

UNIVERSITY OF WALES TRINITY SAINT DAVID

Department of Cyber Security & Digital Forensics

Module: Data Security, Governance and Compliance (ACCA7028)

Lecturer: Dr. Dipo Dunsin

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

Student Name: MD ABDULLAH AL MAMUN

Student ID: 2434327

Date of Submission: 12/12/2025

Word Count: 2,950

1.0 Introduction

NatureGreen (NG), a prominent multinational healthy living brand, currently operates at a critical juncture in its digital transformation journey. The organization's technological infrastructure is characterized by an almost exclusive reliance on wireless connectivity (approximately 95% of its network), extensive adoption of cloud services across multiple global regions, and increasing pressure from executive leadership to implement a comprehensive Bring Your Own Device (BYOD) strategy for enhanced workforce flexibility. While these technological choices undoubtedly support operational agility and cost efficiency, they simultaneously expose NG to significant and multifaceted security vulnerabilities across three primary domains: network security, endpoint management, and cloud governance frameworks.

The current operational environment exists within what can accurately be described as a fundamental governance void. NG operates without established security policies, documented procedural guidelines, or formalized accountability structures for information security management. This governance deficit places the organization's most valuable assets at unacceptable risk, including its multi-billion-dollar intellectual property portfolio comprising proprietary formulations, product development research, and trade secrets, alongside sensitive client data encompassing Personally Identifiable Information (PII) and financial transaction records. As emphasized by Souppaya and Scarfone (2016), organizations implementing BYOD initiatives without adequate governance frameworks expose themselves to substantial data leakage vulnerabilities and endpoint security weaknesses that can undermine even the most robust perimeter defenses.

This report addresses this critical security vacuum by proposing a comprehensive integrated security governance framework that transcends simple compliance

checklists to establish a holistic, sustainable security posture. The framework strategically synthesizes the complementary strengths of three globally recognized models: ITIL 4 for operational service management and process maturity, ISO/IEC 27001:2022 for establishing a formal, auditable Information Security Management System (ISMS), and NIST Cybersecurity Framework (CSF) V1.1 for flexible, risk-based technical control implementation and continuous improvement. The primary objective is to embed a culture of security consciousness throughout NG's operations, ensuring demonstrable compliance with international regulations, establishing robust systems for continuous risk management, and ultimately protecting organizational assets while enabling sustained, secure business innovation in competitive global markets.

2.0 Security Frameworks and Models Research: Comprehensive Analysis

Designing an effective governance structure for NG requires a nuanced understanding of how leading security models interact to manage risk across technological, procedural, and human domains. The selected frameworks must address both strategic governance requirements and the operational realities of NG's highly mobile, cloud-dependent environment.

2.1 ITIL 4: Service Integration and Security Management

ITIL 4 represents a significant evolution in service management philosophy, aligning IT services directly with business value creation through the Service Value System (SVS) (AXELOS, 2019). Unlike traditional security frameworks that treat security as a standalone function, ITIL 4 integrates security considerations throughout the entire service lifecycle, transforming security from a potential business inhibitor to an enabler of secure digital transformation.

The ITIL 4 Service Value Chain (SVC) provides a structured methodology for incorporating security requirements into every phase of service delivery:

- **Plan:** Security leadership, ideally through a dedicated Chief Information Security Officer (CISO), establishes security strategy aligned with business objectives, with particular emphasis on cloud adoption standards and BYOD implementation parameters.
- **Design & Transition:** BYOD policy formulation and supporting technical architecture incorporate security controls from inception, including Mobile Application Management, conditional access policies, and encryption standards, rather than as retroactive additions.
- **Deliver & Support:** Incident Management practices and Service Desk operations are configured to handle security events efficiently, including

reporting lost BYOD devices, responding to suspected breaches, and managing access revocation processes.

- **Improve:** Security audit findings, performance metrics, and threat intelligence feed into the Continual Improvement Practice, ensuring NG's security posture adapts proactively to emerging wireless vulnerabilities, evolving cloud threats, and changing regulatory requirements.

For NG, ITIL 4 provides the essential process maturity required to translate strategic security objectives into repeatable, auditable operational procedures. This ensures security functions support rather than hinder NG's core business objective of digital agility and innovation.

2.2 ISO/IEC 27001:2022 – Foundational ISMS Structure

ISO/IEC 27001:2022 provides the international standard for establishing, implementing, maintaining, and continually improving an Information Security Management System (ISMS) (ISO, 2022). Its strength lies in its systematic, risk-based approach governed by the Plan-Do-Check-Act (PDCA) cycle, which provides a continuous improvement mechanism essential for evolving threat landscapes.

Detailed Application to NG's Context:

The standard provides the structural foundation for managing the confidentiality, integrity, and availability of NG's sensitive assets:

- **PLAN (Establish ISMS):** NG must define a comprehensive scope covering all wireless network segments, cloud service deployments, and BYOD endpoints. This phase involves establishing clear security objectives, conducting rigorous risk assessments, and developing the Data Classification Policy essential for proportionate control application.
- **DO (Implement & Operate):** NG implements controls selected from Annex A, expanded in the 2022 revision to 93 controls across four thematic areas. Particularly relevant controls include A.5 Organisational Controls for policy frameworks, A.6 People Controls for security awareness training, A.7 Physical Controls for infrastructure security, and A.8 Technological Controls specifically addressing cloud service use (A.8.23), encryption standards, and Mobile Application Management (A.8.10).
- **CHECK (Monitor & Review):** Regular internal audits, management reviews, and continuous monitoring of security performance indicators verify control effectiveness and identify improvement opportunities.

- **ACT (Maintain & Improve):** Corrective actions based on audit findings and incident reports drive continuous ISMS improvement, directly aligning with ITIL's Continual Improvement practice.

By pursuing ISO 27001 certification, NG transitions from an informal governance void to a formally certified state, providing stakeholders with assurance that security risks are managed systematically and comprehensively.

2.3 NIST CSF: Risk-Based Implementation Approach

The NIST Cybersecurity Framework offers a flexible, outcome-based approach particularly beneficial for NG's dynamic, wireless-heavy, cloud-dependent environment (NIST, 2018). It organizes security activities into five core, continuous functions: Identify, Protect, Detect, Respond, and Recover, providing a practical implementation roadmap complementary to ISO 27001's structural requirements.

Framework Functions Applied to NG:

- **IDENTIFY:** Establishing foundational understanding of cybersecurity risk to systems, assets, data, and capabilities, including comprehensive asset management and governance structure establishment.
- **PROTECT:** Developing and implementing safeguards to ensure service delivery through MAM deployment, WPA3 implementation, Multi-Factor Authentication, and Role-Based Access Control.
- **DETECT:** Implementing activities to identify cybersecurity events through continuous monitoring of wireless network traffic and cloud API usage.
- **RESPOND:** Developing and implementing response activities for detected incidents via formal Incident Response Plans aligned with ITIL's Incident Management practices.
- **RECOVER:** Maintaining resilience plans and restoring impaired capabilities through cloud data backups and disaster recovery procedures.

NIST CSF Implementation Tiers and NG's Maturity Journey:

NG must progress through four implementation tiers, from Tier 1 (Partial/Reactive) through Tier 2 (Risk Informed), to Tier 3 (Repeatable) as a minimum long-term target, and ultimately toward Tier 4 (Adaptive) as an optimal goal. This progression will ensure policy consistency across global operations while enabling threat intelligence integration into security decision-making processes.

3.0 Proposed Integrated Security Governance Framework

The integration of ITIL 4, ISO 27001, and NIST CSF provides a robust, holistic, and adaptive framework specifically designed for NG's high-agility, high-risk

environment. This integrated approach ensures strategic direction, compliance mandates, and operational execution are intrinsically linked rather than operating in organizational silos.

3.1 Framework Architecture and Synergistic Integration

The proposed framework creates a cohesive governance ecosystem where each component addresses specific aspects of NG's security requirements:

- **ISO 27001 (The Foundation):** Provides the certified ISMS structure requiring mandatory risk assessments, documented policies, and formal management commitment, defining what controls must be implemented.
- **NIST CSF (The Risk Engine):** Provides the operational vocabulary and functions for how to manage cybersecurity risk in NG's specific environment.
- **ITIL 4 (The Service Enabler):** Ensures execution of NIST functions and ISO controls as high-quality services utilizing practices like Change Enablement, Incident Management, and Continual Improvement.

This synergistic approach ensures policy development is risk-driven, formalized, and operationally embedded, creating a sustainable security governance model rather than a temporary compliance exercise.

3.2 Governance Structure and Policy Framework

Effective security governance begins with clear accountability structures and documented policy frameworks enforced through executive leadership and organizational culture.

Governance Structure:

- **Chief Information Security Officer (CISO):** Reports directly to the board, translating business strategy into security objectives and managing ISMS implementation.
- **Security Steering Committee (SSC):** Cross-functional body responsible for policy approval, security budget allocation, and residual risk level approval.
- **Data Protection Officer (DPO):** Mandated for GDPR compliance, focusing on lawful processing, data subject rights, and privacy-by-design principles.

Policy Framework:

1. **Data Classification Policy:** Essential for applying proportionate security controls based on data sensitivity levels.

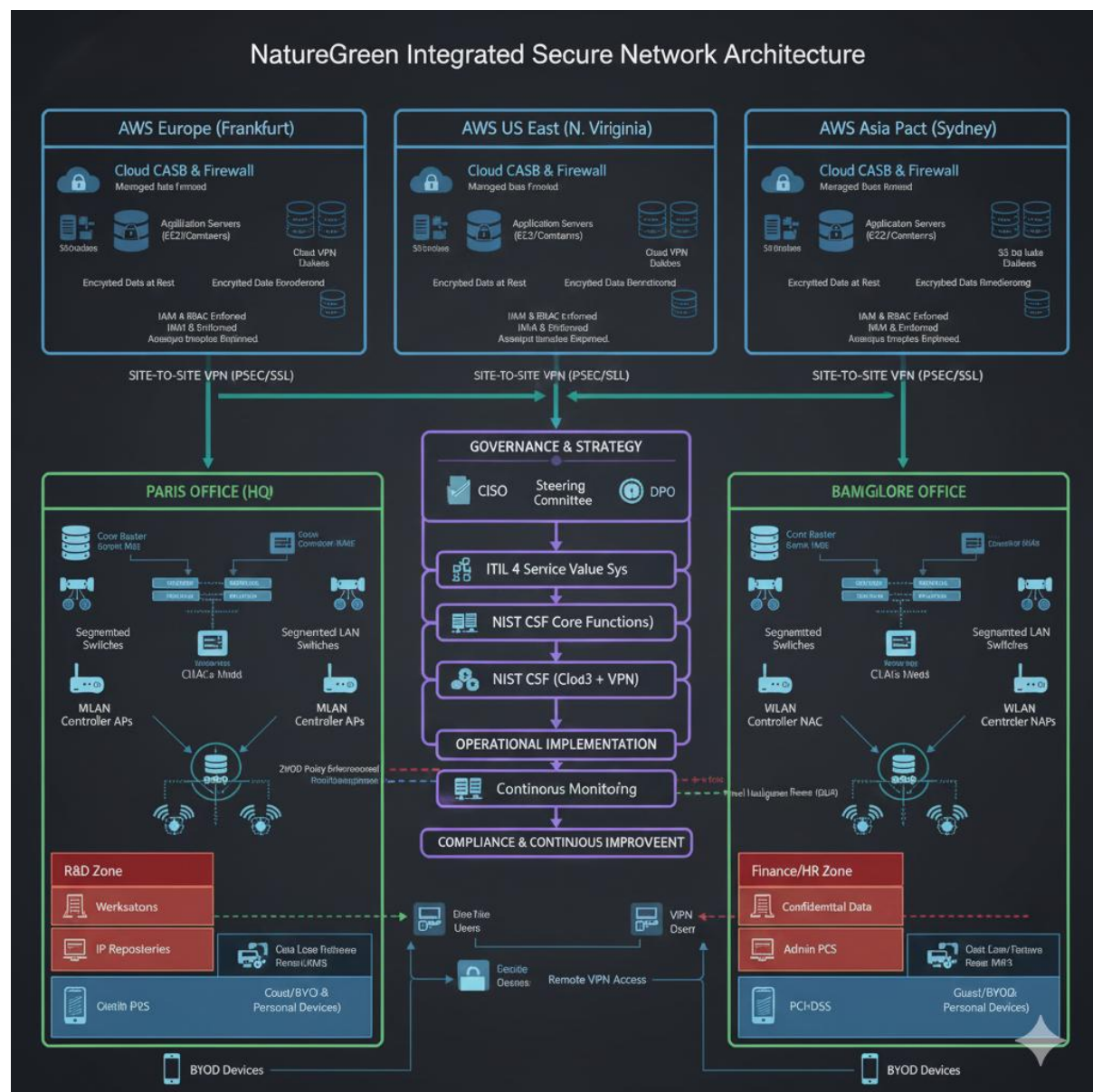
2. **BYOD Policy:** Critical immediate policy covering device requirements, security mandates, permissible applications, and remote wipe authorization.
3. **Acceptable Use Policy:** Defines permitted and prohibited uses of NG's wireless network, cloud services, and endpoints.
4. **Access Control Policy:** Implements Role-Based Access Control principles, least privilege enforcement, and segregation of duties.

3.3 Risk Management Process

The iterative risk management process follows: Identification → Assessment → Treatment → Monitoring & Review, operationalized through a detailed risk treatment plan addressing NG's specific vulnerabilities:

Risk	Likelihood	Impact	Treatment Strategy	Framework Alignment
Data leakage via BYOD	High	High	MAM containerization with Conditional Access	NIST Protect, ISO A.8.10
Wireless interception	High	Medium	WPA3-Enterprise with 802.1X authentication and mandatory VPN	NIST Protect, ISO A.13.1.2
Cloud credential theft	Medium	High	MFA for all cloud services and Zero Trust Network Access	NIST Protect, ISO A.9.4.2
IP theft	Low	Critical	RBAC, Data Loss Prevention, encryption at rest/in transit	NIST Identify, ISO A.8.2.1

Risk	Likelihood	Impact	Treatment Strategy	Framework Alignment
DDoS attacks	Medium	High	Cloud-native DDoS protection and Web Application Firewalls	NIST Protect/Recover



The diagram you provided, titled "NatureGreen Integrated Secure Network Architecture", illustrates a multi-region, multi-office secure network design. It shows three AWS regions (Europe, US East, Asia Pacific) connected via Site-to-Site VPN to two offices (Paris HQ and Bangalore Office). The central part of the diagram outlines a governance and strategy framework including CISO, DPO, ITIL 4, NIST CSF, and continuous monitoring. The bottom part shows specific network zones like R&D, Finance/HR, and BYOD devices.

Architecture," illustrates the holistic security and governance framework designed for the multinational company NatureGreen (NG). It visually connects the company's multi-region cloud deployment, its physical offices, and the integrated governance model that dictates how security is implemented across all layers.

Here is a detailed breakdown of the diagram's major components and their purpose within the assignment's context:

1. Governance and Strategy Core

This central component represents the integrated management structure that translates strategic goals into technical actions:

- **Top Leadership:** Features the CISO (Chief Information Security Officer), the Steering Committee (for high-level policy approval), and the DPO (Data Protection Officer) for privacy and legal compliance.
- **Integrated Frameworks:** Shows the synergy between the core models:
 - **ITIL 4 Service Value System:** Provides the process maturity for operational execution.
 - **NIST CSF (Core Functions):** Provides the risk-based methodology (Identify, Protect, Detect, Respond, Recover).
 - **NIST CSF (Cloud + VPN):** Specifically targets the protection of the wide-area cloud connections.
- **Operational Implementation:** Links policy to practice through Operational Implementation and Continuous Monitoring.
- **Compliance & Continuous Improvement:** Underpins the entire structure, feeding back into the improvement cycle.

2. Multi-Region Cloud Deployment (AWS)

NG utilizes a presence across three major AWS regions, all secured and interconnected: AWS Europe (Frankfurt), AWS US East (N. Virginia), and AWS Asia Pacific (Sydney).

- **Shared Security Model:** Each region features a Cloud CASB & Firewall for managed threat defense.
- **Data Protection:** Data security is ensured by mandatory Encryption at Rest (for databases/S3 buckets) and Encryption in Transit (for application servers).

- **Access Control:** IAM & RBAC Enforced principles are applied across all cloud resources.
- **Connectivity:** All cloud regions are connected back to the physical offices via SITE-TO-SITE VPN (IPSEC/SSL) tunnels, securing all data in transit between locations.

3. 🏢 Physical Offices and Network Segmentation (Paris HQ & Bangalore Office)

The diagram details the internal network architecture, emphasizing segmentation and wireless hardening.

- **Wireless Security:** Both offices use MLAN Controller APs and WLAN Controller NAC to manage the 95% wireless infrastructure. This is where WPA3-Enterprise is enforced.
- **Core Infrastructure:** Core routers, Segmented Switches, and Core/Data Repositories (IP, PII) are centrally located and heavily protected.

Network Zones and Segmentation (VLANs)

Each office is segmented into restricted zones to enforce the principle of least privilege:

- **R&D Zone (Paris HQ):** Contains IP Repositories and Workstations. This segment has the highest protection.
- **Finance/HR Zone (Bangalore Office):** Contains Confidential Data and Admin PCs. This segment also handles PCI-DSS compliance requirements, necessitating strong separation.
- **Guest/BYOD (Personal Devices):** This is the Least Privilege zone. Access is strictly controlled by the VLAN Controller NAC, only granting access after the device is verified for MAM/Conditional Access compliance.

4. 🏠 Endpoint Security and Access

The bottom layer illustrates how users connect securely to the entire infrastructure:

- **BYOD Devices:** These personal devices are secured via MAM Containerisation, which separates and encrypts corporate data from personal data.
- **Remote VPN Access:** Remote VPN Access is required for all off-site connections, ensuring all employees (including C-level executives) comply with the same strong encryption protocols.

- **Access Control:** Access to all systems—from the cloud to local servers—is governed by Zero Trust principles, ensuring that trust is never implicit and is always verified through MFA and device compliance.

This diagram is essential to the assignment because it provides the visual evidence for the security controls discussed in Sections 3.3 (BYOD/MAM) and 4.0 (Network Hardening) and shows the practical application of the theoretical governance frame

3.4 BYOD Implementation Strategy

The executive pressure for BYOD necessitates implementing Mobile Application Management rather than intrusive Mobile Device Management, balancing security requirements with employee privacy expectations.

Technical Implementation Pillars:

1. **Data Segmentation and Containerization:** MAM creates encrypted containers separating corporate data from personal applications, enforcing policies preventing unauthorized data transfer.
2. **Conditional Access Enforcement:** Access conditional upon device compliance verification including screen lock presence, current OS patches, absence of jailbreaking, and successful MFA completion.
3. **User Accountability and Continuous Monitoring:** Annual policy acceptance agreements grant remote wipe authority for corporate containers only, with continuous security reporting feeding into detection functions.

4.0 Network Security Architecture

NG's predominantly wireless environment coupled with multi-region cloud adoption requires architecture built on segmentation, encryption, and zero trust principles rather than traditional perimeter-based security models.

4.1 Wireless and Remote Access Hardening

1. **WPA3-Enterprise Implementation:** Immediate replacement of remaining WPA2 with WPA3-Enterprise utilizing Simultaneous Authentication of Equals to eliminate offline dictionary attacks and key reuse vulnerabilities.
2. **802.1X and NAC Integration:** Centralized authentication via RADIUS servers ensures only authenticated users and devices access wireless networks,

with NAC solutions placing BYOD devices in restricted segments until compliance verification.

3. **Mandatory VPN Usage:** All remote access and inter-site communications must utilize modern VPN tunnels with strong encryption, addressing ISO network service security requirements.

4.2 Cloud and Data Segmentation Strategy

1. **CASB Deployment:** Cloud Access Security Broker solutions enforce security policies between users and cloud providers, monitoring for policy violations and anomalous behavior.
2. **Comprehensive Network Segmentation:** Headquarters network segmentation using firewalls and VLANs creates isolated environments including Restricted R&D, Confidential Finance/HR, and Least Privilege Guest/BYOD zones.
3. **Encryption Implementation:** Comprehensive encryption for data in transit (via WPA3, VPN, TLS 1.2+), data at rest (using AWS KMS), and data in use (through MAM containerization).

5.0 Compliance and Continuous Improvement

NG's multinational operations necessitate simultaneous compliance with multiple regulatory frameworks, making integrated governance essential for efficient assurance management.

5.1 Compliance Mapping and Implementation

Regulation	Key Requirement	NG Control Mechanism	Responsible
GDPR	Data protection by design/default	DPO appointment, mandatory DPIAs, MAM encryption, consent management	DPO
PCI-DSS v4.0	CHD protection and segmentation	Dedicated VLANs, firewall separation, MFA, CHD encryption	CISO/Operations

Regulation	Key Requirement	NG Control Mechanism	Responsible
ISO 27001:2022	ISMS establishment	Policy framework, risk assessments, WPA3/MAM implementation, audits	CISO
NIST CSF V1.1	Risk-based program	Tier 3 maturity target, continuous monitoring, incident response plans	Security Team
UK Data Protection Act 2018	Data minimization	Data classification ensuring necessity, DPO oversight	DPO

5.2 Critical Analysis: Importance of Updated Standards

- 1. Evolving Threat Landscape:** Regulatory frameworks must evolve from perimeter-based assumptions to Zero Trust Architectures reflecting environments like NG's that lack traditional network boundaries.
- 2. Technological Advancements:** ISO 27001:2022 addresses previous gaps with controls for cloud service security and data leakage prevention, while wireless security evolution demonstrates how outdated standards create unacceptable risks.
- 3. Continuous Adaptive Governance:** Updated standards shift organizational mindset from "pass/fail" compliance exercises to continuous improvement cultures, with PDCA cycles and continual improvement practices requiring regular reassessment against evolving standards.

6.0 Conclusion and Strategic Recommendations

NG's current operational environment creates a paradox where digital transformation drivers simultaneously constitute significant security vulnerabilities. The absence of formal governance structures represents an existential risk to NG's multi-billion-dollar intellectual property and client data assets.

The proposed integrated security governance framework provides the comprehensive foundation necessary for NG's transition from policy vacuum to resilient, compliant, and adaptive security posture. This framework addresses the unique challenges of wireless-dominant, cloud-dependent organizations while establishing sustainable governance mechanisms.

Strategic Implementation Roadmap:

Timeline	Action Focus	Key Deliverables	Framework Alignment
Immediate (0-3 months)	Governance & Policy Foundation	CISO/DPO appointment, Security Steering Committee establishment, Data Classification and Acceptable Use Policy approval	ISO Plan, NIST Identify
Short-term (3-6 months)	Core Technical Mitigation	MAM containerization deployment, BYOD policy enforcement with Conditional Access, wireless infrastructure upgrade to WPA3-Enterprise, ISO 27001 gap assessment	NIST Protect, ISO Do, ITIL Design
Mid-term (6-12 months)	Formal Certification & Integration	ISO 27001 certification achievement, full NIST Detect/Respond function implementation (IDS/IPS, continuous monitoring, incident response plans)	ISO Check/Act, NIST Detect/Respond, ITIL Improve

Timeline	Action Focus	Key Deliverables	Framework Alignment
Continuous Activities	Resilience & Adaptation	Quarterly risk assessment reviews, annual security awareness training, regular compliance audits, threat intelligence integration	ITIL Continual Improvement, ISO Check/Act

By adhering to this strategic roadmap, NG will secure its valuable assets against contemporary threats while establishing governance structures demonstrating organizational maturity, regulatory diligence, and ethical responsibility.

7.0 References

AXELOS. (2019). *ITIL® 4 Foundation*. Retrieved from <https://www.axelos.com/certifications/itil-service-management/itil-4-foundation>

Information Commissioner's Office. (2018). *Guide to the General Data Protection Regulation (GDPR)*. Retrieved from <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/>

International Organization for Standardization. (2022). **ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements**. Retrieved from <https://www.iso.org/standard/82875.html>

National Institute of Standards and Technology. (2018). *Framework for Improving Critical Infrastructure Cybersecurity (Version 1.1)*. Retrieved from <https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf>

Souppaya, M., & Scarfone, K. (2016). **Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security (NIST SP 800-46 Rev. 2)**. Retrieved from <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-46r2.pdf>

PCI Security Standards Council. (2022). **Payment Card Industry Data Security Standard (PCI-DSS) Version 4.0**. Retrieved from https://www.pcisecuritystandards.org/document_library

