



# **L7 - Data Security, Governance and Compliance (ACCA7028)**

By  
FATEMA NAMAZI

LECTURER: CARLENE CAMPBELL

ASSIGNMETN SUBMITTED AS PART OF THE REQUIREMENT FOR THE  
AWARD OF MSC IN COMPUTER NETWORKS AND CYBER SECURITY

JANUARY 2023

## INDEX

| Topic                                          | Page no. |
|------------------------------------------------|----------|
| Introduction                                   | 5        |
| Compliance (Laws and Ethics)                   | 6        |
| Governance and Strategic Planning for security | 7        |
| Information Security policies                  | 8        |
| Risk Management                                | 11       |
| Security Management Models and Practices       | 15       |
| Conclusion                                     | 19       |
| References                                     | 20       |

## LIST OF TABLES AND FIGURES

| Figures                                                                                                                                 | Pages no. |
|-----------------------------------------------------------------------------------------------------------------------------------------|-----------|
| Types of Data Security Issues                                                                                                           | 5         |
| Research Model                                                                                                                          | 6         |
| Information Security focus areas                                                                                                        | 8         |
| Maturity of ISP                                                                                                                         | 9         |
| An integrated Risk Management Approach                                                                                                  | 11        |
| Meta Model                                                                                                                              | 14        |
| Hierarchic design to increase compliance.                                                                                               | 16        |
| Goals, criteria/attributes and alternatives.                                                                                            | 17        |
| . External regulation vs Risks assessments to Increasing compliance                                                                     | 17        |
| Identification of applicable legislation and contractual requirements and Intellectual property rights from the Standards' perspective. | 17        |
| . Compliance with security policies and standards vs technical compliance review from the Internal regulation's perspective.            | 18        |
| Compliance with security policies and standards and the technical compliance review from the Risks assessments approach.                | 18        |

## LIST OF ACRONYMS

|       |                             |
|-------|-----------------------------|
| XSS   | Cross-site Scripting        |
| IPsec | Internet Protocol Security  |
| SSE   | server-side encryption      |
| TLS   | Transport Layer Security    |
| DES   | Data Encryption Standard    |
| WAP   | Web Application Protection  |
| DSA   | Digital Signature Algorithm |
| SCD   | Source Code Disclosure      |

## INTRODUCTION

CoffeeBlend is an internationally growing coffee selling company, with massive online and social presence. The company wants to establish their security policy as they are concerned about protecting their billions worth intellectual properties and want to ensure that the personal data of their staff and their clients is secure.

In order to help the company, meet their needs, research into various security framework or model is being conducted with the help of designing an approach for company's information system security, governance, and compliance.

According to National Institute of Standard and Technology (NIST), "Cloud computing is a framework for ubiquitous enabling, convenience, on-demand access to the network to a pool of computing configurable resources that are able to increasingly be released and provisioned with minimum management effort and or provided service interaction" [1]. It's one of the fastest technologies which are emerging in computing. Some of the advantages of cloud computing are accessibility, time management with geographic coverage, infrastructure with less investment, etc but with advantages there are also disadvantages such as lack of expertise and resources, data security etc [1].

In enterprise computing, the data is saved within their organisation, and is in the company's control whereas in cloud computing, the data isn't saved in the consumers place (its stored in the CSP). To ensure there are no data breaches due to security vulnerabilities, one must employ additional security measures [1]. There are six stages in the cycle of data's life, and they are: - Create, Use, Store, Archive, Share and destroy [1]. The assurance that a user cannot deny after performing a duty is nonrepudiation. Four major categories of data security issues are the following,

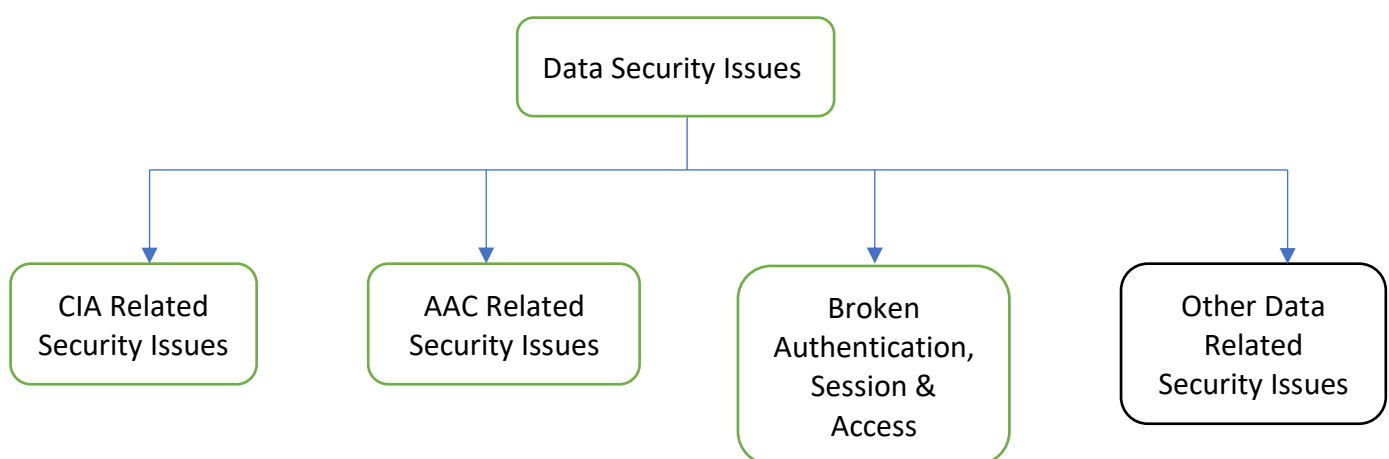


Fig. 1 Types of Data Security Issues

## COMPLIANCE (LAWS AND ETHICS)

For better understanding of the information security compliance in the organisations, here are some of the laws and ethics compliance. Structural equation modelling is used to fulfil this objective, for testing the relationships proposed in the model [2]. For testing the relationships between the unobserved constructs and measured variables, such a technique is used [2].

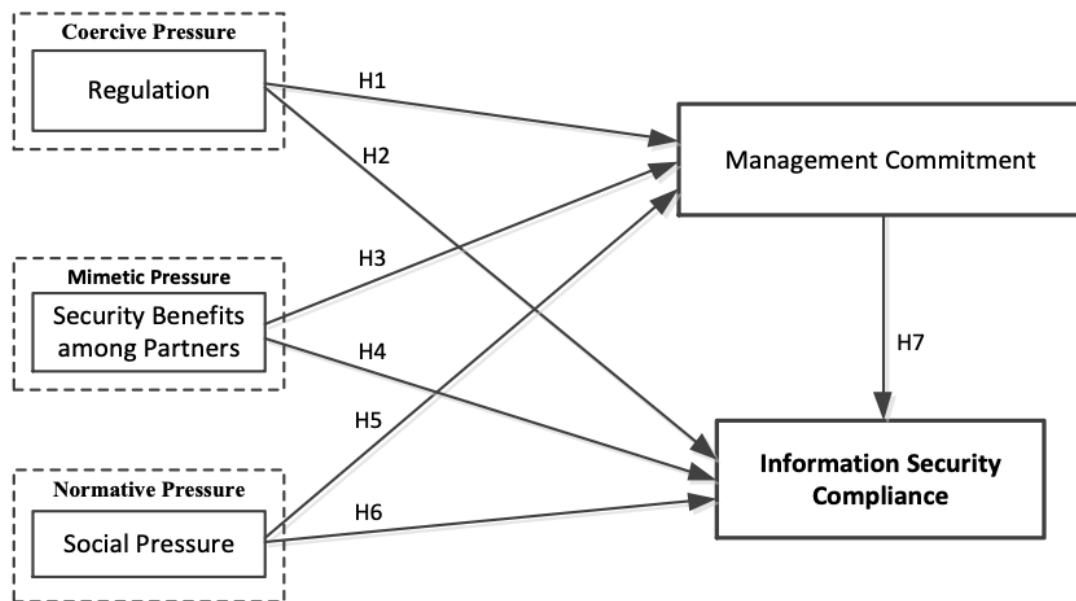


**Figure 1: A research model.**

Due to the potential for extending the theory development, the use of structural equation modelling is appropriate, and its capacity to assess simultaneously the interrelated and multiple depending on relationships [2]. In order to approach the structural equation modelling a two-step approach is used which is structural model and measurement model [2]. The structural model involves strength indicating the path coefficients and the paths sign between the variables [2]. On the other hand, the measurement model contains assessing the contribution of each indicator variable by conducting a confirmatory factor analysis (CFA) and for measurement model to measure the adequacy [2].

## GOVERNANCE AND STRATEGIC PLANNING FOR SECURITY

The following are the strategic and governance planning for security of the company.

### 1. Regulatory Compliance

Meeting the legal and mandatory requirements regarding the security and internal controls is known as regulatory compliance [3]. This helps in promoting the development in accordance with controls with legislation and formalizes the procedure of compliance [3]. This can help in improving the security governance by using the legislation as a catalyst.

### 2. Ensuring Continuous improvements in controls

Control implementation process instituting continuous improvements identifies as a primary objective for increasing security governance [3]. This process should be continuous, iterative, and adaptive for it to work effectively. It involves right controls in right place at the right time which can be achieved through implementing flexible practices.

### 3. Responsibility and accountability structures

Appropriate responsibilities sharing and accounting the stakeholders for their actions is defined and ensured by responsibility and accountability structures [3]. Its job is to make sure that clear organizational responsibilities for compliance are defined as in the appropriate accesses should be made responsible under certain individuals. While encouraging transparency about the accountability [3].

### 4. Corporate control strategy

The establishment of management plan of a corporate risk and controls using consensus of development guidelines is corporate control strategy. Cost of doing business should be viewed as controls [3]. It should be ensured that there is enough planning for the initiatives of governance and to make sure that the security controls is a non-negotiable budget item.

### 5. Control Conscious Culture

For maintaining, creating, and sustaining connections among different security efforts such as processes, policies, and norms it's fundamentally important to emphasize on control culture. To minimize the friction among groups over security issues it's important to promote "prevention mentality" by the control culture of the organization [3]. For the employees to carry out their security responsibilities it's essential to develop standard codes of conduct.

### 6. Clarity in policies and controls

In an organization all the policies should be visible, fair, and easily accessible. To prove the commitment to security governance it should be made sure that there is clarity in policies communicating management commitment [3].

## INFORMATION SECURITY POLICIES

By providing clear instruction of responsibilities in order to follow terms and conditions of policies, the Information Security Policy (ISP) helps the employees to support appropriate behaviour [4]. With the help of ISP there is a clear understanding and implementation of expectations of an organisation and proper implementation of ISP [4]. To define standards for periodic improvements, it's important to validate the strength, scope, and practical applications of ISPs, and to ensure that the policies are regularly examined and evaluated [4].

### Requirements of Information Security Policy

To improve Information Security programme a practical and clear information security programme can help organisations [4]. Any variances that may arise in IS assets should be addressed and observed by the organisation after developing and designing an ISP [4]. If the continuance alteration in organisational structure or procedures influences the effectiveness of its ISPs this can be determined by these intermittent observations which can help the organisation [4]. In terms of information security and safeguarding data, ISP compliance behaviour should not hinder an organisation. There are seven primary areas identified for testing and designing ISPs [4].

Table 1. Information Security Focus Areas.

| ISP focus areas                  | Sub-areas                                                                                                  |
|----------------------------------|------------------------------------------------------------------------------------------------------------|
| Password management              | Locking workstation<br>Password sharing<br>Choosing a good password                                        |
| Email use                        | Forwarding emails<br>Opening attachments<br>IT department's level of responsibility                        |
| Internet use                     | Installing unauthorised software<br>Accessing dubious websites<br>Inappropriate use of the Internet        |
| Social networking site (SNS) use | Amount of work time spent on SNS<br>Consequences of SNS                                                    |
| Mobile computing                 | Sending sensitive information via mobile networks<br>Checking work email via free networks                 |
| Information handling             | Disposing of sensitive documents<br>Inserting DVDs and USB devices<br>Leaving sensitive material unsecured |

### Review of Information Security Policy (ISP)

According to the research IS is based on the following:

1. Internet Use
2. Email Use
3. Mobile Computing
4. Password Management
5. Social Networking Site (SNS)
6. Information Handling.

Table 2. Maturity of ISP

| ISPs focus areas     | Sub-area                                          | Evaluation | Maturity      |
|----------------------|---------------------------------------------------|------------|---------------|
| Password management  | Locking workstation                               | 1          | Below average |
|                      | Password sharing                                  | 3          | Good          |
|                      | Choosing a good password                          | 3          | Good          |
| Email use            | Forwarding emails                                 | 0          | Poor          |
|                      | Opening attachments                               | 2          | Average       |
|                      | IT department level of responsibility             | 1          | Below average |
| Internet use         | Installing unauthorised software                  | 2          | Average       |
|                      | Accessing dubious websites                        | 0          | Poor          |
|                      | Inappropriate use of the Internet                 | 3          | Good          |
| SNS use              | Amount work time spent on SNS                     | 1          | Below average |
|                      | Consequences of SNS                               | 0          | Poor          |
| Mobile computing     | Sending sensitive information via mobile networks | 2          | Average       |
|                      | Checking work email via free networks             | 0          | Poor          |
| Information handling | Disposing of sensitive documents                  | 1          | Below average |
|                      | Inserting DVDs and USB devices                    | 0          | Poor          |
|                      | Leaving sensitive material unsecured              | 1          | Below average |

Note: 0 = nonexistence, 1 = existence, 2 = + acceptable use, 3 = ++ reporting procedure

## Password Management

The different steps users can follow to change their passwords, how the passwords are changed and password management, like regularly changing passwords, strong password selection and password prevention is explained by ISP with the users for better understanding [4]. ISP documentation, such as the acceptable use policy document, had in scattered other password management subareas, subarea for locking workstations, the review revealed that the current ISP at the institution [4].

## Email Use

Number of ISP documents are defined by the general responsibilities of IT department, however, to help users resolve issues such as fishing emails, there is a need to specify IT responsibilities relating to email use [4]. In any ISP document as the institutions, the issue of forwarding emails does not exist. The introduction of risks by security, such as loss of control over sensitive work-related information, is from the automatic forwarding of official emails from work mail servers to external account. Acceptable use documentation, along with other security issues is by the current ISP provides email issues [4].

## Internet Use

Inappropriate use of the internet, which includes use of institutional infrastructure and portals and discussion boards to further talk about sensitive non-work-related matters, should be avoided as advised in several ISP documents. The appropriate use of work portals and websites is discussed by an entire ISP document [4]. Moreover, the right to monitor users generated content to ensure internet use is in accordance with the ISP as stated by the institution [4]. To discuss work related matters, the use of other public websites or virtual communities is not mentioned by the institution [4]. Therefore, users are not permitted from downloading any software apart from licensed products made available in the central IT department portal, in some parts of the ISP [4].

## Social Networking Sites

A specific department to work on the institution's social media accounts for public relations purposes, is appointed using SNS receives minimal attention in the institution's ISP [4]. ISP should have the discussion regarding the appropriate use of these SNS, the consequences of use and potential security threats. The ISP also includes own social media application and specific policy document to outline the purpose of this application and steps practical for using it [4].

## Mobile Computing

The need to manage mobile work activities through secured devices and virtual networks is discussed in an ISP document named 'Access Police' [4]. Discussions in regard to the mobile international networks and Wi-Fi public networks are also to be included in the policy [4]. Among the types of activities which are allowed on the networks and whether it is safe to log onto work email through these networks [4].

## Information Handling

In the current ISP documents, there is minimal attention to information handling [4]. It's allowed after a specific amount of time to dispose work documentation and records as indicated by a short note found in an ISP document which is named as 'Commitment Policy'. Therefore, it is also noted that the same is written in the documents titled 'Leaving Sensitive Material Unsecured' and 'Access Police' [4]. Information handling policy suggests that there should be continual disposal of sensitive documents and users cleaning their systems [4].

## ISP Awareness and Compliance

It's the duty of the deputy managers or directors of each division to maintain the infrastructure of IT and to make sure that the quality of IT services is intact [4]. But a recent study found out that the distributed IT managers were not a part of the ISP development process because of the working culture centralised and the organisational current structure [4]. Therefore, this created a lack of awareness of the current ISP among the IT unit managers [4].

## RISK MANAGEMENT

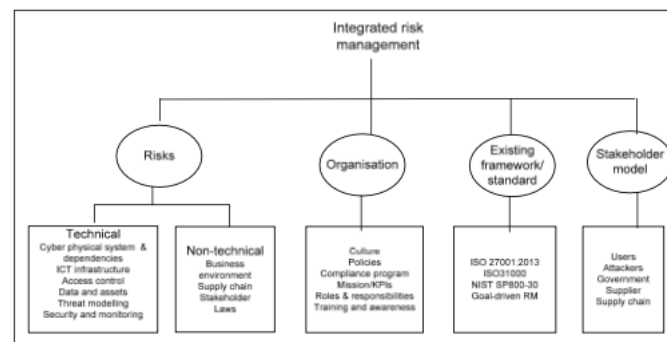


Figure 1. An integrated risk management approach.

### An integrated Risk Management Approach

For the benefit of a critical infrastructure organisation, the proposed scope of the integrated risk management approach is to manage, understand, monitor, and communicate the risks during the operations in the CPS [5]. For describing the properties necessary for cybersecurity risk management, it includes many concepts that serve as a common language. To systematically manage and assess risks proactively, these concepts help. Necessarily, in order to keep the risk level quantified for the suitable countermeasure, we consider assets and their criticalities, relevant vulnerabilities and threat to model the cybersecurity attack scenario [5]. The overview of the integrated risk management concepts of the proposed approach are the following: -

#### Modelling Concepts

The essentials to understand, manage and express cybersecurity risks are proposed in the approach of set of modelling concepts [5]. For the development of the cybersecurity risk management approach, there are a few concepts which are identified as necessary. Based on those concepts as in-depth exploration of several tools, methods, and techniques are used for risk management approach in the association. An overview of the concepts used are the following: -

1. Actor: An actor is a unit, generally can be seen as a system, an organisation, or a human user each with a particular tactical goal within its organisational setting and it carry out activates specific to generate cybersecurity risk management actions or receive the cybersecurity risk generated management actions by another [5] (101). To carry out various tasks to guide and lead in achieving its goals, this requires the organisation to appoint efficient actors [5]. These actors could be identified as government employees, stakeholders, IT providers, and utilities, consumers, employees, owners and operators, users, customers, and providers with skills within a location [5].

2. **Goals:** The overall objectives and aims of an actor who supports the continuity and interest of the business signifies as goals [5]. To support the organization there are expectations, including the KPIs of the organisation, security, and goals of the organisation. The allows the infrastructure critical organisational actors to take a particular decision about the continuity of organisation, which includes the availability, confidentiality, and integrity [5].
3. **Risks:** The possibility of an outcome unwanted as a result of an event, occurrence or an incident, determined by its associated consequences and its likelihood is defined as risk [5]. In a business the risk is inevitable, however, to ensure that the risks are kept to a minimum it's the role of the actors to ensure this in order to achieve goals. It is necessary to have a mitigation plan once the risks are identified or any other solution to counterattack the risks [5]. The potential consequences of the system are risks and possibly could compromise the security of the CPS and expectations of the actor. Security, technical, operational, nontechnical and governance or regulatory are a few parameters which be classified as CPS risk. The requirement of the appropriate assessment and the security of the CPS could be obstructed due to these risks [5]. Likelihood, impact, and residual analysis could be the basis of the risk assessment, which would help in identifying the risks needed to be controlled by the different following the control strategies [5].
4. **Assets:** The tangible or intangible entities are defined as assets which are important and have a value of importance to the organisation. Identification of key assets, and putting a value on each key asset, is an important process of risk management. These key assets could be people, services, facilities, processes, etc [5]. It is important to identify critical assets as well as estimate their critical failure modes or impact of the loss. An asset has two features: Category and Critically. Criticality is defined as a measure of the consequences associated with the degradation or loss of an asset. It is the major indicator used by organizations to determine which asset is of more value to the business continuity. Category classifies assets according to its level of sensitivity and security requirements [5]. The criticality of an asset category can be high, medium, or low, which means that assets with high rating are the most valuable to the organization.
5. **Controls:** The set of security protections or countermeasures to avoid or minimize security risks in CPS critical infrastructure are called controls [5] . Controls are also the mechanism used to provide security to the CPS, and they are characterized by combining technical and nontechnical controls which are used to deter anticipated and unanticipated threats from exploiting known vulnerabilities [5] . They also describe the vital components and actions taken to protect the assets. The overall

goal of risk assessment will be partly defeated if relevant controls are not applied [5].

6. Compliance Programs: These are sets of requirements designed to secure the CPS to operate without any form of disturbance [5] . Critical infrastructures are increasingly using compliance programs as a mechanism for demonstrating cybersecurity for CPS protection. The North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP) is a compliance program designed to secure the assets necessary for operating a bulk electric system [5] . In this case, the SCADA system of the CPS is an asset. Therefore, a significant sum of their budget and time is necessary to ensure security compliance with standards such as NERC CIP, NIST, NIPP, and other relevant standards [5].
7. Cyber-attack scenario: A cyber-attack scenario is an event that leads to a negative impact on the organization's assets when it occurs. There are some certain components that determine a cyber-attack on a CPS [5]. They include threat types, actor's skill, capability and location, assets, events, and time. With certain scenarios, the organization tends to think broadly by developing a range of possible outcomes to increase their readiness for a range of possibilities in the future [5] .
8. Policy: Policies are the principles of action adopted or proposed by an organization [5]. There are several security policies, such as access control and backup that are necessary to formulate and implement the CPS security program [5].
9. Threats and vulnerabilities: Vulnerability is the weakness in an organization security program that is exploited by a threat to gain unauthorized access to an asset [5] . It has three properties. i.e., impact, type, and weight score [5].

The Metamodel illustrated in Figure below shows the relationship between the concepts

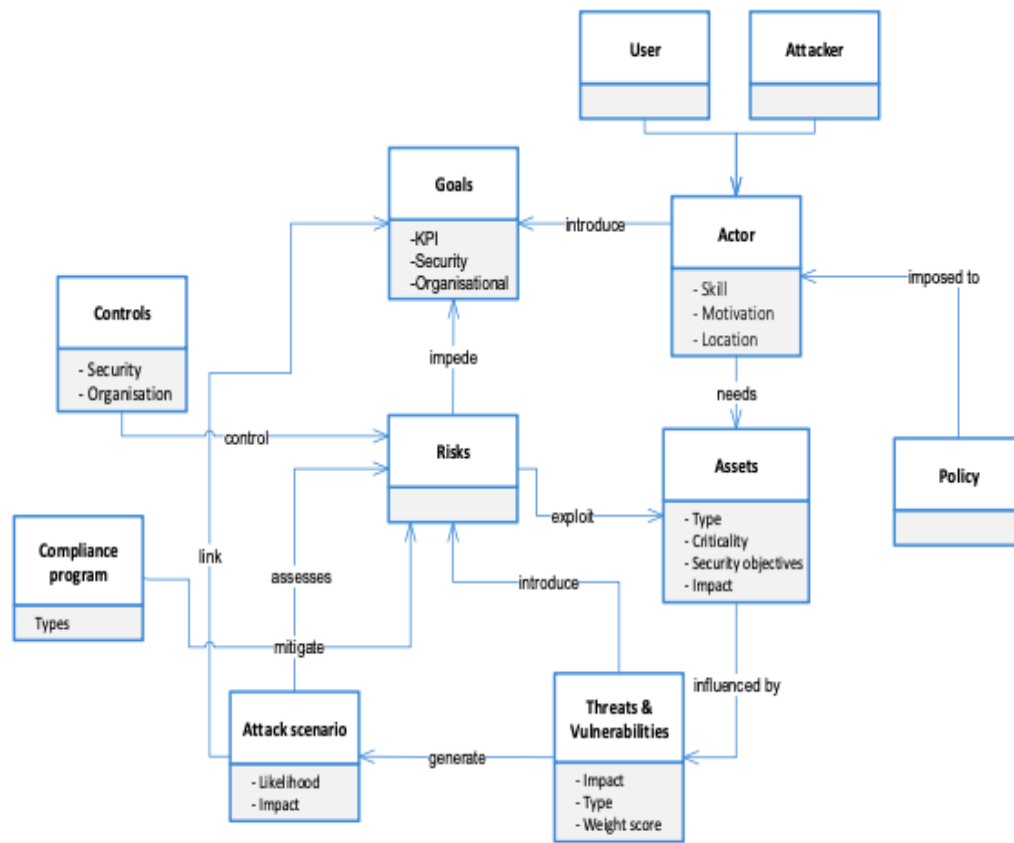


Figure 2. Metamodel.

The data collection tool has been designed from an early stage to have the total control of the process and the standard comprehension of what is related to compliance [6]. Therefore, it has been possible to understand the hierarchic structure and the processes that make exchanges in the pairwise comparisons [6]. Thus, a series of comparison questions have been established by using the Saaty scale (1-9), and subsequently, the matrices have been organized together with the respondent by using the Expert Choice software [6]. Finally, they have been effectively applied to a medium-sized company in the Brazilian industrial sector with a significant level of investment in R&D [6].

This has configured what was sought, the resolution of the problem of hierarchical design research for multicriteria decision making that increases the institutional compliance considering information security [6]. Therefore, the hierarchic structure is established in 3 levels. Main objective is increasing compliance set of related criteria that involve:

1. Standards.
2. External regulation.
3. Internal regulation.
4. Risks assessments.

Alternatives to increase the corporate compliance by considering information security:

1. Identification of applicable legislation and contractual requirements.
2. Intellectual property rights
3. Protections of records.
4. Privacy and protection of personally identifiable information.
5. Regulation of cryptographic controls.
6. Independent review of information security.
7. Compliance with security policies and standards.
8. Technical compliance review.

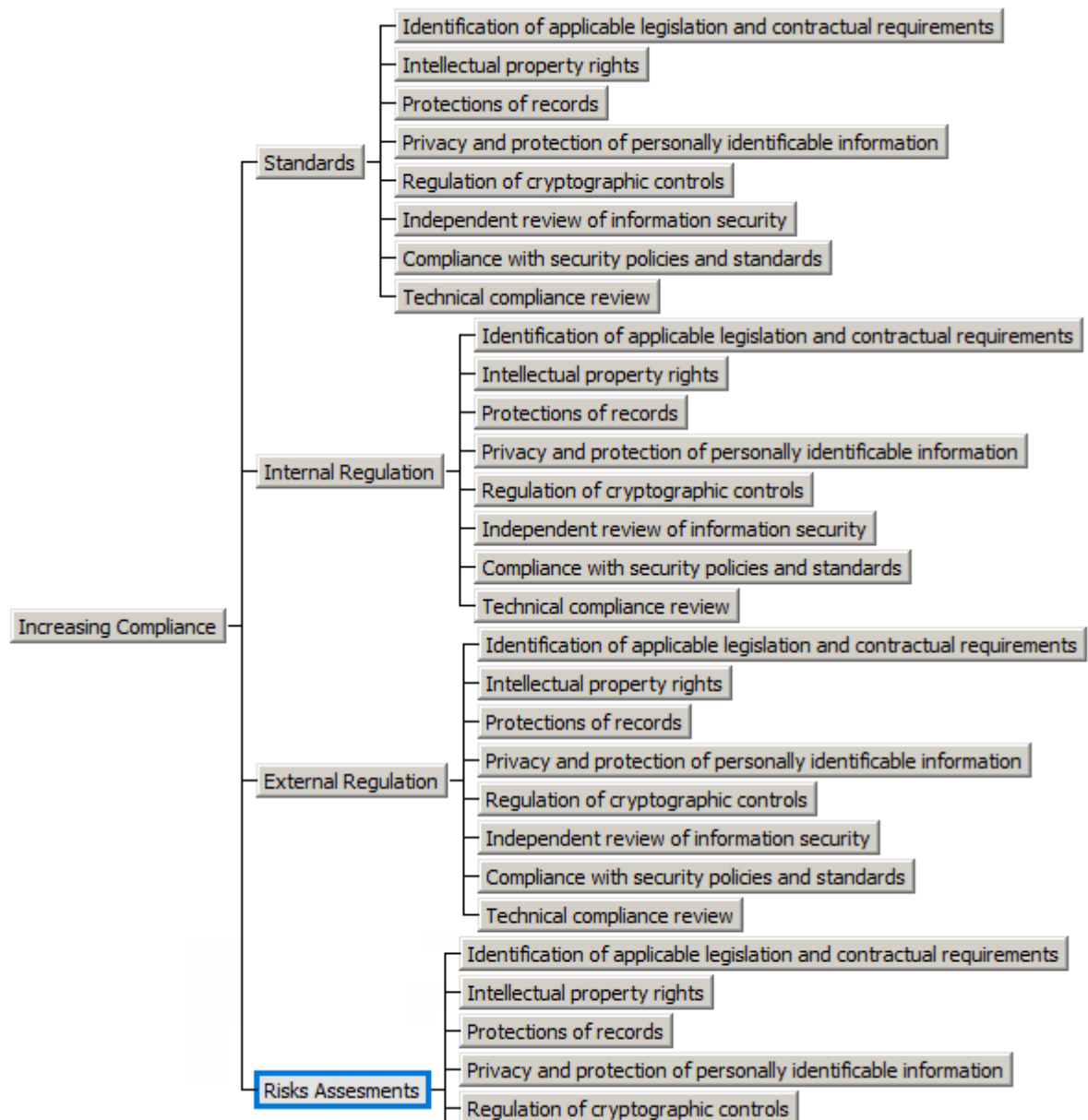


Figure 1. Hierarchic design to increase compliance.

Figure 2 plots the structuring of the research's main goal with its respective criteria and alternatives. Thus, the hierarchic model has been designed in an organized, effective and didactic way by means of a user-friendly interface [6].



Figure 2. Goals, criteria/attributes and alternatives.

The matrices that are presented below for illustrative purposes will subsequently allow to explain the applicability of the model.

Figure 3 represents the beginning of the pairwise comparisons by considering the main goal and the crossing criteria.

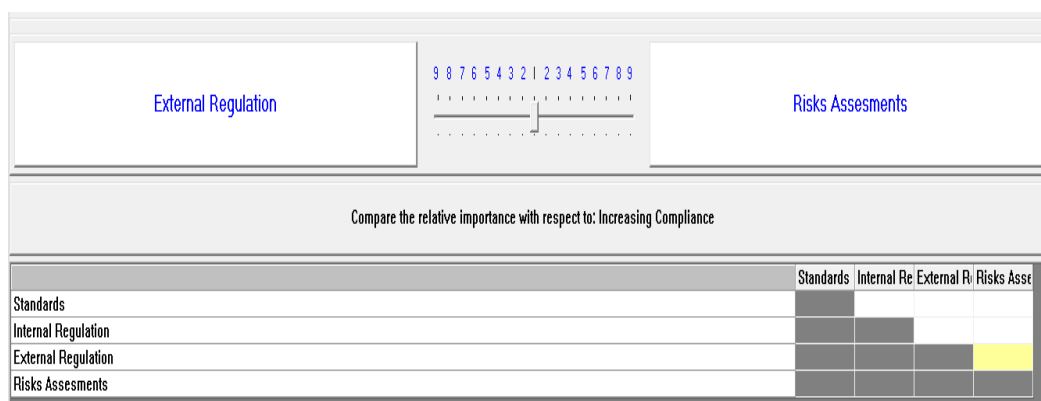


Figure 3. External regulation vs Risks assessments to Increasing compliance.

Figure 4 positions the pairwise comparison between the alternatives Identification of applicable legislation and contractual requirements and Intellectual property rights from the standards' point of view [6].

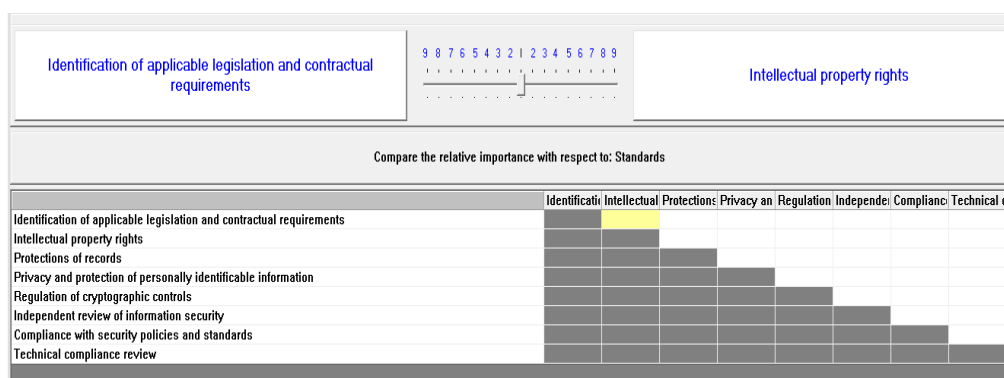


Figure 4. Identification of applicable legislation and contractual requirements and Intellectual property rights from the Standards' perspective.

Figure 5 shows the comparison matrix crossing Compliance with security policies and standards with technical compliance review from the Internal regulation's perspective [6].

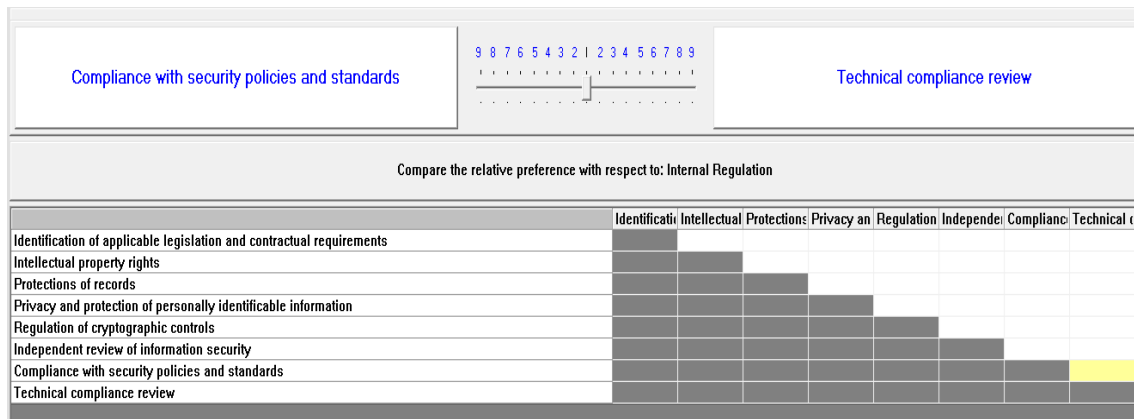


Figure 5. Compliance with security policies and standards vs technical compliance review from the Internal regulation's perspective.

Figure 6 shows the comparison matrix again, crossing the relative importance between Compliance with security policies and standards and the technical compliance review from the Risks assessments approach [6].

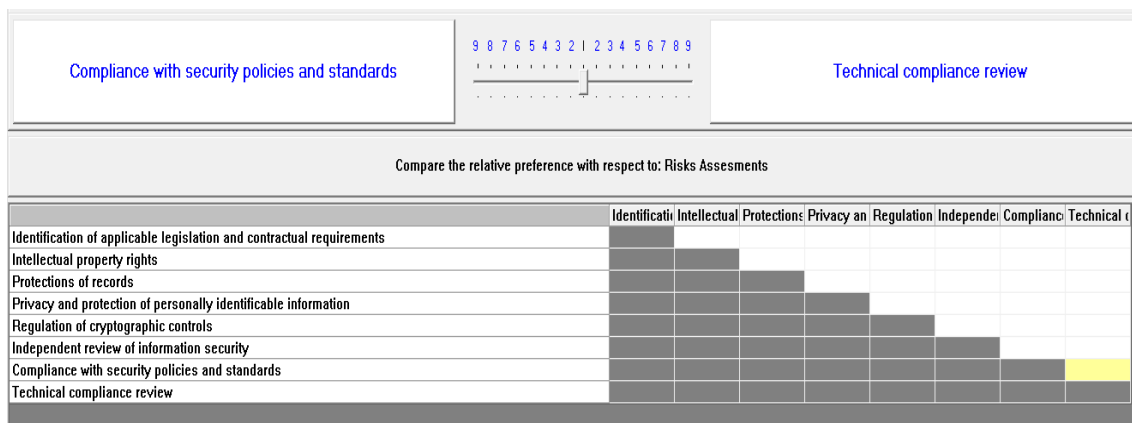


Figure 6. Compliance with security policies and standards and the technical compliance review from the Risks assessments approach.

## CONCLUSION

The study identified in the implementation of ITIL best practices in a public company object of this case, which factors, translated into relevant and priority actions, contributed to the success of this implementation, mitigating the processes, and optimizing resources, under the optics people and processes, aimed at improving the quality of services provided to the society and aligned with the concepts of governance.

For this evaluation and identification, the concepts of compliance (laws and ethics), governance and strategic planning for security, security policies, risk management, security management models and practices, contingencies planning, protection mechanisms, services level agreement, of the ITIL model used in the organisation to conduct research into various security framework or model example, Information Technology Infrastructure Library (ITIL) and security model example, International Organisation for Standardization, ISO 27000. To meet the need of the company, CoffeeBlend which sells Jamaica coffee, one of the best and most sought-after blends in the world. Information system security, governance, and compliance.

The relative data for the analysis of the results obtained with the implementation of ITIL from the point of view of people and that identify success factors were subdivided into three themes: (i) Training; (ii) Knowledge Management; (iii) Knowledge Integration x Professional Development x Work Processes. In terms of processes, the questionnaire addressed the issues related to the final operational processes, focused on the quality and resolution of the services rendered the intermediate operational processes that focus on the processes to support the implementation of the processes and, finally, the operational management with a focus on diagnosis, Monitoring, and optimization of the processes in question.

The results presented allowed us to infer that the implementation of the best practices recommended by the ITIL model allows the Company to reach more challenging stages involving the high capacity and availability of its information systems and to face great pressure from customers and society for the delivery of results in short times.

## REFERENCES

### References

- [1] P. RaviKumar, P. HerbertRaj and P.Jelciana, "Exploring Data Security Issues and Solutions in Cloud Computing," *The 6th International Conference on Smart Computing and Communications*, vol. Volume 125, pp. 691-697, 2018. . DOI: <https://doi.org/10.1016/j.procs.2017.12.089>.
- [2] Ahmed Alkalbani *et al*, "Information Security Compliance in Organisation : An Institutional Perspective," *Data and Information Management*, pp. 1-11, 2017. . DOI: <https://doi.org/10.1515/dim-2017-0006>.
- [3] Sushma Mishra, "Examining organizational security governance (OSG) objectives: How is strategic planning for security is undertaken at ABC corporation?" in *Proceedings of the Conference on Information Systems Applied Research*, 2019, pp. 1-12.
- [4] Fayez Hussain Alqahtani, "Developing an information security policy: A case study approach," in *4th Information Systems International Conference 2017, ISICO 2017, 6-8 November 2017, Bali, Indonesia*, 2018, pp. 691- 697.
- [5] Halima Ibrahim Kure, Shareeful Islam and Mohammad Abdur Razzaque, "An Integrated Cyber Security Risk Management Approach for a Cyber-Physical System," pp. 1-29, 2018. Available: [www.mdpi.com/journal/applsci](http://www.mdpi.com/journal/applsci). DOI: 10.3390/app8060898.
- [6] Pedro Solana-González, Adolfo Alberto Vanti and Karen Hackbart Souza Fontana, "MULTICRITERIA ANALYSIS OF THE COMPLIANCE FOR THE IMPROVEMENT OF INFORMATION SECURITY," *Journal of Information Systems and Technology Management – Jistem USP*, vol. vol 16, pp. 1-19, 2019. . DOI: 10.4301/S1807-1775201916007.