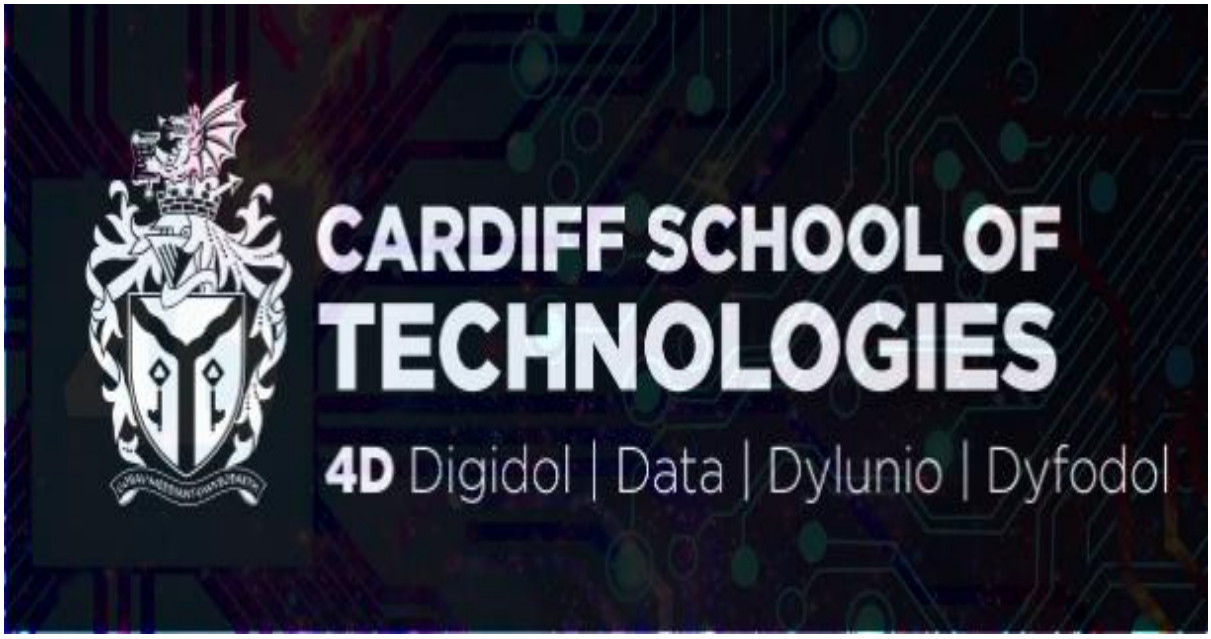

Cardiff Metropolitan University	
Cardiff School of Technologies	
Academic Year: 2022/2023	
Term: 2	
Module Name: Information Security	
Module Code: CIS7028	
Module Leader: Dr. Liqaa Nawaf	
MSc Programme: Data Science	
Assignment Title: Information Security Final Assessment	
Student Name: Derek Ahamioje	**Student ID:** ST20251371
Feedback:	
Signature:	**Date: 01/05/2023**

Contents

Introduction 2
Task 1 2
Task 2 7
Task 2.1 7
Task 2.2 10
Task 3 15
Task 3.1 15
Task 3.2 16
References 18

INTRODUCTION

This information security final assessment is centred around four main tasks. While task 1 is a report that reflects on one of the recent Cyber-attacks recorded, and the lessons to learn from the attack based on vulnerability and possible ways of preventing such an attack, Task 2 and 3 is a report that captures my advisory role as a cyber security consultant.

TASK ONE

THE NVIDIA 2022 CYBER ATTACK

1.0 INTRODUCTION

Founded in 1993 and incorporated in Delaware, Nvidia Corporation is a multinational American technology business. Located in the United States city of California, Nvidia Corporation is notable in the tech industry, for manufacturing integrated circuits, that are useful in several electronic devices, such as personal computers, etc. Nvidia Corporation is a foremost producer of premium graphics processing units (GPUs). On February 23rd, 2022, Nvidia Corporation experienced what could be described as its second and most disastrous cyber-attack, that threatened the existence of the company. This attack came from a criminal gang known as the Lapsus$ group. They had claimed responsibility for the attack shortly after the attack and presented their demands as conditions to avoid further leaking the highly confidential data harvested from the attack. According to wccftech an online tech website, the hackers took possession of over 1 TB of proprietary data belonging to the tech company (WCCFTECH 2022).

Unlike the popular practice in such attacks, the Lapsus$ group did not demand a ransom of money, but rather their demands were,

1. The lapsus$ group had requested from Nvidia, that the lite hash rate feature it had earlier introduced in its RTX 30 series graphic cards be removed. The lite hash rate feature aimed at limiting mining capabilities for Ethereum cryptocurrency, which was observed to be fast depleted in the previous year 2021 (SecureWorld, 2023).
2. The second demand from the Lapsus$ group, was that the graphic processing unit (GPU) giant should open-source its GPU drivers for devices using specified operating systems. These devices are, MacOS, Windows, and Linux devices.

1.1 LOSS SUFFERED BY NVIDIA CORPORATION FROM THE ATTACK.

According to a data breach monitoring website haveiBeenPwnd, in HIBP (2022), Nvidia suffered losses such as;

i. Email of seventy-one thousand, three hundred and thirty-five (71, 335) employees. What this means for Nvidia and its employees is.
   a) Private information can find its way to the hands of their competitors, which is a breach of the General Data Protection Regulation (GDPR) act that most importantly protects personally identifiable information (PII) which may be used to identify a particular individual. This has grave implications as data of over 70,000 employees that under the GDPR, Nvidia is supposed to secure has been let loose.
   b) Potential risk of exposing highly classified official documents that can undermine the market strength of Nvidia if these classified documents get into the hands of their competitors.

ii. **NTLM password hashes**. NTLM which stands for New Technology Lan Manager is a Microsoft Windows suite for authenticating users and protecting integrity and the confidentiality of their activities. It was reported that many of these passwords were cracked and circulated among the hacking community. The implication of this is that the integrity of their security certificates has been compromised. According to reports, the hackers took advantage of this is install malware such as backdoors and rootkits in the systems of unsuspecting product users while updating. The software or code injected by an intruder who gained access to a system is referred to as a backdoor or rootkit. A rootkit alters the operating system to create a backdoor, whereas a backdoor circumvents the standard authentication needed to access a system. The backdoor is then used by attackers to get remote access to the computer.

iii. **STOLEN SOURCE CODE:** To a company like Nvidia and other IT companies, source code is a treasure that keeps them running and unique. However, in this attack, the Lapsus$ group gained access to their source code, putting Nvidia at a disadvantage position. Close rivals can use these source codes to enhance their product to meet or exceed the quality of Nvidia products. Second, having these source codes in the hands of an untrusted group like the Lapsus$ can lead to a chain

of reactions by causing harm to organizations and machines across the entire globe, being a widely distributed product supplier, by signing and verifying stolen certificates, which is further presented to users as an authentic certificate.

1.2 VULNERABILITIES OF NVIDIA

i. The possible area of attack for Nvidia, that is, the major vulnerability exploited in Nvidia was email vulnerability. If there is a flaw in an email client, such a flaw is only exploited if a user downloads and opens a malicious attachment (Mell, Scarfone, and Romanosky, 2007). This can occur when an attacker creates an email that appears to be from a reputable source within the company and then attaches a malicious Word or other document file. The victim goes ahead to open the attachment simply because they trust the sender, which unintentionally leads to the download of ransomware onto their machine and the subsequent ransom demand for their files (Shah and Farik, 2017).

ii. Remote Code Executions is another vulnerability that the Lapsus$ group exploited and used against the Nvidia corporation in the attack. Using the rights of the person running the application, a cybercriminal might leverage this vulnerability to execute malicious code and take over the system.

1.3 MANIFESTATION OF THE ATTACK

The Lapsus$ attack was targeted primarily at the Nvidia corporation's official mailing server. This attack thereafter manifested in the form of a denial-of-service attack.

i. DENIAL OF SERVICE (DoS): According to Lau *et al*., 2000, an intentional attempt by an attacker to prohibit authorized users from using services is what is defined as denial of service. An attacker might try to "inundate" a network and so restrict the bandwidth of an authorized user, block access to a service, or interfere with service to a particular system or user. This was the exact case with the attack on Nvidia corporation, because of the stolen username and passwords, it was easier to make alterations to the services thereby denying the employees access to their accounts and creating limitations to mail correspondence to organizations and, machines that are making use of the services of Nvidia corporations with products. It was reported that the email services were down for two days.

1.4 TOOLS USED BY THE ATTACKERS.

They attacked the email server and installed malware in the Nvidia software distribution server.

i. EMAIL PHISHING: In the absence of receiving help from an insider, phishing which is defined by Subasi and Kremic, 2020 as mimicking the website of a respectable corporation seeking to collect user privacy information, is one likely tool that was used for the attack, since it was not however specified which tool was used, the manifestation of the attack which shows that the email server was compromised suggests that the malware have been installed unknowingly through phishing.

1.5 THREAT PREVENTION

In this session, we delve into best practices that can be used to prevent such attacks by organizations, which incorporates a standard Data Loss Prevention program. For this purpose of this attack, we will zero in on selected specific measures as it is captured in Tally *et al*., 2004 and Tasmin, Thomas, and Van Vleck (2022) includes.

i. **Policies:**

Establish corporate policies and inform employees of them: Establish company guidelines for email content to prevent legitimate emails from being mistaken for phishing. Let employees know about these policies and abide by them.

ii. **Awareness**

Give the staff members a mechanism to confirm the authenticity of the email: The worker ought to know how to tell the difference between an email that is coming from the organization and one from a phisher. To accomplish this, whoever is sending must create a policy requiring the inclusion of authentication data in each email sent to employees.

iii. **Governance:** Watch out for potential phishing websites on the Internet: Before the phishing emails are sent out, the phishing website typically appears somewhere on the Internet. These websites frequently use stolen business trademarks to look official. No matter the programming language or the origin of external input, it is best programming practise to approach any external input as hostile.

iv. **Defense:** Use effective content filtering, anti-spam, and anti-virus software at the Internet gateway: An additional line of defense against desktop anti-virus scanning is offered by gateway anti-virus scanning. At the gateway, filter, and block known

phishing websites. End users can avoid undesired spam and phishing emails with the use of gateway anti-spam screening. Maintain the most recent versions of all software, including operating systems and programmes, and do not ignore update notifications.

TASK TWO

2.1 ALTERNATIVE STANDARDS

With the technological advancement that is been experienced all over the world, and the continuous and increasing incorporation of technology and technological tools into the daily activities of businesses, either on a corporate level or personal/individual level, there is a growing need also for security measures to be in place to prevent, mitigate and manage risks and other hazards associated with the use of technology. In this wise, the knowledge, adoption, and implementation of the appropriate standard security standard are very important. The following underscores some notable standard alternative security policies outside ISO27001. These alternatives include cyber essential plus, COBIT, and NIST

1. **CYBER ESSENTIAL PLUS:**
   A simple yet effective government-sponsored programme called Cyber Essentials helps protect our organisation from the vast majority of the most frequent cyberattacks. It is a programme for safeguarding information administered by the National Cyber Security Centre (isms. online, 2023). Cyber-attacks happen in a wide variety of forms and sizes, but most of them are quite simple in nature and undertaken by people with little to no technical expertise. These basic unskilled practices can be likened to a scenario where a burglar is attempting to check the main entrance to the house to see if the door is not locked. These kinds of attacks are intended to be mitigated by Cyber Essentials. It is the United Kingdom government's effort to make the cyber internet space safer for businesses or organizations of any size and it addresses about 80% of the basic cyber security challenges (isms. online, 2023). The only additional feature incorporated into the Cyber Essential (Plus), is to allow for independent auditing.
2. **NIST**
   NIST, otherwise referred to as the National Institute of Standards and Technology, is part of the U.S. Department of Commerce. The Cybersecurity Framework, developed by NIST, assists companies of all sizes in analyzing, handling, and mitigating cybersecurity vulnerability while also securing their IT systems and data. The Framework is an optional one, that provides a summary of recommended practices for a company to use in deciding where to spend time and money when it comes to cybersecurity protection. The core of the NIST Cybersecurity Framework is on five key functions: Identify, Protect, Detect, Respond, and Recover (Figure 1). Using a

ranking scale of 0 – 4, a final number is obtained that establishes a minimum benchmark for the organization's level of risk maturity in each function (Strongdm, 2023).

Figure 1: NIST Cyber Security framework. (Source: ARI 2023)

3. COBIT

Known as COBIT, this acronym stands for Control Objectives for Information and Related Technology, which we might think of as a collection or blanket, with an emphasis on governance and information technology management. Along with discussing security within an organisation, COBIT also discusses how that organisation plans, arranges, and manages its IT operations. It comprises all controls, methods, and procedures related to information technology. An organisation benefits from aligning its own business projections with its IT ambitions. Additionally, it provides metrics and maturity models to assess the success of an organisation. It also aids in identifying the IT process managers and the organization's primary business responsibilities (Advisera, 2022).

Its benefits include,

i. Improve and maintain high-quality information to support business decisions.
ii. Use IT effectively to achieve business goals.
iii. Use technology to promote operational excellence.
iv. Ensure IT risk is managed effectively.
v. Ensure organizations realize the value of their investments in IT; and
vi. Achieve compliance with laws, regulations, and contractual agreements.

4. ISO27001 AND ITS BENEFITS TO THE ORGANIZATION

However, haven reviewed other alternative cyber security frameworks, it is therefore important to underscore the benefits of ISO27001 over the aforementioned frameworks. An information security management system must be established, put into place, maintained, and improved on a regular basis, according to the ISO27001 standard. The benefits this will have for this organization are.

i. ISO27001 requires certification, which can only be issued after the organization has gone through the two major stages of auditing, which is carried out to ensure that the information security management system uses a risk management method to safeguard the confidentiality, integrity, and availability of information and give people and organisations the confidence that risks are managed properly. (ISO/IEC 27001:2013).
ii. ISO27001 implementation will help this organization to avoid expensive penalties that are associated with non-compliance with such requirements as the General Data Protection Regulation (GDPR)
iii. The implementation of ISO27001, will aid in securing the organization's information assets by putting in place suitable and pertinent security procedures, against security threats.
iv. The implementation of ISO27001 is a demonstration that this organization takes data protection seriously, making the organization better and as such increasing its credibility.
v. Provides the organization with the platform to achieve a market advantage.
vi. Improving risk management by ensuring adequate protection for property rights, client details, etc across the entire security framework.

TASK 2.2

2.2.1 MAIN CLAUSES THAT NEED TO BE IMPLEMENTED UNDER ISO27001.

It is worth establishing that according to the scope of implementation of ISO27001 for an information security management system, The general guidelines in the standards are meant to be used for all organizations irrespective of the type of organization, its size, or nature, and therefore it is expected that every organization should implement the requirements specified in clauses 4 to 10 in conformity with the international standard.

The seven main clauses are summarised as follows (Scott, 2022),

1. **Clause 4: Context of the organization.** This includes sub-clauses like understanding the organization and its context, understanding the needs and expectations of interested parties, and determining the scope of the information system.
2. **Clause 5: Leadership**

   With sub-clauses like, Organisational roles, responsibilities, and authorities, together with leadership and dedication.
3. **Clause 6: Planning**

   The formulation of information security objectives and plans to attain them, as well as actions to address risks and opportunities (such as general, information security risk assessment, and information security risk treatment).
4. **Clause 7: Support**

   Including determining and providing resources for ISO27001, Competence Knowledge, communication, and information that is documented (including General Documentation, creating and updating, and control of documented information)
5. **Clause 8: Operation**

   Including its sub-clauses; Information security risk assessment, operational planning, and control, as well as information security risk management.
6. **Clause 9: Performance evaluation**

   Including its sub-clauses: Monitoring, evaluating, analysing, conducting an internal audit, and conducting a management review.
7. **Clause 10: Improvement**

   Including sub-clauses; Nonconformity and Corrective activity as well as continued growth.

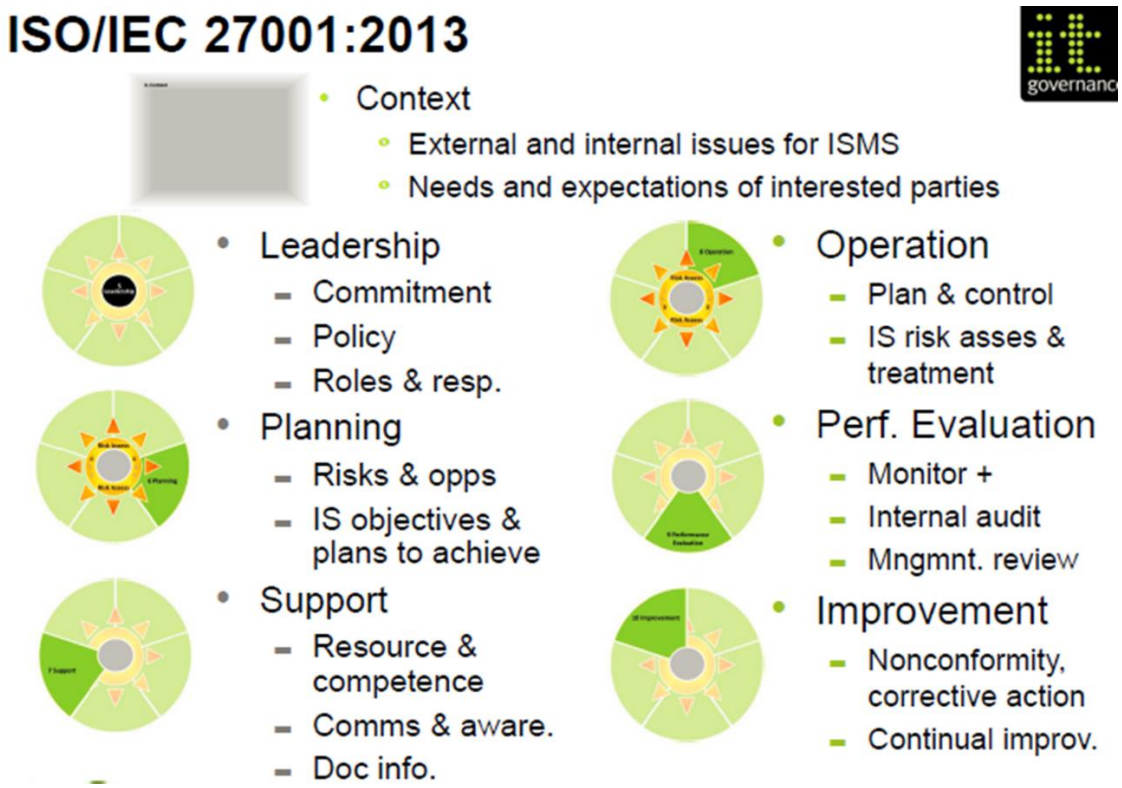

Figure 2: Clauses of ISO27001 (source: IT governance, 2023)

2.2.2 SECURITY CONTROL OBJECTIVES APPLICABLE TO THE CHOSEN COMPANY

Now to establish some sets of security control objectives that will become a guide when evaluating the security measures put in place in the organization, the following standard information security objectives will be established at relevant functions and levels of operations. These standard objectives otherwise called the CIA triads are;

1. **Confidentiality**

   The confidentiality objective of the information security management system (ISMS) is putting all necessary measures in place to make sure that data within the system can only be accessed by relevant and authorized people. This will also comply with the GDPR and the principles of data protection, which puts into consideration, the rights of people.

   i. Provide a secure, reliable cloud stack storage organization-wide.
   ii. To guarantee that information is protected to a sufficient degree.
   iii. Ensuring the orderly exit or change of employment of workers, independent contractors, and third-party users.

2. **Integrity**

   The next key objective is aimed at keeping data accurate and complete at all times, by:

   i. Implementing digital signature.
   ii. Granting permission to third parties while providing assurance that the platform is suitable for handling sensitive data.
   iii. Maintaining proper filing

3. **Availability**

   i. to achieve and maintain adequate asset protection for the organisation.
   ii. Create multiple source data.
   iii. Implement an automated failover.

2.2.3 AUDITING AND CERTIFICATION PROCESS OF ISO27001

As part of its performance evaluation, which will help to identify the information security management systems weaknesses and identify opportunities for continuous improvement, this organisation shall routinely conduct the internal auditing of its information management system to check the level of compliance with the implemented clauses and set control objectives. However, since it is impracticable to monitor everything all the time and based on the security control objectives described in task 2.2.2, The auditing shall be conducted in two stages in compliance with ISO270001.

STAGE ONE AUDIT: INTERNAL AUDIT

1. The Organisation shall set up an internal auditing mechanism for evaluating all documentation regarding the set objectives for the ISMS. The organisation through its Management shall, therefore:

   a) An audit programme must be planned, established, put into action, and maintained, including the frequency, procedures, roles, planning needs, and reporting. The audit programme must take into account the significance of the involved procedures and the findings of earlier audits.
   b) The criteria to be used for the audit shall be clearly defined and the scope equally specified.
   c) Objectivity, sincerity, and impartiality in the conduct of the audit shall be core qualities for choosing auditors for this task.

2. The core responsibility of the internal audit will be conducted under for main clauses, which is

   a) To assess the conformity of the system to
      i. The organization's information security management system requirements; and
      ii. The requirements of ISO27001.
   b) To assess how well the information security management system has been implemented and preserved.
   c) Make sure that the appropriate management receives a report on the audit results; and
   d) As proof of the audit programme and the audit findings, keep all documentation.

STAGE TWO AUDIT: EXTERNAL AUDIT

The date shall be specified for standard auditing by certification by ISO27001.

1. The documentation from the internal audits shall be reviewed.

2. The processes and infrastructures shall be physically accessed for compliance.

TASK THREE

3.1 DATA PROTECTION BY DESIGN AND DEFAULT IMPLEMENTATION POLICY FOR FINTECH GLOBAL RECRUITMENT AGENCY

As part of the UK general data protection regulation (GDPR) framework, and in compliance with the principles of this policy framework, FinTech Global Recruitment Agency as an organisation within the jurisdiction of GDPR is expected to integrate data protection into all aspects of its processing activities (ICO, 2023), which is otherwise referred to as data protection by design and default. In this brief report, are outlined, action steps, Fintech Global Recruitment Agencies need to implement in compliance with the policy;

A. DATA PROTECTION BY DESIGN

At the design stage of the ISMS, we shall,

i. Take data protection concerns into consideration while designing and putting systems, services, products, and business procedures into place.
ii. Ensure that our processing systems and services are designed with data protection as a fundamental component of their primary functionality.
iii. To help us adhere to our data protection by design commitments, we deploy privacy-enhancing technologies (PETs).
iv. For people to maintain their privacy, we make sure that personal data is automatically protected in all IT systems, services, products, and/or business practises.

B. DATA PROTECTION BY DEFAULT

With respect to fundamental data protection principles of data minimisation and purpose limitation.

i. We only process the personal data necessary to fulfil the purpose(s) for which we collected it.
ii. For all public documents, we adhere to a "plain language" approach to allow people to understand easily, how we are using their personal information.
iii. We give people the means to determine how we use their personal information and whether our rules are being followed.

3.2 **MECHANISMS FOR IMPLEMENTING DATA PROTECTION BY DESIGN AND DEFAULT**

1. DATA DISCOVERY

As a part of the Data Loss Protection mechanism, the first step of protection is Data Discovery otherwise known as data audit. Protecting data using this mechanism requires that an inventory of all the data to be handled or handled by the agency is duly identified, collated, categorised. The data audit provides answers to the three questions:

i. What: All the personal data that are processed by the agency
ii. Why: The purpose for holding this data must be clear and well-defined so that the agency can avoid the cost of holding unnecessary data and focus more on the required data.
iii. How: How we use and store the data

2. DATA CLASSIFICATION

Classification of Data is another key component of the Data Loss Protection program, that this organisation must implement. It is aimed at organising data into groups based on the risk involved with handling the respective groups. The General Data Protection Regulation states that there are four main classifications that should hold. They are:

i. Confidential data – Data that should be exclusively available to management only.
ii. Restricted data – Data available to specific line staff
iii. Internal data – Data accessible by all employees.
iv. Public data. – Data accessible by the general public.

3. DATA LOSS PREVENTION (DLP) MECHANISMS

Reducing data leaks should be paramount in Fintech Global Recruitment Agency and as such, needs to employ measures to reduce the risk of loss of data before it occurs. The security program that detects risks in a timely manner is called Data Loss Prevention. The prevention is handled by monitoring data at its three states:

i. **Data at rest -** Any data that is currently in the storage and not currently accessed is classified in this state. E.g., vital documents stored in a hard drive. Measures like encryption, multifactor authentication, and secure server room will help to prevent such data loss.

ii. **Data in use** – The category of data that is being updated, or processed is described as in 'Data in use' state.

iii. **Data in motion** – This refers to data that is being transferred from one location to another whether within the same system or outside the system, from one folder to another, prepared for updates, emails, etc. Encryption is a key preventive measure here.

4. DATA PROCESSING IMPACT ASSESSMENT (DPIA)

As an organisation that processes sensitive data about people that pose a high risk, it is mandatory to conduct DPIA which is a policy requirement for the implementation of GDPR that helps to identify and minimise high risk while processing data. This can be done through systematic monitoring of employees' activities. The Data Controller is responsible for the full conduct of this measure at the early stage before the actual system design begins.

5. PRIVACY ENHANCING TECHNOLOGIES (PETS).

As much as it is possible, the more data we handle the more risk we bear, therefore, to be on the safe side, Fintech Global recruitment agency will need to

REFERENCES

Advisera 2022, *ISO 27001 vs. COBIT: A comparison*, Viewed: 25th April 2023, <https://advisera.com/27001academy/blog/2019/05/06/cobit-vs-iso-27001-how-much-do-they-differ/#:~:text=Key%20difference%20between%20COBIT%20and,of%20information%20technology%20business%20processes.>

ARI 2023, The experimental SIEM, Accessed 25th April 2023, <https://booklet.atosresearch.eu/xl-siem>, Atos Research & Innovation

Cathcart Standard 2021, *AGM AND COMMITTEE,* Viewed 25th April 2023, <https://www.cathcartha.co.uk/sites/default/files/Cathcart%20Standard%20Issue%2042.pdf>

HIBP 2022, *NVIDIA*, viewed 24 April 2023, https://haveibeenpwned.com/PwnedWebsites#NVIDIA.

ICO 2023, Data Protection By Design And Default, Viewed 27th April 2023, <https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/accountability-and-governance/data-protection-by-design-and-default/#:~:text=Data%20protection%20by%20default%20requires,achieve%20your%20purpose(s)>

ISO/IEC 27001:2013, *Information technology, Security techniques, Information security management systems Requirements.*

Isms.online 2023, *Cyber Essentials (Plus) Schemes and Certification Simplified* Viewed: 25th <April 2023, https://www.isms.online/cyber-essentials/>

IT GOVERNANCE 2023, *what is COBIT5, Definition and Explanation,* Viewed 25th April 2023, <https://www.itgovernance.co.uk/cobit>

Lau, F., Rubin, S.H., Smith, M.H. and Trajkovic, L., 2000, October. Distributed denial of service attacks. In Smc 2000 conference proceedings. 2000 IEEE international conference on Systems, Man, and Cybernetics.' Cybernetics evolving to systems, humans, organizations, and their complex interactions'(cat. no. 0 (Vol. 3, pp. 2275-2280). IEEE.

Mell, P., Scarfone, K. and Romanosky, S., 2007, June. A complete guide to the common vulnerability scoring system version 2.0. *In Published by FIRST-forum of incident response and security teams* (Vol. 1, p. 23).

Scott R. Mix, 2022, *Business Continuity, Cybersecurity, and Backup Control Center Standards, References, and Recommendations White Paper*, Viewed 25th April 2023, < https://www.pnnl.gov/main/publications/external/technical_reports/PNNL-32686.pdf?cv=1 > Pacific Northwest National Laboratory

Secureworld 2022, *Hackers Threaten to Release Nvidia Source Code After Breach*, viewed 29 March 2023, https://www.secureworld.io/industry-news/nvidia-source-code-breach

Shah, N. and Farik, M., 2017. Ransomware-Threats Vulnerabilities and Recommendations. *International Journal of Scientific & Technology Research*, *6*(06), pp.307-309.

Strongdm 2023, *NIST vs. ISO: Understanding the Difference*, Viewed 25th April 2023 <https://www.strongdm.com/blog/nist-vs-iso#:~:text=NIST%20CSF%20is%20free%20of,re%20able%20to%20do%20so.>

Subasi, A. and Kremic, E., 2020. Comparison of AdaBoost with multiboosting for phishing website detection. *Procedia Computer Science*, 168, pp.272-278.

Tally, G., Thomas, R. and Van Vleck, T., 2004. Anti-phishing: Best practices for institutions and consumers. *McAfee Research*, Mar.

Tasmin, S., Sarmin, A.K., Shalehin, M. and Haque, A.B., 2022. Combating the Phishing Attacks: Recent Trends and Future Challenges. Advanced Practical Approaches to Web Mining Techniques and Application, pp.106-137.

WCCFTECH 2022, *NVIDIA Fires Back at Hackers By Encrypting 1 TB Stolen Data & Successfully Ransomed Their Systems*, viewed 25 April 2023, <https://wccftech.com/nvidia-fires-back-at-hackers-by-encrypting-1-tb-stolen-data-successfully-ransomed-their-systems/. >