



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

Paper Title:

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

University Name: University of Wales Trinity Saint David

Programme: MSc Software Engineering & Artificial Intelligence

Module: Data Security, Governance and Compliance (ACCA7028)

Component: Coursework – Practical Report

Student Name: Dev Shaileshbhai Mistri

Student ID: 2424033

Abstract

NatureGarden (NG) is an international wellness brand that uses cloud services, primarily wireless networks, and a BYOD culture in its business model. NG has no written policy on security matters and is vulnerable to data loss, regulatory penalties and brand damage. This report synthesises the recent body of research on security frameworks and standards, in order to devise a tailored security architecture and governance approach for NG. The report examines recommendations from ISO 27001, the NIST Cybersecurity Framework 2.0 (CSF 2.0) and Risk Management Framework (RMF), COBIT 2019, ITIL 4 and growing holistic approaches. The common themes include risk-based management, components of governance, and continuous improvement. The report proposes a layered architecture that combines many zero-trust principles, principles of defence-in-depth, and strict BYOD controls. In the governance recommendations the report maps controls to legal obligations, for example, the General Data Protection Regulation (GDPR) and NIS2 Directive. In closing, the report discusses why standards change and the need for a human-centred security culture.

Introduction

Although digital transformation leads to an enlarged attack surface, it also offers immense possibilities. Engage in BYOD has enabled NG to provide wireless access to 95% of its network thus enabling staff and clients to use its services easily. The company also uses various cloud providers to deliver its backend services and appear online. Cloud technologies expose the company's intellectual property and sensitive

data to malware infection, unauthorised access, and insider abuse if it does not put a systematic security program in place. If a data breach occurs, it has the potential to prevent operations from being carried out, erode customer trust, and possibly incur fines under data protection legislation.

Information security aims to protect the confidentiality, integrity and availability of information, whilst governance refers to the systems and processes by which an organisation manages and directs its information assets. Compliance refers to meeting the requirements of applicable rules and legislation. These domains of information assurance are interdependent as good governance will ensure security initiatives align with business objectives; good security can enable compliance; and compliance can provide external benchmarks for security activities. NG must find ways to integrate each of these domains in order to come with an appropriate and resilient posture.

This report aims to support NG by investigating established frameworks and models, proposing a multi-layered security architecture adapted to a cloud-centric BYOD environment, and outlining a governance and compliance strategy. By integrating insights from academic literature, standards bodies and governmental guidance, the report offers practical recommendations that balance security, regulatory requirements and business agility.

Literature Review: Frameworks & Models

Organisations adopt multiple frameworks to address cybersecurity risks and to comply with regulations that occur concurrently with framework implementation. The subsections below summarise significant frameworks for NG.

ISO/IEC 27001 and 27002: ISO/IEC 27001 specifies requirements for an ISMS. The standard takes a holistic, risk-based perspective: first, the organisation identifies its information assets; then, it characterises threats and vulnerabilities as it determines its risk appetite; finally, it selects controls from ISO 27002 [1]. Certification shows that an organisation, either a large organisation or a small and medium-sized enterprises, systematically manages security and continuously improves on the controls specified in ISO 27002 [1]. When considering ISO/IEC 27001, it is important to realise that ISO/IEC 27001 is focused on governance (the organisation's policies, etc), the commitment of senior management, competence of the organisation's personnel, and documentation. ISO 27001 covers all industry sectors and sizes of organisations but requires significant investment in identity as a resource; it does not tell the organisation which technology to use. Many organisations combine ISO 27001 with one or more complimentary frameworks to provide wider coverage [3].

NIST Cybersecurity Framework 2.0: The National Institute of Standards and Technologies' Cybersecurity Framework, published in February 2024, offers a taxonomy of cybersecurity outcomes organized into a framework containing functions, categories, and subcategories. In version 2.0 of the CSF provides functionalities beyond U.S.comply critical infrastructure, and promotes open US export of cybersecurity outcomes to be adopted other countries around the world. A new function called

"Govern" reinforces describes the potential involvement of executive oversight, policy provision, and alignment with organization's objectives in achieving organizational serve by_ssl actions to protect their cyber posture. The framework is flexible and is voluntary as organizations create profiles based on their individual manage threats, their advantages the resources and regulatory requirements. However, the CSF provides no specific list of controls, and thus, is frequently used as a companion to detailed standards such as, NIST SP 800-53.

NIST Risk Management Framework (RMF): NIST's RMF provides a repeatable process for the management of information security and privacy risk. The seven steps – Prepare, Categorize, Select, Implement, Assess, Authorize and Monitor – can link to a set of guidance including SP 800-53 [7]. Organizations use impact levels to determine which controls to select based on risk level, implement and document those controls, assess effectiveness, authorize the system for operation, and monitor for changes [7]. The RMF is highly utilized in government agencies but is applicable in private enterprises. The RMF's process of continuous monitoring aligns with NG's need to be proactive to threats as they evolve.

COBIT 2019: COBIT, released by ISACA, defines the governance and management of enterprise information and technology. The most recent update, from 2019, adds six governance principles, which are stakeholder value, holistic approach, dynamic governance, separation of governance and management, tailors to enterprise needs, and end-to-end coverage (This means covering the whole governance process instead of separate silos.) [3]. COBIT also expands to 40 governance and management objectives, as well as maturity model to measure performance [3]. COBIT helps

organizations align IT goals with business strategy, manage risk, and ensure value creation. COBIT provides high-level guidance to be integrated with more specific frameworks such as ISO 27001.

ITIL 4: ITIL is a framework of best practice for IT service management. The current version, ITIL 4, published in 2019, emphasises collaboration, agility and continual improvement [4]. Its guiding principles—focus on value, start where you are, progress iteratively with feedback, collaborate, think holistically, keep it simple, optimise and automate—provide actionable guidance for IT teams [4]. The Service Value System encompasses governance, practices and continual improvement [4]. ITIL provides operational practices to complement governance frameworks for incident, change and service management.

Holistic Information Security Management and Compliance: A recent open-access paper proposed a framework that allows for the integration of operational, technical, human, and physical security into one action plan, connecting the associated controls with recommended approaches for compliance to evolving regulatory requirements such as GDPR, NIS2 and the AI Act [6]. The authors assert that traditional approaches address these domains separately, which could have gaps involved. In testing the framework against several risk scenarios, the holistic framework was able to demonstrate compliance and flexibility to respond to new threats [6]. For organisations like NG with many technology streams and regulatory compliance requirements, a holistic view supports an integrated approach to managing physical and digital security.

Cybersecurity Framework Review: Taherdoost's review of cybersecurity frameworks finds that there are many standards, and it can often be difficult to determine which is

the best choice [6]. The study notes that standards contain requirements for organisations that must be followed to meet certain security objectives and defend against cybercrime. In making a proper selection, organisations should ensure that they align frameworks with their industry, risk profile, and general regulatory environment.

Zero-Trust Architecture: Security models that leveraged clearly defined perimeters have been the norm for many years; zero-trust, on the other hand, assumes that no implicit trust should exist in any given network location. The Canadian Centre for Cyber Security notes that zero-trust architectures require continuous authentication and authorisation of each interaction; at a minimum, apply least-privilege access, assess user and device context [8]. The need for zero-trust has gained urgency as hybrid cloud computing and remote work have reduced our predefined boundaries [8]. The organisations that implement zero-trust should start thinking about granular access controls, continual monitoring and implementing strong identity management.

BYOD Security Risks and Mitigation: Permitting employees to bring their personal devices creates flexibility but can also expose corporate data to a variety of security threats. The common types of risks include data leakage, downloading of malicious apps, infections from unsecured or compromised devices and managing devices that are no longer the employees [9]. There are ways to mitigate these risks including mobile device management (MDM), provisioning based on the user roles, encrypting the data on the device, enterprise app stores, VPNs and user training [9]. Organizations must find a balance between user convenience and effective technical controls to ensure security and privacy.

Data Protection and Cybersecurity Regulations: The European Union (EU) General Data Protection Regulation (GDPR) applies to any organization processing data related to EU residents and outlines 7 principles to follow: lawfulness, fairness, transparency, purpose limitation, data minimization, accuracy, storage limitation, integrity/confidentiality and accountability [10]. Companies that do not comply with the GDPR can incur fines up to €20 million or 4% of total global revenue, whichever is higher [10]. The NIS2 Directive also expands the cybersecurity obligation vertical and horizontally, needing that organizations carry out risk-management measures and undertake a security evaluation (go through security measures) that is expressed by deriving minimum requirements and are harmonized [11]. NG must get ready to meet the regulations while ensuring data subjects have the exercised rights and reporting of incidents.

Comparative Summary:

Framework/Model	Focus	Key Strengths
ISO 27001/27002	ISMS; risk-based controls	Holistic approach and continuous improvement
NIST CSF 2.0	Taxonomy of cybersecurity outcomes	Flexible; adds governance function and supports global adoption
NIST RMF	Risk management process	Repeatable seven-step cycle; emphasises continuous monitoring

COBIT 2019	IT governance and management	Six principles ensure value and a holistic view; maturity model
ITIL 4	IT service management	Guiding principles promote value, collaboration and iteration
Holistic framework	Integrates technical, human and compliance domains	Aligns with evolving legislation and adapts to new threats
Zero-trust	Continuous authentication	Enforces least-privilege and suits hybrid cloud
BYOD mitigation	Controls for personal devices	Uses MDM, provisioning, encryption and training
GDPR/NIS 2	Regulation of data protection and cybersecurity	Defines data protection principles and risk-management obligations

Proposed Security Architecture: NG's security architecture must protect data across cloud services, wireless networks and personal devices while allowing agility.

The design adopts defence-in-depth and zero-trust principles and aligns controls with frameworks such as ISO 27001, NIST CSF and RMF. Figure 1 depicts the conceptual

architectukljkjljk;jol;j

Framework/Model	Focus	Scope	Key Strengths
ISO/IEC 27001	Risk-based information security management	Applicable to all sizes and sectors	Systematic ISMS implementation
NIST Cybersecurity Framework	Cybersecurity risk management	Flexible across all sizes, sectors	Flexible risk management approach
COBIT 2019	IT governance and management	IT governance across the enterprise	Aligning IT goals with business objectives
ITIL 4	IT service management	IT service lifecycle management	Guiding continuous service improvement
Holistic Information Security Management and Compliance Framework	Integrate Information Security Management and Compliance	Integrates operational, technical, human and physical	Comprehensive controls and compliance

Figure 1: A layered security architecture for NG. Concentric rings represent perimeter and network security, identity and access management, endpoint and application security, data security, monitoring, governance and human factors. Controls are mapped to each layer to prevent, detect and respond to threats.

Layer 1: Perimeter and Network Security

On the outer layer, NG uses next generation firewalls, intrusion prevention systems and web application firewalls to filter traffic. Network segmentation with VLANs or software defined networking establishes corporate, guest and IoT zones. Enterprise class Wi-Fi

protected access (WPA3), wireless intrusion detection systems and separate guest networks protects the wireless environment. Vulnerability scanners, network detection and response, and security information and event management (SIEM) provide visibility to traffic and vulnerabilities.

Layer 2: Identity and Access Management

Zero-trust authentication is essential: users and devices must continuously authenticate with multi-factor authentication, single-sign-on and continuous behavioural monitoring. Role-based access control and user attributed-based policies can enforce least privilege. Privileged access management, handles high-risk accounts using just-in-time provisioning and session recording. Identity governance processes provision and de-provision accounts on time, and conduct access reviews periodically.

Layer 3: Endpoint and Application Security

Personal and corporate devices need to be hardened. Mobile device management provides remote configuration, patching, and ability to wipe BYOD devices by the organization [9]. An enterprise app store will not only distribute approved software to devices but separate device use for personal should it need to be used that way. Devices need to encrypt data, support secure boot, and have an antivirus installed. Network access control means verifying the device posture before granting connectivity to the network. For applications, new generation security technologies (NG) combine a secure software development life-cycle—code scanning, threat modelling, and penetration testing. That includes securing web applications using runtime application self-protection and API gateways.

Layer 4: Data Security

Data must be protected wherever it resides. Data can be protected at rest and in transit using encryption, with strong key management practices, together protects confidentiality. Data loss prevention (DLP) can be used to monitor endpoints and network channels for unauthorized data transfer. Tokenisation or masking techniques are used to protect personal data within the analytics space. Backups should always follow the 3-2-1 structure; immutable (cannot be deleted by malware) and with off-site storage, with tests performed over short intervals for restoration purposes, ensures resilience from ransomware and other disasters.

Layer 5: Monitoring and Incident Response

Continuous monitoring enables early detection and response. SIEM systems aggregate logs from network, cloud and endpoints and correlate events with threat intelligence. User and entity behaviour analytics and security orchestration, automation and response (SOAR) tools assist in triaging alerts and automating responses. NG develops an incident response plan that defines roles, escalation procedures and communication strategies. Regular exercises refine the plan and improve team readiness.

Layer 6: Governance, Risk and Compliance

NG establishes an ISMS based on ISO 27001, setting the scope, identifying interested parties, documenting policies and conducting risk assessments. The NIST RMF guides risk categorisation, control selection, assessment, authorisation and monitoring [7]. Policy management covers acceptable use, BYOD, data classification and incident response. Compliance mapping ensures that controls meet GDPR's principles [10] and

NIS2's risk-management requirements [11]. Performance metrics and audits drive continual improvement.

Layer 7: Human Factors and Security Culture

Human error remains a leading cause of breaches. NG invests in security awareness training on phishing, social engineering, secure BYOD use and incident reporting. Simulated phishing exercises and role-specific training help ingrain safe behaviours. Stakeholder engagement fosters executive support and aligns security with business objectives [3]. An insider-threat programme monitors for anomalous behaviour while respecting privacy. A culture of shared responsibility emphasises ethical data use and diversity.

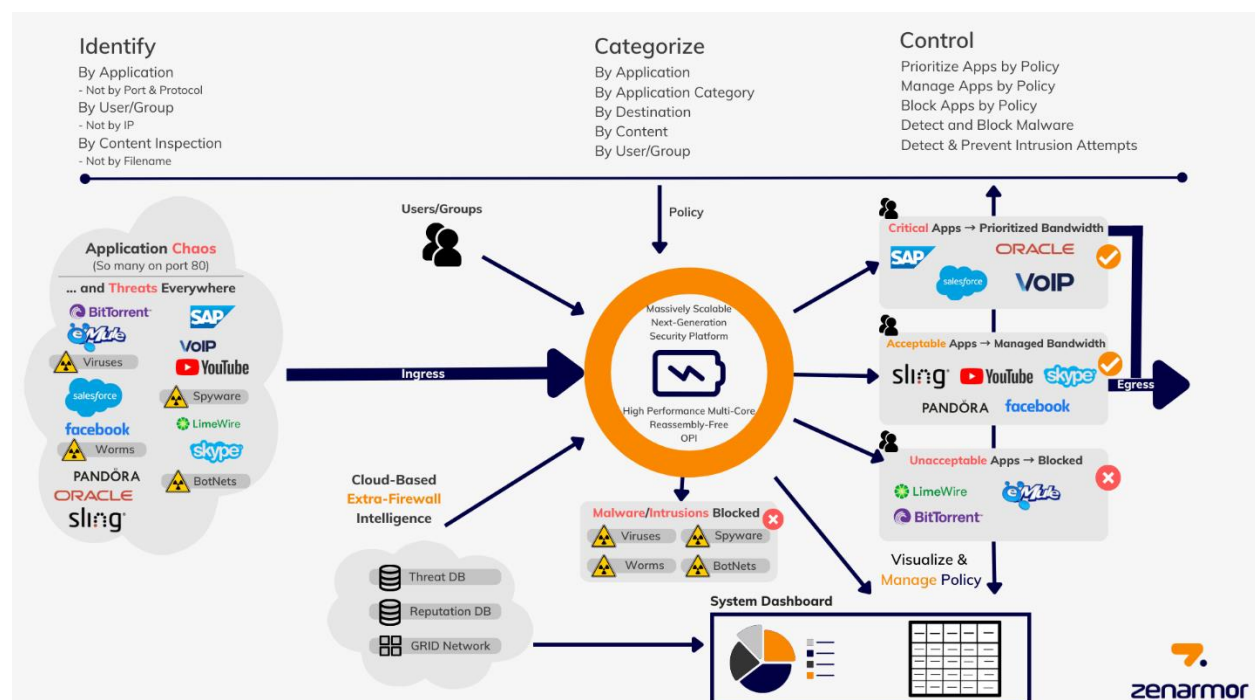


Figure 2: A next-generation perimeter and network security platform illustrating traffic flow from users and cloud intelligence into a central control core. This core categorizes,

inspects, and enforces policies based on user roles, content type, and threat intelligence—allowing business-critical apps (e.g., SAP, Salesforce) while blocking high-risk ones (e.g., BitTorrent). It supports NatureGarden’s zero-trust strategy and BYOD environment through adaptive controls and real-time visibility at network ingress and egress points.

Governance & Compliance Strategy

Security controls are effective only when supported by robust governance and compliance processes. NG’s strategy integrates multiple frameworks and regulatory requirements to manage risk holistically.

Integrated Governance: Applying COBIT 2019’s principles, NG defines clear governance structures and responsibilities. A security steering committee, chaired by an executive, oversees policy development, budgets and risk tolerance. Governance and management functions are separated: the board and committee provide direction, while IT and security teams execute controls [3]. Stakeholder engagement ensures that initiatives deliver value and support strategic objectives [3].

Information Security Management System: NG formalises an ISMS aligned with ISO 27001. The scope encompasses cloud services, wireless infrastructure and BYOD devices. Risk assessments identify threats and vulnerabilities, evaluate likelihood and impact and prioritise treatment options using the NIST RMF methodology [7]. Controls

are selected from ISO 27002 and NIST SP 800-53, documented, implemented and monitored. Internal audits and management reviews evaluate effectiveness and drive continual improvement.

Regulatory Compliance: GDPR and NIS2: GDPR compliance requires embedding data protection principles into the data lifecycle [10]. NG maintains records of processing activities, obtains valid consent, enforces purpose limitation, applies data minimisation and ensures data accuracy. Data subject rights—access, rectification, erasure, portability and restriction—are operationalised through technical and organisational measures. Data protection impact assessments are conducted for high-risk processing and guided by a Data Protection Officer.

NIS2 expands cybersecurity obligations across sectors, requiring risk-management measures, incident reporting and supervision by national authorities [11]. NG evaluates whether it is classified as an essential or important entity, implements technical and organisational measures to mitigate risks, and harmonises evaluation instruments. Incident notification procedures align with both NIS2 and GDPR's 72-hour breach reporting requirement.

IT Service Management and Supply Chain: ITIL 4's guiding principles help NG deliver reliable and secure services. Incident, problem and change management processes are integrated with security operations to ensure rapid recovery and controlled modifications [4]. Service level agreements (SLAs) include security and privacy requirements such as availability, integrity and confidentiality. Supplier management requires due diligence on

cloud providers and third parties: contracts stipulate security obligations, audit rights and breach notification.

Culture and Ethics: Ethical considerations shape governance. NG develops policies on ethical data use, particularly for analytics and artificial intelligence. Diversity and inclusion are promoted by designing training and processes accessible to all. Sustainability is considered when selecting cloud providers and hardware, aligning with environmental goals.

Discussion

Evolving Threat Landscape and Standards: Cyber threats evolve continuously: adversaries use automation, unpatched (zero-day) vulnerabilities, and artificial intelligence. Hybrid cloud architectures and remote work eliminate traditional perimeters [8], and personal devices increase attack vectors [9]. Standards and regulations must evolve with the adaptive threat environment. ISO 27001 is updated periodically; NIST released new CSF v2.0 with new governance function; COBIT 2019 has revised and expanded governance objectives; and zero-trust architectures directly challenge implicit trust concepts [8]. Regulators also are both adjusting: GDPR established an international standard for privacy in 2018 [10], NIS2 broadens sector specificity and increases cybersecurity obligations [11]. NG needs to monitor these evolving threats and standards and modify controls if appropriate.

Balancing Security and Agility: Organizations expect high security but also expect agile delivery of innovation. Too many controls slow innovation, while too few controls provide opportunity for breaches to occur. The proposed architecture balances both needs: use of zero-trust, allows secure access without exposing the network; use of role-based access and automation improves the user experience. ITIL encourages organizations to progress in small increments toward improvements that do not overwhelm users [4]. Regulatory compliance, in many cases, should be viewed as an enabler: attaining ISO 27001 certification facilitates customer trust, being GDPR compliant does not avoid fines but does maintain brand reputation [10].

Human Factors and Culture: To ensure security, technology alone is not sufficient. Social engineering is still a common attack vector. Security awareness training, regular phishing simulations, and clear lines of communication can foster an authentically security-concerning workforce. Leaders must exhibit a commitment to security; otherwise employees might perceive controls as obstacles. A culture of safety that emphasizes shared responsibility, ethically using data, and respecting privacy is preferred. COBIT's holistic principle highlights the reason people and processes should also be included with technology [3].

Integrating Frameworks: No singular framework will fully satisfy all of NG's requirements. ISO 27001 provides an ISMS; NIST CSF provides terminology related to desired outcomes; NIST RMF provides a risk-management framework to follow; COBIT covers strategic alignment; ITIL covers operational best-practice; and zero-trust provides new architecture. There are also statutory policies imposed by GDPR and

NIS2. Integration of all frameworks will help NG to use the good aspects of each framework and mitigate their weaknesses. If controls are mapped across the frameworks they will be consistent. For example the controls from ISO 27001 map against the objectives in COBIT and steps in NIST RMF. A cohesive framework would maximize the synergies of the technical, human and legal aspects we have discussed [6].

Limitations and Future Research: This report presents a high-level design. The detailed implementation will require sequenced priorities based on Network Glasgow's maturity and budget. The proof-of-concept projects, cost/benefit analysis and consultation with stakeholders will offer guidance on implementation. New emerging technologies (e.g. Artificial Intelligence, Quantum Computing and Blockchain) may require new controls and governance. Consistent engagement with legal counsel will help to achieve compliance with developing laws.

Conclusion

NG operates within a complex ecosystem that features, amongst other things, BYOD, cloud services and wireless access. Without a security Programme in place, the organisation is at significant risk. This report shows that, via the analysis of rule sets and frameworks, security must be managed holistically and underpinned by governance, assurance and compliance. The proposed layered architecture leverages concepts such as defence-in-depth and zero-trust, implements sound BYOD controls

and prioritises continuous monitoring, whilst a governance framework built upon COBIT, ISO 27001, NIST CSF and RMF, ITIL 4, and an obligation to comply with GDPR and NIS2 regulations can deliver a sustainable arrangement. Humans and culture are important factors – without engaged people, the technical controls will fail. By implementing the recommendations made in this report, NG can develop a resilient and compliant security posture that can support the domains of innovation, whilst also protecting stakeholders.

References

- [1] International Organization for Standardization, “ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements,” 2022. <https://www.iso.org/standard/27001>
- [2] O. Traynor, “NIST Cybersecurity Framework 2.0: An Overview,” CybelAngel, Mar. 24 2025. https://cybelangel.com/guide_nist_2/
- [3] Legit Security, “What Is the COBIT Framework? IT Governance and Management,” Legit Security Blog, Jun. 4 2025 <https://www.legitsecurity.com/aspm-knowledge-base/what-is-cobit-framework>

- [4] Atlassian, "ITIL Framework Guide: Core Principles & Best Practices," Atlassian, 2024. <https://www.atlassian.com/itsm/itil>
- [5] Š. Grigaliūnas et al., "Holistic Information Security Management and Compliance Framework," *Electronics*, vol. 13, no. 19, pp. 3955, 2024. <https://doi.org/10.3390/electronics13193955>
- [6] H. Taherdoost, "Understanding Cybersecurity Frameworks and Information Security Standards—A Review and Comprehensive Overview," *Electronics*, vol. 11, no. 14, p. 2181, 2022. <https://doi.org/10.3390/electronics11142181>
- [7] National Institute of Standards and Technology, "Risk Management Framework (RMF)," NIST, Jul. 22 2025. <https://csrc.nist.gov/projects/risk-management>
- [8] Canadian Centre for Cyber Security, "A zero trust approach to security architecture – ITSM.10.008," Government of Canada, Mar. 15 2023. <https://www.cyber.gc.ca/en/guidance/zero-trust-approach-security-architecture-itsm10008>
- [9] L. Yacono, "The 8 Top BYOD Security Risks (and How to Mitigate Them)," Cimcor State of Security Blog, Sep. 12 2024. <https://www.cimcor.com/blog/7-scariest-byod-security-risks-how-to-mitigate>
- [10], "What is GDPR, the EU's new data protection law?," 2018. <https://gdpr.eu/what-is-gdpr/>

[11] M. Seeba, M. Valgre and R. Matulevičius, “Evaluating Organization Security: User Stories of European Union NIS2 Directive,” arXiv preprint, Apr. 27 2025.

<https://arxiv.org/pdf/2504.19222>.