

L5 - Data Security and Compliance (DDA - SEM 3) (ACCA5034)

GEORGE QUICK (2315899)

Table of Contents

Task 1	3
Introduction	3
Security Frameworks.....	3
Security Technologies	5
Network Security.....	5
End Point Security	6
Task 2	0
Introduction	0
Organisation Structure/Chart	0
Policies and Procedures.....	0
Data Protection Compliance	1
Security Standards	1
Contingency Planning	2
Governance and Strategic Planning for Security	2
Risk Management.....	3
Conclusion	3
Bibliography.....	4

Task 1

George Quick

Student University of Wales Trinity St David, Swansea, Wales

2315899@student.uwtsd.ac.uk

Abstract -- Data security and compliance are critical elements that modern organisations need to ensure protection, detection, and response to threats against their IT systems and infrastructure. This paper looks at critical security technologies like firewalls, access controls, and VPNs, as well as important security frameworks like NIST and ISO 27000. By offering a thorough analysis of these topics, the paper seeks to highlight the importance of having multiple strategies for data security and compliance.

Introduction

Data security and compliance are critical given how reliant on IT infrastructure and systems businesses are in today's digital environment. Because cyber threats are becoming more complex, robust security measures are needed to protect sensitive data and ensure uninterrupted operations. Serious consequences from data breaches can include financial losses, reputational damage, and legal issues. Consequently, it is important that businesses put comprehensive security plans into place that cover a variety of activities, including employee training, technology defences, and physical security measures. This paper will look at key security frameworks, technologies, and practices to emphasise the need for a comprehensive approach to data security and compliance. In addition, we'll examine how crucial it is for companies to set up settings in which their

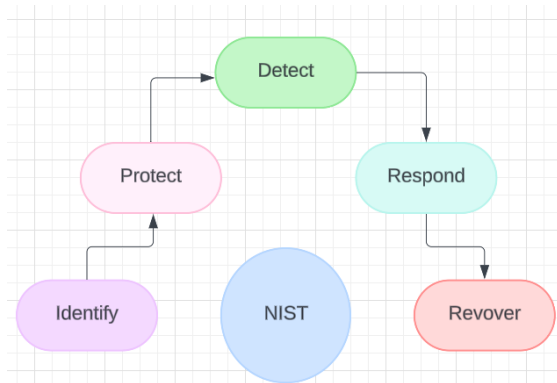
IT systems are employed to safeguard, identify, and respond to applications [1].

Security Frameworks

A family of standards called ISO 27000 was created to support businesses in protecting their information assets. The most well-known standard in this family, ISO 27001, specifies the requirements for developing, implementing, maintaining, and improving an information security management system (ISMS) over time. With the framework, sensitive company data can be handled with care and its security ensured. Organisations can gain better risk management, a stronger reputation, and a solid base for regulatory compliance by putting ISO 27001 into practice. Organisations must follow ISO 27001's requirements to assess their information's security risks, taking into consideration potential threats, weaknesses, and effects. Case studies show that businesses that use ISO 27000 standards have fewer security lapses and are better prepared for crises. Companies have discovered, for example, that after implementing ISO 27001, business risk has decreased by 75% and business trust has increased by roughly 80% [2]. The framework strengthened the organisation's security posture by enhancing its capacity to identify and manage risks.

Another security framework called NIST controls cyber hazards by coming up with practices, advanced methods, principles,

and guidelines for reducing cybercrime. The NIST framework, which consists of five core functions (Identify, Protect, Detect, Respond, Recover) [3], is widely recognised and used across various industries.



For businesses to comprehend, control, and lower their cybersecurity risks, NIST offers a strong framework for private organisations looking to evaluate and enhance their capacity to stop, identify, and react to cyberattacks. It provides a framework of computer security policy guidelines that can be used to improve a company's overall security posture. The NIST cyber security framework also integrates industry standards and best practices to help companies manage their cybersecurity risks [4]. By implementing the NIST framework, organisations can enhance their cybersecurity resilience and fortify their defences against constantly changing cyber threats.

COBIT 5 is a framework designed to help organisations address challenges in regulatory compliance, risk management, and align IT strategy with a company's goals in mind. It was released in 2012 and is based on five principles which are meeting stakeholder needs, covering the enterprise end-to-end, applying a single integrated framework, enabling a holistic approach, and separating governance from management [5]. These principles enable organisations to build a comprehensive framework for IT governance and management, which is built on seven

enablers which are people, policies and frameworks, processes, organisational structures, culture, ethics and behaviour, information, services, infrastructure and applications, and people, skills, and competencies [6]. The benefits of COBIT 5 include improving and maintaining high-quality information, using IT effectively to achieve business goals, managing IT risks effectively, ensuring organisations realise the value of their IT investments, and achieving compliance with laws, regulations, and contractual agreements [7]. The framework is designed with integration at its heart, aligning with best-practice frameworks and standards like ISO 20000, and ISO 27001.

The Payment Card Industry Data Security Standard (PCI DSS) is a set of security requirements developed in 2004 by major credit card companies to ensure the security of credit card processing, storage, and transmission. Building and maintaining secure networks and systems, protecting cardholder data, maintaining a vulnerability management program, implementing strong access control measures, monitoring and testing networks on a regular basis, and maintaining an information security policy are all key components of PCI DSS [8]. Compliance and validation are classified into four levels based on transaction volume, with specific requirements ranging from annual assessments by Qualified Security Assessors (QSAs) for large organisations to self-assessment questionnaires (SAQs) for smaller entities [9]. Companies that collect payment information should utilise a PCI DSS, as it is critical in reducing credit card fraud and safeguarding cardholder data. Despite challenges faced in implementing them, enhanced security practices enhance consumer trust, while continued commitment to the PCI DSS is very important as changes in cybersecurity continue to take place.

A comparison between NIST and ISO 27000 shows that they are two different things in terms of style and emphasis, even though they are similar in the context of raising the cybersecurity profile within companies. On the one hand, ISO 27000 is designed to help establish a complex information systems management system that is fully supported by continuous improvement. On the other hand, NIST provides a method that is adaptable and risk-based, allowing it to be tailored to the specific needs of an organisation's existing practices. COBIT 5 covers more than just cybersecurity, as it is an IT oversight framework for aligning IT strategy with the objectives of the business and tackles more complex areas such as regulations and operations. On the other hand, PCI DSS is a narrow focus on cybersecurity as it aims to protect payment card data by providing detailed controls and requirements that are meant for reducing incidences of credit card fraud.

Security Technologies

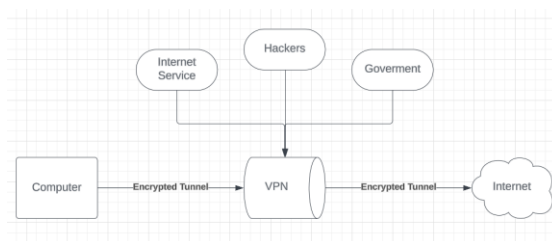
Network Security

Network security depends substantially on firewalls, which are barriers between the internal network of a company and external dangers. They evaluate incoming and outgoing information with reference to previously set security limits. Both hardware and software are the common forms of implementing or combining firewalls in an organisation. Firewalls assist in preventing unauthorised access to valuable information that helps in averting cyberattacks through monitoring network traffic [10]. A firewall could be set so as not to allow information from some areas or applications but to let in those ones that are of significance. Modern firewalls also include features such as stateful inspection, proxying, and packet filtering to provide enhanced security. Another type of firewall is NGFWs, which stand for 'next-generation firewalls.' These are advanced

security devices that integrate additional capabilities such as application awareness, integrated intrusion prevention, and cloud-delivered threat intelligence [11]. NGFWs offer more detailed inspection and precise control over network traffic, allowing enterprises to successfully identify and prevent complex threats.

Another security technology commonly used by companies is called Access controls. Access controls are security measures that limit who or what can view or use resources in a computer environment [12]. They are a critical component of data security, ensuring that only authorised users have access to specific data or systems. Access controls can be implemented at several levels, including physical, administrative, and technical. It is important to use strong access control mechanisms, such as multi-factor authentication (MFA) and role-based access control (RBAC), for protecting sensitive information from unauthorised access. MFA is a security technology that requires users to provide two or more verification factors to gain access, thereby enhancing security beyond just a username and password [13]. RBAC assigns permissions to users based on their job role within the organisation so that they only have access to the information necessary for them to carry out their job functions [14]. Security is further enhanced by groundbreaking technologies for access management like biometric authentication and adaptive access control systems. Biometric authentication is based on unique biological characteristics like fingerprints or facial recognition to confirm someone's identity. On the other hand, adaptive access control modifies its protective measures depending on the nature of the access request, including where a user is at any moment or even what type of equipment he or she might be using [15].

Confidentiality and integrity of data sent over the internet are largely reliant on VPNs. A VPN creates a private encrypted tunnel through which the data travels, meaning even if the data gets intercepted, it cannot be read by unauthorised persons. This makes them particularly significant for organisations with remote workers or branch offices since they facilitate secure connection to the organisation's network from anywhere.



VPNs have two main types that include remote-access VPNs and site-to-site VPNs. Remote-access VPN enables individual users to connect remotely to an organisation's network, while site-to-site VPN establishes all the whole network interconnected with each other, meaning companies can have secure communications between several branches or offices located at different locations. The importance of VPNs has been accelerated with the increased trend towards remote work. More organisations are looking for robust and scalable VPN solutions as they accommodate a rising number of employees who work remotely from home or outside their office locations [16]. But VPNs have some drawbacks, such as slow speeds and the possibility of vulnerabilities arising because of these commands not being properly configured. To reduce such threats, organisations must ensure that their VPN services are well configured in terms of settings and that they are updated on a regular basis.

End Point Security

Technology that provides security for devices that get connected to the network

is named endpoint security. These devices include computers, smartphones, tablets, and more recently, Internet of Things devices. Out of these numerous measures, antivirus and anti-malware software, together with endpoint detection and response (EDR) as well as mobile device management (MDM), are prominent technologies in endpoint security.

Antivirus and anti-malware tools are crucial components of endpoint security. Their main purpose is to sense, block, and eliminate viruses and other harmful software from computers and phones. Antivirus can detect viruses in multiple ways, such as a signature-based detection. This is the most common method, and it uses a database containing known malware signatures. It is very effective in fighting against threats that are already known, but it fails to deal with newly discovered or polymorphic viruses, which continuously alter their code in order to elude detection. Heuristic analysis can detect viruses by analysing the behaviour of programmes and comparing them to usual malware activities. This allows heuristic analysis to identify possibly malicious software based on suspicious behavioural patterns even if such software is not part of a signature database. Another detection method would be behavioural analysis, which is commonly used by modern antivirus solutions to look at the real-time behaviour of applications. In the event that an application behaves in a manner generally associated with viruses, such as unauthorised access to protected files or abnormal network traffic patterns, then the antivirus would be able to recognise and isolate this threat. Antivirus software is like a defensive barrier against varied threats such as worms through trojans, ransomware, or spyware. But these tools are not enough to protect you from all the viruses out there [17]. Advanced Persistent Threats (APTs) are sometimes so advanced that they can easily evade common antivirus programmes, and then

more layers of security must be added. Also, signature-base detection is too insufficient in the light of fast-growing malware varieties [18].

Another component of endpoint security is EDR. Endpoint detection and response represents a more advanced approach to endpoint security, providing continuous monitoring and response capabilities to detect and mitigate sophisticated threats. Unlike traditional antivirus software, EDR solutions offer real-time visibility into endpoint activities, enabling proactive threat detection and response. The ongoing surveillance from EDRs is critical for identifying and responding to threats that may have gotten past primary defences. Advanced Threat Recognition in EDRs can identify features such as APTs with the use of machine learning and artificial intelligence. These tools evaluate massive amounts of endpoint data to identify anomalies or potential safety incidents. EDR significantly improves a company's ability to detect and respond to advanced threats [19]. Continuous monitoring and real-time response capabilities shorten the time spent in the presence of threats, reducing potential damage. However, implementing EDR solutions presents challenges, such as the need for skilled personnel to manage and interpret the data, the possibility of high operational costs, and the complexities of integrating with existing IT infrastructure.

The increase in the use of mobile devices at work has made MDM another vital part of endpoint security. Organisations can use MDM solutions to ensure that corporate data is protected no matter where it is accessed by securing, monitoring, and managing mobile devices. MDM solutions enforce security policies on mobile devices, including encryption, password requirements, and remote wipe capabilities, to protect sensitive data. They manage applications installed on devices, ensuring only approved apps are used and

regularly updated to mitigate vulnerabilities. MDM solutions also monitor device compliance with corporate policies and regulatory requirements, helping organisations maintain data protection regulations like GDPR, HIPAA, and ELD [20]. MDM can ensure consistent security policies and data protection for mobile devices. However, it can be complex to implement and may face resistance from employees concerned about privacy and control over their personal devices.

Malware and viruses have long been fought with antivirus and anti-malware software as one way of fighting known threats. However, they do not work well against sophisticated and rapidly changing threats. Endpoint detection and response systems take a more proactive route to endpoint security, unlike antivirus software's, providing continuous monitoring, advanced threat detection capabilities, as well as real-time responses. Unfortunately, they require expertise personnel, thus making them expensive both in terms of setup and operational costs. Mobile Device Management (MDM) enables securing and managing mobile devices so that data is protected from loss or corruption while complying with company policies or national regulations. However, its implementation can be complex because users may resist it on privacy matters. Each technology tackles different aspects of endpoint security but if used together it can ensure comprehensive protection for modern organisations.

To summarise, the study concluded that diverse data protection and strategies are required for modern organisations. Organisations can greatly improve their ability to safeguard sensitive information against various types of risks, including rising cyber threats, and respond appropriately in the event of an attack by incorporating critical security frameworks

such as ISO 27000, NIST, COBIT 5, and PCI DSS into modern technology such as firewalls, access rights, VPNs, antivirus programmes, EDR, and MDMs. In today's complex virtual environment, it is vital to implement these security feature plans in order to maintain solid data security while also complying with the law requirements.

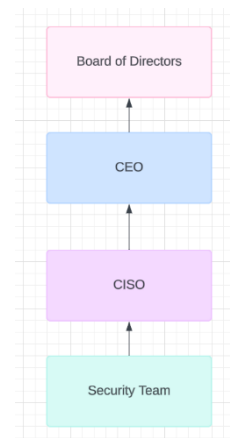
Task 2

Introduction

In today's digital age, information security is very important to the success and lifespan of any organisation. My company, which operates in a highly competitive data-driven environment, must prioritise the security of its information resources. This report will discuss the steps necessary to establish a successful information security unit, including structure, rules, conformity, standards, contingency planning, governance, and risk management. The following sections describe how I intend to build that unit.

Organisation Structure/Chart

The Chief Information Security Officer (CISO) is the leader of the unit and will report directly to the Chief Executive Officer (CEO) and also to the Board of Directors. The CISO will be responsible for managing the key elements of an information security program, including establishing a complex strategy, risk management, security policies and procedures, security awareness, incident response, security architecture, third-party security, regulatory compliance, security incident reporting, budgeting and resource allocation, security technology evaluation, disaster recovery plans, collaboration and communication and continuous monitoring and improvement.



The information security strategy involves establishing a comprehensive plan aligned with organisational goals and addressing current and emerging security threats. Risk management involves conducting risk assessments and developing mitigation strategies. Security policies and procedures are created and implemented, ensuring adherence to regulations and standards. Security awareness and training are encouraged, and an effective incident response plan is developed and managed. The security architecture is designed and implemented, and security technologies are evaluated and selected. Legal and regulatory compliance is monitored, and procedures for reporting security incidents are made. The budget is developed and overseen as well as security technologies are being evaluated and recommended for enhancement. Business continuity and disaster recovery plans are created and sustained and communication is maintained with senior management. The assurance programme is overseen, and continuous monitoring and improvement are ensured to improve the organisation's overall security posture. [21]

Policies and Procedures

Security policies and procedures are very important to the security unit as they make sure that there is a consistent and effective protection of the company's assets. There are various steps to developing these policies. To begin with, I would draft policies that address different areas of security, such as access control, data protection, incident response, network security, and acceptable use. For example, an Access Control Policy should specify how access to systems and data is granted, managed, and revoked so that only authorised personnel can access sensitive information. [22]

After the policies have been outlined, I can develop in-depth procedures that specify how to go about implementing them. Access control procedures, for example, may include user authentication steps, authorisation processes, and reviewing access rights after certain periods of time. The incident response procedure should outline the steps for identifying, containing, and eradicating security breaches, as well as recovering from them, to ensure that potential threats are managed in a planned out way.

Then the policies and procedures should be reviewed by legal and compliance teams after being made to ensure they meet the requirements needed. After review, they should be approved by senior management to demonstrate the company's commitment to security. Regular training sessions are essential to ensure all employees understand and adhere to the security policies and procedures. These sessions can include workshops, e-learning modules, and regular updates on emerging threats and best practices. [23]

Data Protection Compliance

When creating a security unit, it is important I comply with data protection legislation and regulations in order to avoid legal repercussions and keep customers happy. The starting point for attaining compliance with data protection legislation is establishing which regulations are needed for my organisation. Common regulations include the General Data Protection Regulation (GDPR), which applies to organisations handling the personal data of EU residents; the California Consumer Privacy Act (CCPA), which protects the privacy rights of California residents and the Health Insurance Portability and Accountability Act (HIPAA), which regulates the handling of healthcare information in the US [24]. Once the regulations I will use are identified, I will then develop a compliance framework to best suit the business. This includes creating a data inventory to document the types of data collected, stored, and processed. I will also conduct Data Protection Impact Assessments (DPIAs) to identify and mitigate privacy risks. Then I can implement processes for handling data subject requests, such as access, rectification, and deletion, to comply with legal requirements.

If required by law, I will need to appoint a Data Protection Officer (DPO) to oversee data protection activities and ensure that the company is complying with regulations that have been set up, as well as providing advice on data protection impact assessments [25]. Preparing for data protection audits is important for the organisations because it ensures compliance with data protection laws and regulations, maintains data, and avoids potential legal penalties and reputational damage due to noncompliance. To prevent this I will implement a data protection audit with the purpose of processing personal data, its principles, data minimisation, security measures, record-keeping, data rights and a data breach response plan. [26]

Security Standards

Implementing security standards in the security unit ensures a consistent and effective approach to securing the company's assets is set up. Using recognised security standards, such as ISO 27001 or NIST, is a good starting point. ISO 27001 provides a framework for establishing, implementing, maintaining, and continually improving an information security unit, while the NIST Framework offers guidelines for identifying, protecting, detecting, responding to, and recovering from cybersecurity incidents. [27]

Regular assessments and audits are required to ensure compliance with security standards. I will identify and close all gaps using tools such as vulnerability scanners, penetration testing, and security assessments. The results of these assessments, along with any new threats that emerge, should help the company make continuous improvements to the security unit. This allows me to review and update the security norms on a regular basis, ensuring their effectiveness and relevance. [28]

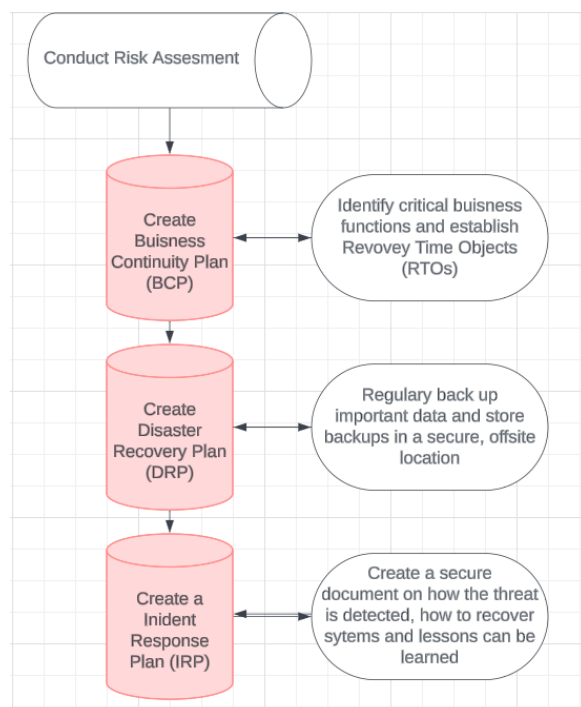
Contingency Planning

Contingency planning prepares my organisation for potential security incidents and disruptions, ensuring the business stays up and running with a quick recovery. The first step in contingency planning is to conduct a risk assessment to identify potential threats and vulnerabilities that may affect my organisation's operations as well as assess the possibility and impact of these threats in order to prioritise them correctly.

To do this, I will create a Business Continuity Plan (BCP) that outlines procedures for continuing operations during and after a disruption. The BCP will identify critical business functions and prioritise their restoration and establish recovery time objectives (RTOs) to determine acceptable downtime for important functions as well as define communication plans for interacting with stakeholders during a disruption.

Then I will create a Disaster Recovery Plan (DRP) with steps for recovering data and systems following a disaster. This includes regularly backing up the important data and storing it in a secure, offsite location for safe keeping. The DRP should outline the steps for restoring systems and data from backups and include regular testing to ensure it is effective.

Finally, I will need to develop an Incident Response Plan (IRP) detailing the process for responding to any security incidents. The IRP should cover detection and analysis of incidents, containment and deletion of threats, recovery of affected systems, and a post-incident review to see what lessons can be learned to improve on for future responses. Regularly testing and updating the IRP ensures it will remain effective and relevant for any future attacks to the unit. [29]



Governance and Strategic Planning for Security

Establishing governance structures and strategic plans is essential for the security unit. The basic security governance framework includes direct guidance of security management, monitoring performance, evaluating results to ensure objectives are met and communicating security status to the stakeholders. This framework includes a governing cycle to direct,

monitor, and evaluate the information security management system, which includes incorporating monitoring results and security management proposals for changes and improvements.

To establish governance and strategic planning for the information security unit, I will define clear policies and procedures, assigning roles and responsibilities and holding regular meetings to provide direction and discuss security strategies. I will use key performance indicators (KPIs) to measure the effectiveness of the security measures and implement tools that look at real-time data. I can then conduct regular evaluations through internal audits, vulnerability assessments, and penetration testing, using the results to update our security strategies and action plans. I will continuously direct, monitor, and evaluate the information security unit by setting clear objectives, monitoring performance, and proposing changes based on monitoring results. I incorporate insights from monitoring to inform security management proposals, such as additional training or technical controls to address vulnerabilities. By doing this I will ensure that the security unit operates effectively, continuously improves, and aligns with the organisation's strategic security plan. [30]

Risk Management

When implementing a risk management program for the unit, it is important for me to establish the context and determine what to do when a risk is at stake. This involves understanding the factors that will impact my risk management decisions, such as the unit's security risks, business objectives, user needs and cyber security obligations. To have a consistent management of risks, I would need to get guidance on risk management from my organisation. To determine what actions to take against a risk, I will work closely with people who are in charge of managing project risks. There are different frameworks on how responses can be classified for example, you can treat, tolerate, transfer or terminate them depending on the situation at hand. I can treat or reduce the risk by implementing security measures that reduce the likelihood of the threat and the severity of the impact. I might tolerate or accept the risk, especially if the chances and impact are low or I can terminate or avoid the risk by adapting the security unit or limiting the exposure. [31]

I will identify and compare mitigation options using the security frameworks i have set for the security unit, considering factors such as effectiveness, duration, associated costs, implementation timelines, and effort required. I will then create a risk treatment plan to measure and reduce all risks to an acceptable level. [32]

Conclusion

In conclusion setting up a new security unit in a company is a difficult but necessary task. By following the procedures outlined in this report, my organisation can establish a strong security framework that protects company assets, ensures rule compliance, and maintains employee data integrity in the security unit. From defining an organisational structure and developing comprehensive policies and procedures to ensuring data protection compliance and implementing security standards, each step is critical to a security unit's success. Contingency planning, governance, strategic planning, and risk management are also important in preparing for potential incidents while maintaining the unit's effectiveness.

Bibliography

- [1] "Closed Door Security - Cyber Security Experts." Available: <https://www.cdsec.co.uk/blog/the-evolution-of-threats-and-increasing-complexity-of-cyber-security-management>
- [2] "ISO 27001:2013 How your organization will benefit," Available: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.bsigroup.com/LocalFiles/EN-AU/ISO%2027001/Documents/27001%20Resources/ISO_27001_CEO_Briefing_WEB_AU.pdf, 2013.
- [3] E. Bresnahan, "NIST Cybersecurity Framework (CSF) Core Explained." Available: <https://www.cybersaint.io/blog/nist-cybersecurity-framework-core-explained#:~:text=The%20core%20functions%20are%20to,reporting%20cybersecurity%20to%20the%20Board.>
- [4] "Risk Management | NIST," NIST, Feb. 13, 2024. Available: [https://www.nist.gov/risk-management#:~:text=NIST%20Cybersecurity%20Framework%20\(CSF\)&text=The%20Framework%20integrates%20industry%20standards,understanding%20of%20their%20cybersecurity%20risks](https://www.nist.gov/risk-management#:~:text=NIST%20Cybersecurity%20Framework%20(CSF)&text=The%20Framework%20integrates%20industry%20standards,understanding%20of%20their%20cybersecurity%20risks)
- [5] "What is COBIT 5? Definition & Explanation." Available: <https://www.itgovernance.co.uk/cobit>
- [6] "COBIT 5 Principles and Enablers Applied to Strategic Planning," ISACA. Available: <https://www.isaca.org/resources/news-and-trends/industry-news/2015/cobit-5-principles-and-enablers-applied-to-strategic-planning>
- [7] Knowlathon, "Top 5 reasons Why Your Company Should Adopt COBIT5," Mar. 28, 2023. Available: <https://www.linkedin.com/pulse/top-5-reasons-why-your-company-should-adopt-cobit5-knowlathon/>
- [8] N. Barney, "What is PCI DSS (Payment Card Industry Data Security Standard)?," Security, May 02, 2024. Available: <https://techtarget.com/searchsecurity/definition/PCI-DSS-Payment-Card-Industry-Data-Security-Standard>
- [9] "The 4 PCI Compliance Levels Explained | Exabeam," Exabeam, Jun. 14, 2024. Available: <https://www.exabeam.com/explainers/pci-compliance/the-4-pci-compliance-levels-explained/>
- [10] "What Is Firewall Security? How to Protect Your Infrastructure," F5, Inc. Available: <https://www.f5.com/glossary/firewall-security#:~:text=Firewalls%20work%20by%20helping%20filter,all%20sorts%20of%20security%20issues>
- [11] "What is a next-generation firewall (NGFW)?," CloudFlare. Available: <https://www.cloudflare.com/en-gb/learning/security/what-is-next-generation-firewall-ngfw/>
- [12] B. Lutkevich, "access control," Security, Jul. 07, 2022. Available: <https://www.techtarget.com/searchsecurity/definition/access-control#:~:text=Access%20control%20is%20a%20security,access%20control%3A%20physical%20and%20logical>

- [13] "Making accounts more secure with multi-factor authentication." Available: <https://support.microsoft.com/en-gb/topic/what-is-multifactor-authentication-e5e39437-121c-be60-d123-eda06bddf661>
- [14] W. Thompson, "What is Role-Based Access Control?," Hexnode Blogs, Oct. 17, 2023. Available: <https://www.hexnode.com/blogs/what-is-role-based-access-control-rbac/>
- [15] "Understanding Adaptive Authentication and How It Works | Okta UK," Okta, Inc. Available: <https://www.okta.com/uk/identity-101/adaptive-authentication/>
- [16] "What is Virtual Private Network (VPN) Security? | NordLayer," NordLayer. Available: <https://nordlayer.com/learn/vpn/what-is-vpn/>
- [17] "What is antivirus software?" Available: <https://www.sophos.com/en-us/cybersecurity-explained/antivirus>.
- [18] A. Shoemaker, What is APT (Advanced Persistent Threat) | APT Security | Imperva. 2023. Available: <https://www.imperva.com/learn/application-security/apt-advanced-persistent-threat/>
- [19] C. Nichols and C. Nichols, "Traditional Antivirus vs. EDR (Endpoint Detection and Response) - Cybriant," Cybriant - Managed Security Services | Managed Cybersecurity Services | Georgia, Sep. 19, 2023. Available: <https://cybriant.com/antivirus-vs-edr/>
- [20] "What is Mobile Device Management (MDM)? | IBM." Available: <https://www.ibm.com/topics/mobile-device-management>
- [21] Pecb, "A Guide to the CISO Role in Information Security." Available: <https://pecb.com/article/a-guide-to-the-ciso-role-in-information-security>
- [22] "Information Security Policy | Unit." Available: <https://www.unit.co/docs/onboarding/information-security-policy/>
- [23] Complyon, "10 ways to ensure a successful policies and procedures strategy - Complyon," Complyon, Feb. 20, 2022. Available: <https://complyon.com/10-ways-to-ensure-a-successful-policies-and-procedures-strategy/>
- [24] "Data Compliance Standards: GDPR, HIPAA, PCI DSS, CCPA," Medium, Oct. 26, 2023. Available: <https://medium.com/@careertechnologymiraroad/data-compliance-standards-gdpr-hippa-pci-dss-ccpa-5fe4be3547d8#:~:text=Examples%20of%20data%20compliance%20standards,healthcare%20data%20privacy%20and%20security>
- [25] "The Data Protection Officer (DPO) Role Under the GDPR." Available: <https://www.itgovernance.co.uk/data-protection-officer-dpo-under-the-gdpr>
- [26] P. Expert, "Preparing for data protection audits: A compliance checklist," Pandectes, Apr. 11, 2023. Available: <https://pandectes.io/blog/preparing-for-data-protection-audits-a-compliance-checklist/#:~:text=Data%20protection%20audits%20are%20assessments%20performed%20to,o,data%20protection%20measures%2C%20ensure%20that%20personal%20data>
- [27] "ISO 27001 vs. NIST Cybersecurity Framework," Blog | OneTrust. Available: <https://www.onetrust.com/blog/iso-27001-vs-nist-cybersecurity-framework/>

[28] “The Importance of Regular Security Audits and Assessments in IT,” May 14, 2024. Available: <https://www.linkedin.com/pulse/importance-regular-security-audits-assessments-computerbusiness-xtxhe/>

[29] M. Flinders and M. Flinders, “Contingency plan examples: A step-by-step guide to help your business prepare for the unexpected,” IBM Blog, Jul. 31, 2023. Available: <https://www.ibm.com/blog/contingency-plan-examples/>

[30] W. Stallings, “2.3 Security Governance Components | Understanding Information Security Governance | InformIT.” Available: <https://www.informit.com/articles/article.aspx?p=2931571&seqNum=3>

[31] “Responding to and mitigating security risks - UK Government Security.” Available: <https://www.security.gov.uk/guidance/secure-by-design/activities/mitigating-security-risks>

[32] P. Schnackenburg, “How to Mitigate IT Security Risks: Best Practices for Effective Risk Management,” Hornetsecurity, Apr. 18, 2024. Available: <https://www.hornetsecurity.com/en/security-awareness/it-security-risk-management/>