

CoffeeBlend: Data Security, Compliance and Governance

*Remote access and working establishment

Vikram Kalta (2209281)

MSc Data and Artificial Intelligence
University of Wales Trinity Saint David
Swansea, UK

Abstract—This paper focuses on designing a Information Security Management System (ISMS) for CoffeeBlend Limited who has come under pressure to allow its staff and clients to access company's resources from outside of company's network. It involves comparing popular information security frameworks such as ITIL (Information Technology Infrastructure Library), COBIT (Control Objectives for Information and Technologies) and ISO27001 on the basis of their success and failure factors. Eventually an information security design is laid out with the help of appropriate knowledge gathered in the framework evaluation phase.

Index Terms—ISO 27001, Information security management system, ISMS

I. INTRODUCTION

After the COVID19 pandemic, a lot of businesses adapted to the hybrid and remote work cultures, where the staff had to be allowed to use their personal devices to access company's network or resource remotely. Following the current trend and to stay competitive in the market CoffeeBlend Limited is also under pressure to allow its staff and clients to use their personal devices to access company's network and resources remotely.

It is estimated that the company's intellectual property is worth billions, the Information Security becomes the most crucial part in this transformation. The private home networks puts organisation's network under threat. Private networks are not completely secured neither they are updated regularly. Ultimately these devices could compromise the network and make it more accessible to vulnerable points to be exploited during a cyberattack. One way of addressing this would be to use encrypted communication such as Virtual Private Network (VPN).

The goal is to protect the assets of the company, be it digital, material form or knowledge based and aim to make the company prepared well to combat any security threats that it poses.

In the literature review section a study is carried out to understand various frameworks such as COBIT, ITIL and ISO 27001, in the next sections a plan is laid out for developing information security management systems (ISMS) using ap-

propriate tools which will help CoffeeBlend Ltd achieve its business and strategic goals.

It is also important to highlight that implementing any new changes in the company is not just dependent on good policies and procedures but also relies on the management efforts to monitor it and make sure implementation is aligned with the supported documentations and also ensures the smooth functioning of the operations. Thus a good ISMS implementation can not be a success unless there are management efforts in place as well continuously to improve the process and update the process wherever required. While this is true and actually all modern information security program requires that the approach is top down. Without stakeholders support executing information security policy is not effective. There is hence a need also to align the information security policy with organisational goals.

II. LITERATURE REVIEW

Information security is a critical concern in today's digital age, as organisations and individuals increasingly rely on digital systems and networks to store and transmit sensitive data. In this section, the most relevant research in the field of information security is used, with a focus on studies that have addressed similar problems. The success of the governance of any organisation is dependent on information technology (IT) governance. In order to succeed in the IT governance, companies use best practices [1] that are formalized in the guides in the form of framework such as COBIT (Control Objectives for Information and Related Technologies), ITIL (Information Technology Infrastructure Library) etc. The authors in [1] discusses the design of an ITIL implementation model based on its advantages. The authors highlights critical success factors in ITIL implementation in the previous studies using a table which displays frequency of occurrence, percentage and cumulative percentage of each factor analysed. From which it indicated that 4 top most important factors were training (21%) senior management commitment (18%), awareness(11%) and change management (9%) The author also conducts a case study of the ITIL implementation in a large services company, with a workforce of more than 500. The implementation involved incident management process in accordance with

ITIL framework. The implementation followed with some advantages such as a single contact for taking responsibilities for managing and treatment of incidents, procedures for managing incidents are formalized and implemented etc. But has limitations as well such as the awareness is not sufficiently large compared to importance of the project. Then the authors talks about the design to implement ITIL based on the results of the previous studies. Author highlights that the success factors for ITIL implementation are commitment from the top management and also from the staff and their managers.

In [2] authors ITIL framework is used to implement service desk in a financial company, according to ITIL service desk is "The single point of contact between users and IT service management". Here authors stresses on factors which causes ITIL to fail such as culture shift, appropriate management tool and clear measurement target.

In [3] authors comments on COBIT (Control Objectives for Information and Related Technology) 4.1 version. COBIT 4.1 has 34 processes of 4 main processes. COBIT aims IT to work

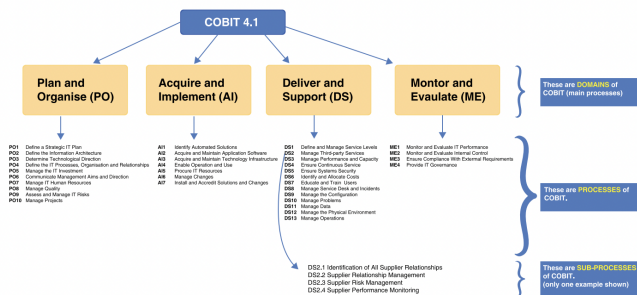


Fig. 1. Processes in COBIT

in line with the company's strategic goals. Authors highlights that full implementation of COBIT is costly, hence the partial implementation of COBIT makes it a primary implementation problem. COBIT is designed to provide integrated IT governance from planning to monitoring. The authors further stresses partial implementation too requires a lot of care when selecting the processes to be implemented such as if PO2 is ignored, the organisation may face problems with data operations such as protection controls, authorization, data storage and destruction criteria. Also how the processes are inter-dependent on each other is well highlighted.

In [4] author describes information security management systems (ISMS) as a set of frameworks, policies, procedures and guidelines that an organization needs to follow to make sure the confidentiality, integrity and availability of its information and systems are maintained. The common structure of ISMS which is used industry wide is plan-do-check-act (PDCA) cycle. Which are as follows:

- PLAN: Designing ISMS.
- DO: Implementing and operating ISMS
- CHECK: Monitoring and reviewing ISMS

- ACT: Maintaining and enhancing ISMS

Further the author stresses how being certified based on ISO standards would provide organisations with better credentials and assurance towards its users that their information is safely protected. ISO 27001 is one of the standards which is adopted globally by several industries. The standard defines processes for creation, operation and maintenance of ISMS. ISO 27001 is not a control, however it is a process management and assessment standard. ISO 27001 is generally acknowledged to be an excellent standard for coverage of security domain and most widely employed security-related standard. As per the ISO 27001:2013 Annex A has 14 major clauses or control areas numbered from A.5 to A.18 [5]. Each of which identified one or more control objectives. The annexes are as follow:

- A5: Information security policies
- A6: Organisation of information security
- A7: Human resource security
- A8: Asset management
- A9: Access control
- A10: Cryptography
- A11: Physical and environmental security
- A12: Operations security
- A13: Communications security
- A14: System acquisition, development and maintenance
- A15: Supplier relationships
- A16: Information security incident management
- A17: Information security aspects of business continuity management
- A18: Compliance.

III. DESIGN AND IMPLEMENTATION

After evaluating certain models/frameworks for information security it turns out that for a company like CoffeeBlend Ltd who has a major concern for information security, ISO 27001 would be the best fit for establishing an ISMS. A group of IT professionals are required to establish an ISMS across the organization. Information security team in conjunction with other relevant departments and stakeholders such as security manager, the chief information officer (CIO) and other IT and security professionals are required to finalise the design and implementation of ISO 27001. The most crucial steps in order to establish a successful ISMS are as follows:

A. Project establishment

Firstly the ISMS implementation is established as a project. A project manager shall be allocated dedicated to this project and teams are created to achieve specific goals. The project manager's job is to monitor each team's activities on a daily basis and help them reach their goals as much as he/she can.

Some key considerations and tasks involved in such a project might include:

- Budget allocation for hiring information security professionals and time invested in the training of the staff and finally get the approval from management.

- Developing a clear policy outlining the expectations, guidelines and procedures for remote work. For example in general implementing a bring your own device (BYOD) policy can be a part of this task. It is also covered under ISO 27001 A 13.2.1. Benefits of BYOD is mentioned here [12].
- Equipping employees and clients with tools and resources to access the network remotely. Such as laptops, virtual private network (VPN) connections etc.
- Ensuring the availability and accessibility of data to users remotely.
- Setup processes for communication and collaboration among team members who are working remotely.
- Protocols establishment for tracking and managing work progress and performance.
- Arranging support and training programs for employees as needed to ensure smooth transition to remote work.

B. Identifying requirements

As a part of next step all the requirements are identified and gathered to execute this project. Some of the requirements are as follows:

- Identifying interested parties: This step involves identifying the interested parties or groups who have a stake in the outcome of the project. For example a few of the stakeholders in this case are the staff and the clients. During planning and executing a project it is highly important to consider needs and expectations of the interested parties as they have high impact on the project's success.
Expected outcome of this step is to ensure the level of protection to the interested party's which is expected by them.
- Legal requirements: Identifying legal requirements also plays an important role in this phase which are laws and regulations that the project must comply with. The organization implementing an ISMS needs to be aware of and adhere to relevant regulatory requirements to avoid potential issues and penalties. These requirements includes data privacy. The GDPR requires the issue of consent [6]. GDPR requires clear privacy notices to be highlighted to individuals that they are giving personal data and that may have an effect on their privacy, thus allowing them to make an informed decision on whether they consent to allow their data to be stored and used.
- Regulatory requirements: These are the rules and guidelines that are set by the government bodies. This includes cybersecurity regulations. For example this may include Payment Card Industry Data Security Standard (PCI DSS) for handling credit card transactions.

C. Define scope

This step involves defining the information security policy. The scope of information security policy is to be defined and communicated to all relevant parties. A sample

information security policy may look like the following:

TITLE: INFORMATION SECURITY <i>Policy Purpose: The purpose of this policy is to ensure the confidentiality, integrity and availability of the organization's information assets, including data, systems and networks.</i> <i>Scope: This policy applies to all employees, contractors and other authorised user of organization's information assets regardless of location.</i> <i>Policy:</i> • All employees and authorised users are responsible for protecting the organization's information assets, and ensuring their proper use. • Access to information assets is granted on a need-to-know basis and is limited to authorized users only. • Sensitive information, such as financial data or personal information, must be protected with additional security measures, such as encryption or password protection.
--

Although this sample security policy does not contain full list of required policies but should be enough to give an idea of the goals to be achieved.

D. Implement support procedures

This step requires to establish procedures for document control and internal audit.

Document control is the process of managing and organising documents in a way that they are accurate, up to date and easily accessible. The following steps to be taken to follow document control:

- Identifying the types of documents that need to be controlled and establishing a system for organising and storing them such as document management system.
- Establish a process for creating, reviewing, approving and distributing documents.
- Implement procedures for maintaining the accuracy and currency of documents. Regularly review and update documents.
- Establish procedure for access control for documents. This will involve who can view, edit or delete documents.

Internal audit is the process of independently and objectively evaluating an organization's activities and process to determine whether they operate efficiently and in compliance with relevant laws, regulations and policies.

- Establish an audit plan that outlines scope, timing and resources for the audit.
- Identify any issues or areas of concern and recommend corrective actions.
- Report results of audit to stakeholders, board of directors and management.

E. Designing the process of Risk assessment and treatment

The next planning step is the information security risk assessment. Risk assessment is dealt with in clauses 6.1.2 and 8.2 of ISO27001 [7].

Risk assessment methodology is a systematic process for evaluating potential risks associated with a particular activity or decision. It involves identifying hazards or sources of risk, analysing the likelihood and potential consequences of those risks.

There are several methodologies for risk assessment. A few of them were picked to be studied and evaluated on the basis of current trends in the industry for most effective methodologies such as Qualitative, Cost-benefit analysis and Quantitative assessment.

In qualitative assessment, rather than basing its decisions on numerical or statistical data it is subjective and are not grounded in theory [8]. Apart from that it depends on the knowledge and expertise of the individuals who conducts the assessment. Cost-benefit analysis is a traditional method. Applying cost-benefit analysis to choosing the optimal level of security may be tenuous because of the difficulty in quantifying the risk and the benefits associated with increased security. Therefore a methodology that overcomes these uncertainties and provides dependable results related to investment on security is required. Thus a careful study on quantitative assessment methodology is required. This is claimed to be the more reliable and a better balance between risk and cost of providing security to mitigate the risk can be achieved.

The few challenges with risk assessment is that the data are limited on risk factors, such as likelihood of a sophisticated hacker attack and the cost of damages, loss or disruption caused by events that exploit security weaknesses. Precise estimation is often not possible. Even if the precise information is available, it would soon be out of date due to the changes that occur in the technologies. Quantitative assessment is designed to estimate the maximum potential loss to be expected over a period of time. Hence there is a need to quantify the risk by finding the maximum possible loss due to a security breach over a certain period of time.

As part of first step, all the threats needs to be identified. The potential risks faced in the production environment can be malicious acts, denial of service, unauthorised access to private information, deleting or altering sensitive company information, viruses, worms, password cracking, hacking, frauds, natural disasters, sabotage and user error. A survey conducted with help of information security managers to identify all possible threats would be of a great use in this step. Because there are always huge threats and to almost every asset in the company. What is most important is to "prioritise". So understanding your mission critical assets is key when you try to assess what assets needs to be protected the most. For example if the company has a trade secret say on a file server

that probably needs to be protected more than a normal server used just for daily computing purpose.

Second step is to do a estimation of threats. This may involve exploring current studies to identify the frequency of each of the security breach and to gather the most relevant data.

Another step involves to plan risk acceptance criteria. The risk acceptance criteria are used to determine whether a particular risk should be accepted or mitigated. Some factors which affects the risk acceptance criteria are as follows:

- Risk appetite: An organization can have low or high risk appetite depending upon the impact of overall information security on business.
- The likelihood and impact plays an important role in deciding the criteria. A risk with high likelihood and high impact will be more hard to accept and hence mitigated.
- Cost of mitigation is another factor. If the overall cost of implementing controls to mitigate a risk is more than the cost of mitigating the risk, we might have to accept the risk.

F. Perform risk assessment and treatment

As given below there are certain elements of risk in information security [9]

Assets: A list of assets that has potential effect on the financial performance of the company. The following items can be the assets included in the implementation of the risk assessor:

- Customer data, including personal and financial information.
- Intellectual property, such as trademarks and proprietary recipes.
- Physical assets such as stores, equipment and vehicles.
- Reputation and brand image.
- Supplier and vendor relationships.
- Remote access (VPN corporate).
- Employee data, including personal and financial information.

Threats: The threats associated with the list above have been considered are as follows:

- Cyber attacks leading to data breaches.
- Physical theft or destruction of assets.
- Denial of service: A malicious attacker causes a spike in resource usage and service requests are dropped.
- Reputational damage due to negative media coverage of customer complaints.
- Supply chain disruptions.
- Accessing private networks.
- Legal liabilities related to data privacy, security or product quality.
- Changes in consumer preferences or purchasing habits.

Vulnerabilities: The vulnerabilities associated with the list are as:

- Weaknesses in cyber security measures.
- Lack of physical security measures or protocols.
- Dependence on small number of key personal.
- Lack of a robust crisis management plan.
- Dependence on a single supplier or a small number of suppliers.
- Lack of legal compliance with data privacy and security compliance.
- Inadequate customer service or reputation management strategies.

A sample quantitative assessment sheet is shown below in Table 1. Note that codes are used in risk columns. Which are described below.

- R1: Cyber attack leading to data breach
- R2: Loss of key personnel
- R3: Supply chain disruption

TABLE I
QUANTITATIVE RISK ASSESSMENT SHEET

Risk	Likelihood(%)	Impact(\$)	Risk Level(\$)	Risk Treatment
R1	0.2	500,000	100,000	Mitigate
R2	0.05	100,000	15,000	Accept
R3	0.15	50,000	2,500	Accept

Table 1.

The purpose of each columns are explained below:

- Risk: A description of the risk being assessed.
- Likelihood: The likelihood of the risk occurring, based on statistical data or probability estimates. This can be expressed as a percentage or a decimal.
- Impact: The potential impact of the risk occurring, expressed in numerical terms (e.g., dollars).
- Risk level: The calculated risk level, based on the likelihood and impact estimates. This can be calculated by multiplying the likelihood and impact estimates.
- Risk treatment: Can be one of the following: Accept, Transfer, Mitigate, Avoid. This depends on the risk level.

G. Statement of Applicability (SoA)

After conducting risk assessment and taking decisions regarding the treatment of those assessed risks, the results regarding the treatment of those assessed risks, the results needs to be documented. This document is known as Statement of Applicability (SoA).

The SoA lists all the controls that are selected alongside a justification for their selection and also the ones which are not selected alongside a justification [10]. This is also a document reviewed by the certifying bodies so makes it really important part of the ISO 27001 implementation. Here is a sample SoA.

TITLE: STATEMENT OF APPLICABILITY

Organization: CoffeeBlend limited

Date: January 1, 2022

This document serves as the statement of applicability for CoffeeBlend Ltd's ISMS, which is based on the requirements of ISO 27001. The following control objectives from Annex A have been included in the ISMS:

- A.5.1.1 Policies for information security. CoffeeBlend Ltd approved an information security policy that conforms to the guidance of ISO 27002:2013 on 1st Jan, 2022 and has published and communicated it to all employees and relevant external parties.
- A.5.1.2 Review of the policies for information security. All policies related to information security are reviewed at least annually or when determined necessary by the information security or when determined necessary by the information security steering group.
- A.6.1.1 Information security roles and responsibilities. CoffeeBlend Ltd has established an information security steering group, which reports to CEO, and which includes representatives from all the key parts of the organization. This group approved and is responsible for regular reviews of the information security policy and is responsible for assigning and/or resourcing security roles within an organization.

Please note that not each of the controls specified under Annex A are shown in the document as it will be done in a separate document.

H. Implement all required controls

In this step document or a set of documents is created that provides evidence of how we implemented a specific standard or set of standards is implemented. The purpose is to demonstrate that the organization have followed the requirements of the standard and have implemented processes and procedures to ensure compliance. This document is called record of implementation.

Record of implementation may include various types of documents, such as policies, procedures, training materials and records of activities related to the implementation of the standard. Record of implementation may contain the following items:

- Information security policies: These are high-level documents that outline the organization's approach. to information security and set out the general principles and guidelines that employees are expected to follow.
- Standard operating procedures (SOPs): These are more detailed documents that outline the specific steps that employees are expected to follow when carrying out specific tasks.
- Training materials: These may include presentations, manuals and other resources that are used to educate

employees about the org information security policies and procedures.

- Records of internal audits and corrective actions: These are documents that detail findings of internal audits and any corrective actions.
- Evidence of risk assessments and risk treatment: This may include documents such as risk treatment plans, which outline the organization's approach to identifying and mitigating information security risks.

I. Conducting internal review

In this step an internal audit is conducted. Internal audit helps in assessing the effectiveness of its information security controls and identify areas for improvement.

Internal audit is a systematic and independent evaluation of activities and processes to determine whether they align with the information security policies and procedures as well as with relevant laws, regulations and standards. It is typically conducted by an internal audit team, which maybe made up of internal staff.

During the internal audit, the audit team will review the information security policies, procedures and controls to ensure that they are being followed and are effective. This step is further divided into phases, such as given below:

- Planning: The audit team will develop an audit plan that outlines the scope of the audit, the resources that will be required and the timeline for completing the audit.
- Preparation: The team will review the information security policies, procedures and controls to become familiar with the ISMS.
- Fieldwork: The team will conduct the audit by gathering evidence to assess.

J. Results and discussions

This paper explored three important IT frameworks to establish a robust information security system such that clients and staff are allowed to use their personal devices outside of the company's network. This paper studied ITIL, COBIT and ISO27001 and through some case studies and academic research identified advantages and disadvantages behind each of them. While ISO standards investigate the supporting guidelines, procedures, processes, improvements and requirements necessary for effective and successful ISMS in depth with all headings, ITIL does not address most of these headings in depth [11]. While COBIT is termed as a costly implementation and thus a partial implementation is a major issue and a lot of processes has to be carefully selected since some processes are inter-dependent on each other. The best fit found was ISO 27001 to implement an ISMS. In order to implement ISO 27001, organizations are required to prepare and produce specific documents. The standard specifies several clauses some of which are mandatory if the organisation wants to be compliant to the standard. The risk assessment and treatment phase takes the longest time. Each of the risk is quantified

to measure its impact and risk acceptance criteria is decided on based of that. Then next SoA is produced which specifies the list of controls implemented and the ones which are not and also justifies each of the decision. The ISO 27001 can have a huge benefit on company's business and strategic goals. Risk assessment gives a lot of transparency to company in knowing its weaknesses and strengths if done cautiously. If a company can anticipate cyberattacks or any kind of threats to its information system, then it can prepare itself well and reduce the impact it can have on the business.

K. Conclusions

This paper intended to come up with a design for ISMS for CoffeeBlend such that it can act well to the threats to its information security and in the process can confidently allow its staff and clients to access company's network from the outside. This paper also presented a brief comparison between ITIL, COBIT and ISO27001. This was done with the help of previous studies on implementation of each of the frameworks. The steps that the ISO27001 implementation goes through were addressed. Risk assessment and treatment was found to be the lengthiest phase. The controls to be implemented depends a lot on risk assessment and hence makes it the most important step in the whole process. As a final note seeing the various steps involved with ISO27001 implementation, it is evident that it takes a lot of time when an organization starts implementing it sometimes month. So the organization would also scope it down to the critical business first. While the policies and standards can be towards whole organization but implementing them in this case should start with the most critical business area so it can protect what's most important. Then extend it to other business areas.

REFERENCES

- [1] Said Sebaoui, Mohammed Lamrini, Aboubakr Bouayad, Laila El Abbadi, "Design of an ITIL, Implementation Model in a Company". 2019
- [2] Dwi Handoko and Abba Suganda Girsang, "Service Desk Implementation with Information Technology Infrastructure Library Framework (Study Case Financial Company)". 2018
- [3] Yunus Emre GÜRBÜZ, Zübeyir ERGENEKON, "Partial Implementation of COBIT and Possible Risks," 2020
- [4] Zaidatulnajla Hamdi, "A Comparative Review of ISMS Implementation Based on ISO 27000 Series in Organizations of Different Business Sectors," 2019.
- [5] ALAN CALDER, "Chapter Title: ISO27001 ANNEX A. Book Title: ISO27001 / ISO27002. Book Subtitle: A Pocket Guide," .
- [6] Claire Laybats and John Davies, "GDPR: Implementing the regulations," 2018
- [7] ALAN CALDER, "Chapter Title: RISK ASSESSMENT Book Title: ISO27001 / ISO27002. Book Subtitle: A Pocket Guide," .
- [8] Yasin Ozcelik and Jackie Rees, "A New Approach for Information Security Risk Assessment: Value at Risk", 2005
- [9] K. Djemame, D. Armstrong, J. Guitart and M. Macias, "A Risk Assessment Framework for Cloud Computing," in IEEE Transactions on Cloud Computing, vol. 4, no. 3, pp. 265-278, 2016

- [10] ALAN CALDER and STEVE G WATKINS, "Chapter Title: THE STATEMENT OF APPLICABILITY Book Title: Information Security Risk Management for ISO 27001/ISO 27002, third edition," 2019
- [11] Yavuz Ozdemir, Huseyin Basligil, Pelin Alcan, Bahadir Murat Kandemirli, "EVALUATION AND COMPARISON OF COBIT, ITIL AND ISO27K1/2 STANDARDS WITHIN THE FRAMEWORK OF INFORMATION SECURITY", 2014
- [12] Joseph M. Bradley, "<https://blogs.cisco.com/news/new-analysis-comprehensive-byod-implementation-increases-productivity-decreases-costs>", 2013