**Northumbria University, Newcastle**

**Faculty of Engineering and Environment**

**Department of Computer and Information Sciences**

**LD7087 Information Governance and Cyber Security**

**Individual Assignment (Tasks 1, 2, 3)**

**Submitted By**

|  |  |
| --- | --- |
| **Name:** | **Busra Ecem Sakar** |
| **ID:** | **22065255** |
| **Programme:** | **MSc Big Data and Data Science Technology** |
| **Semester:** | **1** |
| **Group:** | **1** |
| **Assignment Group:** | **G** |
| **Tutor:** | **Prof. Karim Mohammed Rezaul** |
| **Date:** | **11/01/2023** |
| **Word Count:** | **2592 (Include content and references)** |

**Table of Contents**

[**1.** **Task 1: Information Governance Need & Cyber Security Threats** 2](#_Toc124216459)

[**1.1.** **Information Governance** 2](#_Toc124216460)

[**1.1.1 Information Governance: Why Is It Important?** 2](#_Toc124216461)

[**1.1.2 The Goals of Information Governance** 3](#_Toc124216462)

[**1.1.3 Information Governance Requirements Within the Provided Scenario (247E&G)** 3](#_Toc124216463)

[**2. Task 2: Framework** 4](#_Toc124216464)

[**2.1 Information Governance Frameworks** 4](#_Toc124216465)

[**2.2 Information Governance Framework Components** 5](#_Toc124216466)

[**2.3 GDPR and ISO27001 for 247E&G’s Framework** 7](#_Toc124216467)

[**Task 3: Risk Assessment** 8](#_Toc124216468)

[**3.1** **Information Security** 8](#_Toc124216469)

[**3.2** **Information Security Risk Assessment** 8](#_Toc124216470)

[**3.3 Information Security Incidents** 9](#_Toc124216471)

[**4.** **Part B: Group Task** 10](#_Toc124216472)

[**Reference** 11](#_Toc124216473)

**Figures:**

[**Figure 1. Information Governence Framework Components (Dwyer, Linton, 2013)** 6](#_Toc124215342)

[**Figure 2. Information Security Risk Assessment (ISRA) methodologies are categorised (Shameli-Sendi, et all, 2016)** 10](#_Toc124215343)

# **Task 1: Information Governance Need & Cyber Security Threats**

## **Information Governance**

Businesses have the enormous burden of reducing risk and generating profit across ever-growing data collections. The capacity to manage and govern that data to derive crucial insights is a major business differentiator and gives organisations a competitive advantage over the industry in the current era of information overload caused by a massive surge in business data quantities and velocity (Smallwood, 2016). Due to increased regulation, and new security risks like hacking, and data breaches, the discipline of information governance has evolved to address the issues of current information management in a regulated and litigious business context. Records management, data privacy, content management, IT and data governance, information security, data privacy, risk management, litigation readiness, regulatory compliance, and business intelligence are just a few of the fundamental principles that make up information governance (Smallwood, 2016).

By adopting procedures, roles, checks, and measurements that view information, information governance takes a comprehensive approach to managing corporate information. Information governance, according to Smallwood (2016), is "the activities and technology that businesses use to maximise the value of their information while reducing associated risks and costs.

### **1.1.1 Information Governance: Why Is It Important?**

The underlying principles of traditional data and big data are the same, but big data's volume, velocity, and variety can exponentially increase risks and make the processes and technology needed to extract the most value more difficult. Information governance offers methods to optimise value, reduce risk, and achieve these goals.

Willis (Willis, 2005) claims that good information and records management meets the following six essential criteria for effective corporate governance.

1. Making things transparent so they may be properly scrutinised

2. Accountability - Being held responsible for one's actions.

3. Due process - The procedure of carrying out actions in a predetermined, recorded, and controlled manner.

4. Compliance - Ensuring that procedures are followed correctly and in accordance with laws.

5. Fulfilling statutory and common law obligations - Making sure that the relevant legal obligations are fulfilled.

6. Personal and business information security - Ensuring the safety of data in systems.

### **1.1.2 The Goals of Information Governance**

Making information a credible, shared resource for decision-making is the core objective of information governance. Processes, roles, rules, standards, and other measures that guarantee the efficient use of information are included in order for a company to accomplish its goals as The data is seen as a resource for the business (Akoka, Comyn-Wattiau, 2019).

The purposes of Information governance are (Hulme, (2012)

- Provides reliable information to help people gain more understanding and make decisions that are better in line with their company's objectives.

- By automating Information Governance methods, wasteful time and money associated with managing information can be eliminated.

- Throughout the lifecycle of the information, makes sure it is cost-effective, high-quality, and safeguarded across your IT ecosystem.

- Aligns information with business needs so that the company receives the information it requires at the precise time it requires it.

- Assures adherence to corporate, industry, and legal mandates.

### **1.1.3 Information Governance Requirements Within the Provided Scenario (247E&G)**

Every institution and organisation must therefore take great care to safeguard, conceal, and keep information. In order to reap the rewards of investments and opportunities that result from these investments to the fullest extent, information security must be ensured. In order to assure continuity and reduce financial losses, the idea of information security protection has emerged. Valuable information and assets can be handled and secured by looking at ISO 27001 Information Security Management System standards. While implementing ISMS standarts, these steps can be followed;

*1. Make an ISMS policy, first.*

The major reason for creating an ISMS is stated.

The objectives that we hope to accomplish are listed.

It is believed that the information security officer (ISO) will play a role in the organisational implementation of a system.

Take the necessary action.

*2. List and categorise assets.*

Information that has to be protected, including the kind of assets and information it contains, is identified.

For example, the credit card number of clients has to be protected against theft. This information is too sensitive than a client's electric id number.

*3. Create organisational and risk management frameworks for ISMS.*

*4. Create control strategies.*

*5. Run the ISMS.*

*6. Verify the KPIs and results.*

*7. Correct errors and exercise prudence.*

*8. A management review.*

# **2. Task 2: Framework**

## **2.1 Information Governance Frameworks**

Information security must be integrated into a framework for IT governance, risk management, and must span the entire company because it addresses concerns with people and processes in addition to technology. Information technologies offer many chances for businesses to improve their products, services, markets, labour processes, and commercial relationships as the world's markets grow and businesses become more competitive.

The principles that make it possible to create and maintain information security, such as an information security policy, risk analyses, technical controls, and information security awareness, are known as information security components. These elements can be included in an information security governance framework that shows how the elements relate to one another (Da Veiga, Martins, and Eloff, 2007).

First, ISO 27001 might be considered the industry benchmark for information security management systems in the given scenario. The other frameworks are shown at below;

*Cyber Essentials Scheme*; a successful government-backed programme that aids in defending your organisation against a variety of the most frequent cyber-attacks.

*The NIST Standard*; NIST recommendations include a list of guidelines for suggested security measures for information systems at federal agencies.

*GDPR (General Data Protection Regulation);* is the law that controls how personal data about individuals is processed.

## **2.2 Information Governance Framework Components**

Leadership supports and takes action in support of governance frameworks that actively recognise and safeguard the organization's information assets. Six essential elements go into building and maintaining an information asset governance framework that is shown Figure1. (Dwyer, Linton, 2013);

* Strategy
* Policy
* Systems
* Support
* Quality assurance
* Continuous improvement



**Figure 1. Information Governence Framework Components (Dwyer, Linton, 2013)**

***Strategy:*** An information strategy outlines a comprehensive approach to how information will support an organization's goals, lower risk and expense, and boost efficiency and compliance.

***Policy:*** Policies are crucial for outlining an organization's information and data protection guidelines for how information is gathered, processed, kept, shared, and finally deleted.

***Systems:*** Systems should be chosen based on their usability and functionality. In order to boost productivity, provide better internal and external services, and lower risk in accordance with both the organisation plan and the information management strategy.

***Support:*** An important component of a governance structure is support. Building a governance framework with formal controls over strategy, rules, processes, and systems is insufficient if you want it to be used.

***Quality assurance:*** An information governance system should not confine its understanding of quality assurance to the collection of records and their accurate naming or to the integrity of structured data. It must also establish procedures to record how effectively information assets are being managed.

***Continuous improvement:*** Every year and every three years, or more frequently in rapidly changing contexts, strategy should be examined and altered.

## **2.3 GDPR and ISO27001 for 247E&G’s Framework**

Considering the diversity and importance of data that Company 247E&G will produce in its web-based development, one of the harshest and broadest data protection regulations in the world is the General Data Protection Regulation is chosen.

The General Data Protection Regulation was created and authored by the European Union and released in May 2018. (EU). However, if foreign organisations dealing with data subjects situated in EU member states are located elsewhere in the globe, GDPR compliance applies to them (Goddard, 2017)

The international framework for information security management is represented by the ISO 27001 standard. The three "pillars" of effective information security that ISO 27001 identifies are people, procedures, and technology (Irwin, 2018).

In the given scenario, ISO 27001 should be followed because the following benefits to enterprises come from implementing an ISO/IEC 27001 information security management system:

• It makes it possible to find and remove risks and weaknesses;

• It offers all stakeholders (customers, partners, and others) security and trust;

• It increases sensitivity to security;

• It improves one's ability to anticipate, control, and endure a tragedy;

• It increases understanding of the organization's operations, resources, and liabilities;

• It guarantees business continuity; • It gives the organisation genuine awareness of the risk it confronts;

• It aids in the enhancement of procedures and services while lowering costs;

• It guarantees adherence to the rules of the law;

• It lowers expenses related to "non-security"

Organizations that have achieved certification to the Standard are already halfway to GDPR compliance because of the parallels between the ISO 27001 framework and the Regulation's obligations (Irwin, 2018).

How GDPR regulations can be met with ISO 27001 (Dattani, 2019):

1 - Assurance: To give the necessary assurance that the firm is successfully managing its information security risks

2 - Not just personal information: ISO 27001 adheres to global best practises and will assist businesses in putting processes in place that protect all information assets.

3 - Controls and security framework: Mandates that enterprises choose the right organisational and technical controls to reduce the risks that have been identified.

4 - People, Processes, and Technology: companies can safeguard their operations against not only technological risks but also other, employees and inefficient procedures.

5 - Accountability: Top leadership must back security policies and incorporate them into the organization's culture and strategy.

6 - Risk assessments: Find risks and weaknesses that could impact an organization's information assets and to take precautions to safeguard that data.

7 - Continuous improvement: Businesses must continuously monitor, update, and review their ISMS, which means it must change as their business does through a process of continuous improvement.

8 - Testing and audits: A company must conduct frequent testing and audits in order to be GDPR compliant.

9 - Certification: Businesses must take the required actions to ensure that the security controls operate as intended.

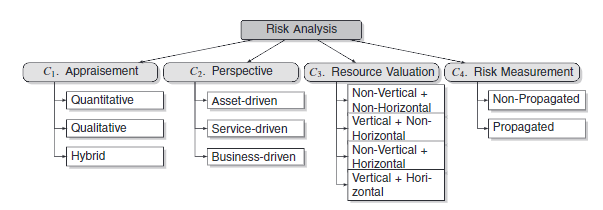
# **Task 3: Risk Assessment**

## **Information Security**

Confidentiality, information integrity, and information availability are the three components of information security (ISO 17799:2009). Integrity refers to the inability of data to be changed secretly. Availability presupposes that the data must be available to authorised users whenever and whenever they need it (Susanto, Almunawar, 2018)

## **Information Security Risk Assessment**

Risk analysis and risk assessment make up the two processes that make up the complex activity of risk management, which has as its goal the cost-effective protection of organisational assets (Karakaneva, Pavlov, 2001) Approaches to information security risk assessment is shown Figure 2.



**Figure 2. Information Security Risk Assessment (ISRA) methodologies are categorised (Shameli-Sendi, et all, 2016)**

***Appraisement;*** Three categories of information security risk assessment appraisals exist: Hybrid, Quantitative, or Qualitative.

The quantitative appraisal uses actual data, labor-intensive calculations, probability theory, and statistics to gauge how much a company is exposed to risk.

Quantitative appraisals is the drawn-out and time-consuming method that depends on comprehensive information. Implementing this strategy won't be simple due to firms' limited time, financial, and human resources (Hulitt, Vaughn, 2008).

Since they are much simpler to comprehend and utilise, qualitative appraisals are frequently used because there are frequently insufficient reliable historical data to calculate the impact and likelihood of occurrence of risk scenarios (Wheeler, 2011).

However, they are not sufficiently measurable to support management's cost-effective decision-making (Hulitt and Vaughn, 2008). Additionally, because they are reliant on the expertise and experience of those participating in the process (assessors and stakeholders), these appraisals are more arbitrary, subject to error, and less accurate than their quantitative equivalents (Wheeler, 2011).

## **3.3 Information Security Incidents**

There is a good chance that one or more unforeseen incidents will compromise corporate operations and jeopardise information security. For instance, service interruptions, device or equipment failures, system errors, human mistakes violations of the rules governing physical security, unchecked system changes, access violations, etc. are all examples of security incidents (Susanto, Almunawar, 2018).

***Threats***

A threat is a possible catalyst for an unwelcome event that could be detrimental to a system or organisation. In our scenario, for example, Malware, ransomware, phishing scams can be threats.

***Vulnerability***

A vulnerability is a flaw in one or more assets that allows a threat to attack them. In our scenario, these are should be;

*Broken Authentication*: User identities and sessions may be taken over if authentication credentials are stolen.

*SQL Injection*: a malicious code injection attempt to access database content.

*Cross-Site Scripting Attack*. Users are the subject of it, which exposes them to the risk of having their private information stolen.

*Cross-Site Request Forgery (CSRF*): A CSRF attack tries to persuade an authenticated user to take a step that they did not want to.

# **Part B: Group Task**

***Submitted on behalf of the group G***

# **Reference**

Akoka, J. and Comyn-Wattiau, I., 2019, July. Evaluation of Big Data Governance-Combining a Multi-Criteria Approach and Systems Theory. In *2019 IEEE World Congress on Services (SERVICES)* (Vol. 2642, pp. 398-399). IEEE.

Antoniou, G.S. (2018) “A framework for the governance of information security: Can it be used in an organization,” *SoutheastCon 2018* [Preprint]. Available at: https://doi.org/10.1109/secon.2018.8479032.

Da Veiga, A., Martins, N. and Eloff, J.H., 2007. Information security culture-validation of an assessment instrument. *Southern African Business Review*, 11(1), pp.147-166

Dattani Follow, I. (2017) *GDPR and ISO 27001 - how to be compliant*, *Share and Discover Knowledge on SlideShare*. Available at: https://www.slideshare.net/IleshDattani/gdpr-and-iso-27001-how-to-be-compliant (Accessed: January 1, 2023).

Dwyer, K. and Linton, M., 2013. Unlocking the value of information. *IQ: The RIMPA Quarterly Magazine*, 29(3), pp.19-23.

Goddard, M. (2017) “The EU general data protection regulation (GDPR): European regulation that has a global impact,” *International Journal of Market Research*, 59(6), pp. 703–705. Available at: https://doi.org/10.2501/ijmr-2017-050.

Hulitt, E. and Vaughn, R.B. (2008) “Information System Security Compliance to FISMA standard: A quantitative measure,” *2008 International Multiconference on Computer Science and Information Technology* [Preprint]. Available at: https://doi.org/10.1109/imcsit.2008.4747334.

Hulme, T. (2012) “Information governance: Sharing the IBM approach,” *Business Information Review*, 29(2), pp. 99–104. Available at: https://doi.org/10.1177/0266382112449221.

Irwin, L., 2018. How ISO 27001 can help you achive GDPR compliance. IT Governance.

Karakaneva, Y. and Pavlov, G. (2001) “Advanced Technologies for Defense Information System Support,” *Information & Security: An International Journal*, 6, pp. 122–131. Available at: https://doi.org/10.11610/isij.0610.

Shameli-Sendi, A., Aghababaei-Barzegar, R. and Cheriet, M. (2016) “Taxonomy of Information Security Risk Assessment (ISRA),” *Computers & Security*, 57, pp. 14–30. Available at: https://doi.org/10.1016/j.cose.2015.11.001.

Smallwood, R.F., 2016. *Information governance for executives: fundamentals and strategies*. Bacchus Books.

Susanto, H. and Almunawar, M.N. (2018) *Information Security Management Systems: A novel framework and software as a tool for compliance with information security standards*. Waretown, NJ, New York: Apple Academic Press.

Wheeler, E., 2011. *Security risk management: Building an information security risk management program from the Ground Up*. Elsevier.

Willis, A. (2005) “Corporate Governance and Management of Information and Records,” *Records Management Journal*, 15(2), pp. 86–97. Available at: <https://doi.org/10.1108/09565690510614238>.