what compliance actually means. It is used by cybersecurity analysts, as well as provide an overview of the major threats and vulnerabilities that face organizations today. This is intended for anyone involved in cybersecurity, including information security analysts, information security risk managers, cybersecurity compliance officers, and others. The traditional approach to cyber security is to monitor and control the systems that are “known” to be vulnerable. This approach, however, is ineffective at preventing an attacker from launching an attack in the first place. The goal of Cyber Security is to identify and eliminate vulnerabilities before an attacker can exploit them. This approach is known as Cyber Security Governance.

So, information technology and Cyber security as a whole is important to business and GRC as new regulations place a high priority on information security, and organizations must have a framework to secure their own data as well as that of their clients. This makes compliance a critical component of governance. Regulation and compliance issues directly increase risk. Governance, risk, and compliance have thus begun to move together in organizations

.[ii]

Frameworks for IT GRC

Cybersecurity can be aligned with IT GRC frameworks in order to align IT with business. In order to ensure IT goals are aligned with business goals, IT governance frameworks must be optimally integrated. Rules and methods for monitoring IT risks, regulating IT assets, complying with laws and regulations, and managing records, as well as alignment, are all included in IT governance. It's a mix of risk, compliance, and governance.[iii]

As a result, the ITG frameworks serve as the foundation for an IT GRC model. ITG frameworks are used to implement IT governance, and each one has its own set of IT GRC operations. A global has survey revealed that external IT governance frameworks used in the enterprise governance of IT as ITIL/ISO 20000, ISO 17799/ISO 27000, Six Sigma, ISO 38500, Business Model of Information Security, PRINCE 2, COBIT 5, PMI/PMBOK, Risk IT, IT Assurance Framework, CMMI and COSO ERM and all of them focusing on different IT aspect of company. From a practitioner's perspective, the most commonly mentioned IT-related frameworks are the COBIT, ITIL, the Integrated Capability Maturity Model (CMMI), International Standards Organization (ISO) Standards number 17799 and 9000 [iv]. ITIL and COBIT are mostly used for IT governance implementations. The COBIT framework was developed to support effective IT management in integrated and holistic manner, moreover, ITIL is a collection of recommendation and publications that describes the best practices for enhancing efficiency and cost-effectiveness in numerous IT operations domains.

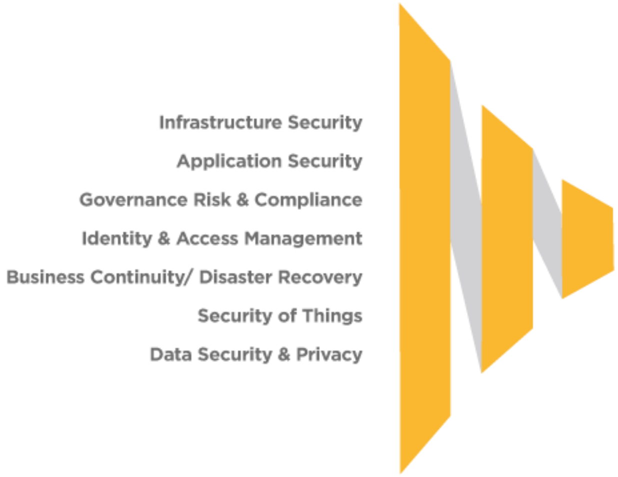
And the implementation of COBIT, ITIL, and ISO 17799 is beneficial to an organization's growth and success since they provide a guideline for compliance, reduce risks, optimize costs and help benchmark the results of IT investments which is very beneficial for any organisation as without these, the risk for the organisation increases through internal conflict or through online cyber-attacks targeting any sorts of information that can damage the value of business, which can be mitigated through cybersecurity. IT GRC implementations have typically used generic frameworks, but there have been instances when specific IT-related models have been used, including the software development life cycle (SDLC) that integrates project management with ITIL after implementing it. Practitioners lack guidance on selecting IT GRC frameworks given that there are multiple ITG frameworks to choose from.v

Based on the National Institute of Standards and Technology's (NIST) cybersecurity framework core, business cybersecurity capabilities were determined, and the completeness of these capabilities was confirmed by mapping them against COBIT (Adler 2007), ISO/IEC 27001:2005 (ISO/IEC 2005) and SANS (SANS Institute 2013).

The identified business cybersecurity capabilities identified are:

- Identify
    - Asset Management • Business Environment • Governance
- Protect
    - Access Control • Awareness and Training • Data Security
    - Information Protection Processes and Procedures • Maintenance
    - Protective Technology
- Detect
    - •Anomalies and Events • Security Continuous Monitoring

    - Detection Processes
- Respond
    - Response Planning • Communications
    - Analysis • Mitigation •Improvements
- Recover
    - Recovery Planning • Improvements • Communications [vi]


Infrastructure Security
Application Security
Governance Risk & Compliance
Identity & Access Management
Business Continuity/ Disaster Recovery
Security of Things
Data Security & Privacy

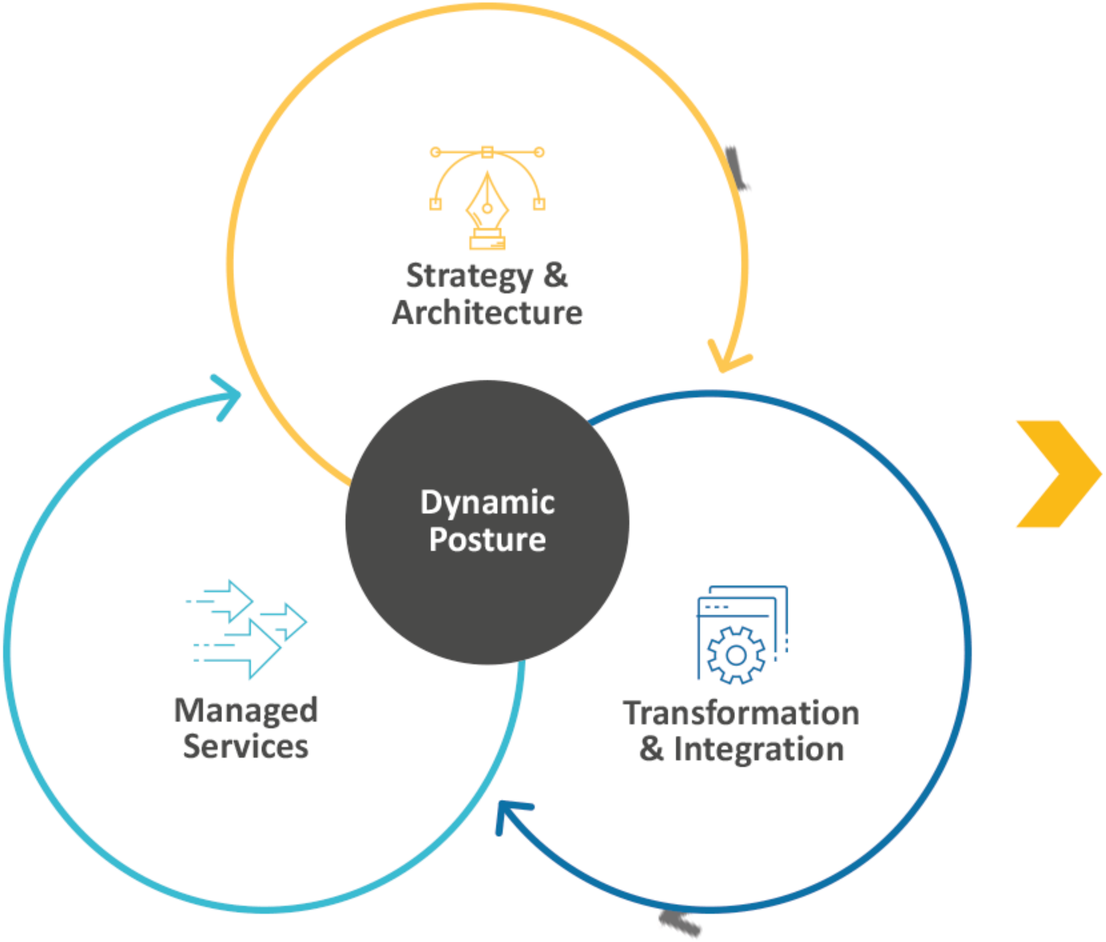


Figure1 Dynamic cybersecurity[vii]

Research Methodology

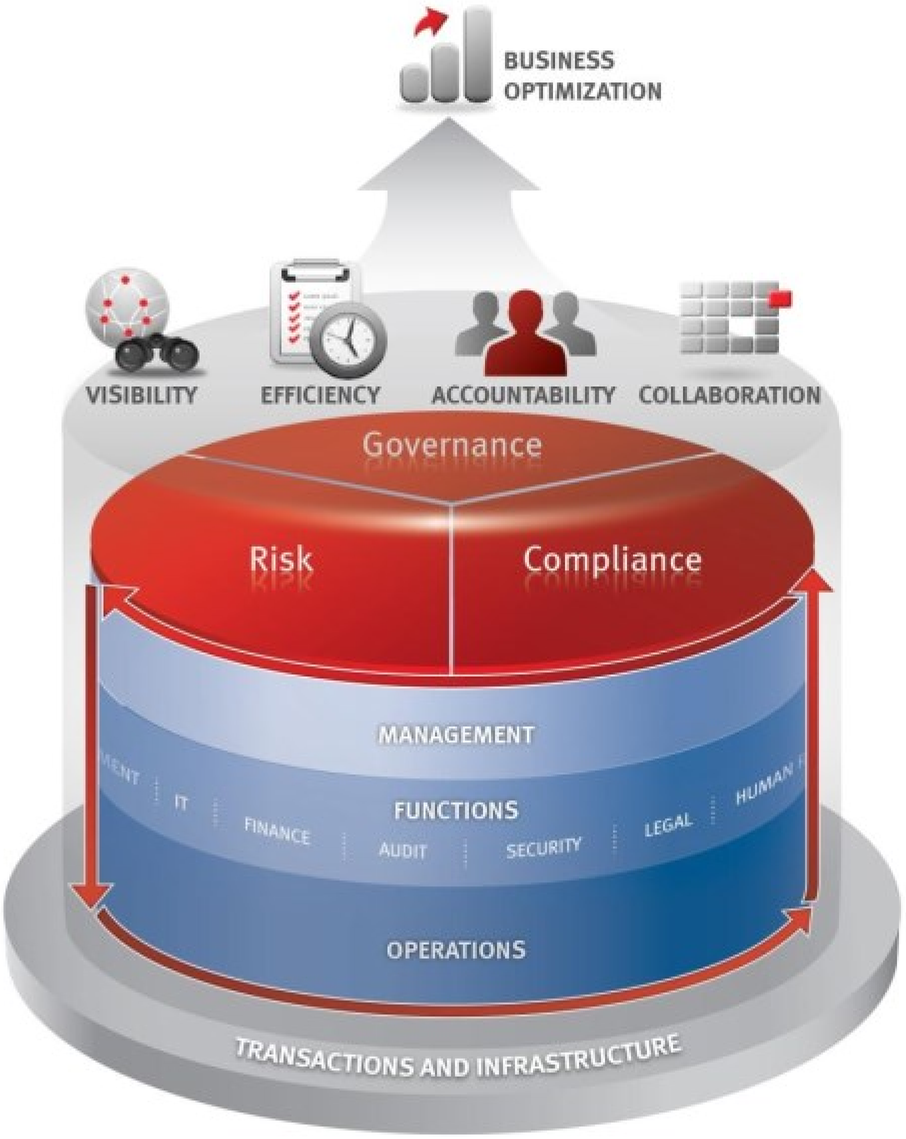


Figure 2 GRC and management [viii]

How the GRC can benefit the business in managing the contributions to IT of organisation and the research procedure (written by going through various articles, journals, and books about surveys, case studies related to cyber security and GRC) can be explained as The New South Wales Small Business Commissioner's Office and Symantec released a study that shows cyber security is becoming more important to businesses and it is becoming a higher priority. However, its complexity also makes it difficult for businesses to implement policies. There have been numerous high-profile breaches of privacy, prompting calls for more regulation and security. As of the end of 2018, there were 87 million Facebook accounts compromised, 150 million MyFitnessPal accounts compromised, and the Aadhaar data breach in India exposed the private information of 1.1 billion citizens. Governments are increasingly focused on implementing stronger data protection strategies, which means businesses must prepare for increased cybersecurity regulatory requirements as even the government that has the control of all the data of the population can be target as there are many groups prioritizing hacking, phishing, ransomware etc.

ix

In all industries, business is increasingly conducted digitally, so cyber security must be prioritized. As with physical security, consider cyber security the same way you would protect your office, such as locking your doors when you leave or protecting your confidential information from competitors. These are not only applicable to larger businesses but the larger or corporate enterprises as the whole world are heading towards the online market, social media, and users. Thus, GRC aligns its business objective with IT by managing risk and compiling to achieve goals. Since the purpose of GRC is to reduce cost and risk and doubling of effort and can be only achieved by mitigating outside risks like cyber and network attacks by using means of Application Security, Internet of Things Security, Network Security, Infrastructure security, and limiting access to sensitive information.

Finding and Discussion

To act upon the above statement on Research Methodology the best governance model is needed to check upon suppliers and connect to users while preserving their privacy and footprints. So, the findings and discussions from all the books, surveys, and journals are shown and discussed below;

Why is cyber security needed?

A GRC function can collaborate with IT and security departments to assess the scope of the cybersecurity framework and document its strengths and weaknesses. From a technical standpoint, we can explain the types of cybersecurity dangers detected, and GRC can add a business viewpoint to list additional concerns. The combination of these two levels of reasoning in aids in the development of a thorough understanding of corporate risk. The company can then decide whether to invest in a new firewall or managed service, for example.

Risking the business by doing nothing with the consequences of a successful cyber assault can result in downfall even with a good GRC framework.

Which framework to use?

IT governance framework are carried out to seek what is needed for key metric management, how the IT department are working out and what sorts of investment returns is IT giving to business.

Where ITIL helps to simplify service and operations and COBIT and COSO are used mainly for risk. Also, CMMI was initially intended for software engineering, however, now involves processes in service delivery, hardware development and purchasing. As previously mentioned, FAIR is squarely for assessing operational and cyber security risks.

When reviewing frameworks, consider your corporate culture. Does a particular framework or model seem like a natural fit for your organization? Does it resonate with your stakeholders? That framework is probably the best choice.[x]

Vulnerabilities

Social media, Websites, Applications platforms of different ranges and genres like Facebook, Google, Amazon where user record their personal data from their emails, bank details, medical history with passwords and privacy are a confidential thing and very sensitive matter and it is the duty of such media companies to protect such sensitive information however it was reported that such Tech giants could not protect their user information, some examples are;

Facebook - There was a disclosure in April 2019 that two Facebook app datasets pertaining to more than 530 million Facebook users had been leaked onto the public internet.

LinkedIn - A dark web forum posted information associated with 700 million users in June 2021, impacting more than 90% of its users.

Adobe -Adobe in October 2013 reported that hackers had stolen credit card data for almost three million customers and login details for an unknown number of users.

[xi]

The Solution for cyber risk in any business and value the of GRC

The solution is for persons in charge of cybersecurity in an Organisation to recognize the value of GRC knowledge. Cybersecurity workers in the financial business are obliged to understand their organizations' legal and regulatory standards, and the same approach should be applied to other industries as well. Because many of their tasks are now closely related to risk and compliance, IT leaders need to be educated and informed about legal and regulatory obligations.

Employees in any business must be given the appropriate tools for their new function in addition to being trained. For firms who are only now combining cybersecurity with GRC, understand that a Cybersecurity platform is critical. The platform will help employees as well as make the transition to the new model easier. IT cybersecurity is far too complicated and critical to be managed manually; it must be automatically monitored and tracked to ensure that nothing goes wrong.

The GRC team will also play an important role in incident response planning and programs along with initializing self-audit. GRC may play a crucial role in incident response that doesn't require the technical aspects under IT's supervision, whether it's assisting with the coordination of crisis management and testing exercises or interactions and filings with regulators in the case of an actual breach.

With each passing day, cyber-attacks get more complex. There are currently attacks that are unstoppable by any firewall or antivirus program. The only way to prevent such assaults is to take the appropriate approach to cybersecurity. Cybersecurity GRC improves the security of the entire business process. Antivirus software and firewalls can catch viruses and attacks that enter through IT infrastructure flaws, but GRC can completely eradicate these vulnerabilities.[xii]

Conclusion

From the above studies, it can be concluded why Cyber security and GRC play an undeniable positive and inter-relatable part in any business and why a good relationship between them enhances the positive enforcement in business saving business, time, value, and sensitive information while minimizing risk, cost, and duplication of efforts.

Also, the GRC framework are aligned with many other frameworks such as COBIT5, ITIL, CMMI, and ITIL, and COBIT is mostly used for the implementation of governance and its framework in IT. The COBIT framework was developed to support effective IT management in an integrated and holistic manner, in contrast, ITIL describes best practices in several areas of IT operations that promote efficiency and cost-effectiveness.

Therefore, the overview is that the cyber-attacks is getting more complex and there currently are attacks that are unstoppable by any firewall or antivirus program. The only way to prevent such assaults is to take the appropriate approach to cybersecurity. Cybersecurity GRC improves the security of the entire business process. Antivirus software and firewalls can catch viruses and attacks that enter through IT infrastructure flaws, but GRC can completely eradicate these vulnerabilities.

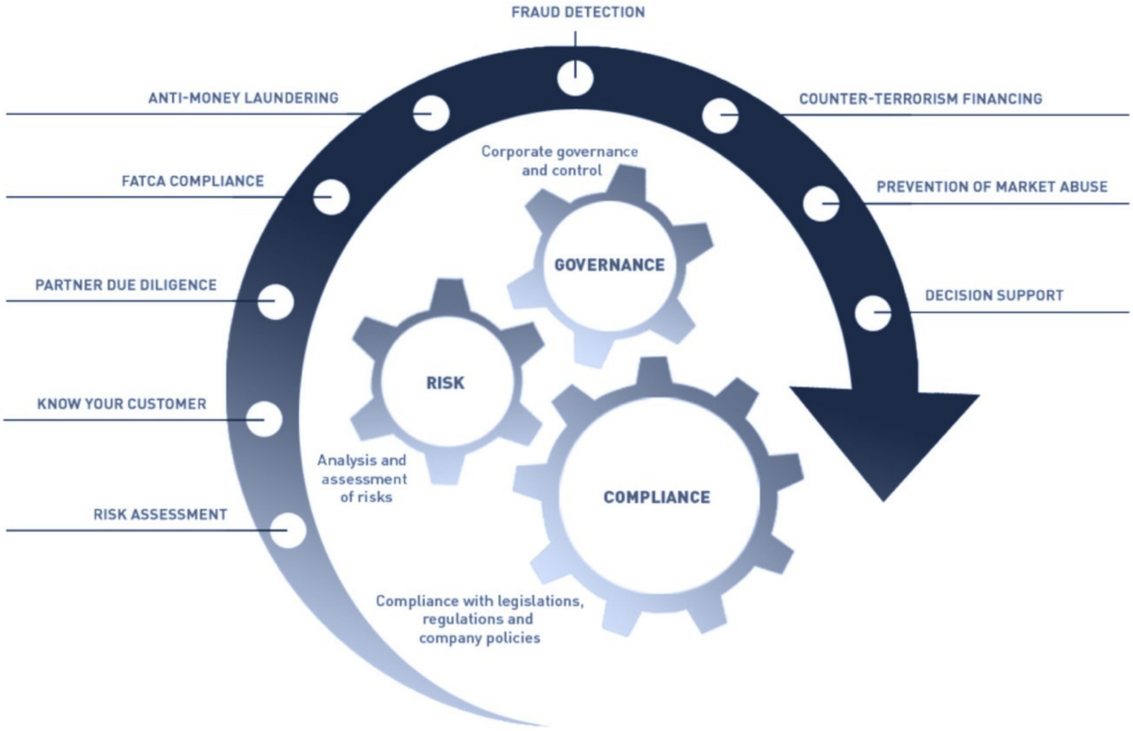

FRAUD DETECTION
ANTI-MONEY LAUNDERING
COUNTER-TERRORISM FINANCING
FATCA COMPLIANCE
PREVENTION OF MARKET ABUSE
PARTNER DUE DILIGENCE
DECISION SUPPORT
KNOW YOUR CUSTOMER
RISK ASSESSMENT
Corporate governance and control
GOVERNANCE
RISK
Analysis and assessment of risks
COMPLIANCE
Compliance with legislations, regulations and company policies

Figure3 GRC and Cyber security approach[xiii]

References

[1] Jacobs, P., von Solms, S. and Grobler, M., 2016. "*Towards a framework for the growth of business cybersecurity capabilities.*" Cberuk.com
https://cberuk.com/cdn/conference_proceedings/conference_40254.pdf

[2] Hamilton, S., 2018. "*What is GRC And How It Empowers Cyber Security?* ". 360factors.com.
https://www.360factors.com/Blog/what-is-GRc/

[3] Hamaker, S.: '*Spotlight on Governance'*, Information Systems Control Journal, 2003, 1, pp. 15-19

[4]ITGI: '*Global Status Report on the Governance of Enterprise IT (GEIT)*' (ISACA & IT Governance Institute, 2011. 2011)

[5] Polkard, C.E., Gupta, D., and Satzinger, J.W.: '*Teaching Systems Development*: A Compelling Case for Integrating the SDLC with the ITSM Lifecycle', Information Systems Management, 2010, 27, (2), pp. 113-122

[6]Jacobs, P., von Solms, S. and Grobler, M., 2016. "*Towards a framework for the growth of business cybersecurity capabilities.*" Cberuk.com https://cberuk.com/cdn/conference_proceedings/conference_40254.pdf

[7]Cybersecurity & GRC Services HCL Technologies. "*Dynamic Cybersecurity*" Www.hcltech.com. https://www.hcltech.com/cyber-security-grc-services

[8]Unal Perendi. (2020, January 2). "*The GRC approach to Cyber Security"*. GOVERNIFY. Retrieved April 3, 2022, from https://governify.com/2020/01/02/the-grc-approach-to-cyber-security/

[9] *Cyber Security: The Small Business Best Practice Guide"*. https://static1.squarespace.com/static/52b5f387e4b08c16746b6b70/t/60d01fb868579e7a02a3d1fc/1624252345505/ASBFEO-cyber-security-research-report.pdf

[10] Lindros, K. (Ed.). (2017, July 31). What is it governance? A formal way to align IT & business strategy. CIO. Retrieved April 6, 2022, from https://www.cio.com/article/272051/governanceit-governance-definition-and-solutions.html

[11]Swinhoe, D., & Hill, M. (2021, July 16). "*The 18 biggest Data breaches of the 21st Century"*. CSO Online. https://www.csoonline.com/article/2130877/the-biggest-Data-breaches-of-the-21st-century./

[12] Hamilton, S., 2018. "*What is GRC And How It Empowers Cyber Security?* ". 360factors.com. https://www.360factors.com/Blog/What-is-grc/ .

[13] "*Expert GRC Cyber Security Services*". ESecurity Solutions. https://www.esecuritysolutions.com/security-services/