INFORMATION RISK MANAGEMENT

STUDENT NAME: PRANEETHRAJ
STUDENT ID: 21071235

A COMPREHENSIVE REPORT AND QUALITATIVE ANALYSIS FOR FINTECH PLUS ORGANISATION ON SECURITY IMPLEMENTATION

REPORT WORDS: 2755

SUMMARY: ***An Organised Study And Implementation Of ISO27001 With ISMS Over It And Answering The Questions That Help To Identify And Bring Company To A Standard Operating Procedure Regarding Security.***

Contents

1. INTRODUCTION

Based on the recent attack on Fin-tech Plus, one of the UK's largest digital banking platforms suffered a cyber attack which caused to leak of sensitive information in around 0.16% of its customer data, accounting for more than 50,000 customer data. In this report, we analyse the incident based on WHY, WHAT and HOW approaches around the incident. Moreover, develop a strategy to implement ISMS or FAIR based on the compatibility to organisational structure and assumed event. Also, we take points from the analysis and present the solution to the company directors of three domains about the incident. The report format follows a bullet point explanation structure in all possible sections.

Majorly we will answer the following points.

1. How to **baseline risk level**? **Usage of ISMS and FAIR** and its steps to implement for assumed organisation policy and practice.
2. How is the **ISMS approach** helpful in **Fin-tech Companies**, which aligns with the **Agile Project management domain**
3. The effectiveness of controls (risk response) be measured **using ISO/IEC 27001 implementation chart.** Furthermore, using ISMS Risk Register, risk quantification measures and metrics are **calculated from LOW to CRITICAL.**
4. How to monitor ongoing (residual) risk?

2. FIN-TECH PLUS ORGANISATION INTRODUCTION

Fin-Tech Plus(assumed) is one of the fintech and banking companies with a rooted network in the United Kingdom with more than 200 Countries and Regions interlinking for money exchange and other financial services. It also accounts for more than 25 million personal users and 50,000 business sectors association. It employs 3,500 (2022) staff in the London head office who operate on **AGILE methodology for their core project**. The company operates from different locations worldwide and has customers from all over the world. The application works like a digital wallet and links the customer's banking detail to the app. Then users can pay from their account money. It has a mighty server at the London office and hosts applications worldwide from here. Unfortunately, a catastrophic loss of 30% of the overall company occurred due to the recent cyber attack. Also, it caused business relations reputation loss, and integrity issues forced CTO and Information Security Vice President to resign.

2.1 STRATEGIC OBJECTIVES

- Create instant multi-currency accounts
- Issue physical and virtual corporate cards
- Make and receive transfers in 28 currencies to pay suppliers or employees overseas without being penalised by poor exchange rates.
- Add team members or accountants to their account
- Set permissions and define payment approval flows
- Integrate with popular apps such as Slack, Xero, FreeAgent and Zapier
- Create bulk, scheduled and other complex payments, as well as automate payments through an API
- Access 24/7 customer support

2.2 CURRENT REQUIREMENT

Due to a lack of information on risk management policy updates and the resignation of top management policymakers, the data breach occurred and as **I am in charge of an organisational risk management strategy across three distinct departments** required to perform precise auditing of existing policies compared with ISMS to examine the integrity, availability, and confidentiality of information.

3. CYBER INCIDENT - CONTEXT DESCRIPTION

In this case study, a highly targeted cyber attack is assumed, which lasted for one hour and that gave unauthorised third-party access to the personal information of tens of thousands of clients. Breach accounted for losing personal data such as email addresses, full names, postal addresses, phone numbers, limited payment card data and account data. Also, the company confirmed that attackers did not access card details, PINs, or passwords. The incident was isolated within a few hours and reported to be cleared in two hours of occurrence. However, a broadcast of emails was sent to affected users, most of whom were from the European Union, according to the State Data Protection Inspectorate of Lithuania.

4. INFORMATION SECURITY RISK MANAGEMENT

Answering Point 1 to **baseline risk level, and Usage of ISMS and FAIR** and its steps to implement for assumed organisation policy and practice. From the understanding of ISMS and FAIR and the organisation's situation of heavy loss and project methodology, the **baseline aligns** with ISO27001:2022, which in turn, following **ISMS policy** can help **solve**

challenges **faster in a qualitative** way and also future upgradation and **maintenance will be easy**.

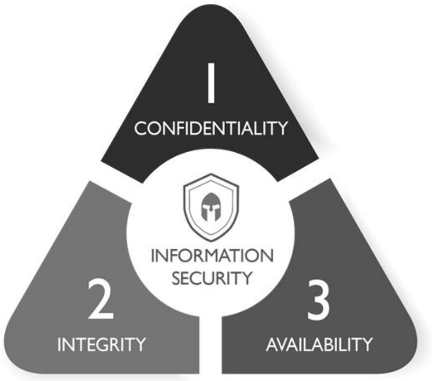


Figure1. ('What is C I A Triad ?', 2021)

Also, in this case, the Availability of the application is intact. However, current and lost users need more confidence in the company data handling process, and the internal integrity of the company itself is lost due to the resignation of top management.
So Fast and upgradable framework, ISMS, suits best in this organisation and situation and we will provide EVIDENCE in the following explanation.

4.1 FAIR - FACTOR ANALYSIS OF INFORMATION RISK.

The Factor Analysis for Information Risk (FAIR), "From a Compliance-based to a Risk-based Approach to Cyber Risk Quantification and Operational Risk". Due to the Risk of the company's different asset directly hitting the business and financial ups and down, an Immediate approach to sort out the problem is to make sure the roots of the issues are handled even before it sprouts. So FAIR classifies Risk into two parts; the Loss Event Frequency and Loss Magnitude, and within them are factors identified to cause magnitude losses. The lost event Frequency helps to understand event occurrence and frequency of records. At the same time, the loss magnitude assesses the primary and secondary Risks of having a vulnerable asset. It is one of the procedures to convenience a company to follow specific steps to follow to sustain threats from different vulnerabilities mandatorily. Also, this can include the use of insurance, a reduction in recurring threats, and a backup business continuity plan.

In the FAIR analysis process, there are four major modules to be assessed the internal steps are not mentioned as figure 1 explains the flow, as listed below
a) Stage 1 Identify components of the scenario
    Step 1 – Identify assets
    Step 2 – Identify the community of threats under consideration.

b) Stage 2 Evaluate Loss Event Frequency (LEF)

- Step 3 – Estimate probable Threat Event Frequency (TEF)
- Step 4 – Estimate Threat Capability (TCAP)
- Step 5 – Estimate Control Strength (CS)
- Step 6 – Derive Vulnerability (Vuln)
- Step 7 – Derive Loss Event Frequency (LEF)

c) Stage 3 Evaluate Probable Loss Magnitude (PLM)

- Step 8 – Estimate worst-case loss
- Step 9 – Estimate probable loss

d) Stage 4 Derive and articulate risk

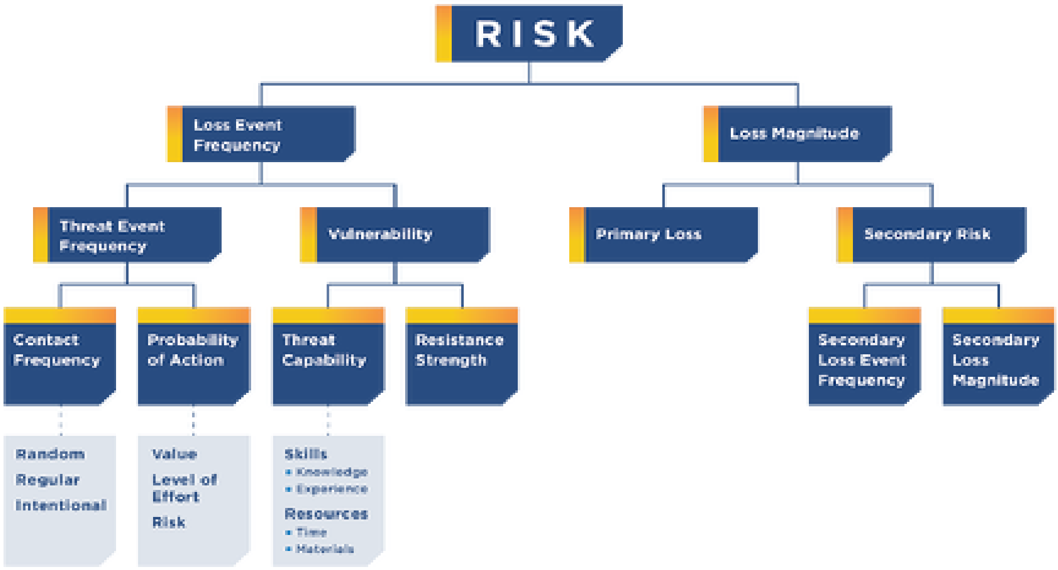


Figure 2: FAIR Stages Flowchart (McCoy, 2017)

4.2 ISMS - INFORMATION SECURITY MANAGEMENT SYSTEM

An effective measure followed to assess threat even before it raises the risk of catastrophic business loss or reputation damage, this approach which is built over ISO27001, helps to question the situation in different angles, which helps to lead to answers that will help to protect the assets of an organisation. Companies implementing ISO/IEC 27001 certification policy will create a safe shield around the internal and sensitive information and helps defend or contain a cyber attack within risk-assessed parameters.

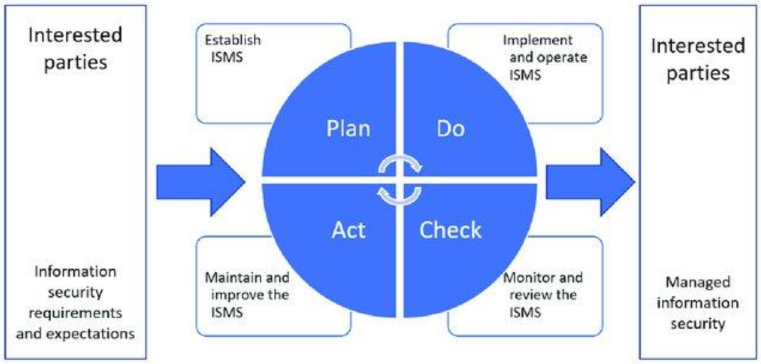

Interested parties
Information security requirements and expectations
Establish ISMS
Implement and operate ISMS
Plan
Do
Act
Check
Maintain and improve the ISMS
Monitor and review the ISMS
Interested parties
Managed information security

Figure 3. Image of ISMS Management implementation from (Mažeika and Butleris, 2020).

The PLAN, DO, CHECK, ACT cycle will help in continuous improvement and also helps in agile projects that are current;y in trend. This also aligns with the secure software development cycle where ISMS is implemented in this research and case study and the ISMS Scope, Steps and Policy are discussed in the next section.

5. IMPLEMENTATION OF ISMS - DETAILED APPROACH

Answering the Point 2:How ISMS approach is helpful in Fin-tech Companies, which aligns with the Agile Project management domain.

5.1 ISMS SCOPE AND STEPS

According to BSI-ISO27001:2022(E) Clause, the main scope of implementation binds with potential vulnerabilities internally and externally present across the security landscape, leading to exposure which enables a cyber incident against the Infrastructure, services and applications.

5.2 ISMS POLICY

The aim and objectives set up according to clauses 5.2 and 6.3 for setting up security objectives which will maintain reputation, business continuity, Resilience and maintain Confidentiality, Integrity and/or Availability bearing the total cost of implementation in mind. **Risk In Detail:** Documents risk assessment, risk Identification, the risk from threat and vulnerability and its impacts, Undertake Risk assessment and report business impacts (and answers Question 2 of requirement). **Risk Control and Treatment:** Evaluation and Metric about risk treatment, Risk Control objectives and implementation of controls, Record the measurement and reduced risk after implementing controls. Finally, statement of applicability.

6. ISMS - RISK IN DETAIL

6.1. RISK ASSESSMENT WITH ISMS AS BASELINE OVER ISO27001

Initially, as an auditor, used the ISO27001 Asset framework to identify assets of the company and implement ISMS on top of it.

From ISO 27001 Asset Management and OCTAVE Framework in this case, the followings are asses for this case study

- **Hardware**
- **Software**
- **Information**
- **Infrastructure**
- **Company Staffs**
- **Outsourced services**

Details are in ANNEX 1: LIST OF ASSETS, from the assessment outcome, different aspects of risk need to be identified by the framed assets from each category.

All the risk that applies to the following domains are considered, and each asset's segregation goes as listed below.

(SEE ANNEX 1 FOR CHART DATA)

1. IT & Infrastructure Domain

   Software Dashboard / Internal Software system, Network Infrastructure, Internal official data, Mail Server, Operating Server. Backup Server, Company Laptop

2. Equipment Domain

   Printer, CC TV, Office Files.RFID System

3. Logistics & Support Services Domain

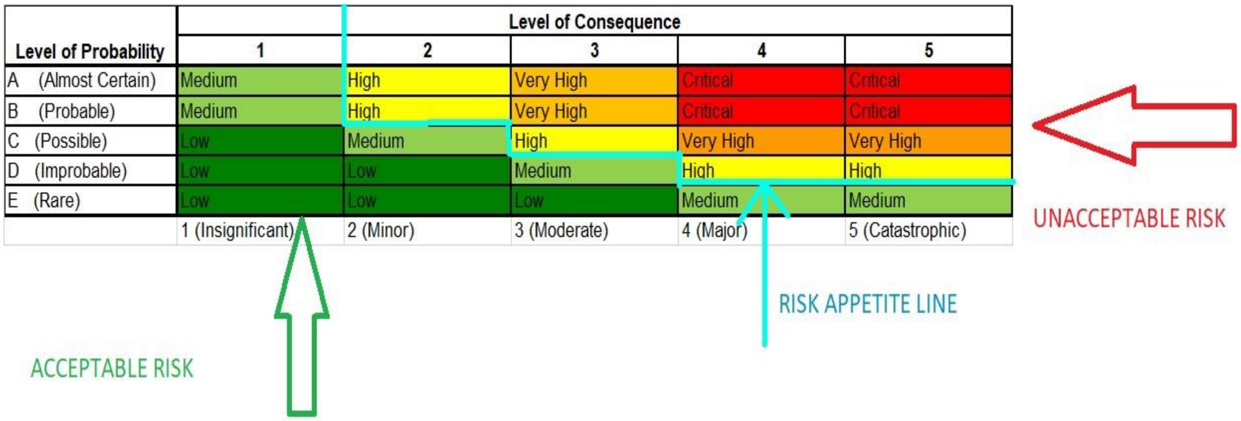
   Payment services, Financial system, payment gateway, Database, Network, Company Data, User sensitive data

6.2. RISK IDENTIFICATION AND APPETITE

From the assets, we identify the risk which is currently in place as well as that may occur in the coming days, there may be a possibility or probability of threats that can be considered Based on the ISO framework, we have followed phases to understand the asset and some of the major incidents are listed below

1. An externally supplied software module of the payment gateway is not checked for security issues and is being used as the supplier instructed.
2. User-side application security has no security policy applied and is found to be a vulnerable open-source app.
3. Company printers log information says it printed some screenshots of the desktop and the incident was ignored.
4. Company laptops have no active directory control and one of the employees found old user personal data.
5. Strong cryptographic encryption for Data storage is used, but Intranet data transfer is in clear text.
6. External API and services are connected for managing disasters and maintaining business continuity but supplier security is unclear.

Based on all the above risk factors and vulnerabilities audited and assessed, the information of acceptable risk is described with the perception of what it is and how it is relevant to this organisation. From figure 4, we understand the risk appetite and ANNEX 2&3 Dives more details



	Level of Consequence				
Level of Probability	1	2	3	4	5
A (Almost Certain)	Medium	High	Very High	Critical	Critical
B (Probable)	Medium	High	Very High	Critical	Critical
C (Possible)	Low	Medium	High	Very High	Very High
D (Improbable)	Low	Low	Medium	High	High
E (Rare)	Low	Low	Low	Medium	Medium
	1 (Insignificant)	2 (Minor)	3 (Moderate)	4 (Major)	5 (Catastrophic)

UNACCEPTABLE RISK
RISK APPETITE LINE
ACCEPTABLE RISK

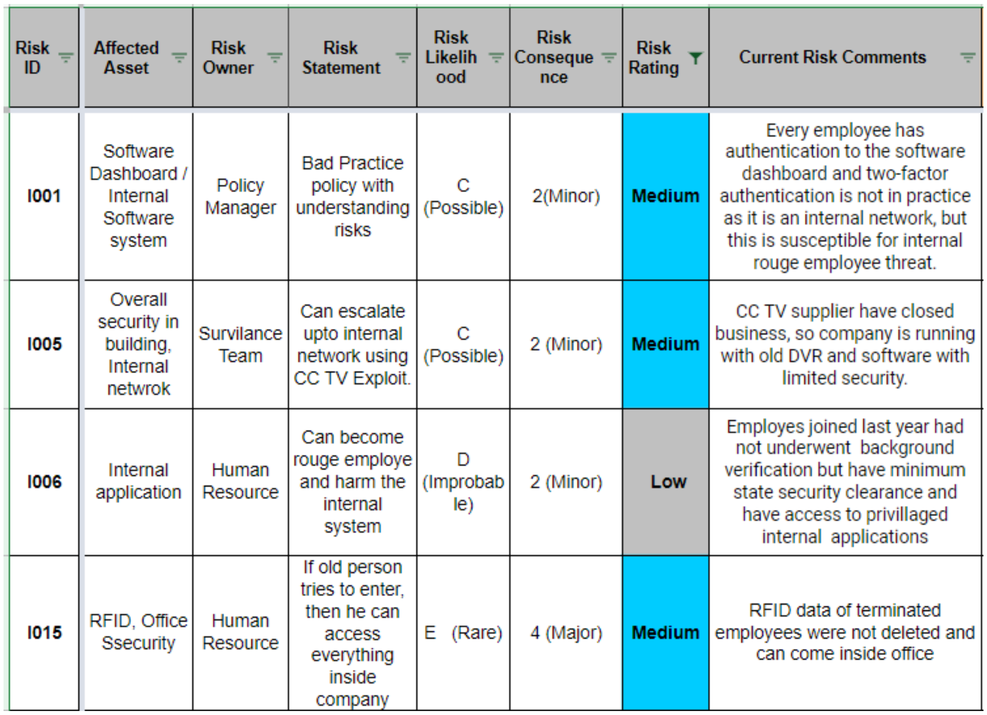
Figure 4: Risk Apatite line and representing unacceptable and acceptable risks

From understanding, Risk Appetite means " risk appetite is the level of risk that an organisation is prepared to take on to achieve its objectives" ('Do You Know Your Cyber Risk Appetite?', n.d.) here, we also discuss risks that organisations expose to, company security priorities, risks that company is immune to and are these risks acceptable. **Here we**

understand that only risk that affects the internal system or it has the capacity to stop the organisation process in such a way that it needs security inspection and recovery process.

From the assessed 18 different issues in the organisation, only four assets are under risk appetite condition as they fall below the very high, risk appetite zone.

- I001 - No present risk, but it might occur rarely
- I005 - If CC tv DVR network is hacked, either the hacker can surveillance the office or delete the recording data, but no effect to the organisation's running systems.
- I006 - Improper background verification process, needs verification from the Human Resource department, there is no existing threat
- I015 - Again, Human Resource, Terminated employs RFID is still working, which they used to access entry to office, This is unacceptable, but no immediate threat.



Risk ID	Affected Asset	Risk Owner	Risk Statement	Risk Likelihood	Risk Consequence	Risk Rating	Current Risk Comments
I001	Software Dashboard / Internal Software system	Policy Manager	Bad Practice policy with understanding risks	C (Possible)	2(Minor)	Medium	Every employee has authentication to the software dashboard and two-factor authentication is not in practice as it is an internal network, but this is susceptible for internal rouge employee threat.
I005	Overall security in building, Internal netwrok	Survilance Team	Can escalate upto internal network using CC TV Exploit.	C (Possible)	2 (Minor)	Medium	CC TV supplier have closed business, so company is running with old DVR and software with limited security.
I006	Internal application	Human Resource	Can become rouge employe and harm the internal system	D (Improbable)	2 (Minor)	Low	Employes joined last year had not underwent background verification but have minimum state security clearance and have access to privillaged internal applications
I015	RFID, Office Ssecurity	Human Resource	If old person tries to enter, then he can access everything inside company	E (Rare)	4 (Major)	Medium	RFID data of terminated employees were not deleted and can come inside office

Figure 5. Screenshot from worked ISMS Risk-Rigister.

All other analysis is attached in ANNEX 4

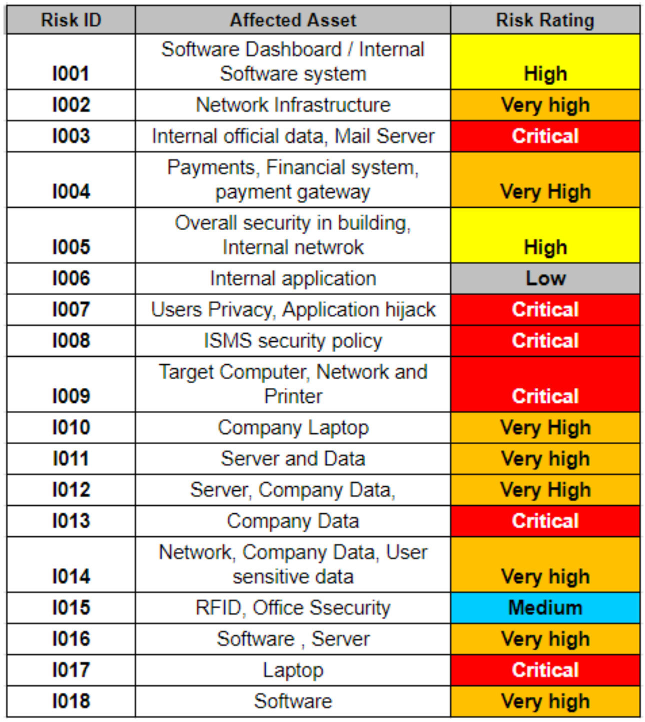
7. RISK CONTROLS AND TREATMENT

To Answer Point 3, The effectiveness of controls (risk response) be measured **using ISO/IEC 27001 implementation chart.** And using ISMS Risk Register, risk quantification measures and metrics are **measured from LOW to CRITIAL.**

Using the ISMS Current / Treated Risk Matrix to aid in assessing the risks identified of the Likelihood Vs Impact. A quantitative approach is touched as qualitative requires more time, which should be done since it looks at the risk at more in-depth in the following chart
Some of the risk treatment measures discussed below for the mentioned risk are as:

- Make sure network engineers apply Intrusion Prevention System
- Undertake security scrutinisation of employees under Screening criteria
- Terminate the use of open source applications and develop in-house for security stake of user-sensitive information
- Remove all old accounts and sensitive data from the database
  Others are listed and attached in Annex3

Risk quantification and metrics is the part of the major discussion area, From Figure 6, all the risks and its rating are mentioned, which summaries that most of the current procedures are not up to point and fall under the critical conditions which must be fixed ASAP.



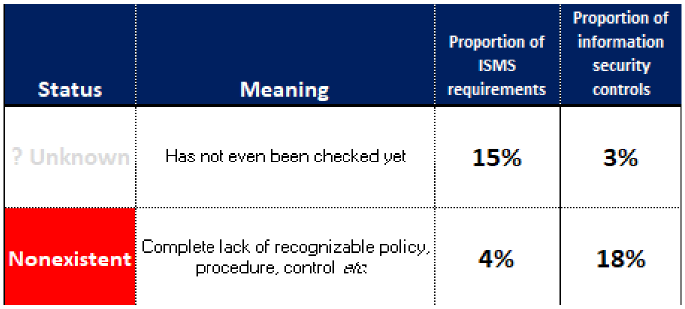
Risk ID	Affected Asset	Risk Rating
I001	Software Dashboard / Internal Software system	High
I002	Network Infrastructure	Very high
I003	Internal official data, Mail Server	Critical
I004	Payments, Financial system, payment gateway	Very High
I005	Overall security in building, Internal netwrok	High
I006	Internal application	Low
I007	Users Privacy, Application hijack	Critical
I008	ISMS security policy	Critical
I009	Target Computer, Network and Printer	Critical
I010	Company Laptop	Very High
I011	Server and Data	Very high
I012	Server, Company Data,	Very High
I013	Company Data	Critical
I014	Network, Company Data, User sensitive data	Very high
I015	RFID, Office Ssecurity	Medium
I016	Software , Server	Very high
I017	Laptop	Critical
I018	Software	Very high

Figure 6: Sorted Risk Matrix

Straight to the point, The control measures helped, and the Infosec control pie chart defines the possible risk and their effects. Have performed based on assumed data and 18 points of risk from ANNEX 3.

To understand the status better, we have mentioned the complete implementation of **Mandatory ISMS requirements** as well, as all 133 clauses are defined and attached in ANNEX 3 where ISMS helped understand the risk in a fast-paced environment.

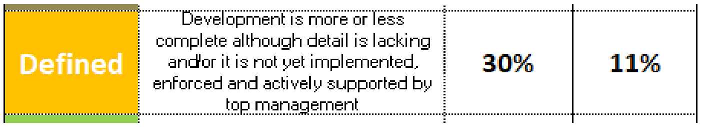
The effectiveness of risk control results shows that many clauses is in place, and almost 30% of basics are defined, but the proportion results show many are not in practise, and almost 18% are non-existent. Around 15% have not been checked yet and as ISO 27001 Suggest those that have not been checked might cause more than what is assessed already. So Initially, we need to address these first **this is also a major part of the ongoing risk,** and the major next threat can develop from this point.



Status	Meaning	Proportion of ISMS requirements	Proportion of information security controls
? Unknown	Has not even been checked yet	15%	3%
Nonexistent	Complete lack of recognizable policy, procedure, control etc.	4%	18%

Figure 8 : Analysis Result - Nonexistent

Also, from Figure 10 it is evident that most of the policies are in place but have yet to be practised, only enforcing the criteria to practise also can solve all the internal issues and help other teams to overcome the risk and threats that the company is facing.



Defined	Development is more or less complete although detail is lacking and/or it is not yet implemented, enforced and actively supported by top management	30%	11%

Figure 10 : Analysis Result - Limited

All other analysis is attached in ANNEX 5

8. DOMAIN-BASED CRITICAL REFLECTION AND CONCLUSION

The analysis funnelled to the critical evaluation outcome is as follows:

- ☑ The main point of analysis is how to reduce risk and where to reduce risk.
- ☑ Which domain is under major risk
- ☑ How business reputation can be saved immediately with the risk treatment.
- ☑ Where can Confidentiality and Integrity be tightened
- ☑ How Availability can be leveraged with business
- ☑ The end economic and reputation gain out of the analysis.

ISO27001 helped to understand the essential requirement of security, where ISMS control strategies helped funnelling the risk by risk identification, thereat and Vulnerability. Nevertheless, the study on FAIR-U is complex in an urgent situation as the log analysis required the Finance department's intervention for marking gains and losses, although it has sophisticated tools.

1. IT & Infrastructure
2. Equipment
3. Logistics & Support services

Out of all, there were many critical risks, including Antivirus and Active Directory missing in work-from-home laptops and the Usage of externally supplied payment API falling under extreme risk to the company. However, by ANNEX 4 most of all problems could be addressed and only 3% fell under Unknown criteria of controls. Also, the after-effects and risk treatment had only one risk falling above the risk appetite level, which is the same as external API for payment, where this is a supplier issue and no control from inside the company; hence, this must be addressed carefully.

I strongly recommend ISMS over ISO27001 to get the company back on track and helping upgrade the business and recover the financial loss, also proportionally gain user confidence.

All these show the efficiency of ISMS and implemented quality among various risk.

The final statement, **"If you don`t invest in risk management, it doesn`t matter what business you`re in, it's a risky business."** Cohn(n.d)

9. ANNEX

ANNEX 1: LIST OF ASSETS

ANNEX 2: ASSET VS RISK MATCH AND TREATMENT DECISION

ANNEX 3: RISK LEVEL BEFORE AND AFTER CONTROLS

ANNEX 4: ISMS - RISK REGISTER

ANNEX 5: MANDATORY ISMS REQUIREMENT IMPLEMENTED

ANNEX 6: ANNEX A CONTROLS IMPLEMENTED

ANNEX 7: METRICS RESULTS

10. REFERENCES

‘Do You Know Your Cyber Risk Appetite?’ (no date) *www.dig8ital.com*. [online]. Available from: https://www.dig8ital.com/post/its-time-to-identify-your-cyber-security-risk-appetite [Accessed 16 December 2022].

‘Global Leadership’ (no date) *Revolut*. [online]. Available from: https://www.revolut.com/leadership-and-governance/.

Mažeika, D. and Butleris, R. (2020) MBSEsec: Model-Based Systems Engineering Method for Creating Secure Systems. *Applied Sciences*. [online]. 10 (7), p.2574.

Cohn, G. (n.d) Risk Warden - Blogs - Compliance and Risk Management. Available from: https://riskwarden.com/blog/ [Accessed 16 December 2022].

McCoy, V. (2017) *FAIR On-A-Page: Same Great Model, Fresh New Look www.fairinstitute.org*.17 May 2017 [online]. Available from: https://www.fairinstitute.org/blog/fair-model-on-a-page.

Ohr, T. (2019) *Revolut aims to transform business banking with the launch of new accounts EU-Startups*.24 July 2019 [online]. Available from: https://www.eu-startups.com/2019/07/revolut-aims-to-transform-business-banking-with-the-launch-of-new-accounts/ [Accessed 12 December 2022].

Tunggal, A. (2022) *What is Information Risk Management? | UpGuard www.upguard.com*.19 June 2022 [online]. Available from: https://www.upguard.com/blog/information-risk-management.

‘What is C I A Triad ?’ (2021) *howtoinfosec*.12 March 2021 [online]. Available from: https://howtoinfosec.com/2021/03/12/c-i-a-triad/ [Accessed 16 December 2022].

ANNEX 01 : LIST OF ASSETS

Hardware	Software	Information	Infrastructure	Company Staff	Outsourced Services
Laptops Servers Printers Point of Sale Devices Entry security devices CC Camera DVR and Hard Disk.	User App, App for Business owners Payment Gateway Continuity API Company Human Resource Management Software Enterprise resource planning(ERP) Software	All legal policy data Credit and Debit Card Details User private and confidential information like passwords etc. Authentication user details saved in database Excel sheets about latest leads Customers enquiry forms	Head Office Parking Lot Generator room Power Room CC TV and Air conditioning monitoring room	From the Chief Operating Officer to till the security staffs who are allow people inside the office.	Business Continuity API and server

ANNEX 02: ASSET VS RISK MATCH AND TREATEMENT DECISION

Affected Asset	Risk Statement	Current Risk Comments	Risk Treatment Decision
Software Dashboard / Internal Software system	Bad Practice policy with understanding risks	Every employee has authentication to the software dashboard and two-factor authentication is not in practice as it is an internal network, but this is susceptible for internal rouge employee threat.	Mitigate
Network Infrastructure	incocious use of known techlical solution	Company network is fairly secured by firewall with intrusion detection but intrusion prevention and SIEM tools are not installed.	Avoid
Internal official data, Mail Server	Lead to leak of sensitive details, abuse can harm employes mental health.	Emails are not monitored under community guidelines and accept abusive words in clear text. Also employees communicate official information via WhatsApp.	Mitigate and Accept
Payments, Financial system, payment gateway	Total financial chaos, unavoidable risk of payments	An externally supplied software module of the payment gateway is not checked for security issues and is being used as the supplier instructed.	Mitigate
Overall security in building, Internal netwrok	Can escalate upto internal network using CC TV Exploit.	CC TV supplier have closed business, so company is running with old DVR and software with limited security.	Accept
Internal application	Can become rouge employe and harm the internal system	Employes joined last year had not underwent background verification but have minimum state security clearance and have access to privillaged internal applications	Mitigate
Users Privacy, Application hijack	Open source are vulnerable as code is public	User side application security has no security policy applied and found to be vulnerable open source app	Avoid
ISMS security policy	Outdated security measures risk everythhing in company	No external or SME consultation records found for security policy and followed old fashion security adapted by old managers	Mitigate
Target Computer, Network and Printer	investigation not done, printers can be used to hack whole company system	Company printers log information says it printed some screenshots of desktop and incident was ignored	Avoid
Company Laptop	No control over laptop, Company privacy at risk	Company laptops has no active directory control and one of the employe found old user personal data.	Mitigate
Server and Data	USB can be a threat to install malcious software to entire service	USB and harddisk are used in server room, no physical checking is in place.	Avoid
Server, Company Data,	If passwords is compromised or cracked then server can be compromised	Login to backup server has only single authentication.	Mitigate
Company Data	Can send and recive any internal information	Resigned employe emails accounts are still active.	Avoid
Network, Company Data, User sensitive data	Compromised intranet gives access to everything in company	Strong cryptographic encryption for Data storage is used, but Intranet data transfer is in clear text.	Avoid
RFID, Office Ssecurity	If old person tries to enter, then he can access everything inside company	RFID data of terminated employees were not deleted and can come inside office	Avoid
Software , Server	Testing environment can bring n additional risk due to lack of configuration	Testing of new application is performed in same operational environment without password for test machines	Avoid
Laptop	All laptops are suseptible for virus attack	Antivirus is good and updated in company systems, laptops don’t have any.	Mitiagte
Software	Running business will be vulnerable during disaster when in API mode	External API and services are connected for managing disaster and maintaining business continuity but supplier security is unclear	Accept

ANNEX 03: RISK LEVEL BEFORE AND AFTER CONTROLS

Risk ID	Affected Asset	Risk Rating Before Controls	Risk After Treatemetn and Control
I001	Software Dashboard / Internal Software system	**High**	**Low**
I002	Network Infrastructure	**Very high**	**Low**
I003	Internal official data, Mail Server	**Critical**	**Medium**
I004	Payments, Financial system, payment gateway	**Very High**	**Low**
I005	Overall security in building, Internal netwrok	**High**	**Low**
I006	Internal application	**Low**	**Low**
I007	Users Privacy, Application hijack	**Critical**	**Low**
I008	ISMS security policy	**Critical**	**Low**
I009	Target Computer, Network and Printer	**Critical**	**Low**
I010	Company Laptop	**Very High**	**Low**
I011	Server and Data	**Very high**	**Low**
I012	Server, Company Data,	**Very High**	**Low**
I013	Company Data	**Critical**	**Low**
I014	Network, Company Data, User sensitive data	**Very high**	**Low**
I015	RFID, Office Ssecurity	**Medium**	**Low**
I016	Software , Server	**Very high**	**Medium**
I017	Laptop	**Critical**	**Low**
I018	Software	**Very high**	**high**

ANNEX 04: ISMS - RISK REGISTER

Risk ID	Affected Asset	Risk Owner	Risk Statement	Risk Likelihood	Risk Consequence	Risk Rating	Current Risk Comments	Control areas for existing controls	Risk Treatment Decision	Risk Treatment Plan	Control areas for new treatment measures	Treated Residual Risk Likelihood	Treated Residual Risk Consequence	Treated Residual Risk
I001	Software Dashboard / Internal Software system	Policy Manager	Bad Practice policy with understanding risks	B (Probable)	2(Minor)	**High**	Every employee has authentication to the software dashboard and two-factor authentication is not in practice as it is an internal network, but this is susceptible for internal rouge employee threat.		Mitigate	Make two factor authentication as manditory organisation technical policy	A.5 27 A. 8.9	E (Rare)	3 (Moderate)	**Low**
I002	Network Infrastructure	Network Security Engineer	incocious use of known techlical solution	B (Probable)	3 (Moderate)	**Very high**	Company network is fairly secured by firewall with intrusion detection, but intrusion prevention and SIEM tools are not installed.		Avoid	Make sure network engineers apply IPS	A13.1.2 A7.2.2	E (Rare)	1 (insignificant)	**Low**
I003	Internal official data, Mail Server	Communication policy Manager	Lead to leak of sensitive details, abuse can harm employes mental health.	A (Almost Certain)	4 (Major)	**Critical**	Emails are not monitored under community guidelines and accept abusive words in clear text. Also employees communicate official information via WhatsApp.		Mitigate and Accept	Mitigate the use of abuse words and terminate the external communication system in office, but inavoidable.	A13.2.4 A13.2.1 13.2.2	C (Possible)	2 (Minor)	**Medium**
I004	Payments, Financial system, payment gateway	Software testing and Secure Software development team	Total financial chaos, unavoidable risk of payments	C (Possible)	4 (Major)	**Very High**	An externally supplied software module of the payment gateway is not checked for security issues and is being used as the supplier instructed.		Mitigate	Stop the use and immedately check for vulnerabilities in the outsourced module	A14.2.1 A14.2.3 A15.1.1 A15.2.1	E (Rare)	1 (insignificant)	**Low**
I005	Overall security in building, Internal netwrok	Survilance Team	Can escalate upto internal network using CC TV Exploit.	C (Possible)	3 (Moderate)	**High**	CC TV supplier have closed business, so company is running with old DVR and software with limited security.		Accept	Separate the cc tv network and check for security vulnerability, Change if necessary	A11.2.3 A11.1.3 A13.1.3 A15.2.2	C (Possible)	1 (Insignificant)	**Low**
I006	Internal application	Human Resource	Can become rouge employe and harm the internal system	D (Improbable)	2 (Minor)	**Low**	Employes joined last year had not underwent background verification but have minimum state security clearance and have access to privillaged internal applications		Mitigate	Undertake security scrutinisation of employes under this crieteria	A7.1.1 A7.2.1 A9.2.6	E (Rare)	2 (Minor)	**Low**
I007	Users Privacy, Application hijack	Software testing and Secure Software development team	Open source are vulnerable as code is public	B (Probable)	4 (Major)	**Critical**	User side application security has no security policy applied and found to be vulnerable open source app		Avoid	Terminate the use of open source application and develop inhouse for security stake of user sensitive information	A14.2.1 A14.2.2 A14.2.5	E (Rare)	1 (Insignificant)	**Low**
I008	ISMS security policy	Internal Security Consultant	Outdated security measures risk everything in company	A (Almost Certain)	5 (Catastrophic)	**Critical**	No external or SME consultation records found for security policy and followed old fashion security adapted by old managers		Mitigate	Update all security policy according to current date and procedure	A17.1.1 A17.1.3 A6.1.1 A6.1.4	D (Unlikely)	2 (Minor)	**Low**
I009	Target Computer, Network and Printer	Security Engineer	investigation not done, printers can be used to hack whole company system	A (Almost Certain)	4 (Major)	**Critical**	Company printers log information says it printed some screenshots of desktop and incident was ignored		Avoid	Check what caused and investigate and then avoid such incident further.	A11.2.2 A11.2.9 A16.1.4 A16.1.7	E (Rare)	1 (Insignificant)	**Low**
I010	Company Laptop	Human Resource and Security Engineer	No control over laptop, Company privacy at risk	C (Possible)	4 (Major)	**Very High**	Company laptops has no active directory control and one of the employe found old user personal data.		Mitigate	Apply security measures and hr dept to deliver device in clean state.	A7.2.2 A8.1.4 A10.1.2 A9.4.3 A12.1.2 A12.5.1 A18.1.4 A16.1.5	E (Rare)	2 (Minor)	**Low**
I011	Server and Data	Security Checking Staff	USB can be a threat to install malcious software to entire service	C (Possible)	5 (Catastrophic)	**Very high**	USB and harddisk are used in server room, no physical checking is in place.		Avoid	Restrict use of USB in office environment	A8.3.1 A11.2.6 A14.2.6 A12.1.1 A11.1.3 A11.1.2	E (Rare)	3 (Moderate)	**Low**
I012	Server, Company Data,	Server Security Team	If passwords is compromised or cracked then server can be compromised	C (Possible)	5 (Catastrophic)	**Very High**	Login to backup server has only single authentication.		Mitigate	Use additional multi factor authentication	A9.4.2 A9.1.2 A9.3.1 A13.1.2	E (Rare)	3 (Moderate)	**Low**
I013	Company Data	Human Resource	Can send and recive any internal information	B (Probable)	4 (Major)	**Critical**	Resigned employe emails accounts are still active.		Avoid	Remove all old accounts and sensitive data	A9.2.1 A9.2.6 A12.1.2 A16.1.5 A13.1.2 A12.7.1	E (Rare)	2 (Minor)	**Low**
I014	Network, Company Data, User sensitive data	Network Security Engineer	Compromised intranet gives access to everything in company	C (Possible)	5 (Catastrophic)	**Very high**	Strong cryptographic encryption for Data storage is used, but Intranet data transfer is in clear text.		Avoid	Use encryption or VPN for internal communication	A13.1.2 A10.1.1 A14.1.2 A12.6.1 A14.2.6 A17.1.1	E (Rare)	1 (Insignificant)	**Low**
I015	RFID, Office Ssecurity	Human Resource	If old person tries to enter, then he can access everything inside company	E (Rare)	4 (Major)	**Medium**	RFID data of terminated employees were not deleted and can come inside office		Avoid	Delete the old data and ask Human Resource team sould take trainig and assess entry security	A11.1.2 A7.2.1 A7.2.2 A7.3.1 A9.2.6	E (Rare)	1 (Insignificant)	**Low**

I016	Software , Server	Software testing and Secure Software development team	Testing environment can bring n additional risk due to lack of configuration	B (Probable)	3 (Moderate)	**Very high**	Testing of new application is performed in same operational environment without password for test machines		Avoid	Separate test and live environment and use proper access control	A12.1.4 A14.3.1 A14.2.6 **A12.1.1** A17.1.3 A9.2.6	E (Rare)	4 (Major)	**Medium**
I017	Laptop	Security Engineers	All laptops are suseptible for virus attack	A (Almost Certain)	5 (Catastrophic)	**Critical**	Antivirus is good and updated in company systems, laptops don't have any.		Mitiagte	Install necessary protection for all official devices	A11.2.1 A12.2.1 A14.2.6 A18.1.1 A17.1.3	E (Rare)	2 (Minor)	**Low**
I018	Software	Software testing and Secure Software development team	Running business will be vulnerable during disaster when in API mode	C (Possible)	5 (Catastrophic)	**Very high**	External API and services are connected for managing disaster and maintaining business continuity but supplier security is unclear		Accept	Maintain security review protocols but avoid loose ends	A18.2.1 A17.1.3 A17.2.1	C (Possible)	3 (Moderate)	**high**

ANNEX 05: MANDITORY ISMS REQUIREMENTS IMPLEMENTED

Status of ISO/IEC 27001 implementation

Section	ISO/IEC 27001 requirement	Status	Notes
4	**Context of the organisation**		
4.1	**Organisational context**		
4.1	Determine the organization's **ISMS objectives** and any issues that might affect its effectiveness	Defined	Standard ISMS policy in place, but not refind and audited based on company upgradation.
4.2	**Interested parties**		
4.2 (a)	Identify **interested parties** including applicable laws, regulations, contracts *etc*.	Optimized	All the laws and regulations are followed with the help of external legal advisor.
4.2 (b)	Determine their information security-relevant **requirements** and obligations	Limited	No record of background verification of legal advisors before selection.
4.3	**ISMS scope**		
4.3	Determine and document the **ISMS scope**	Defined	The scope is defined well and satisfies ISO27001 requirements
4.4	**ISMS**		
4.4	Establish, implement, maintain and continually improve an **ISMS** according to the standard!	Nonexistent	No recent update on policy, hence some assets seem vulnerable.
5	**Leadership**		
5.1	**Leadership & commitment**		
5.1	Top management must demonstrate **leadership & commitment** to the ISMS	Defined	Commitment to application is in place, followed based on flexibility.
5.2	**Policy**		
5.2	Document the **information security policy**	Initial	Rarely checked and update of policy which led to the mishandling of some internal data.
5.3	**Organizational roles, responsibilities & authorities**		
5.3	Assign and communicate information security **rôles & responsibilities**	Managed	Security Managers and Policy Managers are hired nad designated in the company.
6	**Planning**		
6.1	**Actions to address risks & opportunities**		
6.1.1	Design/plan the ISMS to satisfy the requirements, addressing risks & opportunities	Limited	No recent chnages found and vulnerability not addressed.
6.1.2	Define and apply an **information security risk assessment process**	Defined	Procedure is in practice, but limited to top management.
6.1.3	Document and apply an **information security risk treatment process**	Initial	No records from last 8 months.
6.2	**Information security objectives & plans**		
6.2	Establish and document the **information security objectives and plans**	Managed	Documents present as per objectives,biut not followd in practice
7	**Support**		
7.1	**Resources**		
7.1	Determine and allocate necessary **resources** for the ISMS	Defined	Yes, resource are present to support the ISMS
7.2	**Competence**		
7.2	Determine, document and make available necessary **competences**	Initial	No enugh practice of competences
7.3	**Awareness**		
7.3	Establish a **security awareness** program	Limited	Started thw awareness due to incident, but have lot more to finish
7.4	**Communication**		
7.4	Determine the need for **internal and external communications** relevant to the ISMS	Limited	Strategy are defind and practised amoung old employes
7.5	**Documented information**		
7.5.1	Provide **documentation** required by the standard plus that required by the organization	Optimized	All applicable documents are available
7.5.2	Provide document **titles**, authors *etc*., **format** them consistently, and **review & approve** them	Defined	restricted tol last year employees
7.5.3	**Control the documentation** properly	Limited	Yes, all policies are maintained
8	**Operation**		
8.1	**Operational planning and control**		
8.1	Plan, implement, control & document ISMS processes to manage risks (*i.e.* a **risk treatment plan**)	Limited	Will finishing planning phase in few weeks
8.2	**Information security risk assessment**		
8.2	**(Re)assess & document information security risks** regularly & on changes	? Unknown	Not worked yet
8.3	**Information security risk treatment**		
8.3	Implement the risk treatment plan **(treat the risks!)** and document the results	? Unknown	Not worked yet
9	**Performance evaluation**		
9.1	**Monitoring, measurement, analysis and evaluation**		
9.1	**Monitor, measure, analyze and evaluate** the ISMS and the controls	Defined	Documentation is comlete, but not evaluvated to implement
9.2	**Internal audit**		
9.2	Plan & conduct **internal audits** of the ISMS	Managed	One phase of audit is complete 8 months ago
9.3	**Management review**		
9.3	Undertake regular **management reviews** of the ISMS	Defined	Documented but not enfored in action plan
10	**Improvement**		
10.1	**Nonconformity and corrective action**		
10.1	Identify, fix and take action to prevent recurrence of **nonconformities**, documenting the actions	? Unknown	Now work in action plan
10.2	**Continual improvement**		
10.2	Continually **improve** the ISMS	? Unknown	Not started yet

ANNEX 06: ANNEX A - IMPLEMENTED

Statement of Applicability and status of information security controls

Section	Information security control	Status	Notes
A5	**Information security policies**		
A5.1	**Management direction for information security**		
A5.1.1	Policies for information security	Limited	Policies are in place and planned to implement
A5.1.2	Review of the policies for information security	Nonexistent	There was no update for policy as the technology updated
A6	**Organization of information security**		
A6.1	**Internal organization**		
A6.1.1	Information security roles and responsibilities	Optimized	All the roles and human resources available to take actions
A6.1.2	Segregation of duties	Optimized	Duties are defined
A6.1.3	Contact with authorities	Defined	Contacted administration team, but no response and update
A6.1.4	Contact with special interest groups	? Unknown	No extrernal SME consulted for issue
A6.1.5	Information security in project management	Initial	Only principles are known but not in place
A6.2	**Mobile devices and teleworking**		
A6.2.1	Mobile device policy	? Unknown	Everyone are on their own and no policy defined
A6.2.2	Teleworking	Defined	Intercom and emails regulations are in place
A7	**Human resource security**		
A7.1	**Prior to employment**		
A7.1.1	Screening	? Unknown	No screening was done from last year
A7.1.2	Terms and conditions of employment	Limited	Yes, there are, only limited to old operations
A7.2	**During employment**		
A7.2.1	Management responsibilities	Optimized	All management teams follow to achive goals
A7.2.2	Information security awareness, education and training	Initial	No special trainings have been conducted for cyber awareness
A7.2.3	Disciplinary process	Limited	Employees are on their own and bad culture in place, only few termination rocords
A7.3	**Termination and change of employment**		
A7.3.1	Termination or change of employment responsibilities	Defined	Terminated, but retained the relation digitally
A8	**Asset management**		
A8.1	**Responsibility for assets**		
A8.1.1	Inventory of assets	Managed	All the assets are under policy structure and maintained
A8.1.2	Ownership of assets	Optimized	All the assets are managed by perticular domain manager
A8.1.3	Acceptable use of assets	Managed	Aassets are in useful condition and working normally
A8.1.4	Return of assets	Optimized	Records and log book maintained for dispatched assests like : laptop etc
A8.2	**Information classification**		
A8.2.1	Classification of information	Managed	All the inforamtion is classifed based on domain
A8.2.2	Labelling of information	Managed	All information are defind since an year
A8.2.3	Handling of assets	Defined	Some abnormalities are found in usage, not minitored
A8.3	**Media handling**		
A8.3.1	Management of removable media	Initial	Bad practice os use of USB devices
A8.3.2	Disposal of media	Nonexistent	No care taken to wipe previous user data
A8.3.3	Physical media transfer	Not applicable	Not applicable
A9	**Access control**		
A9.1	**Business requirements of access control**		
A9.1.1	Access control policy	Limited	Some basic security in palce
A9.1.2	Access to networks and network services	Defined	Proper authentication used and maintained
A9.2	**User access management**		
A9.2.1	User registration and de-registration	Nonexistent	Bad maintenance, emails and other data left behind
A9.2.2	User access provisioning	Initial	Only access given ,some face issues
A9.2.3	Management of privileged access rights	Limited	Defined but not in practise
A9.2.4	Management of secret authentication information of users	Managed	User side is more secure, but internally in clear text
A9.2.5	Review of user access rights	Optimized	All user rights are defined and practised

Statement of Applicability and status of information security controls

Section	Information security control	Status	Notes
A9.2.6	Removal or adjustment of access rights	Nonexistent	Old employs can access mails, bad practise
A9.3	**User responsibilities**		
A9.3.1	Use of secret authentication information	Defined	Only single factor is used , crtitcal issue
A9.4	**System and application access control**		
A9.4.1	Information access restriction	Managed	All users have proper rights assigned for access
A9.4.2	Secure log-on procedures	Optimized	Dashboard is secuired with login process
A9.4.3	Password management system	Optimized	Proper encrypted password storage
A9.4.4	Use of privileged utility programs	Managed	Privilages are defined and practised
A9.4.5	Access control to program source code	Optimized	Yes, only management team have access to secure codes.
A10	**Cryptography**		
A10.1	**Cryptographic controls**		
A10.1.1	Policy on the use of cryptographic controls	Initial	No control for internal network
A10.1.2	Key management	Limited	Bad key practiose for intranet in office
A11	**Physical and environmental security**		
A11.1	**Secure areas**		
A11.1.1	Physical security perimeter	Optimized	CC TV in place and security roam in perimeter
A11.1.2	Physical entry controls	Managed	Office entry is with RFID, and physical check
A11.1.3	Securing offices, rooms and facilities	Managed	RFID access to rooms
A11.1.4	Protecting against external and environmental threats	Nonexistent	No external caretaken, old RFID data still present
A11.1.5	Working in secure areas	Defined	Office is secured with some restrictions
A11.1.6	Delivery and loading areas	Not applicable	
A11.2	**Equipment**		
A11.2.1	Equipment siting and protection	Managed	Proper mangement of equipments are in place
A11.2.2	Supporting utilities	Not applicable	
A11.2.3	Cabling security	Initial	No specific wired intrusion detection in place
A11.2.4	Equipment maintenance	Limited	Only in documentation, not dine since a year
A11.2.5	Removal of assets	Initial	Old printers are still connected to network
A11.2.6	Security of equipment and assets off-premises	Not applicable	
A11.2.7	Secure disposal or reuse of equipment	Nonexistent	Very bad practise, old dat exists
A11.2.8	Unattended user equipment	Defined	Policy of clean tabel in place
A11.2.9	Clear desk and clear screen policy	Optimized	Policy in place and everyone follows
A12	**Operations security**		
A12.1	**Operational procedures and responsibilities**		
A12.1.1	Documented operating procedures	Managed	SOP in practise
A12.1.2	Change management	Initial	Not under maintenance
A12.1.3	Capacity management	Limited	Human resource are under pressure
A12.1.4	Separation of development, testing and operational environments	Nonexistent	All environment reside in same server and disruptions found
A12.2	**Protection from malware**		
A12.2.1	Controls against malware	Optimized	Office system have security
A12.3	**Backup**		
A12.3.1	Information backup	Optimized	Remote server is used for backup
A12.3	**Logging and monitoring**		
A12.4.1	Event logging	Initial	No SIEM tool used
A12.4.2	Protection of log information	Nonexistent	No logs
A12.4.3	Administrator and operator logs	Nonexistent	No Logs
A12.4.4	Clock synchronisation	Nonexistent	Not in practise
A12.5	**Control of operational software**		
A12.5.1	Installation of software on operational systems	Optimized	Lisenced OS used and installed
A12.6	**Technical vulnerability management**		
A12.6.1	Management of technical vulnerabilities	Limited	Only threats are mitigated
A12.6.2	Restrictions on software installation	Nonexistent	No active directory rules defined
A12.7	**Information systems audit considerations**		

Statement of Applicability and status of information security controls

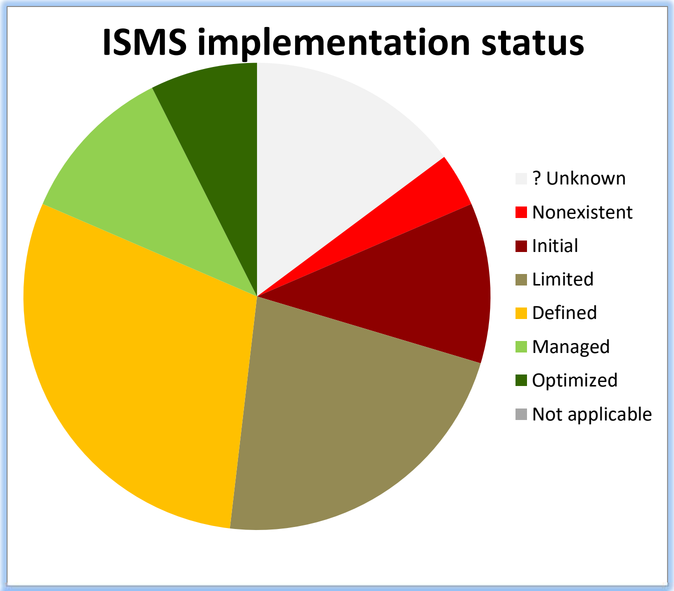
Section	Information security control	Status	Notes
A12.7.1	Information systems audit controls	Initial	Only limited understanding
A13	**Communications security**		
A13.1	**Network security management**		
A13.1.1	Network controls	Defined	Office system have Intrusion detection system
A13.1.2	Security of network services	Initial	SIEM andIntrusion Prevention just initiated to apply
A13.1.3	Segregation in networks	Managed	All network operate in a good way
A13.2	**Information transfer**		
A13.2.1	Information transfer policies and procedures	Initial	No procedure followed
A13.2.2	Agreements on information transfer	Nonexistent	Not in practise
A13.2.3	Electronic messaging	Nonexistent	Bad policy, Using external communication methods
A13.2.4	Confidentiality or nondisclosure agreements	Limited	NDA is signed while joinign
A14	**System acquisition, development & maintenance**		
A14.1	**Security requirements of information systems**		
A14.1.1	Information security requirements analysis and specification	Managed	Top managemet follow things properly
A14.1.2	Securing application services on public networks	Optimized	Cryptopgraphic encryption in place for user application
A14.1.3	Protecting application services transactions	Optimized	AS in policy , everything is normal
A14.2	**Security in development and support processes**		
A14.2.1	Secure development policy	Limited	Only few departments follow
A14.2.2	System change control procedures	Initial	No change mangement procedure in place
A14.2.3	Technical review of applications after operating platform changes	Not applicable	
A14.2.4	Restrictions on changes to software packages	Nonexistent	No restrictions found
A14.2.5	Secure system engineering principles	Not applicable	
A14.2.6	Secure Development Environment	Managed	Environment is secuired with necessary protection
A14.2.7	Outsourced development	Nonexistent	Bad outsourcing policy, not reviwed suppliers
A14.2.8	System security testing	Nonexistent	No testing phase
A14.2.9	System acceptance testing	Nonexistent	Not in practise
A14.3	**Test data**		
A14.3.1	Protection of test data	Initial	only basic protection
A15	**Supplier relationships**		
A15.1	**Information security in supplier relationships**		
A15.1.1	Information security policy for supplier relationships	Nonexistent	Not scrutinised supplier background
A15.1.2	Addressing security within supplier agreements	Defined	Agreemtns in place, not in practise
A15.1.3	ICT supply chain	Not applicable	
A15.2	**Supplier service delivery management**		
A15.2.1	Monitoring and review of supplier services	Nonexistent	Not reviewed
A15.2.2	Managing changes to supplier services	Limited	Change of supplier is ongoing
A16	**Information security incident management**		
A16.1	**Management of information security incidents & improvements**		
A16.1.1	Responsibilities and procedures	Defined	Incidentds are taken care if catastrophic
A16.1.2	Reporting information security events	Managed	Incident response procedure in practise
A16.1.3	Reporting information security weaknesses	Limited	Not aware about existing vulnerability
A16.1.4	Assessment of and decision on information security events	Not applicable	
A16.1.5	Response to information security incidents	Defined	Users are notified about incidents
A16.1.6	Learning from information security incidents	Optimized	All unacceptabel risk are fixed
A16.1.7	Collection of evidence	Limited	Started from a month
A17	**Information security aspects of BCM**		**BCM is Business Continuity Management**
A17.1	**Information security continuity**		
A17.1.1	Planning information security continuity	Optimized	Outsourced BCM provider
A17.1.2	Implementing information security continuity	Managed	Depending on provider
A17.1.3	Verify, review and evaluate information security continuity	Initial	Not revied current policy of BCM provider

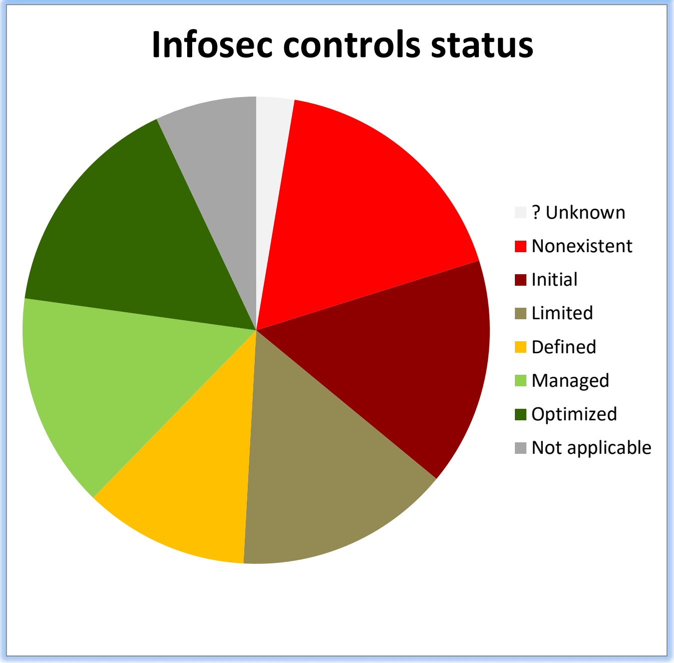
Statement of Applicability and status of information security controls

Section	Information security control	Status	Notes
A17.2	**Redundancies**		
A17.2.1	Availability of information processing facilities	Limited	Only rare case for understanding
A18	**Compliance**		
A18.1	**Compliance with legal and contractual requirements**		
A18.1.1	Identification of applicable legislation and contractual requirements	Initial	Not in practise
A18.1.2	Intellectual property rights	Nonexistent	No records for property owner information
A18.1.3	Protection of records	Defined	Only using basic password for protection, not encrypted data
A18.1.4	Privacy and protection of personally identifiable information	Limited	Privacy of users in place
A18.1.5	Regulation of cryptographic controls	Initial	Usned only for user application, not internally
A18.2	**Information security reviews**		
A18.2.1	Independent review of information security	Managed	Performed last year
A18.2.2	Compliance with security policies and standards	Initial	No enforcement to follow, only in document
A18.2.3	Technical compliance review	Limited	Technical resource are practised as policy

ANNEX 07: ISMS - RESULTING METRICS

Status	Meaning	Proportion of ISMS requirements	Proportion of information security controls
? Unknown	Has not even been checked yet	15%	3%
Nonexistent	Complete lack of recognizable policy, procedure, control *etc.*	4%	18%
Initial	Development has barely started and will require significant work to fulfill the requirements	11%	16%
Limited	Progressing nicely but not yet complete	22%	15%
Defined	Development is more or less complete although detail is lacking and/or it is not yet implemented, enforced and actively supported by top management	30%	11%
Managed	Development is complete, the process/control has been implemented and recently started operating	11%	15%
Optimized	The requirement is fully satisfied, is operating fully as expected, is being actively monitored and improved, and there is substantial evidence to prove all that to the auditors	7%	16%
Not applicable	ALL requirements in the main body of ISO/IEC 27001 are mandatory IF your ISMS is to be certified. Otherwise, managemnent can ignore them.	0%	7%
	Total	100%	100%


ISMS implementation status
? Unknown
Nonexistent
Initial
Limited
Defined
Managed
Optimized
Not applicable


Infosec controls status
? Unknown
Nonexistent
Initial
Limited
Defined
Managed
Optimized
Not applicable