

Name: Md. Mashrurul Haque

ID: 2435257

Module: Data Security, Governance and Compliance

Programme: MSc in Cybersecurity and Digital Forensics

Date of Submission: 19/12/2025

Table of Contents

1. Introduction.....	4
2. Case Overview: NatureGreen (NG).....	5
3. Research on Frameworks and Models.....	6
3.1 ISO/IEC 27001 and ISO/IEC 27002 (ISMS and Control Guidance).....	6
3.2 NIST Cybersecurity Framework (CSF) (Outcomes Based Structure)	6
3.3 NIST RMF (SP 800-37) and NIST SP 800-53 (Risk Process and Control Catalogue).....	6
3.4 CIS Critical Security Controls (Prioritised, Practical Safeguards).....	7
3.5 COBIT 2019 (Governance of Information and Technology)	7
3.6 ITIL 4 (Service Management and Operational Stability).....	7
3.7 PCI DSS (Payment Security Compliance, Where Relevant)	8
3.8 SOC 2 and the Trust Services Criteria (Assurance for Service Organisations)	8
3.9 Zero Trust (Architecture Approach for BYOD, Cloud, Wireless).....	8
4. Selected Frameworks/Models for NatureGreen (NG)	9
5. Architecture Figure	11
6. Domain Mapping and Security Design for NG	12
7. Conclusion	14
8. References.....	15

List of Figures:

Fig. 1: Conceptual secure IT architecture for NatureGreen (NG).....	11
---	----

List of Tables:

Table 1: Selected frameworks and their role in NG's security programme	09
--	----

Table 2: 7 Domains mapped to key controls for NatureGreen (NG)	12
--	----

1. Introduction

NatureGreen (NG) operates in a modern digital environment where cloud services, extensive wireless connectivity, and a strong online presence create clear business value but also introduce significant information security and compliance challenges. In NG's case, the organisation relies heavily on cloud services for staff and customer-facing systems and estimates that around 95% of its network is wireless. At the same time, NG faces pressure to permit Bring Your Own Device (BYOD) access for both staff and customers, while also protecting sensitive personal information and high-value intellectual property (IP). These characteristics collectively expand the attack surface and increase the likelihood of security incidents if appropriate governance, policies, and technical controls are not in place.

Information security in this context cannot be treated as a purely technical activity. Effective protection requires a balanced focus on people, process, and technology, because human behaviour, unclear responsibilities, and weak organisational practices can undermine even well-designed technical controls [1]. In addition, organisations must demonstrate due care and due diligence by aligning security practices with legal and ethical responsibilities, particularly when processing personal data at scale and operating across multiple jurisdictions [2].

This report builds a clear path from recognised security frameworks to a practical approach for NG. It reviews major frameworks and models, including ISO/IEC 27001/27002, NIST CSF, NIST RMF and SP 800-53, CIS Controls, COBIT 2019, ITIL 4, PCI DSS, SOC 2, and Zero Trust. It then selects a focused set that best fits NG's cloud, wireless, and BYOD environment and maps key principles and controls to infrastructure domains to show how security can be implemented in a structured and realistic way [1].

Finally, the report explains why standards and regulations must be updated regularly. Technology, threats, and legal expectations change quickly, so organisations must continuously maintain and improve their governance, policies, and controls to protect people and data and to remain compliant [2].

2. Case Overview: NatureGreen (NG)

NatureGreen (NG) is a global health and wellness brand with a large workforce and an international customer base. In the case scenario, NG uses cloud services to deliver IT services to staff and customers and operates a network that is heavily wireless (around 95%). The organisation also has a strong online and social media presence for marketing and customer engagement. A key pressure facing NG is the demand to support Bring Your Own Device (BYOD) access for both staff and customers. At the same time, NG must protect sensitive personal information (staff and customer data) and safeguard valuable intellectual property (IP) that could be extremely damaging if stolen or exposed.

From an information security point of view, NG's most critical assets can be grouped into two broad categories: privacy data of individuals and corporate intellectual property. These are the types of information that typically require the strongest protection because their compromise can create legal, financial, and reputational harm. Protecting them also directly supports the core security goals of confidentiality, integrity, and availability (CIA). [1]

NG's operating model creates multiple "risk hotspots" across its environment. A wireless-first infrastructure increases exposure to unauthorised access and interception if access control and segmentation are not strong. BYOD increases endpoint risk because personal devices may be poorly configured, unpatched, or shared, and are harder to govern than corporate-managed endpoints. In addition, heavy cloud reliance increases the importance of strong identity and authentication, secure configuration, and monitoring, because cloud misconfiguration and credential compromise are common pathways to data exposure. These issues often become visible first in the user domain, where human behaviour is frequently described as the weakest link in security and where poor decisions (for example clicking unsafe links or sharing credentials) can bypass technical defences. [1]

A further challenge in the scenario is a clear governance and policy gap. Good security does not happen simply because tools exist; it requires a foundation of policies, standards, and practices that define responsibilities, guide acceptable behaviour, and ensure controls are consistently applied. Governance also matters because it links security to organisational objectives and ensures oversight at senior levels, rather than leaving security decisions scattered across teams. [3]

For NG, the practical need is therefore to move from "security in disarray" to a structured approach that combines: (i) clear governance and policies, (ii) risk management to prioritise what matters most, and (iii) technical and operational controls that work in a cloud, wireless and BYOD environment. Risk management is especially important because it provides a repeatable way to identify, analyse, evaluate, and treat risks, and it links security investment to real business impact. [4]

3. Research on Frameworks and Models

A useful way to think about security frameworks is that they are maps, not a one-size-that-fits-all. They help an organisation avoid starting from scratch by providing proven structures for governance, risk decisions, policies, and controls but they still need to be tailored to the real environment and business priorities. This matters for NG because its cloud-heavy, wireless-heavy, BYOD-friendly environment means the security approach must be consistent, measurable, and repeatable across many locations and users [3].

To keep this section clear, the frameworks below are grouped by the main job they do: (1) management system, (2) outcomes-based improvement, (3) control catalogues and prioritised safeguards, (4) governance and service management, and (5) assurance/compliance and modern architecture.

3.1 ISO/IEC 27001 and ISO/IEC 27002 (ISMS and Control Guidance)

ISO/IEC 27001 is best understood as the “management system backbone” for information security. It specifies what an organisation must put in place to run an Information Security Management System (ISMS) including leadership commitment, risk-based planning, internal audits, continual improvement, and evidence that controls are operating (not just written down) [5].

ISO/IEC 27002 then supports this by offering practical control guidance a structured catalogue of controls and implementation advice that helps translate a security policy into concrete safeguards [6]. In NG’s case, this is valuable because the company currently has no established security policy, and ISO-style structure helps turn “security is a priority” into a managed programme with clear scope, ownership, documentation, and improvement cycles [5].

Why it’s helpful for NG: ISO is strong for building order from disarray: policies → risk decisions → controls → audits → improvements. That fits NG’s need to protect customer data and valuable IP consistently across countries and teams [5].

3.2 NIST Cybersecurity Framework (CSF) (Outcomes Based Structure)

The NIST Cybersecurity Framework (CSF) is widely used as a practical “organising structure” for cybersecurity outcomes. The original CSF is often taught using five core functions (Identify, Protect, Detect, Respond, Recover) [8].

However, the latest NIST CSF 2.0 expands this model by adding Govern as an explicit function. This matters because it puts decision-making, roles, oversight, and risk direction on the same level as technical protection work [7].

Why it’s helpful for NG: CSF is excellent for explaining security to non-technical leadership and showing maturity gaps. For NG, it can be used to structure the programme around outcomes like knowing what assets exist (including BYOD), protecting wireless access, detecting abnormal access, responding to incidents quickly, and recovering services under clear governance [8].

3.3 NIST RMF (SP 800-37) and NIST SP 800-53 (Risk Process and Control Catalogue)

Where CSF is “what good looks like”, the NIST Risk Management Framework (RMF) is a disciplined process for managing security and privacy risk across the system life cycle. It

describes a structured approach that includes categorisation, control selection, implementation, assessment, authorisation, and continuous monitoring [9].

NIST SP 800-53 Rev. 5 is the companion control catalogue used in many RMF implementations. It provides a comprehensive set of security and privacy controls, organised in families, and designed to be tailored based on risk and context [10].

Why it's helpful for NG: NG needs repeatability. RMF gives a cycle for “how we manage risk properly,” while SP 800-53 provides the detailed control options for things like access control, audit logging, configuration management, incident response, and supplier risk [9], [10]. This connects directly with your course view that risk management requires a formal methodology and must be continuously monitored and improved not treated as a one-off activity [4].

3.4 CIS Critical Security Controls (Prioritised, Practical Safeguards)

The CIS Critical Security Controls are a set of prioritised safeguards focused on defending against common, real-world attacks. CIS presents them as practical, measurable best practices and explicitly frames them to strengthen security in a prioritised manner [11].

Why it's helpful for NG: CIS Controls are particularly useful when a company needs to move fast and reduce risk quickly especially in environments dealing with mobility, cloud use, and changing attacker tactics [11]. For NG, CIS can provide an “action list” for the first 90–180 days (e.g., asset inventories for devices and software, secure configuration baselines, vulnerability management, logging, MFA and access control management, and incident readiness).

3.5 COBIT 2019 (Governance of Information and Technology)

COBIT 2019 focuses on enterprise governance of information and technology helping organisations align security and IT with business goals, define decision rights, set performance measures, and ensure accountability. COBIT 2019 is structured around governance and management objectives (commonly described as 40 objectives organised into domains), providing a clear model for who decides what, and how results are monitored [12].

Why it's helpful for NG: NG's problem is not only technical “everything is in disarray.” COBIT helps design an operating model where the board/senior management can set direction and ensure security investments deliver value, while management executes. This also matches the course emphasis on governance as the bridge that turns compliance into actionable strategy [3].

3.6 ITIL 4 (Service Management and Operational Stability)

ITIL 4 is not a “security framework” in the same way as ISO 27001 or NIST RMF, but it matters because security controls often fail due to weak operations (poor change control, unclear incident handling, inconsistent service ownership). ITIL 4 describes service management concepts like governance, the service value chain, and continual improvement [13].

Why it's helpful for NG: With cloud services and heavy wireless reliance, NG must run security as part of normal IT operations especially for change enablement, incident management, problem management, and supplier management. ITIL supports consistency and

helps make security “how we operate” rather than “extra work when something goes wrong” [13].

3.7 PCI DSS (Payment Security Compliance, Where Relevant)

PCI DSS is a global security standard designed to protect payment account data in environments that store, process, or transmit cardholder data [14]. The PCI Security Standards Council also publishes updates and supporting materials (e.g., v4.0.1 revisions and validation tools like SAQs) to keep requirements clear and usable [15].

Why it’s helpful for NG: If NG sells online and handles card payments (directly or via partners), PCI DSS becomes a non-negotiable compliance driver for that part of the environment. Even if payment processing is outsourced, PCI still influences supplier requirements, segmentation decisions, logging, and access controls [14].

3.8 SOC 2 and the Trust Services Criteria (Assurance for Service Organisations)

A SOC 2 examination/report is an attestation focused on controls relevant to the Trust Services Criteria categories: security, availability, processing integrity, confidentiality, and privacy. The Trust Services Criteria are published by the AICPA and used as the basis for evaluating controls in SOC reporting engagements [16].

Why it’s helpful for NG: NG uses cloud services and likely relies on third-party platforms. SOC 2 is valuable for supplier assurance (choosing vendors that can prove control effectiveness) and for NG’s own credibility if it provides digital services to customers and partners [16].

3.9 Zero Trust (Architecture Approach for BYOD, Cloud, Wireless)

Zero Trust is an approach that moves security away from assuming “inside the network = trusted.” Instead, it focuses on verifying users, devices, and access requests continuously, with strong identity, device posture, segmentation, and monitoring. NIST SP 800-207 defines Zero Trust as an evolving set of paradigms shifting defence from static perimeters to users, assets, and resources [17].

Why it’s helpful for NG: NG’s biggest risk drivers (BYOD pressure, cloud usage, and 95% wireless) all weaken traditional perimeter thinking. Zero Trust fits because it treats BYOD devices and remote users as untrusted by default, and it supports safer access to sensitive data and IP through identity-driven access control, least privilege, and continuous evaluation [17].

4. Selected Frameworks/Models for NatureGreen (NG)

NG's environment is cloud-driven, heavily wireless, and under pressure to support BYOD for both staff and customers. In a situation like this, it is not realistic to implement every framework fully. A better approach is to select a small set of complementary frameworks each with a clear role, so the security programme is both manageable and auditable. For NG, the recommended approach is a hybrid model: ISO/IEC 27001/27002 as the core management system and control baseline, NIST CSF 2.0 as the organising structure for cybersecurity outcomes and maturity, Zero Trust as the access and security architecture for cloud/wireless/BYOD, and the CIS Controls as a practical set of prioritised safeguards to implement key protections quickly. [5], [6], [7], [11], [17]

To support governance and day-to-day operations, COBIT 2019 is used to define decision rights and oversight at senior levels, while ITIL 4 is used to operationalise security through consistent processes such as incident management, change enablement, and service continuity. [12], [13] Finally, PCI DSS and SOC 2 / Trust Services Criteria are treated as “assurance and compliance overlays,” applied where relevant and PCI DSS for payment environments (if NG processes or stores card data) and SOC 2/TSC to strengthen third-party assurance and supplier selection for cloud services. [14], [15], [16]

Table 1: Selected frameworks and their role in NG's security programme

Framework / Model	Why Selected	Key NG Risks Addressed
ISO/IEC 27001	Gives NG structure: scope, policies, risk cycle, audits, improvement	“Security in disarray”, lack of policies, inconsistent practices [5]
ISO/IEC 27002	Provides control guidance to translate policy into safeguards	Access control, data protection, operational security [6]
NIST CSF 2.0	Organises security into Govern/Identify/Protect/Detect/Respond/Recover	Cloud, wireless, BYOD capability coverage and gap identification [7]
Zero Trust (NIST SP 800-207)	Removes implicit trust, continuous verification for users/devices	Credential theft, BYOD risks, lateral movement on wireless networks [17]
CIS Controls v8	Practical “what to do first” controls and measurable actions	Phishing, endpoint compromise, cloud misconfiguration, weak logging [11]
COBIT 2019	Clarifies who decides, who owns risk, and how performance is monitored	Governance gaps, risk ownership, strategic alignment [12]

ITIL 4	Makes security reliable through incident/change/continuity practices	Slow response, uncontrolled changes, weak resilience [13]
PCI DSS (if applicable)	Mandatory requirements for cardholder data environments	Payment fraud, cardholder data exposure [14], [15]
SOC 2 / TSC	Improves supplier assurance and trust for cloud/third parties	Third-party risk, customer trust, evidence of controls [16]

5. Architecture Figure

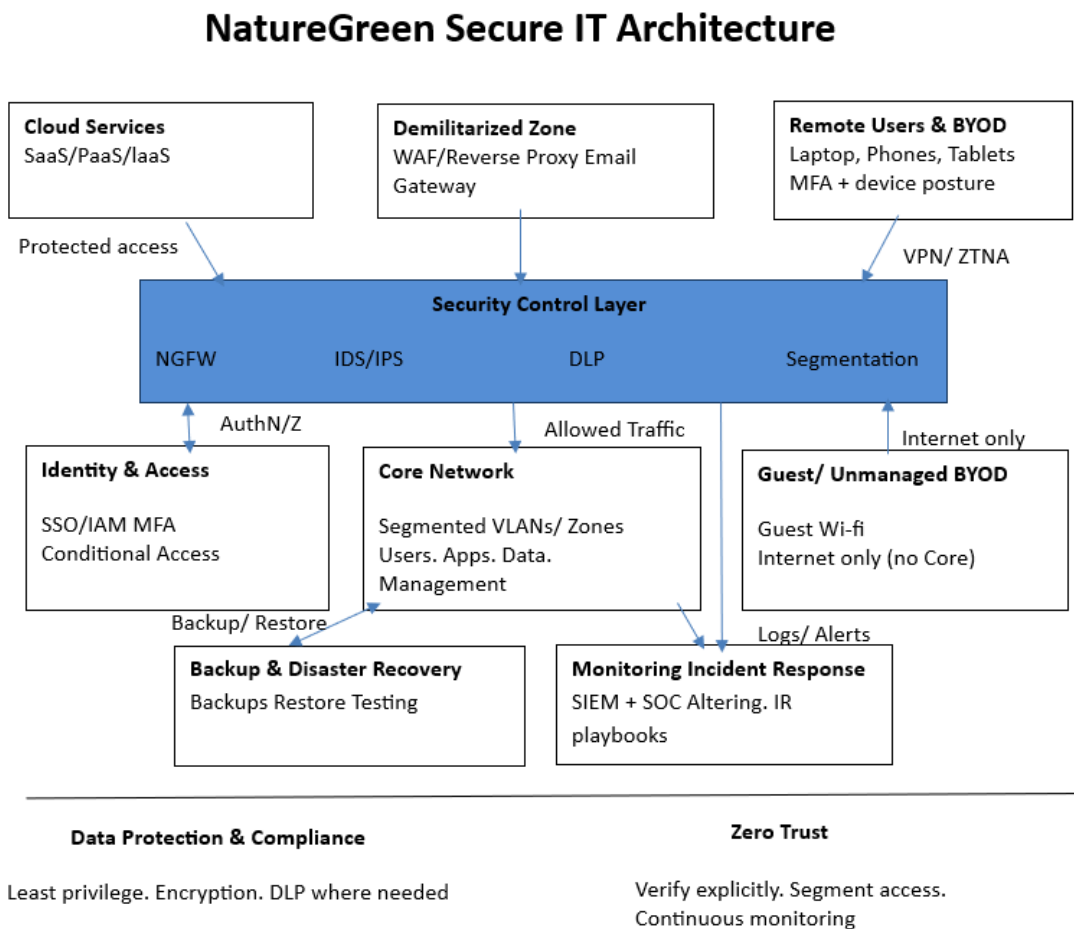


Fig. 1: Conceptual secure IT architecture for NatureGreen (NG)

This diagram summarises a simple but complete security design for NG. Users (including remote users and BYOD devices) access services through controlled entry points (DMZ) and strong identity controls (MFA/IAM). Traffic and data flows are then protected by a dedicated security control layer that combines prevention (next-gen firewall, DLP), detection (IDS/IPS, SIEM/SOC), and response (incident handling). Separate guest/BYOD networking reduces risk by limiting lateral movement, while backup and disaster recovery support service continuity and recovery. Overall, the architecture is designed to be practical for NG's cloud and wireless environment while remaining aligned with recognised security management and Zero Trust guidance. [5], [6], [7], [11], [13], [17]

6. Domain Mapping and Security Design for NG

This section explains how NG can turn the selected frameworks into practical controls by mapping them to the 7 domains of IT infrastructure (User, Workstation, LAN, LAN-to-WAN, WAN, Remote Access, and System/Application). This approach is helpful because it breaks a complex environment into smaller parts, making risks easier to see and controls easier to assign and manage. [1]

Table 2: 7 Domains mapped to key controls for NatureGreen (NG)

7 Domains of IT Infrastructure	What it covers at NG	Key security controls (what NG should implement)	Framework links
1) User Domain	Employees, admins, contractors, customers	Security awareness + phishing training; Acceptable Use + BYOD agreement; MFA for staff/admins; least privilege; periodic access reviews; monitoring of suspicious behaviour	ISO 27001/27002 [5], [6]; NIST CSF [7], [8]; NIST 800-53 [10]; CIS [11]; Zero Trust [17]
2) Workstation Domain	Corporate endpoints + personal BYOD devices	Asset inventory (devices/software); patching; endpoint protection (EDR/AV); device encryption; MDM / device posture checks for BYOD; baseline secure configuration	CIS Controls v8[11]; NIST 800-53 [10]; Zero Trust posture-based access [17]
3) LAN Domain	Internal wired + wireless networks (critical for NG)	Network segmentation (VLANs); separate corporate vs guest/BYOD SSIDs; NAC/802.1X; internal traffic monitoring; restrict lateral movement	NIST CSF Detect [8]; CIS [11]; Zero Trust segmentation [17]; ISO control guidance [6]
4) LAN-to-WAN Domain	Perimeter, gateways, DMZ, internet-facing services	DMZ for web/email; next-gen firewalls; IDS/IPS; secure DNS/web filtering; centralised logs to SIEM/SOC	CIS [11]; NIST CSF Protect/Detect [8]; ITIL incident escalation [13]
5) WAN Domain	Internet + cloud connectivity + third parties	Encrypted connections (TLS/VPN); secure APIs; cloud configuration monitoring; vendor/security requirements in contracts; supplier assurance (SOC-aligned)	NIST 800-53 [10]; CIS Control[11]; SOC 2/TSC assurance [16]; COBIT governance oversight [12]
6) Remote Access Domain	Remote staff, travelling users, partner access	MFA + step-up authentication; conditional access (risk-based); ZTNA-style access; restrict admin access; session monitoring	Zero Trust [17]; NIST 800-53 identity/access [10]; NIST CSF [7]
7) System/Application Domain	Cloud workloads, applications,	Strong access control + logging; secure configuration baselines; vulnerability management;	ISO ISMS governance [5], ISO controls [6]; NIST RMF [9]; NIST

	databases (PII + IP)	controlled change; backups/DR; incident response playbooks	800-53 [10]; ITIL change/incident [13]; CIS [11]
--	----------------------	--	--

Even with a strong design, NG cannot treat security as done. Threats evolve, technology changes, and legal expectations shift especially for global companies handling personal data and operating across jurisdictions. This is why organisations are expected to demonstrate ongoing due care and due diligence, meaning policies and controls must be reviewed, updated, and tested regularly. [2]

From a practical perspective:

- New attack methods (e.g., phishing techniques, credential theft patterns) require updated awareness training and detection rules. [8], [11]
- Cloud platforms and services evolve quickly, which creates new configuration and identity risks. [11]
- Governance must keep pace: roles, accountability, and risk appetite must be reviewed as the business grows and changes. [12]
- Operational practices must improve continuously so incident response and recovery stay effective in real events. [13]

This continuous improvement mindset is consistent with an ISMS approach and helps NG remain resilient, compliant, and trustworthy over time. [5], [2]

7. Conclusion

NatureGreen (NG) operates in a high-exposure environment where cloud services, a largely wireless network, and growing BYOD demand significantly increase security and compliance risk. To address this, the report reviewed major security frameworks and then selected a focused set that fits NG's reality: ISO/IEC 27001/27002 to provide an ISMS foundation and control baseline, NIST CSF to structure outcomes and maturity, Zero Trust to manage access in cloud/wireless/BYOD conditions, and the CIS Controls to support practical implementation. Governance and operational consistency are strengthened through COBIT and ITIL, while PCI DSS and SOC 2/TSC can be applied where specific compliance or supplier assurance is needed. [5],[6],[7]

By mapping these frameworks to the 7 domains of IT infrastructure, NG can move from an ad hoc security posture to a structured programme where responsibilities, controls, and monitoring are clearly defined across users, devices, networks, remote access, and critical applications. Finally, continuously updating policies, standards, and controls is essential for NG because threats, technologies, and legal expectations change rapidly; ongoing review and improvement demonstrates due care and due diligence and helps maintain trust with customers and stakeholders. [2], [5], [8], [13]

8. References

- [1] “Week 1: Introduction to Information Security,” lecture slides, 2025.
- [2] “Week 3: Compliance, Law and Ethics,” lecture slides, 2025.
- [3] “Week 4: Governance and Strategic Planning for Security,” lecture slides, 2025.
- [4] “Week 7: Risk Management,” lecture slides, 2025.
- [5] ISO/IEC, ISO/IEC 27001:2022 Information Security, Cybersecurity and Privacy Protection Information Security Management Systems Requirements, Geneva, Switzerland: International Organization for Standardization, 2022.
- [6] ISO/IEC, ISO/IEC 27002:2022 Information Security, Cybersecurity and Privacy Protection Information Security Controls, Geneva, Switzerland: International Organization for Standardization, 2022.
- [7] National Institute of Standards and Technology, The NIST Cybersecurity Framework (CSF) 2.0, Gaithersburg, MD, USA: NIST, 2024.
- [8] National Institute of Standards and Technology, Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1, Gaithersburg, MD, USA: NIST, 2018.
- [9] R. Ross, V. Pillitteri, G. Dempsey, M. Riddle, and J. Guissanie, Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy, NIST Special Publication 800-37 Rev. 2, Gaithersburg, MD, USA: NIST, 2018.
- [10] J. T. Force et al., Security and Privacy Controls for Information Systems and Organizations, NIST Special Publication 800-53 Rev. 5, Gaithersburg, MD, USA: NIST, 2020.
- [11] Center for Internet Security, CIS Critical Security Controls v8, East Greenbush, NY, USA: CIS, 2021.
- [12] ISACA, COBIT 2019 Framework: Governance and Management Objectives, Schaumburg, IL, USA: ISACA, 2018.
- [13] AXELOS, ITIL Foundation: ITIL 4 Edition, London, U.K.: TSO (The Stationery Office), 2019.
- [14] PCI Security Standards Council, Payment Card Industry Data Security Standard (PCI DSS), Version 4.0, Wakefield, MA, USA: PCI SSC, 2022.
- [15] PCI Security Standards Council, Payment Card Industry Data Security Standard (PCI DSS), Version 4.0.1, Wakefield, MA, USA: PCI SSC, 2023.
- [16] American Institute of CPAs, Trust Services Criteria, New York, NY, USA: AICPA, 2017.
- [17] S. Rose, O. Borchert, S. Mitchell, and S. Connelly, Zero Trust Architecture, NIST Special Publication 800-207, Gaithersburg, MD, USA: NIST, 2020.