



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

University of Wales Trinity Saint David, London

Data Security, Governance and Compliance ACCA7028

Title: Apply the principles and practices of Data security, Governance and Compliance based on a given scenario.

Submitted by	: Shafee Ul Mahmud Chowdhury
Student ID	: 2436374
Programme	: M.Sc in Cybersecurity and digital forensic
Submitted to	: Dr. Dipo Dunsin
Submission Date	: 19 th December 2025

Abstract

Worldwide health and wellness firm, Nature-Green (NG), which relies heavily on connectivity for its business operations and also promotes the use of Bring-Your-Own-Device (BYOD) policies is exposed to serious cyber threats. to counter these troubles we propose an integrated Security methodology, by aggregating the best practice of cybersecurity frameworks (NIST, ITIL, COBIT, GDPR and ISO/IEC27001) to develop security controls. The emergent Nature-Green Security Framework (NG-SF) balances the governance and technical relatedness based on NGs operational and regulatory requirements. The model materializes an awareness-based architecture crafted for NG's wireless cloud-centric domain, including Zero Trust Architecture (ZTA), Mobile Device Management (MDM), network segmentation, cloud access security and IP protection. A risk-reward analysis proves that the NG-SF dramatically mitigates risks and improves compliance in a cost-effective manner, making it easier for customers to securely adopt BYOD-while helping to secure customer data, employee privacy and very valuable intellectual property worth over one billion dollars.

Table of Contents

Abstract.....	2
1.Introduction	3
2.Literature overview.....	4
2.1 BYOD Security Challenge.....	4
2.2 Wireless Network Vulnerabilities.....	4
3. Overview of Major Security Frameworks	4
3.1 What is security framework.....	4
3.1.1 NIST Framework.....	4
Fig1: NIST Framework V1 vs V2.0	5
3.1.2 IT Infrastructure Library (ITIL)	5
Fig2: ITIL core service management functions and process	5
3.1.3 ISO/IEC Standards	5
Fig-03: ISO/SEC 27001:2022 security control categories.....	6
Fig-04: ISO/IEC 27002 key concept	6
3.1.4 General Data Protection Regulation	6
3.1.5 COBIT.....	6
3.1.6 HIPPA.....	6
3.1.7 Zero trust architechture.....	7
3.1.8 Cloud security framework.....	7
4. Formulation of the NatureGreen Security Framework (NG-SF)	7
5. Suggested Technicaland Enterprise Solution for NG	8

Figure05: Proposed Architecture of NG pharma	9
Figure-06:- Packet flow of proposed infrastructure	10
5.1 Zero Trust Architecture	11
5.2 Mobile Device Management &BYOD Policies	11
5.3 Network Segmentation & Wireless Security.....	11
5.4 Cloud Access Security Broker (CASB)	12
5.5 Data Loss Prevention & Intellectual Property Protection	12
5.6 Business continuity plan	12
5.7 Data Recovery plan	12
5.8 Governance, Compliance & Training	12
6.Conclusion.....	13
7.References	13

1.Introduction

Computers have made our lives multifaceted and easier, while digital systems have made the modern world faster and more dynamic. In this information-based environment, people and organizations benefit greatly; however, it has also increased security-related risks. As individuals' critical assets are now stored digitally, cybersecurity and system dependence have become highly relevant issues.

By definition, cybercrime refers to illegal or harmful activities involving a computer or digital system, carried out through devices or networks. This can include theft of information, financial loss, or other types of damage. Essentially, cybercrime occurs when someone gains unauthorized access to a system and uses its resources to harm others. Therefore, any malicious activity conducted via digital means—such as mobile phones, the internet, or computers—can be classified as cybercrime. [1]

Nature Green is a large, international brand that uses cloud services to provide IT solutions to its clients and employees. The company's main challenge is ensuring the security of client and employee data. Additional challenges arise when a large workforce and international clients access the system using personal devices. Protecting the company's valuable intellectual property is also a major concern.

Intellectual property (IP) refers to unique and intangible assets, including writings, ideas, audio, patents, videos, and other creative works. These assets are highly valuable for organizations, as they preserve the uniqueness of a company and enhance its business competitiveness. Therefore, it is essential for organizations to protect their intellectual property. Cybersecurity is a critical element in safeguarding IP, as it prevents unauthorized access, theft, and other cyber threats. [2]

Notably, approximately 95% of users are connected via wireless networks. While wireless connectivity provides convenience, it also introduces high security risks and can cause delayed network responses due to high latency[[3]]Many organizations face similar challenges. The primary objective of this assignment is to propose an effective solution using a cybersecurity framework. Frameworks such as ISO 27001, NIST, and others will be discussed. By integrating the key features of these frameworks, a new comprehensive model has been developed to ensure information security, effective management, and reliable data availability. [4]

This coursework aim is to cover

Dive into the academic research on security threats of BYOD, cloud and wireless penetration;

Examine major international cybersecurity frameworks;

Construct a new combined G&S model termed as the NatureGreen Security Framework (NG-SF);

Propose a practical five-layer converged security system.

Rationalize it to begin by doing a cost–benefit on the introduction.

2.Literature overview

2.1 BYOD Security Challenge

BYOD type environments significantly expand attack surface area for the organisation through device diversity, inconsistent patching and uncontrolled 3rd party applications. Researches demonstrate that BYOD deployment poses several threats to organizations, such as credential compromise, malware spreading and data stealing via private cloud services [5]. This risk is increased on personal devices for two primary reasons: not only can the organisation not control and secure them, but they also have limited visibility and monitoring capabilities. Disterer highlights privacy issues, lack of clarity in governing responsibilities, and insufficient policy acceptance as typical issues that Organisation will face when attempting to implement a BYOD strategy. These inconsistencies can lead employees to accidentally subvert security measures or mismanage sensitive information. [6].

2.2 Wireless Network Vulnerabilities

Nature Green's 95% network operating wirelessly, the organisation faces severe exposure to compromise such as rogue access points, KRACK attacks, and various forms of impersonation or man-in-the-middle attacks. Enterprise Wi-Fi vulnerabilities commonly stem from weak authentication protocols, poor certificate management, misconfigured access points, and inadequate network segmentation that allows lateral movement [7]

3. Overview of Major Security Frameworks

3.1 What is security framework

A security policy is a hierarchical representation of thresholds on various parameters, organized in the form of modules and each module will have its own threshold. [8]. Various standards like ISO 27001, NIST, COBIT have their unique control and standard which will help in securing the systems. In most cases, a specific framework is not suitable and organizations customize frameworks by incorporating attributes from a variety of models in order to match their particular security needs.[[9]

3.1.1 NIST Framework

Essential guidance is provided by the NIST Framework for improving the cybersecurity of Critical Infrastructure. through its five core functions: Identify, Protect, Detect, Respond, and Recover. These

functions are further detailed by categories, subcategories, and tools such as NIST SP 800-53 (which describes security controls) or the Risk Management Framework to support practical implementation.[10] Visual representations, like diagrams, charts may illustrate how functions are connected with one another and their significance in the framework's categories and tiers.[11]

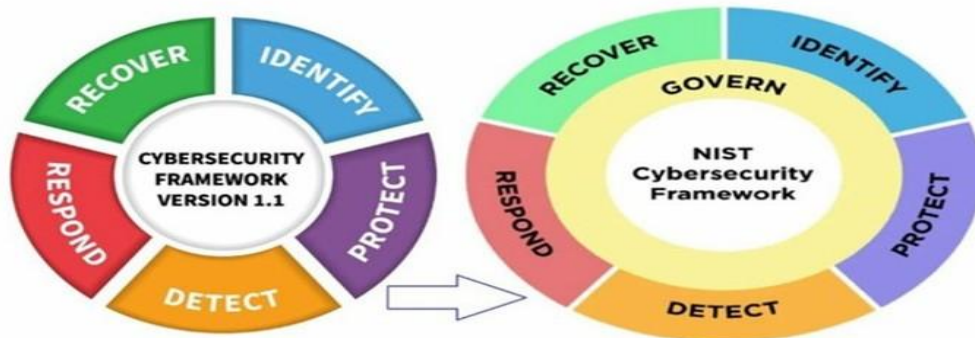


Fig1: NIST Framework V1 vs V2.0

3.1.2 IT Infrastructure Library (ITIL)

The ITIL structure arranges the various IT services in such a way that they are aligned with the objectives of business and implemented through best practices. Its area security management includes access control, incident handling, service continuity and a robust Change Management that evaluates and approves modifications to reduce risk. Although less technologically detailed than NIST [11]ITIL greatly enhances service governance, continuity in operations and ensures accountability which is described in fig:2 [12]

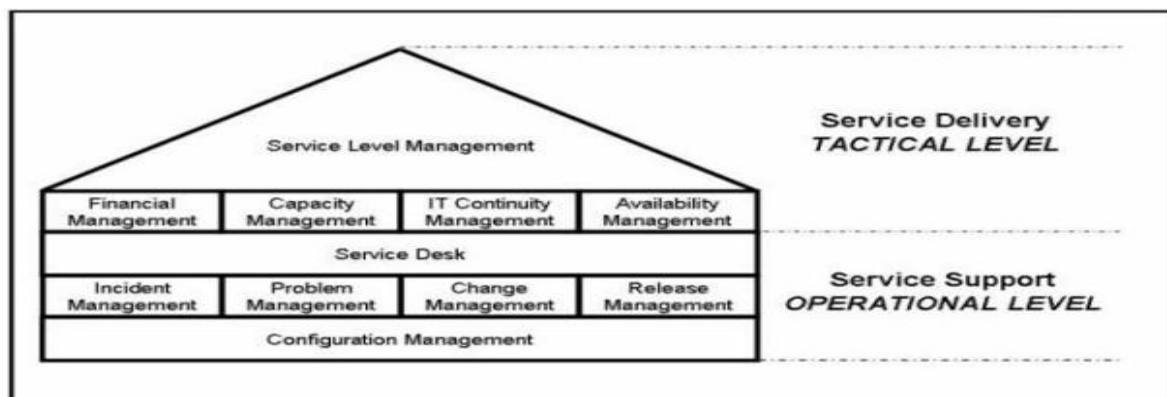


Fig2: ITIL core service management functions and process

3.1.3 ISO/IEC Standards

The ISO/IEC 27000-standard is an internationally accepted solution in the area of information security governance. ISO/IEC 27001 contains mandatory requirements for ISMS implementation and design, analysis of risks, and the management of an ISMS. This is supplemented with more specific control objectives and controls to achieve these in domains such as access control, cryptographic protection, incident response, and asset management by ISO/IEC 27002. These standards developed from the BS

7799 series, providing a model for establishing implementing, monitoring and improving ISMS. Below figure will describe features at a glance fig-03, fig-04 [11]

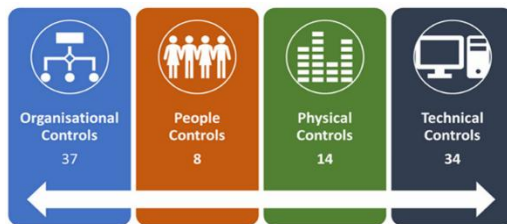


Fig-03: ISO/SEC 27001:2022 security control categories



Fig-04: ISO/IEC 27002 key concept

3.1.4 General Data Protection Regulation

GDPR presides over how personal data is processed, necessitating transparency, the principle of least processing, grounds for lawful processing and technical/organizational measures. NG should perform DPIAs on BYOD access and executive secure processing on customer and employee related data [13]

3.1.5 COBIT

COBIT Governance Model provides an overall framework for enterprise governance addressing IT risk management, performance measurement and compliance. It deals with how to ensure that IT services support business processes and needs, demonstrating value, enabling strategic change and minimizing risk. For groups like NG, COBIT serves as a top-down governance compound that provides decision-makers guidance for deciding what cyber security investments; and abiding by various policies and regulations. COBIT is used by organizations to increase control, standardization and accountability of IT as well as business processes. [14]

3.1.6 HIPAA

The HIPAA Security Rule contains national regulations requiring U.S. health providers to safeguard ePHI. It requires precautions to protect health information, administrative, physical and technical safeguards, such as access limitation, audit trails, encryption and secure transmission of health information. Adherence maintains patient information to be confidential, reliable and available with reduced risk of exposure and unauthorized release.[15]

3.1.7 Zero trust architecture

A Zero Trust Architecture (ZTA) considers all users, devices, and resources as untrusted—regardless of location—and calls for continuous identity verification, least-privilege access and dynamic policy enforcement. ZTA is a fundamental shift of the security paradigm from the perimeter-focused value chains to resource-based protection—every access request is authenticated and authorized based on identity, device posture, and contextual attributes; every asset's trustworthiness is constantly evaluated. This assists in mitigating lateral movement, reducing exposure and being proactive to threats. This makes ZTA especially relevant for today's mixed cloud, remote work and BYOD environments. [16]

3.1.8 Cloud security framework

The CSA Cloud Controls Matrix (CCM), Microsoft Azure Security Benchmark, AWS Well-Architected Framework – Security Pillar and Google Cloud Security Foundations are major cloud-specific security frameworks. As a result, the CCM provides an all-inclusive control framework for cloud security and compliance across 17 domains. Cloud Security Alliance+2Hyperproof+2 The standards developed by Azure, AWS and Google Cloud include vendor-specific best practices for secure architecture related to identity, data protection, governance, threat detection and compliance. These tools help cloud users put the appropriate controls in place and manage risk in the public, private, or hybrid cloud. [17]

4. Formulation of the NatureGreen Security Framework (NG-SF)

Drawing from cyber security best practices, the Nature Green Security Framework (NG-SF) combines guidelines provided by leading cybersecurity frameworks (for example NIST, ISO 27001 / GAISP, COBIT/VALIT, ITIL and GDPR) sharing adequate cloud security standard objectives to address for a complete guide specific to the NG's environment.

NG-SF Core Pillars:

Drawing from the ideas of the above frameworks, NatureGreen Security Framework (NG-SF) is a combination:

- Blockchain as a Transparent Blind Signature and Partial Information Disclosure Since detection data returned to UWB tags comes from numerous normal points accumulates in centralized point, then blockchain can be used to prevent security information between tags and anchor positions.

NG-SF Core Pillars

(Governance & Compliance (COBIT, ISO 27001, GDPR) [9]

- Policies, RA's, DPIA's, audit cycles.

I&AM (NIST CSF, Zero Trust) [16]

- MFA, conditional device access. [5]

Device & Endpoint Management (NIST, ISO) Device and endpoint management standards Guidelines to enhance the defenses in depth for device services across sectors. [16]

- Enroll BYOD, MDM, compliance checks. [5]

Network Security (NIST, Zero Trust)

- Segmentation, micro-segmentation, NAC, WPA3 and 802.1X. [3]

Security In The Cloud (NIST + GDPR principles)

- CASB, encryption, logs and least privilege.

Data Protection & IP Security (GDPR with ISO)

- DLP, IRM/DRM, encryption, logging.

Operational And Incident Management (ITIL + ISO) [12]

- Monitoring, incident response run books, reporting.

People & competence (ITIL + ISO) [9]

- Awareness programs, phishing simulations.

Business continuity and Data Recovery Plan

5. Suggested Technical and Enterprise Solution for NG

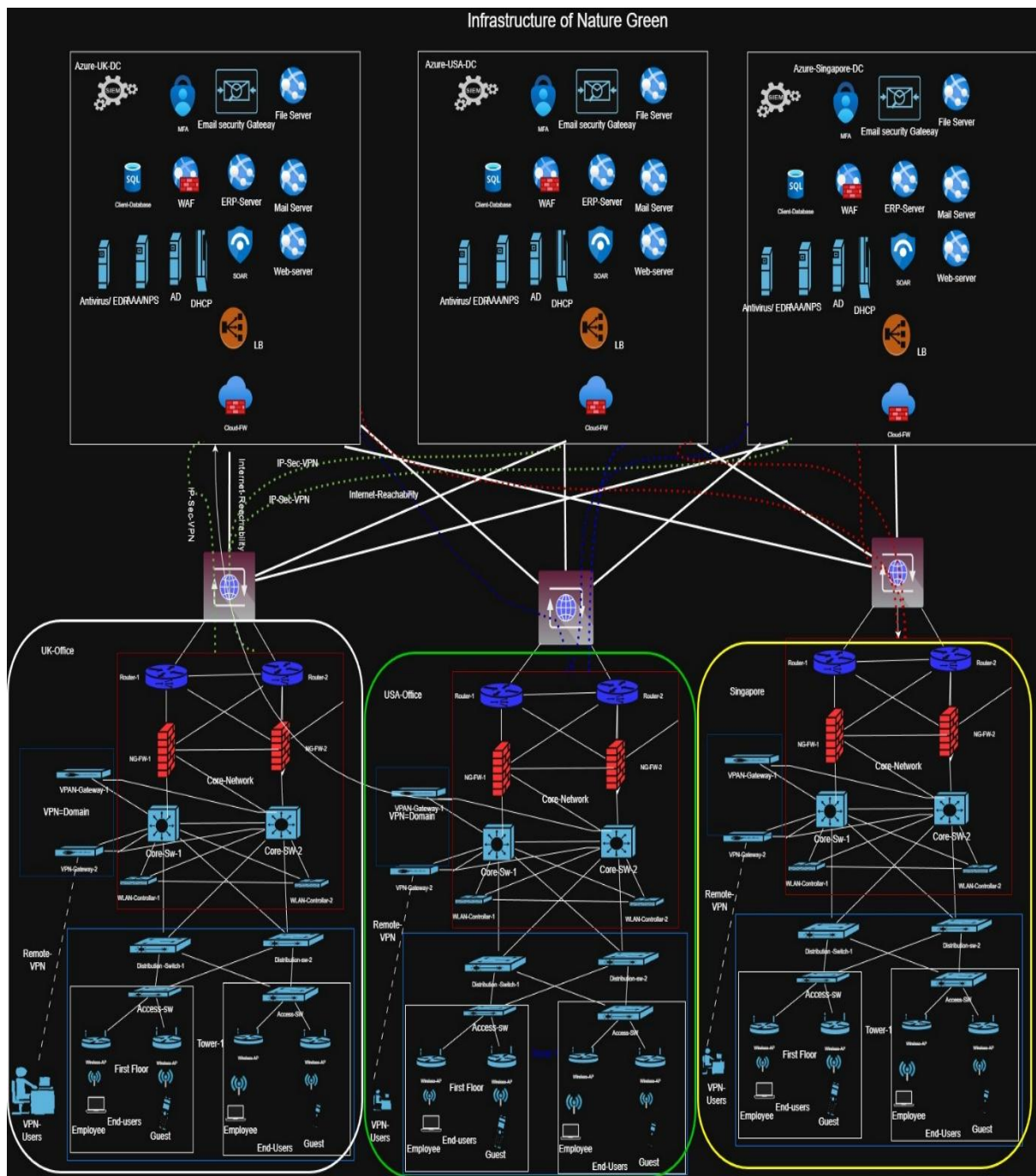


Figure05: Proposed Architecture of NG pharma

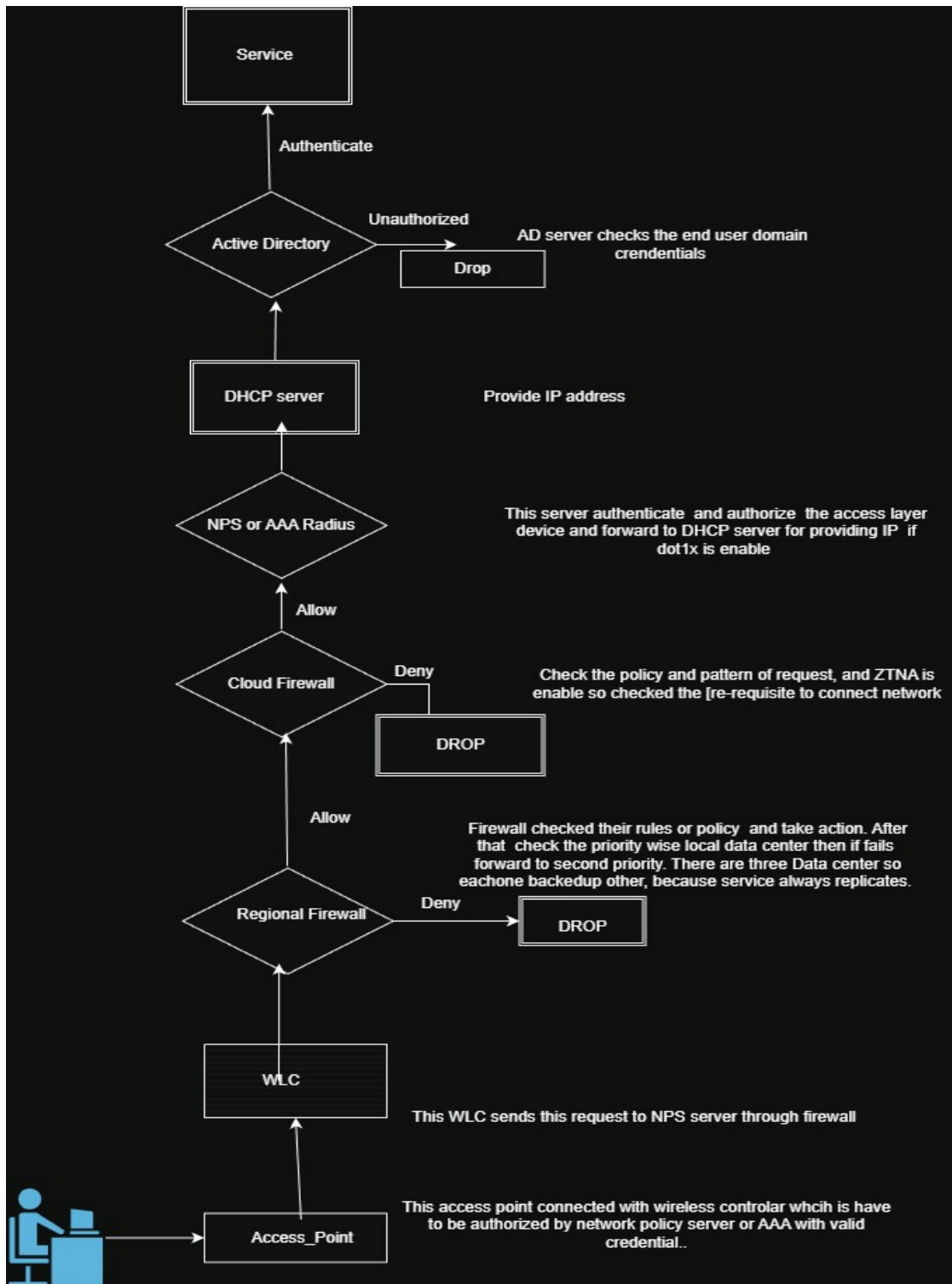


Figure-06:- Packet flow of proposed infrastructure

To provide robust cybersecurity in NG's complex IT and cloud environment requires a comprehensive strategy that links together different layers of technical defences such as Zero Trust Architecture (ZTA), Mobile Device Management (MDM), advanced network security, cloud access monitoring, data protection mechanisms, and oversight. The various components of this framework are elaborated in the following chapters.

5.1 Zero Trust Architecture

The Zero Trust Architecture (ZTA) model attempts to eliminate the implicit trust that traditional security systems entail. In environments with mobile and BYOD (Bring Your Own Device) practices, trust-based relationships are used by attackers to move laterally around a network. It is a ZTA requirement that every user and equipment should be subject to dynamic authentication, no matter what part of the network they occupy. By making sure it is always true, this ongoing authentication means that there is much less risk of breaches being caused--for example, in relation to BYOD [16]

However, by implementing ZTA, NG can eliminate insider threats, reduce lateral movement and even in a distributed system or one that is fully integrated with the cloud, provide secure access.

5.2 Mobile Device Management & BYOD Policies

There are no written restrictions, but as NG mutated into a required legal performance burden, all companies have given preferential attention to the reliability and security of Mobile Device Management (MDM) and Enterprise Mobility Management (EMM). MDM makes it possible make devices accessing business resources more systematic and easier to manage by watching over them, administering policies that are made in real time, and coping with irregular situations when necessary. It can also be customized. [5]

Compulsory Multi-Factor Authentication (MFA): By requiring additional verification factors, MFA strengthens the access controls, and reduces instances of successful credential-based attacks. [18]

VPN: It allows employees to securely connect with regional office network or single user as well [19]

NG can thus introduce BYOD practices in confidence using these MDM measures to provide secure access to corporate systems while also respecting user privacy. [6]

5.3 Network Segmentation & Wireless Security

The next generation network (NG) wireless infrastructure zooms in on a variety of hazards, among which are hostile access points, fraudulent access (or impersonation). To address these risks effectively, businesses must establish rigorous and comprehensive security mechanisms for wireless networking. Enterprises are therefore advised to implement WPA3 Enterprise for stronger encryption [3] adopt 802.1X/EAP authentication to control access to the network, as well as setting Network Access Control (NAC) capabilities that check whether devices entering a domain comply with health standards prior to being given access over said domain [20] In addition, when beacons are separated into groups for corporate use, BYOD and guest access respectively, the possibility of cross-contamination is minimized; while at the same time IP-sensitive environments are enabled by means of micro-segmentation [i.e: VLANs] achieved step by step with Segmentation itself becomes easier. Real-time monitoring tracks any abnormal wireless activity left unchecked by Wireless Intrusion Prevention Systems (WIPS) [21] for as yet unexplained reasons. Employing these techniques accords with best practice in corporate WI-Fi settings and, when added together, enhances overall network security through defense in depth, particularly if combined with Zero Trust Access (ZTA) limits the attacker's movement within any area of any network [16]

5.4 Cloud Access Security Broker (CASB)

Cloud services multiply the problems, especially within BYOD. Cloud Access Security Brokers (CASB) act as intermediaries between users and cloud services, allowing security policies to be implemented. [22]The main features of CASB for Next Generation (NG) are that Cloud Data Loss Prevention (DLP) prevents data from escaping, shadow IT discovery acts like a detective for unauthorized apps, context-aware access control based on device type and user roles gives users freedom or restrictions according to their role in the System, and sensitive data is encrypted or tokenized to fit in under GDPR. [13].Deploying NG enables CASB to enforce uniform cloud security policies, track usage trends, and solve problems that arise from multi-cloud to hybrid environments.

5.5 Data Loss Prevention & Intellectual Property Protection

The need for an integration of Data Loss Protection (DLP) with IPR protection has also become more urgent. Global threats require global measures. Endpoint- and cloud-based DLP and mail interception technology can prevent unauthorized data transfers [2]Wang, Ma, and Xu (2004) insist on the necessity to combine cloud encryption with Digital Rights Management--firewalls and other conventional forms of defence offer no security at all. [23]

5.6 Business continuity plan

Business Continuity Plan A Business Continuity Plan (BCP) is the blueprint for maintaining all critical business functions in case of a disruption, be it natural disasters, cyber-attacks or equipment failures. It identifies essential functions, resources, roles and procedures to mitigate downtime and operational disruption. Regular (inter)national testing and updates strengthen the organization's organizational resilience [24]

5.7 Data Recovery plan

A Recovery Plan in Data Recovery is the process of trying to retrieve IT systems, applications and data following a disturbance. This comprises backup tactics, recovery goals and restoration techniques and verification measures. DRP: guaranteeing reduced data loss; minimum downtime and compliance to regulation. Frequent testing ensures effectiveness [24]

5.8 Governance, Compliance & Training

Effective cybersecurity requires systematic administration, regulatory compliance, and provides individualized training for every end user. [25]NG is to establish an Information Security Steering Committee at the strategic level to execute oversight and risk management responsibilities. [26]Important security measures include: carrying out an annual COBIT/ISO 27001 risk assessment to identify any vulnerabilities; training employees to be aware of cyber threats and how secure information should be handled; ensuring GDPR compliance in terms both of privacy notices and Data Protection Impact Assessments (DPIAs); drawing up for standardized handling of security incidents Incident Response playbooks; and ensuring that suppliers are doing their best to comply with NG's security policies. By combining organization, supervision, and good training methods, one can create safety awareness throughout a company's culture that enhances technical defences. [1]

6. Conclusion

NG suffers from more and more the threat of cybersecurity which is because NG heavily depends on wireless technology and its heavy use of cloud computing. The corporation faces a variety of risks from multiple attack surfaces. In order to mitigate these difficulties, a holistic NatureGreen Security Framework (NG-SF) was developed, taking into account up-to-date studies in the fields of BYOD [5], cloud security and wireless security and international standards like NIST CSF, ISO27001 AND GDPR [6], [26], [18] [12]. NG-SF focuses on governance, compliance, identity-based access control, device and endpoint compliance, network segmentation, and employee awareness of data breaches preventing and IP protection. [16] It is expected that the framework will dramatically curb data breaches and improve NG's overall security operations, thus a cost effective capital expenditure to underpin future innovation and updating in accordance with emerging threats. [23] NG-SF, in the end, provides a secure answer for the open of BYOD to advocate those around-the-world businesses and business entities/users worldwide as well as global employees, customers and their related assets from potential cyber-attacks. [6]

7. References

- [1]B. Reuben-Owoh and E. Haig, “A Systematic Review of Voluntary Cybersecurity Standards and Frameworks,” *International Journal of Information Security*, vol. 24
- [2]Sougata Chattopadhyay “Intellectual Property Rights in Digital Environment”
- [3]L.-Y. Ong, and M.-C. Leow, “Wireless Security Protocols WPA3: A Systematic Literature Review,
- [4]R. Villalón-Fonseca, “The nature of security: A conceptual framework for integral-comprehensive modeling of IT security and cybersecurity,”. 2022
- [5]M. Eslahi, M. V. Naseri, H. Hashim, N. M. Tahir and E. H. M. Saad, "BYOD: Current state and security challenges," 2014
- [6]K. Hussain, A. R. Rahmatyar, B. Riskhan, M. A. U. Sheikh, and S. R. Sindiramutty, “Threats and Vulnerabilities of Wireless Networks in the Internet of Things -2024
- [7]H. Taherdoost, “Understanding cybersecurity frameworks and information security standards—A review and comprehensive overview,” 2022,
- [8]F. Schiliro, “Building a resilient cybersecurity posture: A framework for leveraging prevent, detect and respond functions and law enforcement collaboration 2023
- [9]K. AL-Dosari and N. Fetais, “Risk-Management Framework and Information-Security Systems for Small and Medium Enterprises (SMEs): A Meta-Analysis Approach,

- [10]B. Reuben-Owoh and E. Haig, "A systematic review of voluntary cybersecurity standards and frameworks," -2025
- [11]M. Talla and R. Valverde, "An implementation of ITIL guidelines for IT support process in a service organization," *International Journal of Information and Electronics Engineering*, 2013
- [12]N. Gruschka, V. Mavroeidis, K. Vishi, and M. Jensen, "Privacy issues and data protection in big data: A case study analysis under GDPR,". 2018,
- [13]R. Handayani, E. Utami, and E. T. Luthfi, "Systematic literature review on auditing information technology risk management using the COBIT framework Oct. 2023
- [14]R. Wu, G.-J. Ahn, and H. Hu, "Towards HIPAA-compliant healthcare systems," in **Proc. 2nd ACM SIGHIT Int. Health Informatics Symp. (IHI'12)**, Miami, FL, USA, Jan. 2012
- [15]S. Rose, O. Borchert, S. Mitchell, and S. Connelly, **Zero Trust Architecture**, NIST Special Publication 800-207, National Institute of Standards and Technology, Gaithersburg, MD, Aug. 2020
- [16]B. Thuraisingham, "Cloud Governance," Beijing, China, 2020,
- [17]B. O. ALSaleem and A. I. Alshoshan, "Multi-Factor Authentication to Systems Login," in **2021 National Computing Colleges Conference (NCCC)**, Taif, Saudi Arabia, 2021
- [18]Y. Daldoul, "A robust certificate management system to prevent evil twin attacks in IEEE 802.11 networks," Feb. 2023.
- [19]T. Sobh, "Wired and wireless intrusion detection system: Classifications, good characteristics and state-of-the-art," **Computer Standards & Interfaces**, 2006
- [20]S. Ahmad, S. Mehruz, F. Mebarek-Oudina, and J. Beg, "RSM analysis based cloud access security broker: a systematic literature review," **Cluster Computing**, Oct. 2022
- [21]S. Rana and D. Mishra, "An authenticated access control framework for digital right management system," 25270, 2021,
- [22]D. M. Kesa, "Ensuring resilience: Integrating IT disaster recovery planning and business continuity for sustainable information technology operations," **World Journal of Advanced Research and Reviews**, 2023
- [23]G. Hardy, "Using IT governance and COBIT to deliver value with IT and respond to legal, regulatory and compliance challenges," **Information Security Technical Report**, 2006
- [24]A. Safitri, I. Syafii, and K. Adi, "Measuring the performance of information system governance using framework COBIT 2019," April-2021
- [25] G.Hardy "Using IT governance and COBIT to deliver value with IT and respond to legal, regulatory and compliance challenges," **Information Security Technical Report*
- [26]A. Safitri, I. Syafii, and K. Adi, "Measuring the performance of information system governance using framework COBIT 2019," April-2021