



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

An internationally growing company known as CoffeeBlend is a coffee selling company with massive social presence online. The company CoffeeBlend is concerned about protecting their billions worth intellectual properties and wants to establish their security policy. They want to make sure that their staff's personal data and client's intellectual properties are secure. The company in order to secure their network and company's infrastructure and to meet their needs into various frameworks of security and model with the help of designing and is being conducted with the help of it for the company's secure information and governance.

The National Institute of Standard and Technology (NIST) states that, "The framework for enabling access to the network is termed as Cloud Computing to pool of resources which are configurable that are increasingly be able to release and minimum managerial provisioned effort and or interaction service provided" [1]. In the computing the cloud computing is among the fastest technology which has emerged in the recent years. Accessibility, infrastructure, and time management etc are some of the advantages of the cloud computing along with lack of expertise, data security and resources being some of the disadvantages of it [1].

The securing of the data in the enterprise computing within the organisation is performed in the cloud computing and accordingly the data is saved in the CSP and not saved in the place of the consumers. Due to vulnerabilities of the security of the network and to ensure there are no data breaches in it, it is beneficial to employ additional security measures [1]. The data lifecycle has 6 stages in it which are Store, create, use, archive, share and destroy [1]. After performing the duty, the data lifecycle, assures that a user after performing cannot deny a duty as it is nonrepudiation. The data security issues are categorized in 4 types which are the following. Four major categories of data security issues are the following.

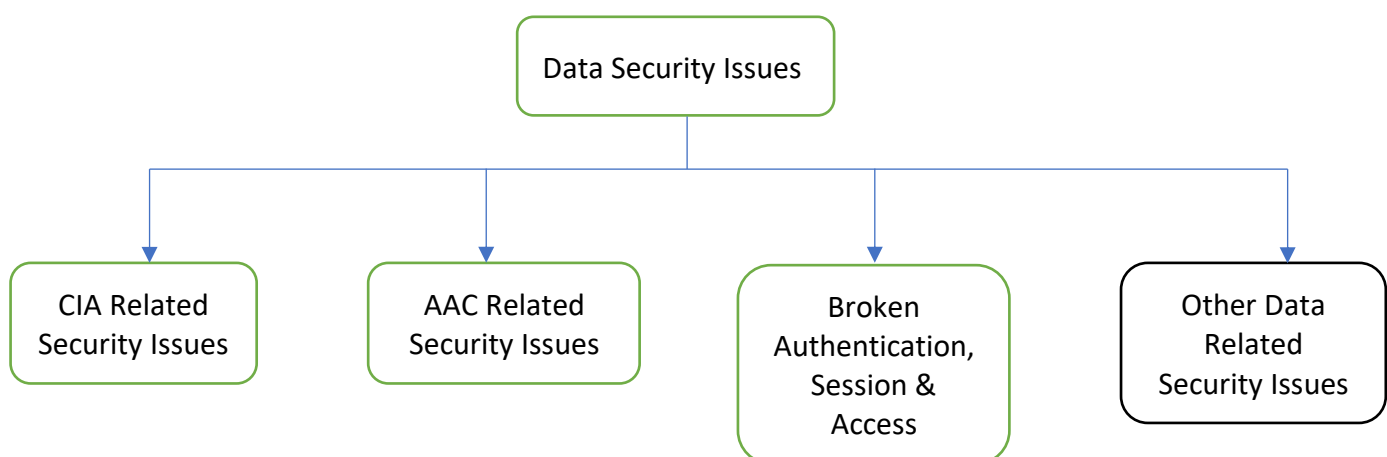


Fig. 1 Types of Data Security Issues

In the Organization in the department of the information security compliance for its better understanding there are some ethics and law compliances. For the relationship proposed testing in the model and to fulfil this objective structural equation modelling is used [2]. Between the measured variables and unobserved constructs for testing the relationship such techniques are used [2].

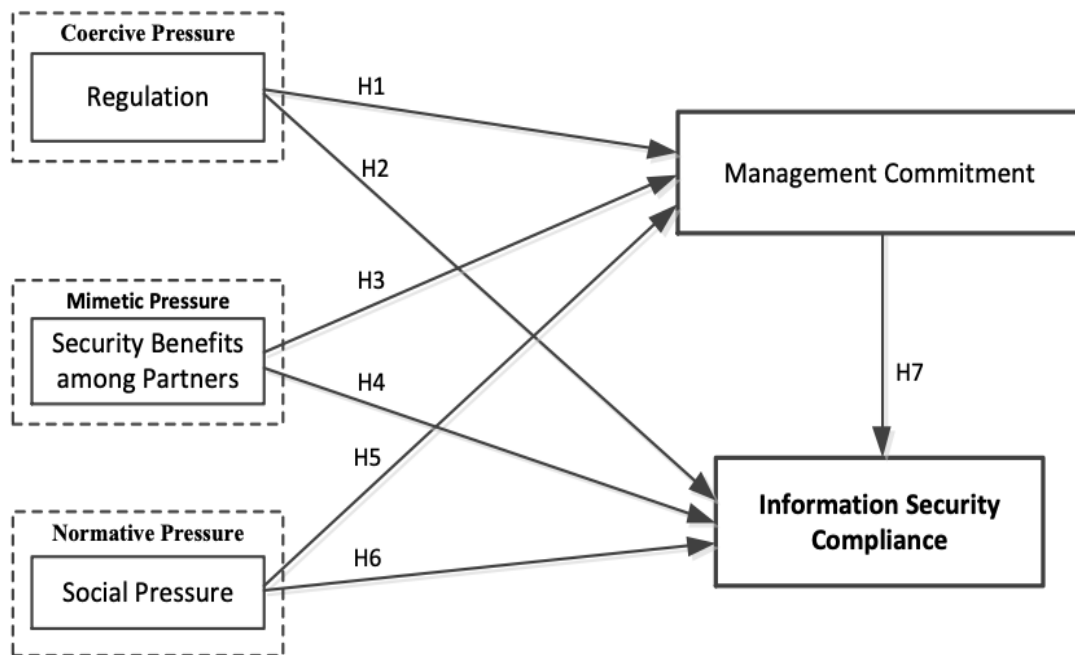


Figure 1: A research model.

The theory development for its extension and due to its potential, there is use of appropriate structural equation modelling, to assess simultaneously is its capacity of the multiple and interrelated depending on the relationships [2]. The structural equation modelling, in order to approach it there is use of a two-step approach and it is measurements and structural model [2]. The sign of the paths in between the variables and the path coefficients in the structural model which involves indication of the strength [2]. Conducting a CFA which is known as conducting a confirmatory factor analysis it is contained in the measurement model which assess each indicator variable's contribution by conducting CFA for also measuring the adequacy for the measurement model [2].

The governance and strategic planning for the company's security are the following :-

1. Regulatory Compliance

All the requirements are met in terms of mandatory and legal, regarding the internal control and security which is known as regulatory compliance [3]. The procedure of the compliance in accordance with the legislation controls and procedure formalities this helps in promoting the development of the regulatory compliance [3]. By using the legislation, the security governance can be improved, legislation as catalyst.

2. Ensuring Continuous Improvements in Controls

The primary objective is the control implementation process for increasing security governance instituting continuous improvements identifies [3]. For ensuring continuous improvements in control to work effectively this process should be iterative, adaptive, and continuous. Through implementing flexible practices, in the right place at the right time involving right controls.

3. Responsibility and accountability structures

Ensured and defined structures by responsibility and accountability, are the appropriate responsibilities accounting and sharing their actions of the stakeholders [3]. Under certain individuals, appropriate accesses should be made responsible for compliance of the organizational responsibilities, they should be clear this is made sure by the responsibility and accountability structures [3].

4. Corporate control strategy

The corporate control strategy using consensus of the guideline's development, is the establishment of the plan of management of a control and corporate risk. Controls should be viewed as the business cost [3]. For the initiatives of governance and it should be made sure that there is enough planning and non-negotiable budget item are in security controls.

5. Control Conscious Culture

To emphasize on control culture policies, processes and norms are fundamentally important, among different security efforts for creating, maintaining, and sustaining connections. The control culture of the organization should promote 'prevention mentality' over the security issues it's important to decrease the friction among the groups [3]. It's essential for the employees to develop standard conduct codes by carrying out their security responsibilities .

6. Clarity in policies and controls

Visible, easily accessible and fair should be the attributes of the policies in all the organizations. The management commitment communications policies should be clear to make sure that the commitments to the security governance are proved [3].

INFORMATION SECURITY POLICIES

The appropriate behaviour of the employees is supported through the information security policy (ISP) and to follow the conditions and terms of the policies clear instructions are provided [4]. Proper implementation of the ISP there is clear expectations of the organization set [4]. Ensuring there is regular examination of the policies and validation of the strength, scope, and practical applications of the ISPs to define periodic improvements standards [4].

Requirements of Information Security Policy

The organizations can be helped through setting clear and practical information security programme and thus improving information security programme [4]. After developing and designing an ISP, IS assets should be address and observed for any variances that may arise by the organization [4]. The organisations ISP compliance behaviour should not be hindering with respect to the information security and securing data. For testing and designing ISPs there are seven areas which are the following [4].

Table 1. Information Security Focus Areas.

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

Review of Information Security Policy (ISP)

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 ISP explains the various steps which the users follow for passwords, i.e., password changing and managing passwords [4]. The ISP documentation reveals the policy documentation acceptance which has the password management subareas for locking workstation at the institution [4].

Email Use

The IT responsibilities relating to the email use which helps the users resolve issues such as phishing emails, these IT responsibilities are defined by the number of ISP documents [4]. The forward email issue does not exist in the ISP documents. From work mail servers to the external account all is from the automatic forwarding official emails which leads to the risks by security such as loss of control of sensitive data. The current ISP provide email issues which are acceptable documentations along the other security issues [4].

Internet Use

As advised in the ISP documents there should be no inappropriate use of the internet which is using infrastructure and portals of the institution and discussing sensitive data matter should be avoided. The ISP document discusses the use of websites and work portals [4]. As stated by the institution there should be rights given to monitor the users content for as to ensure that the internet is working in accordance with the ISP [4]. Thus, only products available in the IT department portal should be permitted to download and any other software should not be permitted [4].

Social Networking Sites

Using SNS the institution's social media accounts are worked on by a special department for public relation purposes to receive minimal attention in the ISP institution [4]. ISP discusses the consequences of the inappropriate use of the SNS and the potential security threats by it.

Mobile Computing

'Access Policy' an ISP document which manages the mobile work activities and virtual network through secured devices [4]. The policy also includes the mobile international networks and the Wi-Fi public networks [4].

Information Handling

It suggests that sensitive data should be continuously disposed, and the users should continuously clean their systems. 'Commitment Policy' is an ISP document which indicates in a short note that there is only short amount of time allowed to dispose the work documentation and records. The same is also noted in the 'Access Policy' and the 'Leaving Sensitive Material Unsecured' [4].

ISP Awareness and Compliance

There should be more awareness of the ISP and its compliance because in the recent study it was found that the IT managers because of the culture of work environment are not developing the ISP procedure [4]. Thus, the IT unit managers is lacking awareness of the ISP [4].

RISK MANAGEMENT

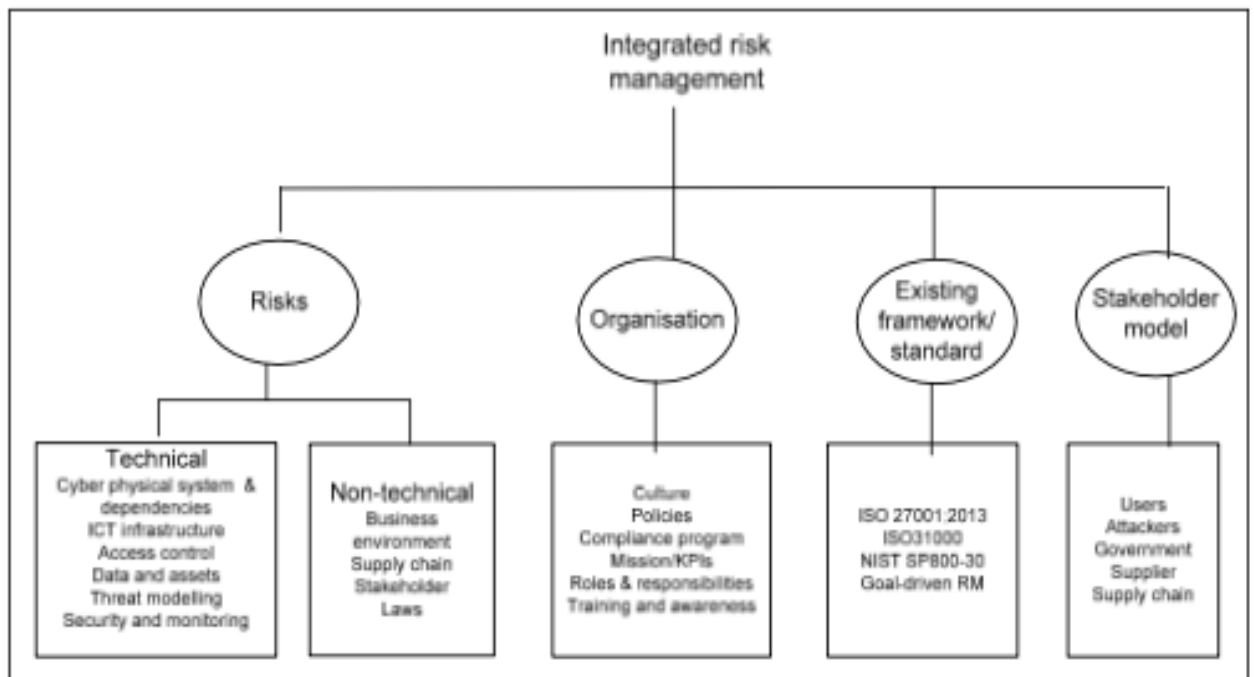


Figure 1. An integrated risk management approach.

An integrated Risk Management Approach

The risks during the operations in the CPS should be monitored and communicated for the benefit of the organisation's infrastructure [5]. Many concepts serve as a common language, they help in describing concepts of the cybersecurity risk management. Their properties help in managing the risks actively. However, to model the cyber security attack scenario, the risk level is quantified for the suitable countermeasure [5]. The following are the integrated risk management concepts :-

Modelling Concepts

The following approach set of the modelling concepts of the cyber security risks are essential to understand [5].

1. Actor: It's a unit which can occur as an organisation, system, or a human user. The unit plays an important role within the settings of the organization, as it activates cyber security risk management actions or receives by another management [5]. To appoint actors to the organisation is important for the various tasks to be carried out to achieve the goals and to guide [5].

2. **Goals:** The goals are the objectives and aims of the actor in order to support the interest of the organization [5]. There are goals of the organization to support its expectations including the KPIs and its security. Including the availability, confidentiality, and integrity such decisions are taken for the continuity of the organisation by the organisational actors for the infrastructure critical organisation [5].
3. **Risks:** Risks are determined by its consequences associated and the possibility of an outcome of an event, occurrence, or an incident [5]. Once the risks are identified its important to have a plan of mitigation to counterattack the risks [5]. The expectations of the actor, the security of the CPS and the system of the association can be at potential risks. The CPS risk is classified as the following parameters i.e., technical, security, non-technical, operational, regulatory and governance. These risks could obstruct the security of the CPS and the appropriate assessment requirements [5].
4. **Assets:** Assets are the entities which are tangible or intangible which have a high value of importance to the organisation. An important process of risk management is the key assets identification and valuing the key assets. Services, people, facilities , processes etc can be defined as these key assets [5]. Loss impact or the critical failure modes are estimated as the identification of the critical assets. Category and critically are the two main features of the assets. Associated with the loss or the degradation of an asset are the measurements of their consequences this is defined as Criticality. To the business continuity these are the assets which are of more value which are determined by the organizations as the major indication. The level of security and sensitivity requirements are set accordingly to the assets classified by category [5]. The most valuable assets to the organisation with the high ratings are categorized by the criticality of an assets which can be high, medium, or low.
5. **Controls:** Controls are defined as the minimization , countermeasures or set of security protections of the security risks in the CPS critical infrastructure [5] . If the relevant controls are not applied the overall goal of risk assessment will be partly defeated [5].
6. **Compliance Programs:** To secure the CPS in operating without any disturbance there are a set of requirements which are called compliance programs [5] . For demonstrating cyber security for CPS protection using the compliance program as a mechanism are increasing by the day as critical infrastructures.

7. Cyber-attack scenario: Cyber-attack scenario is a scenario which when occurs leads to a negative impact , it's an event on the organization's assets. The cyber-attack on a CPS is determined by certain components [5]. These components are the following actor's skill, threat type, location and capability, events, assets and time.
8. Policy: Policies are proposed or adopted by an organization these are defined as the principles of actions [5]. It's necessary to formulate and implement the basics in the CPS security program these are security several policies such as backup and access control [5].
9. Threats and vulnerabilities: To gain unauthorized access to an asset by the threat exploitation as the weakness in an organization security program is known to be threats and vulnerabilities [5] . Some of the properties of these threats and vulnerabilities are impact, type, and weight score [5].

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

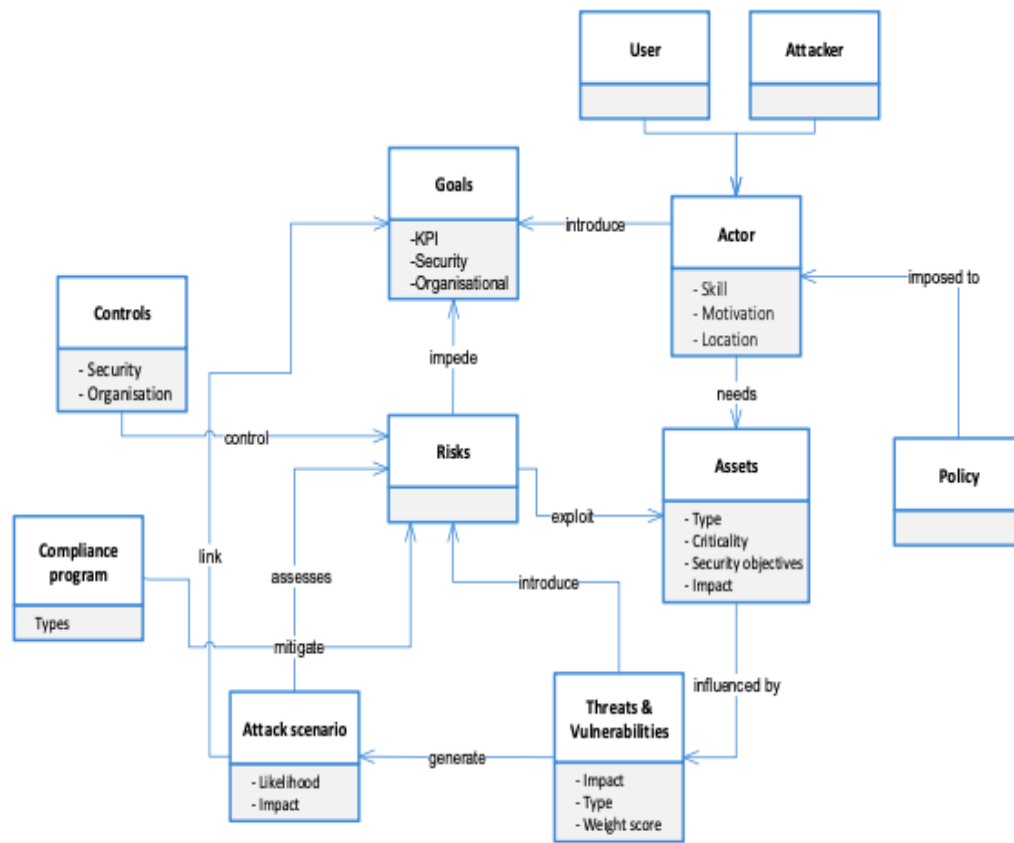


Figure 2. Metamodel.

The security management models and practices are to have control of the process of the data collection tool and the standard comprehension of what is related to compliance [6]. Thus, the processes that exchanges in the comparison pairwise and the possible understanding of the hierarchic structure [6]. Therefore, using the Saaty scale (1-9), a series of comparison question can be established and subsequently the matrices can be organized together with the respondent using the software Expert Choice [6].

The hierarchic structure is established in 3 levels. Main objective is increasing compliance to set a related criteria that involve:

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

Alternatively, by considering information security to increase the corporate compliance these can be defined by the following :

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.

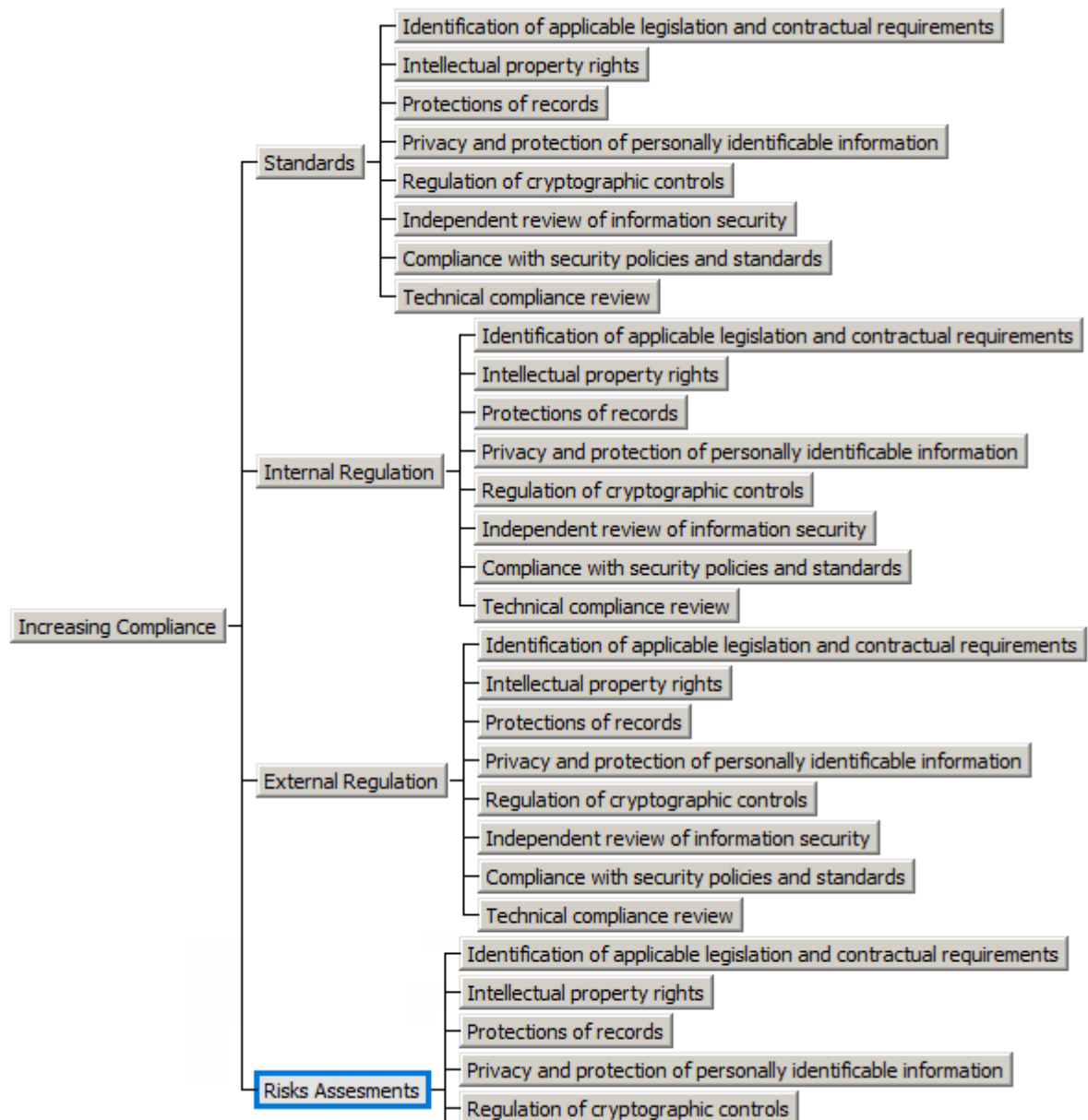


Figure 1. Hierarchic design to increase compliance.

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.

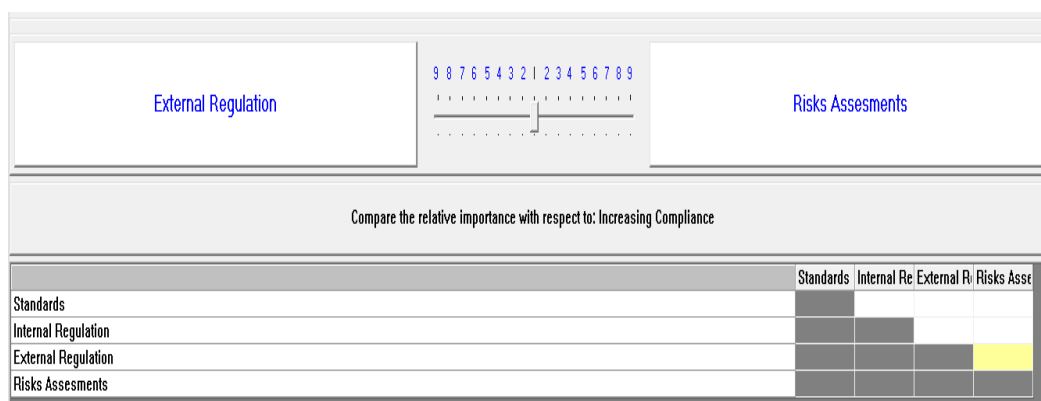


Figure 3. External regulation vs Risks assessments to Increasing compliance.

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].

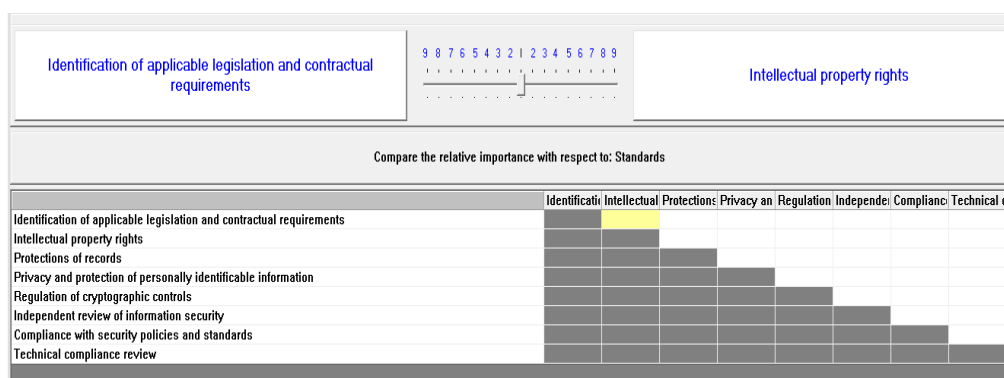


Figure 4. Identification of applicable legislation and contractual requirements and Intellectual property rights from the Standards' perspective.

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

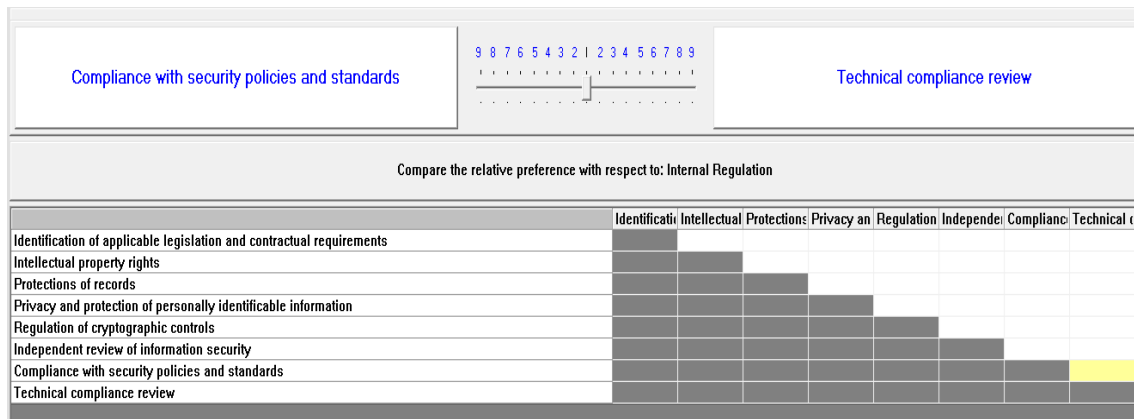


Figure 5. Compliance with security policies and standards vs technical compliance review from the Internal regulation's perspective.

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].

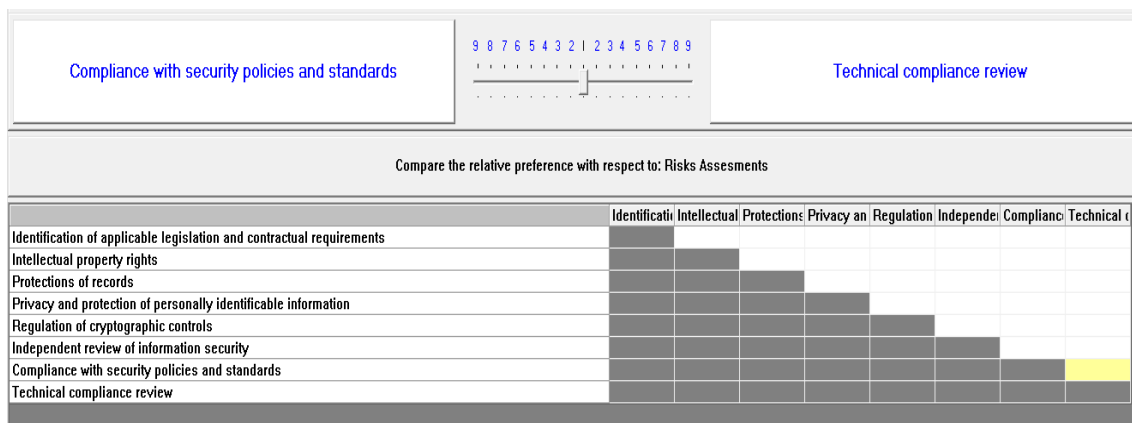


Figure 6. Compliance with security policies and standards and the technical compliance review from the Risks assessments approach.

CONCLUSION

The implementation of ITIL best practices identified by the study in a public company for the object of this case, which translates into priority and relevant actions, for the successful implementation it has been contributed, like processes mitigation, and resources optimizing, under the optics of processes and people, improving the quality as aimed for the services provided to the society and concepts of governance aligned.

For this concepts of compliance its evaluation and identification, strategic and governance security planning, policies of security, management of risk, security management practices and models, planning contingencies, mechanisms protection, level agreement services, of the model ITIL to conduct research used in the organization into various security model or framework example, security model example and Information Technology Infrastructure Library (ITIL) , International Organisation for Standardization ISO 27000.

CoffeeBlend which sells Jamaica coffee, to meet the need of the company, one of the best and most sought-after blends in the world. Information system security, governance, and compliance are improved and looked into.

For the analysis of the results, the relevant data is obtained with the implementation of ITIL from the viewpoint of the experts and that identify success factors were subdivided into three categories : (i) Training; (li) Knowledge Management; (lii) Knowledge Integration x Professional Development x Work Processes. In terms of the process, the final operational processes are addressed related to the questionnaire, focused on the resolution and quality of the services rendered the intermediate operational processes that the processes focus to support the implementation of the processes and, thus, the operational management with a focus on monitoring, diagnosis, and optimization of the doubts in processes.

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