

University of Wales Trinity Saint David (UWTSD)

Program: MSc Cybersecurity and Digital Forensics

Module Name: Data Security, Governance and Compliance

Module Code: ACCA7028

Assessment Title: Apply the Principles and Practices of Data Security,
Governance and Compliance Based on a Given Scenario

Lecturer: Dr. Ayman Al Hajjar

Student Name: Md. Asaddoz Jaman

Student ID: 2526322

University Email: 2526322@student.uwtsd.ac.uk

Submission Date: 29 April 2026

Word Count: 3000

Declaration:

I declare that this assessment is my own work and that all sources have been properly acknowledged in accordance with academic integrity and referencing guidelines. I understand the university regulations on plagiarism and confirm that this submission complies with those requirements.

Table of Contents

ABSTRACT.....	3
1. INTRODUCTION.....	4
2. FRAMEWORK ANALYSIS.....	4
2.1 ISO/IEC 27001 Framework.....	5
2.2 NIST Cybersecurity Framework.....	5
2.3 ITIL Framework.....	6
2.4 Zero Trust Model.....	6
2.5 Comparative Analysis.....	7
3. PROPOSED MODEL.....	7
3.1 Governance Layer	8
3.2 Risk Management	8
3.3 Security Architecture	9
3.4 Compliance Framework	11
3.5 Incident Response and Recovery	11
3.6 Service Level Agreements (SLA) and Third-Party Risk.....	12
3.7 Frameworks Integration.....	12
3.8 Summary of model's benefits	13
4. CRITICAL DISCUSSION	13
5. CONCLUSION.....	14
REFERENCES.....	16

ABSTRACT

This assignment provides a thorough evaluation of information security management, governance, and compliance frameworks within the modern business context. The main goal of the investigation is to highlight the necessity of proper structured governance that would help minimize the cybersecurity risks and ensure full compliance with all necessary data protection requirements on an international level. In today's world, companies face numerous challenges associated with the digital nature of their operations, including data breaches, hacking, and mismanagement of sensitive organizational assets. This report highlights several such problems and develops a strategic approach aimed at securing organizational information.

The research methodology consists of two major elements – a thorough risk assessment, during which fourteen possible sources of danger were identified. These risks vary from hardware theft and employee misconduct to computer viruses and information leakage. Based on the degree of impact, each of the risks was classified according to its significance. In addition, the report evaluates the use of the ISO/IEC 27001 framework and GDPR as fundamental components of the data security strategy and organizational risk reduction process.

The key insights provided by the analysis are that data security is more than just a technical aspect of governance but also requires the commitment and engagement of management. The primary action plans that need to be considered at this point in time are the implementation of multi-factor authentication measures, the undertaking of periodic security audits, proper training of all employees in terms of the best practices for securing data, and the development of a "assume breach" mindset. It becomes quite clear from the overall analysis that adopting a proactive strategy can help achieve business continuity and gain the trust of stakeholders.

1. INTRODUCTION

As a result of fast digitalisation in the financial industry, the functioning of banks has seen significant transformation due to the use of cloud-based solutions, mobile apps, and digital platforms. Although this approach makes banks more effective from the business perspective, at the same time, it creates various issues connected to cybersecurity, governance, and regulation. As an example, modern banking institutions like FinSure Bank (FSB) have to deal with the issue of cyber risks that may be represented by different kinds of threats including data breaches, phishing, insider attacks, and unauthorised access due to the digitalisation of the network.

Modern banks should pay close attention to the protection of financial and personal data. In this context, there are different regulations including GDPR, which set certain conditions for collecting and processing data, making IT governance a necessary practice for banks. Thus, in the context of emerging challenges, banks have to take dynamic approaches towards cybersecurity.

In order to address issues emerging in the course of time, some internationally accepted methodologies appear. Hence, ISO/IEC 27001 represents an information security management methodology based on ISMS (Information Security Management System) and providing confidentiality, integrity, and availability of information [1]. It is supplemented by the NIST CSF (Cybersecurity Framework) methodology that also implements risk-based life cycle including the following components: Identify, Protect, Detect, Respond, and Recover [2]. Another important contribution to security issues is made by ITIL (Information Technology Infrastructure Library) addressing ITSM and implementing standard processes including incident, change, and service continuity management [3]. Finally, Zero Trust security approach emphasizes the need to remove implicit trust and introduce verification always [4].

However, having analyzed strengths of each of these methodologies separately, it should be noted that these frameworks do not provide enough to meet current demands of cybersecurity of digital financial institutions. This happens because each of these frameworks addresses only specific aspects related to security, namely governance, operations, services, and access controls, and no integration can be implemented.

Therefore, there is a necessity to create a unified approach that will incorporate the benefits of all various approaches into one single approach that will be able to solve problems regarding security, governance, and compliance.

The objective of this study is the creation and evaluation of a unified approach that will be applicable to the cloud banking environment of FSB. Utilization of more than one framework for the integration of the model can prove to be very beneficial in improving cybersecurity, regulatory compliance, and operational resilience of financial organizations.

2. FRAMEWORK ANALYSIS

The aspects of data security, data governance, and compliance of financial organizations necessitate the use of some frameworks or models. Specifically, the FinSure Bank (FSB) organization that operates

under cloud computing and mobility is supposed to apply the implementation of these frameworks for managing risks such as cyber-attacks, violation of data confidentiality, regulatory non-compliance, and other challenges. The discussion of this section will concentrate on the ISO/IEC 27001 Framework, NIST Cybersecurity Framework, ITIL, and Zero Trust framework as applied to FSB.

2.1 ISO/IEC 27001 Framework

ISO/IEC 27001 is one of the most popular international standards regarding data security through the Information Security Management System (ISMS). This standard takes into account data security based on the risk factor and guarantees the protection, integrity, and accessibility of data [1]. The standard is structured around PDCA Cycle and allows constant improvement of security management process. It can be seen from Figure 1 that ISO 27001 standard offers a chance to evaluate data risk, implement control actions, and manage security.

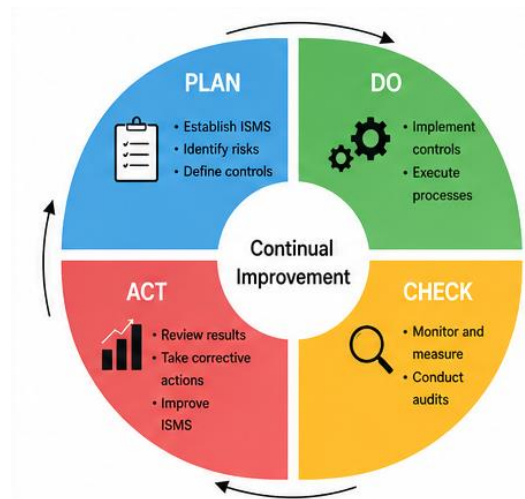


Figure 01: Cycle of information security management.

ISO/IEC 27001 may be considered applicable to FSB insofar as it provides a systematic and managed approach to data security management within the cloud and mobile setting. With the adoption of this standard, it becomes possible for organizations to detect and mitigate risks associated with data security efficiently. But, the process may be time-consuming and costly.

2.2 NIST Cybersecurity Framework

The National Institute of Standards and Technology (NIST) framework for cybersecurity consists of five risk management processes, including Identification, Protection, Detection, Response, and Recovery [2]. The framework reflects the lifecycle of the process, as presented in Fig. 2, allowing an organisation to actively counteract potential threats or attacks.

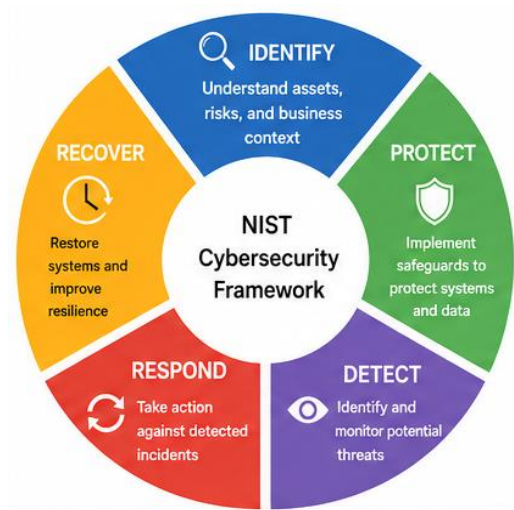


Figure 02: Core functions of NIST cybersecurity framework.

In regard to the FSB, the framework would be useful owing to its flexibility. It enables the organisation to identify its assets, secure itself through multiple means such as encryption, identify any incidents or attacks, and counteract them immediately. Furthermore, the recovery phase enables the business to continue operating following any disruptions. Unlike ISO 27001, however, NIST cannot be used for certification purposes. Additionally, NIST may require considerable organisational guidance due to its flexible nature.

2.3 ITIL Framework

The first and foremost thing is that ITIL concentrates more on IT service management, thus ensuring that IT services are aligned with organizational objectives. Though not a security model in itself, ITIL does provide security through processes like incident management, change management, and service continuity [3].

For FSB, it is necessary to have ITIL for offering reliable service without causing disruptions. Thus, it will be possible for the firm to deal with security issues without making changes to systems which may compromise security. There are certain limitations of security offered by ITIL.

2.4 Zero Trust Model

The Zero Trust security model works on the principle of 'never trust and always verify'. This means that there must be continuous authentication and authorization of the user and device [4]. The key difference between the Zero Trust and a perimeter-based security model is that Zero Trust not only focuses on the threats originating internally but also external to the network.

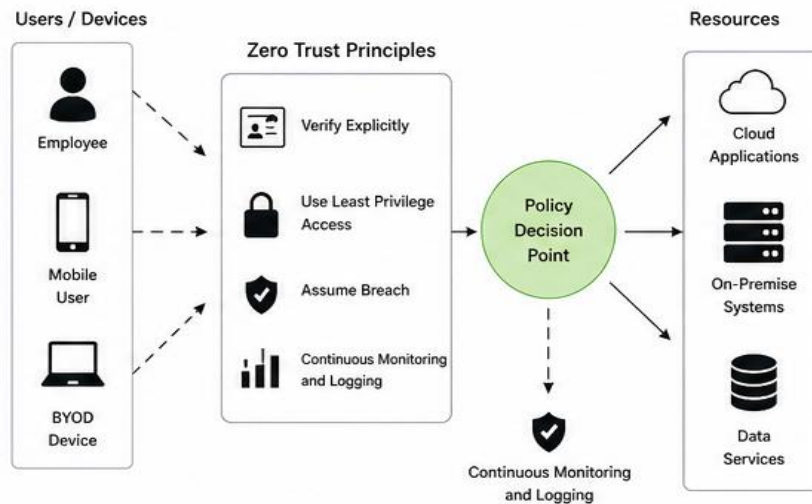


Figure 03: Verification Model of Zero Trust Security Architecture and Continuous Access.

This approach can be widely applied in FSB due to its justification that it has a BYOD approach and thus requires remote access to resources. The approach is effective in ensuring high levels of security through limiting access permissions and reducing the risk of insider attacks. However, this approach might not be easy to implement.

2.5 Comparative Analysis

The above-mentioned frameworks contribute uniquely to the matters concerning data security and governance. The governance process is facilitated through ISO 27001 framework; NIST allows greater freedom of choice in terms of risk management. ITIL is useful in ensuring efficiency in service, while zero trust approach enables improvement of access control. In regards to FinSure Bank (FSB), the combined use of all mentioned frameworks would be the most effective solution.

3. PROPOSED MODEL

In a totally digitized environment, FinSure Bank (FSB) relies on cloud computing, mobile banking applications, and services of other companies. While this offers some huge advantages, there are a number of critical risks related to this strategy, such as cybersecurity threats, governance problems, and non-compliance issues. This can involve such problems as lack of access controls, lack of governance, increased BYOD risks, and penalties, including fines for violating GDPR [6].

It is necessary to come up with the way of overcoming these risks, and in this regard, this chapter will attempt to create the integrated framework for security, governance, and compliance. Several frameworks will be used in developing this framework, namely: ISO/IEC 27001, NIST Cybersecurity Framework, ITIL, and Zero Trust.

3.1 Governance Layer

The uppermost layer within the framework will therefore be the Governance Layer, whose primary function will be strategic direction and governance in information security.

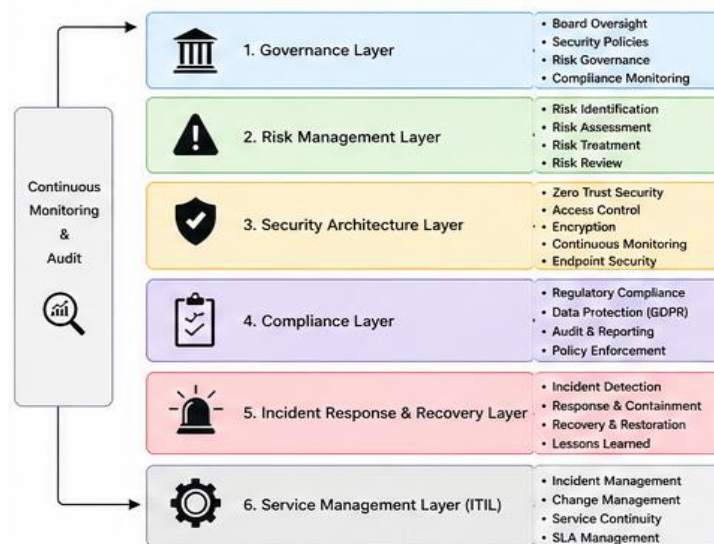


Figure 04: Integrated security governance model for finsure bank (FSB)

Based on Figure 4, the governance layer entails the following:

- Security board-level awareness
- Security policy
- Security risk management committee
- Information security compliance monitoring unit

Governance ensures that the information security is not looked upon as a tactical issue, but rather a strategic one. The policy must address the areas of data protection, acceptable use policy, BYOD policy, and access control.

The ISO/IEC 27001 framework requires governance and organizational leadership [1].

3.2 Risk Management

The second element of the framework focuses on the process of risk management, which plays a vital role in identifying potential cyber security threats.

This includes an ISO 27001 risk management process including:

- Risk identification
- Risk analysis

- Risk assessment
- Risk treatment



Figure 05: Risk management lifecycle for organisational security.

Figure 5: Lifecycle of Risk Management at FSB

The various risks that the organization faces include:

- Cloud misconfiguration risks
- Insider threat risks
- Phishing risks
- Phishing risks
- Unauthorized BYOD
- Risks of third-party data breaches

The NIST Cyber Security Framework helps the organization accomplish this objective through its Identify and Protect capabilities [2].

Various risk treatments can include:

- Sensitive information encryption
- Multi-factor authentication
- Role-based access control
- Continuous monitoring

3.3 Security Architecture

Another layer of the model is the Security Architecture Layer, which will ensure the implementation of all mentioned preventive and detective controls.

Main components include:

(a) Zero Trust Security Model

Zero Trust model plays an important role in the architecture. This approach follows the "never trust, always verify" rule and provides for the continuous authentication and authorization of all participants of interaction.

According to Figure 3: Zero Trust Architecture Model, access is granted only after verification of who or what device attempts to gain access.

Such architecture is crucial for FSB, as the organization uses:

- BYOD
- remotely available network services
- cloud environment

Zero Trust model protects the network against insiders and lateral movement [4].

(b) Encryption and Data Protection

To ensure safety of the sensitive information, there must be implemented:

- data encryption
- data transmission encryption
- key management system

This point corresponds to the GDPR principle regarding personal data protection [6].

(c) Endpoint Security

Moreover, considering BYOD, FSB must pay special attention to the issue of securing endpoints as well:

- MDM software
- antimalware programs
- compliance of devices

(d) Continuous Monitoring

There must be introduced Security Information and Event Management (SIEM) systems, performing the following actions:

- network traffic monitoring

- logs analysis
- anomalies identification
- alerts generation

This measure correlates with Detect and Respond functions from NIST CSF [2].

3.4 Compliance Framework

The Compliance Layer ensures the laws, regulations, and standards are complied with.

FSB is expected to comply with:

- GDPR (Data Privacy & Protection) [6]
- Financial regulations
- Standards of Internal Audits

A few compliance techniques include:

- Security audits
- Classification of data
- Data retention
- Logging of accesses

The ISO 27001 standard helps in ensuring compliance through documentation and auditing [1].

A Compliance Dashboard should be developed for tracking the following issues:

- Policy violations
- Audit results
- Likelihood of exposure

3.5 Incident Response and Recovery

Incident response planning is essential for minimizing any damage caused by cyber attacks.

The framework outlined above follows the sequence shown in Figure 6: Incident Response Lifecycle, which consists of the following stages:

- Preparation
- Detection
- Containment
- Eradication
- Recovery
- Lessons learned

Furthermore, the company must establish a dedicated SOC for dealing with incidents.

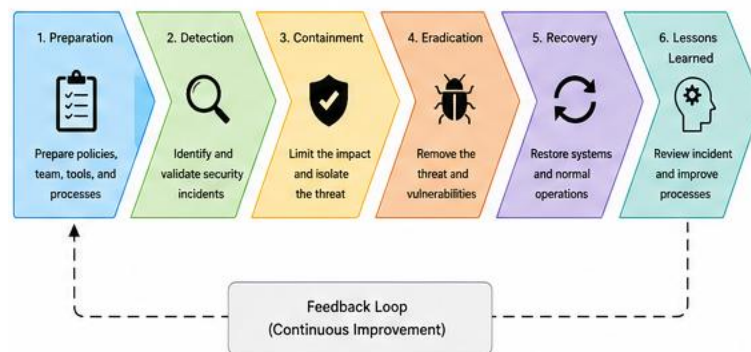


Figure 06: Cybersecurity incident response lifecycle and recovery process.

It is consistent with the NIST Respond and Recover actions intended to ensure business continuity post-cyber-attacks [2]. In this situation, DRP and BCP must be established to ensure system availability during disaster events.

3.6 Service Level Agreements (SLA) and Third-Party Risk

In connection with the use of cloud technology by FSB, SLAs should include:

- Promises of uptime;
- The obligations of security;
- The ownership of data;
- Deadlines for responding.

The importance of third-party risk management lies in the following fact – third parties might become possible targets of any cyber-attack.

Guidelines from ITIL could be useful for SLA management through the introduction of a systematic service management approach [3].

3.7 Frameworks Integration

The proposed framework is not limited to one particular framework, but includes multiple industrial standards:

- ISO/IEC 27001 -> Governance and ISMS framework
- NIST CSF -> Lifecycle of cybersecurity operations
- ITIL -> Services and continuity management

- Zero Trust -> Security access control and architecture

Using those frameworks together would help FSB ensure:

- Governance effectiveness;
- Risk management effectiveness;
- Operations efficiency;
- Effectiveness of security enforcement.

Combination of frameworks is demonstrated in Figure 4, which highlights the interaction of all layers in order to create an ecosystem of security.

3.8 Summary of model's benefits

Some of the advantages that the proposed model would bring in are as follows:

- Greater compliance
- Lesser risk due to cyber attacks
- Safer cloud environment
- Efficient identification & access control
- Better response to incidents
- Enhanced visibility into governance

In essence, this model will ensure that FSB moves from a non-integrated to fully integrated approach towards cybersecurity.

4. CRITICAL DISCUSSION

When analyzing the security, governance, and compliance models for FinSure Bank (FSB), one can consider both benefits and drawbacks of applying the existing industry standards to cope with today's cybersecurity threats. Thus, while the ISO/IEC 27001, NIST CSF, ITIL, and Zero Trust frameworks provide certain advantages if adopted by organizations, the effectiveness of implementing these frameworks often depends on how they will be utilized in organizational operations.

The ISO/IEC 27001 standard provides a solid foundation for developing the ISMS. The reason is that it allows for organizing the management process in a systematic manner with regard to risk analysis. Furthermore, the ISO/IEC 27001 framework is highly suitable for the financial sector, where confidentiality, integrity, and availability (CIA) are critical for cybersecurity. In other words, FSB should protect confidential information, maintain the integrity of data, and ensure its accessibility at any time [1]. However, the biggest drawback of the ISO/IEC 27001 standard is its rigidity. While providing opportunities for continuous improvement according to the PDCA cycle, the standard involves significant administrative and financial investments.

In turn, the NIST Cyber Security Framework allows for an agile model. The identification, protection, detection, response, and recovery as the basic functions within the NIST Cyber Security Framework assist in managing the cyber-security on a lifecycle basis [2]. The ability to be agile proves advantageous in the case of the NIST CSF because it operates in the dynamic digital banking industry environment. However, the lack of formal certification within NIST CSF undermines its application concerning compliance. If companies are required to comply with the rules, it would be better to apply ISO 27001 although it is less applicable.

ITIL can contribute to the effective governance of IT services through the provision of systematic and efficient delivery. In particular, the application of the ITIL approach to incident management and change management allows minimizing outages and avoiding security configuration errors due to the change of the system [3]. It should be stated that ITIL, however, does not serve as a cybersecurity framework by definition. Due to the limited nature of technical cybersecurity within ITIL, its incapability of dealing with advanced cyber threats like the one posed by an insider threat becomes evident.

Regarding FSB, another framework in security that would be worth considering when dealing with contemporary cyber threats would be Zero Trust. With the application of Zero Trust, there is a drastic shift from the current security paradigm based on trust to a completely different security paradigm based on no trust at all [4]. The key importance of Zero Trust is that it allows for continuous validation of the user, device, and access request. Although Zero Trust will ensure mitigation of lateral movements and insider risks, its application might be challenging and expensive for businesses.

What is essential to consider is that none of the security models stated above can address challenges effectively. ISO 27001 addresses governance issues; NIST addresses operational cybersecurity; ITIL addresses service management; and Zero Trust addresses access control. Hence, gaps may arise due to the absence of overlap between those models. It is necessary to fill those gaps through integration, which would require developing a hybrid framework for FSB and any other similar organisations.

The combination of both frameworks would be beneficial for FSB to adopt the correct security strategy since ISO 27001 provides compliance and governance, NIST – resiliency of operations, ITIL – resiliency of services, while Zero Trust will provide security enforcement. In addition, the combination of the two approaches aligns with the recommendations regarding cybersecurity adopted by modern companies [5], [6].

However, it is also important to mention that the use of two approaches creates challenges as well. First, overlapping of two frameworks could be identified, which makes implementation costly and complicated.

5. CONCLUSION

In this study, key concepts in regards to cybersecurity, IT service management and governance associated with FinSure Bank (FSB) have been evaluated in depth. Those concepts include ISO/IEC

27001, NIST Cybersecurity Framework, ITIL, and Zero Trust. An integration framework was proposed which can help address the security, governance and compliance challenges faced by FinSure Bank (FSB).

Upon reviewing all four models, it is clear that they each have their unique advantages. For example, the ISO/IEC 27001 provides an integrated governance framework that enables proper risk management and international standards compliance [1]. The NIST Cybersecurity Framework supports dealing with cyber security threats via identification, protection, detection, response and recovery lifecycle approach [2]. In addition, ITIL framework contributes to increasing operational efficiency via implementing effective processes in regards to incident and change management under the scope of IT Service Management [3].

However, in spite of all those strengths, the research proves that it is impossible to address all cybersecurity challenges that the FSB faces by applying only any of those models. ISO 27001 is too rigid, NIST lacks certification processes, ITIL does not cover any deep security strategies, and the Zero Trust concept is extremely complex. Therefore, it is necessary to apply all these models at once.

This integration of models will ensure that all aspects of governance, risk management, security operations, and access control become parts of one security strategy. Thus, it will become possible to comply with all regulations, enhance incident detection and management, improve the security of data and achieve business continuity in any cyber-attack situation. In addition, this model will enable the application of GDPR requirements in practice, which is essential for banks dealing with private information of their clients [6].

However, the successful implementation of such an approach would demand organizational commitment, qualified personnel, and utilization of advanced security technologies. Assessment, audits, and change of policies are essential processes that will ensure the effectiveness of such a system. Lastly, the company should avoid the emergence of any duplications and inefficient activities due to the adoption of the framework.

To sum up, the integration of ISO 27001, NIST CSF, ITIL, and Zero Trust framework is an ideal strategy in terms of solving the current problems associated with cybersecurity in FSB. In other words, this comprehensive security approach will help FSB move from fragmented security initiatives to a complex security management system that will be regulated by the principles of risk management and compliance. The above mentioned approach will be important in terms of securing the digital financial systems and gaining customer trust [5], [7].

REFERENCES

- [1] ISO/IEC, "ISO/IEC 27001: Information Security Management Systems," ISO, 2022.
- [2] NIST, "Framework for Improving Critical Infrastructure Cybersecurity," National Institute of Standards and Technology, 2023.
- [3] AXELOS, "ITIL 4 Foundation: IT Service Management," 2021.
- [4] S. Rose et al., "Zero Trust Architecture," NIST SP 800-207, 2020.
- [5] ENISA, "Threat Landscape Report 2023," European Union Agency for Cybersecurity, 2023.
- [6] European Union, "General Data Protection Regulation (GDPR)," Regulation 2016/679, 2018.
- [7] A. Behl and K. Behl, Cybersecurity and Cyberwar: What Everyone Needs to Know. Oxford University Press, 2020.