Prifysgol Cymru
Y Drindod Dewi Sant
University of Wales
Trinity Saint David

STUDENT NAME	:	LIKHITHA PYNENI
STUDENT ID	:	2509981
MODULE	:	DATA SECURITY , GOVERNANCE AND COMPLIANCE
MODULE CODE	:	ACCA7028
LECTURER	:	DR. DIPO DUNSIN

Table of Contents

1. Introduction 3

2. Security frameworks and models 3

2.1 Information security frameworsks 3

2.2 ISO/IEC 27000 series 4

2.3 NIST cybersecurity framework (CSF) 4

2.4 COBIT (Control objectives for information and related technologies) 5

3. Security models 6

3.1 Bell-LaPadula model (BLP) 6

3.2 Clark-Wilson integrity model 7

4. Designing a security approach for NG 9

4.1 Security governance and compliance strategy 9

4.2 Justification for security measures 12

5. Importance of regular updates to regulations and standards 13

6. Conclusion 14

7. References 15

1. Introduction

NatureGreen operates globally as a healthy living products company that depends heavily on wireless networks and cloud-based IT services in multiple locations worldwide. NG depends on its complex digital structure that unites internal and external information systems so it needs strong controls for maintaining data security and governance and meeting compliance requirements. The extensive use of Internet-based services by NG creates multiple cybersecurity threats that involve unapproved network access and data violations as well as intellectual property theft.

Evaluation of proven security frameworks alongside models is necessary to resolve present security problems. Leading information security frameworks represented by the *ISO/IEC 27000 series* that serve as guidelines for creating and sustaining efficient Information Security Management Systems (ISMS) are investigated in this report. The study examines two different organizational frameworks namely NIST Cybersecurity Framework (CSF) and COBIT that provide systematic approaches to IT governance and risk management. Security research evaluates these security models together with the Bell-LaPadula model which depends on data confidentiality protection and the Clark-Wilson model which maintains data integrity through strict control programs.

Analysis of different security frameworks, models, and systems helps develop complete security solutions for NG's operational environment. The study focuses on three major security dangers that result from staff using personal devices alongside cloud system vulnerabilities and wireless network issues. Continuous updates are required for security regulations to create alert governance strategies that both respond to evolving cyber threats and match internationally approved best practices and relevant regulations.

2. Security frameworks and models

2.1 Information security frameworks

Information Security Frameworks present a planned systematic structure to handle security risks by ensuring proper asset protection and supervision for organizations. An organization benefits from security framework integration through the deployment of security controls which focus on a combination of technical and managerial aspects. The information security frameworks which have gained widespread popularity include *ISO/IEC 27000 series*, *NIST Cybersecurity Framework (CSF)* and *COBIT (Control Objectives for Information and Related Technologies)*.

2.2 ISO/IEC 27000 series

Standardization framework created by the ISO/IEC 27000 series reaches peak significance in its definition of the Information Security Management System standard as ISO/IEC 27001. The standard details mandatory criteria for executing and supervising information security process implementation alongside permanent enhancement activities. The framework adopts risk-based standards for security defense systems which need individualized protection measures for organization-specific threats (Alshar'e, 2023). The Information Security Management System depends on documentation systems and internal audits along with management reviews to evaluate control effectiveness continuously. Customer trust grows for organizations that implement the ISO/IEC 27000 series standards which creates strong regulatory compliance and forms an established security operational framework.

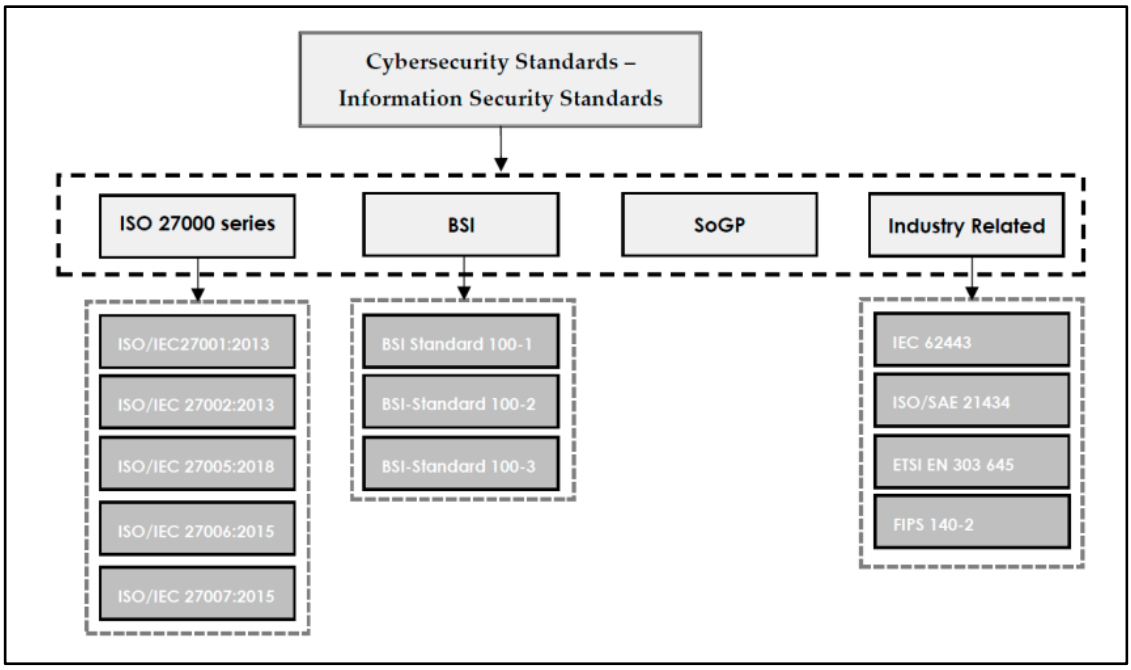

Figure 1: ISO 27001 Framework Components

(Source: Taherdoost, 2022)

ISO/IEC 27001 enables organizations to properly define roles through structured framework assignments necessary for handling incidents with efficiency and securing fast responses to security breaches.

2.3 NIST cybersecurity framework (CSF)

NIST Cybersecurity Framework (CSF) provides organizations with an adaptable risk management system for cybersecurity threats that originally targeted critical infrastructure but now benefits various industries. The framework contains five major functions that include Identify, Protect, Detect, Respond and Recover. Organizations need asset management with

risk assessment and appropriate governance policies to grasp their risk-based environment under the Identity core function (Koza, 2022). The Protect function consists of establishing protective measures for critical service delivery using access control protocols and awareness education together with data security strategies.

Function Identifier	Function	Category Identifier	Category
ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
		ID.SC	Supply Chain Risk Management
PR	Protect	PR.AC	Identity Management and Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes and Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology
DE	Detect	DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
RS	Respond	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

Figure 2: NIST Cybersecurity Framework Functions

(Source: Delgado *et al.* 2021)

Detect practice underlines organizations' need to maintain permanent surveillance which leads to prompt detection of security incidents. Organizations create response protocols through the Respond function to handle discovered incidents while reducing their consequences. Service restoration plans and their execution form the basis of the Recover function. Through its complete structure the NIST CSF helps organizations build resilient cybersecurity posture by integrating its functions with existing risk management processes.

2.4 COBIT (Control objectives for information and related technologies)

COBIT (Control Objectives for Information and Related Technologies) functions as a governance framework which links information security projects to corporate business aims. COBIT delivers best practices together with control objectives which establish effective methods to manage IT governance (Kesuma *et al.* 2022). Through its established framework organizations acquire productivity tools to monitor IT systems and measure their operational effectiveness. COBIT helps organizations validate security investments which enable the

fulfilment of extended organizational goals due to its capability of connecting IT strategy to business approaches.

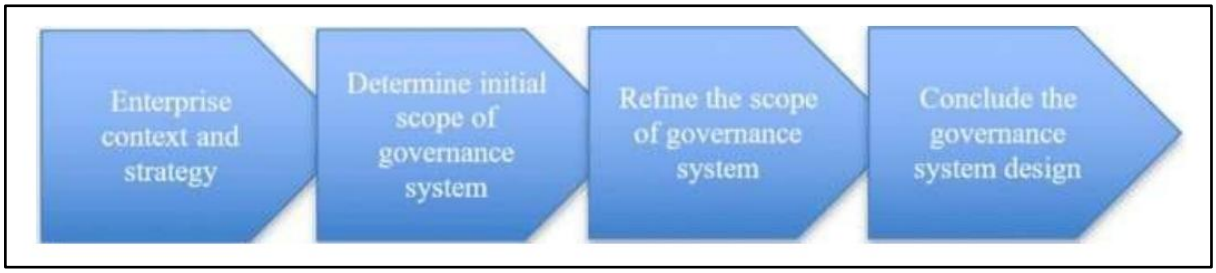

Figure 3: COBIT Governance Structure

(Source: Wulyatiningsih *et al.* 2024)

COBIT framework implements a systematic auditing system and performance evaluation process to fulfil compliance needs. IT function transparency and accountability improve because of this strategic alignment which creates a risk conscious environment for continuous improvement.

These specific security frameworks present separate strengths that help organizations build up their security position. The ISO/IEC 27000 series presents organizations with an internationally accepted comprehensive methodology to handle information security by focusing on risk evaluation and continuous advancement. The NIST CSF offers organizations a risk management solution through its function-based framework which adapts well to changing cybersecurity conditions. COBIT serves as a bridge between IT governance and business objectives to ensure that security initiatives support broader organizational goals. The mentioned frameworks comprise a strong base that assures that data is secured, governed and proved in depth, across complexly executional environments.

3. Security models

Security models offer a methodical procedure to make sure that sensitive data will stay secure from People having no legal access to it and ineffectively disposed of. *Bell-LaPadula (BLP)* and *Clark-Wilson Integrity Model* are two well-known models which are able to solve different information assurance issues, solely, confidentiality and integrity, respectively (Tesfamicael *et al.* 2021).

3.1 Bell-LaPadula model (BLP)

Bell-LaPadula Model (BLP) is focused mainly for the enforcement of the data confidentiality in situation where access control to the classified data is of critical nature, like in government and military systems. At the core of BLP is the classification of security for both subjects (users) and objects (data) and building upon this hierarchy to determine access levels.

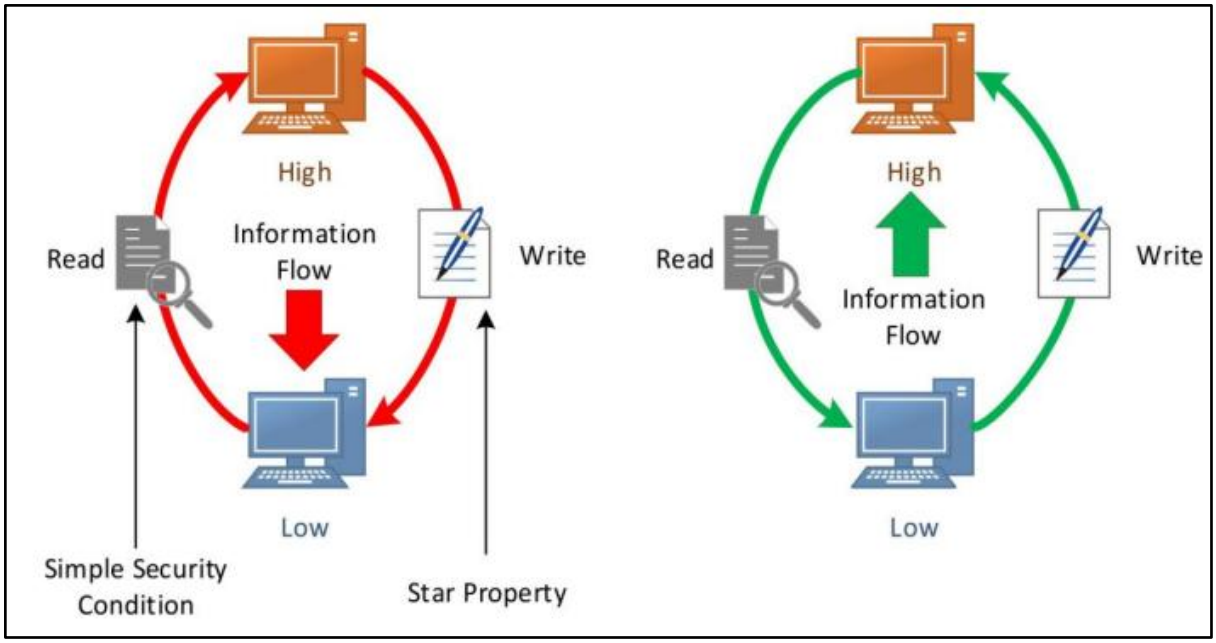

Figure 4: Bell-LaPadula Model Diagram

(Source: Bai, and Son, 2024)

Bell-LaPadula model preserves two distinct properties: the simple security property, which denies the subjects of reading data of higher classification (also known as "no read up"), and the *-property (star property), which denies the subjects of writing data of lower classification ("no write down"). These rules prevent sensitive information from leaking from higher to lower security levels thus preventing data leaks (Delbugio, and Madisetti, 2024). The current model is able to prove effective yet its absolute hierarchical structure reduces adaptability in commercial fields that need fluid access controls.

3.2 Clark-Wilson integrity model

Clark-Wilson Integrity Model provides necessary data integrity protection for commercial and financial sectors that need accurate consistent information. The model moves beyond access regulation to validate that every system transaction proceeds through authorized standard procedures.

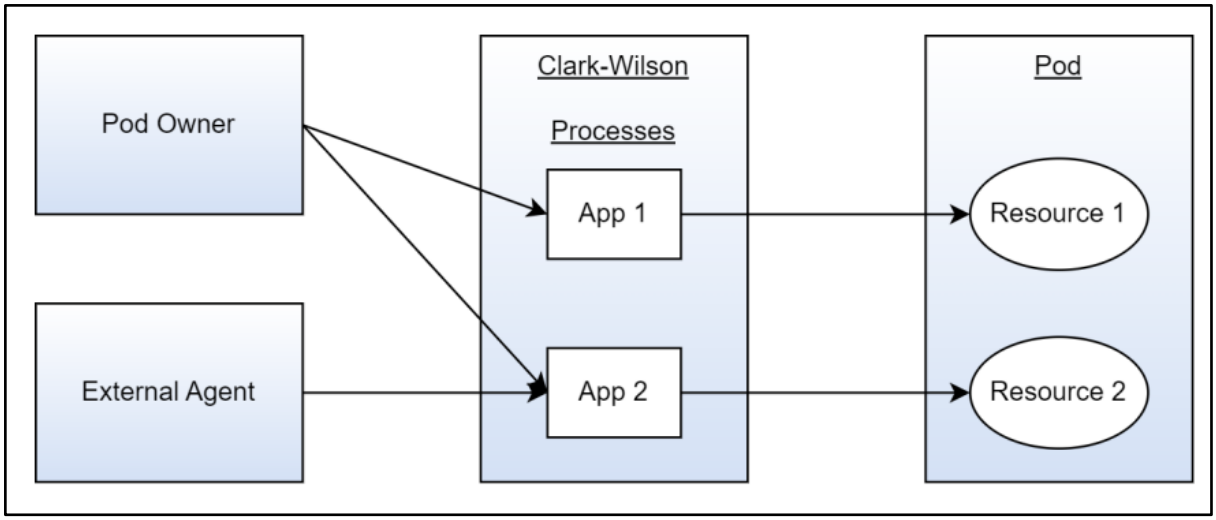

Figure 5: Clark-Wilson model diagram

(Source: Forsyth, and Horne, 2024)

Clark-Wilson model is capable to apply two core elements called constrained data items and transformation procedures for managing critical information processes. Stop data errors and fraud through its complete separation of duties can be done using Clark-Wilson Integrity Model. It is able to minimizes individual control of data processing systems (Yesin *et al.* 2021). The model's integrity goals receive support through certification and enforcement rules with regular auditing functions designed to find unauthorized modifications.

Model	Concentrations/Focus	Applications
Clark-Wilson Security	Separation of duties through Integrity Verification Procedures.	Data integrity
Chinese Wall Security/Brewer and Nash	Information security access controls to mitigate conflict of interest	Authenticity, Authorization
Bell–LaPadula	Protection of information from unauthorized disclosures.	Data Confidentiality
Graham Denning	Assignment of specific access rights	Authentication
Harrison-Ruzzo-Ullman	Discretionary Access Control	Authentication

Figure 6: Comparison of Bell-LaPadula vs. Clark-Wilson Models

(Source: Omollo, 2024)

The two systems serve different parts in information security implementation. The Bell-LaPadula model creates a strong system to protect sensitive data confidentiality and the Clark-Wilson model establishes practical techniques for maintaining data integrity through transactional controls combined with different personnel tasks (Xu *et al.* 2022). Strategic

security operations benefit from the unified concepts of these models which preserve both vital information security and critical data asset integrity in present-day complex operational zones.

4. Designing a security approach for NG

4.1 Security governance and compliance strategy

Security governance and compliance is a very crucial framework in the security of information assets as they seek to maintain their security by keeping them secure, accurate, and accessible. A systematic plan of management of security ensures its integration with corporate goals, maintaining compliance with laws and rules (Folorunso *et al*., 2024). Any security control and risk management plan must therefore mean integrating policies, controls, risk management, and compliance frameworks for new-generation threats. Security governance is a strategic approach to deliberate on security risks and offers an organized procedure of oversight for an organization (Eltayeb, 2024). This involves setting up security activities and measures that specify who should do what as well as aspects such as policies and measures in terms of enforcement of security practices. Security management consists of the identification of a leadership body for security management, security objectives, risk management implementation, and adherence to industry standards (Boeken, 2024).

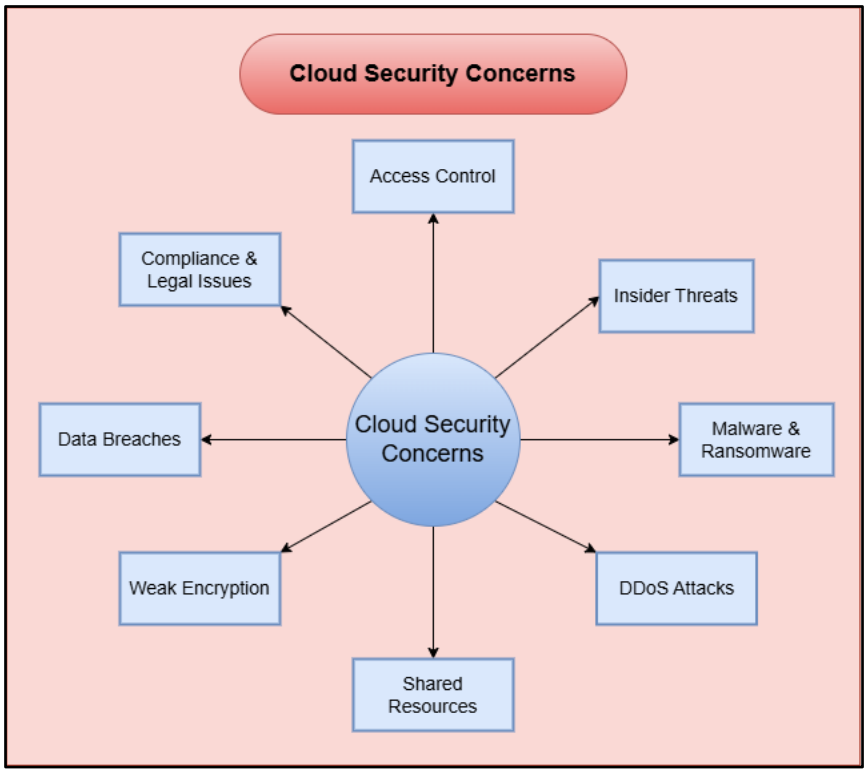

Figure 7: Cloud Security Concerns

Security principles should be spelled out in policy about the protection of data, users' rights, and operations security. The ISO 27001 is an international standard on how to implement

controls in an organization's environment and maintain compliance while the NIST Cybersecurity Framework is a set of guidelines that an organization can use in developing and operating cybersecurity systems (Wang *et al*., 2024). Risk management also forms part of security governance that involves the identification, assessment, and control of risks. Risk management can be described as a definitive approach covering highly valuable resources, assessing their exposure, and adopting the most effective protective measures against threats (Ilori *et al*., 2024). The daily check can enable a constant evaluation of the risk levels to make constant and appropriate amendments to security measures. Security awareness programs also support governance since they offer the employees security risks, compliance requirements, and measures that can be taken to prevent human factors in security (Sargiotis, 2024).

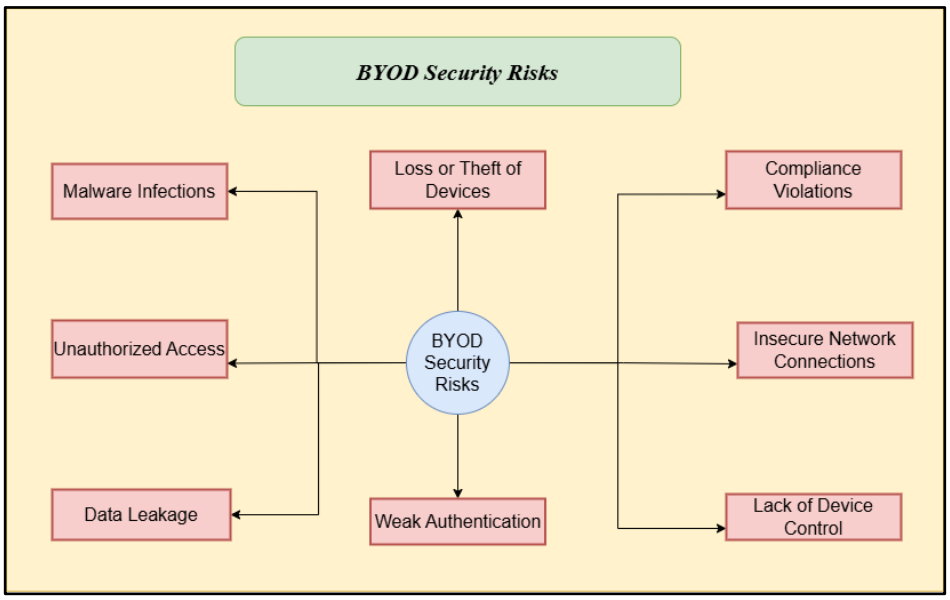

Figure 8: BYOD Security Risks

There can be certain inherent dangers in implementing security training, but with the right approach, a security training program prevents such occurrences and ensures that staff follow the best security practices (Efunniyi *et al*., 2024). Response and business continuity strategy are segments of the technical security management system. A structured incident response plan will lead to quick identification of an incident, distortion of the situation, and eradicating it. It also entails the use of forensics, threat intelligence, and after-incident positions to enhance security measures (Tjilen *et al*., 2024). That is why it is crucial to make sure that an organization has an adequate response strategy formulated and implemented in order to avoid or at least limit the consequences of such incidents as well as to prevent significant financial and reputational losses.

Table 1: Security governance and compliance strategy

Component	***Description***
Framework for security governance	It sets out the roles and responsibilities of enforcing and oversight authorities, as well as the penalties.
Security policies	It provides organizational, administrative, physical, technical, and communication security measures for data captured on different mediums and platforms, as well as provisions for access control.
Risk management	It reviews and controls the enterprise security risks trip, assesses, and minimizes the security threats in an organization.
Security awareness training	It sensitizes the employees to the dangers of such threats and empowers them with ways that they can avert them.
Response and recovery to incidents	It is used for the quick identification, isolation, and prevention of occurrences and their resolution.
Observance of regulations	Compliance with legal standards and all the industry regulations usually plays a good role, consequently, it should be strictly followed.
Data privacy and protection	It helps to decide and apply methods of protecting data from being accessed by unauthorized people.
Risk management for third parties	It periodically evaluates the security measures in dealing with the vendors and creates agreements with them.
Constant tracking and reporting	It uses solutions that are based on SIEM and can help detect threats in real time.
Model of zero trust security	It adopts high levels of authentication and authorization procedures and policies.
Multi-level defense approach	It combines firewalls IDS and endpoint protection mechanisms.
Design-based security	Embeds security controls in system development.
Automation and policy enforcement	It incorporates automation when performing security measures to optimize security.
Regulatory evaluations and audits	It assesses the security standards and their adherence and maps any deficiencies.

Compliance management defines the process of maintaining an organization's compliance with rules and regulations that concern information security and contractual obligations. These duly chosen standards are *GDPR, ISO 27001, PCI DSS, HIPAA, and SOC 2,* through which certain steps are already framed and laid out to secure information and manage risks (Sun *et al*., 2025). Compliance audits and assessments ensure the adequacy and operating effectiveness of security measures and the potential weaknesses need to be reviewed regularly to meet regulatory standards. A company's internal and external audits play a critical role in upholding accountability while, at the same time, managing risks and developing a company's security outlook. Rules to protect the data include the use of encryption, access control systems, and data classification to minimize access to sensitive data.

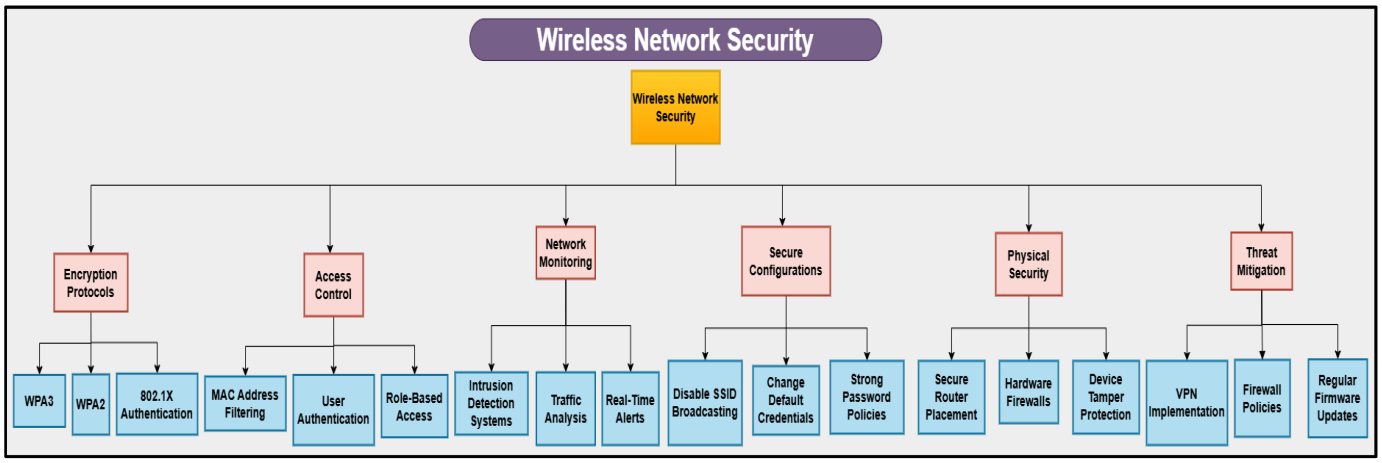

Figure 9: Wireless Network Security

Advertisement emphasizes privacy regulations that are aimed at protecting personal and business-critical information to minimize cases of violation and legal risks. Third-party risk management goes a step further in security governance as it evaluates the systems and procedures security of companies' vendors, partners, or cloud services providers (Solaimani, 2024). About external security risks, one can mention the following: Scheduling agreements of the service level, signing security agreements, and periodic third-party assessment.

4.2 Justification for security measures

Security measures need to be initiated to protect information within an organization, to ensure witnessed compliance with the guidelines of the industry, and to counter potential risks from pure cyber threats. A systematic security arrangement helps in managing security for the protection of data confidentiality, data integrity, and data availability for business use. In order to justify security measures one must factor such things as the security threats or risks and the regulatory mandate, operational risks, and of course the future security gains. The danger posed

by cybercriminals has not been reduced as they resort to using complex strategies like ransomware, phishing, and APTs. If there are no strict security policies in an organization, it results in financial loss, loss of reputation, and fines.

Legal requirements necessitate the adoption of the measures of securing personal and corporate information. GDPR, HIPAA, and PCI DSS Working frameworks have strict protocols for data security. These include fines, legal sanctions, legal prosecution, and restrictions on the operation of an organization. Those requirements are met by employing encryption, secure access controls, and constant compliance checks. Risk management forms the basis for security justifications for their investments (Akbas, 2024). Any business must decide on the organization's weak points, determine possible attacks and their likelihoods, and adopt defenses to minimize risks. A risk assessment mechanism incorporates a Threat Risk Assessment as well as vulnerability scans also known as Penetration testing and security audits that help in evaluating vulnerabilities before they can be effectively exploited. ISO 27001 or NIST Cybersecurity Framework are valuable since they offer structures on how to identify the risks and how to manage them.

Business continuity and disaster recovery planning can be regarded as the prime reasons for implementing proactive security controls. Malicious events like data leakage and DoS attacks have the potential of crippling any business and bringing operations to a halt thus resulting in losses. Business continuity involves having sources of power supply, the avails and backup power supplies, plans as well as arranged recovering systems (Gnatyuk *et al*., 2024). SIEM solutions help in increasing real-time monitoring and response, thus improving the short time taken to resolve the incidents. Internal threats remain a challenge to any organization, meaning that there should be strict policies governing users and their activities. In this case, insiders are those people who are part of the organization or work as contractors or even those performing freelance jobs for the organization.

5. Importance of regular updates to regulations and standards

Continuous updates of the regulations and the standards are important since the new types of threats are being developed from time to time. Technological advancement poses new threats that cybercriminals seize hence the need to increase security mechanisms (Shabina *et al*., 2024). The regulatory bodies and the standardization organizations modify them from time to time to reflect new developments in risk scenarios and to see that the organizations put in place measures that will protect the information (Lincke, 2024). Some of the cyber threats are ransomware, advanced persistent threats (APTs), and zero-day vulnerabilities, all of which are

dynamic. Old policies do not meet the current threats that are employed which makes organizations vulnerable to security threats (Wang *et al*., 2024). The need to update the standards will make security controls relevant across the growing new threats such as encryption, authentications, and network security.

Staying up to date with the new laws helps avoid future repercussions of a legal and fiscal nature. A company that neglects the rules of different updated legislation like GDPR, or certain industrial norms like the PCI DSS can face heavy penalties, legal procedures, and tarnished reputations. Continual updates act as a means of ensuring that the security policies meet the existing and applicable legal requirements hence reducing the probability of getting into trouble for not following the legal aspects that are provided on the issue of security (i Alnuhait and Ahamad, 2024). Some of the forms of change are cloud computing, artificial intelligence (AI), and the Internet of Things (IoT), called the new and progressive generation, which has brought changes that need technologically advanced security measures. New regulations are up to date to handle security threats provoked by new technologies, so that risk management is optimal (Manzoor *et al*., 2024). ISO 27001 and more recently the NIST Cybersecurity Framework adapt continuously, to include newer means of security adding up to the defense against cyber threats.

6. Conclusion

Research on the Security framework evaluation of Nature Green helps to conclude that modern organizations should establish formal governance structures as well as effective risk control strategies for digital environments. The effectiveness of technical control alignment with organizational goals becomes evident through the evaluation process of international standards like ISO/IEC 27001 as well as fitting NIST Cybersecurity Framework and COBIT models. The Bell-La Padula model alongside its Clark-Wilson counterpart has been studied as it demonstrates particular control solutions to stop data confidentiality issues and data integrity violations while protecting against unauthorized system access and data breaches. Since regulatory updates persist without interruption it proves that active security practices and legal fulfilment need continuous monitoring to counter new cyber threats. The establishment of a key security stance depends on methodical risk evaluations planned incident responses and user security instruction programs that protect intellectual property contents and protect sensitive data for seamless operations. Successful execution of such defensive measures results in superior protection from modern cyber risks which preserves the organization's worldwide market advantages.

7. References

Akbas, E., 2024, October. Assessing the Frontiers of SIEM Technology: A Rigorous Evaluation and Validation of Innovative Features in SIEM Solutions. In *Proceeding of the 2024 6th International Conference on Information Technology and Computer Communications* (pp. 21-29).

Alshar'e, M., 2023. Cyber security framework selection: Comparision of NIST and ISO27001. *Applied computing Journal*, pp.245-255.

Bai, R. and Son, J., 2024. Developing and Building a Multi-Level Security Access Control Policy Using OWL. *Pan-Pacific Journal of Business Research*, *15*(1).

Boeken, J., 2024. From compliance to security, responsibility beyond law. *Computer Law & Security Review*, *52*, p.105926.

Delbugio, J.M. and Madisetti, V.K., 2024. Enhanced memory-safe linux security modules (eLSMs) for improving security of docker containers for data centers. *Journal of Software Engineering and Applications*, *17*(5), pp.259-269.

Delgado, M.F., Esenarro, D., Regalado, F.F.J. and Reátegui, M.D., 2021. Methodology based on the NIST cybersecurity framework as a proposal for cybersecurity management in government organizations. *3 c TIC: cuadernos de desarrollo aplicados a las TIC*, *10*(2), pp.123-141.

Efunniyi, C.P., Abhulimen, A.O., Obiki-Osafiele, A.N., Osundare, O.S., Agu, E.E. and Adeniran, I.A., 2024. Strengthening corporate governance and financial compliance: Enhancing accountability and transparency. *Finance & Accounting Research Journal*, *6*(8), pp.1597-1616.

Eltayeb, O., 2024. The Crucial Significance of Governance, Risk and Compliance in Identity and Access Management. *Journal of Ecohumanism*, *3*(4), pp.2395-2405.

Folorunso, A., Wada, I., Samuel, B. and Mohammed, V., 2024. Security compliance and its implication for cybersecurity. *World Journal of Advanced Research and Reviews*, *24*(01), pp.2105-2121.

Forsyth, E. and Horne, R., 2024. Clark-Wilson Policies in ACP: Controlling Information Flow Between Solid Apps.

Gnatyuk, S., Berdibayev, R., Aleksander, M., Sydorenko, V., Zhyharevych, O. and Polozhentsev, A., 2024. Software System for Cybersecurity Events Correlation and Incident Management in Critical Infrastructure. In *Data-Centric Business and Applications: Advancements in Information and Knowledge Management, Volume 1* (pp. 247-269). Cham: Springer Nature Switzerland.

i Alnuhait, N.M. and Ahamad, S.S., 2024. RESILIENT FINANCIAL TECHNOLOGY FRAMEWORK WITH TRANSACTION SECURITY AND FAIRNESS. *Journal of Data Acquisition and Processing*, *39*(1), pp.846-860.

Ilori, O., Nwosu, N.T. and Naiho, H.N.N., 2024. Third-party vendor risks in IT security: A comprehensive audit review and mitigation strategies. *World Journal of Advanced Research and Reviews*, *22*(3), pp.213-224.

Kesuma, M., Saputra, R.H., Syaputra, M.A., Fitra, J. and Romahdoni, M.R., 2022. Design Of Information Technology (IT) Governance Using Framework Cobit 2019 Subdomain APO01 (Case Study: Instidla). *J. Teknol. Komput. dan Sist. Inf*, *5*(3), pp.157-162.

Koza, E., 2022. Semantic analysis of ISO/IEC 27000 standard series and NIST cybersecurity framework to outline differences and consistencies in the context of operational and strategic information security. *Med. Eng. Themes*, *2*, pp.26-39.

Lincke, S., 2024. Complying with the PCI DSS Standard. In *Information Security Planning: A Practical Approach* (pp. 45-63). Cham: Springer International Publishing.

Manzoor, J., Waleed, A., Jamali, A.F. and Masood, A., 2024. Cybersecurity on a budget: Evaluating security and performance of open-source SIEM solutions for SMEs. *Plos one*, *19*(3), p.e0301183.

Omollo, R., 2024. A Comparative Review of Business Models in Information Security.

Sargiotis, D., 2024. Data security and privacy: Protecting sensitive information. In *Data governance: a guide* (pp. 217-245). Cham: Springer Nature Switzerland.

Shabina, Ali, R.F., Jahankhani, H., Siddiqi, Y. and Hassan, B., 2024. Ensuring Securing PII Data in the AWS Cloud: A Comprehensive Guide to PCI DSS Compliance. In *Cybersecurity and Artificial Intelligence: Transformational Strategies and Disruptive Innovation* (pp. 185-216). Cham: Springer Nature Switzerland.

Solaimani, S., 2024. From Compliance to Capability: On the Role of Data and Technology in Environment, Social, and Governance. *Sustainability*, *16*(14), p.6061.

Sun, Y., Zhang, Y.F., Wang, Y. and Zhang, S., 2025. Cooperative governance mechanisms for personal information security: an evolutionary game approach. *Kybernetes*, *54*(1), pp.431-455.

Taherdoost, H., 2022. Understanding cybersecurity frameworks and information security standards—a review and comprehensive overview. *Electronics*, *11*(14), p.2181.

Tesfamicael, A.D., Liu, V., Mckague, M. and Caelli, W., 2021. An architecture to facilitate security assurance and legal compliance for call auditing in the wholesale electricity market. *IEEE Access*, *9*, pp.146437-146453.

Tjilen, A.P., Tambaip, B., Dharmawan, B., Adrianus, A., Riyanto, P. and Ohoiwutun, Y., 2024. Engaging stakeholders in policy decision-making for food security governance: Identification, perception, and contribution. *Corporate Governance and Organizational Behavior Review*, *8*(1), pp.144-154.

Wang, W., Sadjadi, S.M. and Rishe, N., 2024, May. A Survey of Major Cybersecurity Compliance Frameworks. In *2024 IEEE 10th Conference on Big Data Security on Cloud (BigDataSecurity)* (pp. 23-34). IEEE.

Wulyatiningsih, T., Mokodaser, W.G. and Mambu, J.Y., 2024. Information Technology Governance Analysis Using COBIT 2019 Framework at Bank Mandiri Girian Bitung Branch. *J. Inf. Syst. Informatics*, *6*(2), pp.865-881.

Xu, D., Wang, W., Zhu, L., Zhao, J., Wu, F. and Gao, J., 2022. CL-BC: A Secure Data Storage Model for Social Networks. *Security and Communication Networks*, *2022*(1), p.5428539.

Yesin, V., Karpinski, M., Yesina, M., Vilihura, V. and Warwas, K., 2021. Ensuring data integrity in databases with the universal basis of relations. *Applied Sciences*, *11*(18), p.8781.