Sri Lanka Institute of Information Technology

Cyber Security - Year 3, Semester 1

IE3102 - Enterprise Standards for Information Security

Assignment 01 - Implementing ISO 27001 for an organization

Submitted by:

IT20017774 – R.M.T Jaliya

IT20627928 – H.M.T.D Herath

Executive Summary

By bringing information security under effective management control, the Information Security Management System will enable guidance and improvement where necessary. The risk (chance of occurrence and/or unfavorable consequences) of events will decrease with improved information security, lowering incident-related losses and costs. A method for managing information security that is organized, consistent, and professional and that is compatible with other ISO management systems. Complete risk assessment and management for information security in accordance with business and security objectives. Evidence of strong governance utilizing generally accepted security procedures

Since information security is a business and regulatory need, the majority of related expenditures would be spent anyway. The extra expenses especially associated with the ISMS include the following. Project management for the ISMS installation and operation project, which requires resources.

What is an ISMS?

Information Security Management System is referred to as ISMS. It is a documented management system made up of a number of security measures that guard against risks to the assets' confidentiality, availability, and integrity.

Organizations may prevent the compromising of their sensitive, private, and confidential data by building, deploying, administering, and maintaining an ISMS.

The deployment of an ISMS may be approached in a variety of ways. The "Plan Do Check Act" technique is the most popular one to use.

The international security standard ISO 27001 outlines the specifications for an ISMS.

ISO 27001

An organization may benefit from having information. It may be found in any format, including spoken, printed, electronic, and written.

Due to this asset's importance, it is crucial that it be well protected.

A corporation must set up, put into practice, and keep up a continuous improvement strategy to manage its ISMS, according to ISO 27001 standards.

It is a methodical strategy or framework for handling confidential business data that guarantees its availability and security. It aids in recognizing, controlling, and quantifying the variety of dangers that information is often exposed to.

Not a technical process, information security is a management process. The "AC Neilson" research states that 64 nations now have 5797 enterprises with ISO 27001 certification. Some famous ISO 27001 certified businesses include Xerox, Sun Microsystems, EDS, SAP, and Price Waterhouse Coopers.

A member of the ISO 27001 family. The group is referred to as the ISO 27000 series

• Deals with every possible Vulnerability and Threat to Information

• 11 major categories of controls/ countermeasures called domains

• 133 countermeasures to control Vulnerabilities and Threats

Development of ISO 27001 "family" of Standards

ISO/IEC Standard	Description
27000	Vocabulary and definitions
27001	Specification (BS7799-2) Issued Oct. 2005
27002	Code of Practice (IS017799:2005)
27003	Implementation Guidance
27004	Metrics and Measurement
27005	Risk Management (BS 7799-3)
27006 -27010	Allocation for future use

Data Qualities

Confidentiality –
Measures for maintaining confidentiality are intended to guard against unauthorized access to sensitive data. Data is often classified based on the scope and nature of the harm that might result from it getting into the wrong hands. These categories may then be used to impose more or less strict measures.

Integrity –
Involves ensuring that data is reliable, consistent, and accurate across its entire lifespan. Data cannot be modified while in transit, and measures must be taken to prevent unauthorized parties from changing the data (for example, in a breach of confidentiality).

Availability –
Implies that information should always be easily and consistently available to authorized people. This entails keeping up with the systems, hardware, and technological infrastructure that store and show the data.

This is done by placing the following in the appropriate places.

People – Employees of the company must be informed of their obligations

Product – The systems or goods being utilized have built-in security measures.

Procedures – The methods used to complete jobs must be standardized

Policies – Documentation of the organization's policies is required

Asset, Vulnerability, Threat, Risk & Control

Anything of value to the company is an asset.

• Vulnerability - Any Asset Weakness

• Danger: any potential threat

• Risk: Threat exposed Vulnerability

• Control: Risk-lowering measures

Why Policies & Standards?

Attacks through People:	**Attacks through Technology:**
Misuse of Powers Trojan, worm, and virus	(D-)DOS attacks
Engineering , Social	SQL injection
Physical entry to disable controls	Buffer overflow
System Misuse	Password cracking
Guessing passwords	Brute force attack

Laptop theft & storage device theft.	

Organization Introduction, Scope & Purpose

Since the creation of the primary telegraphic line between Galle and Colombo in 1858, one of the major communications service providers has been SLTMobitel, previously known as Sri Lanka Telecom. With more than 7.9 million customers, SLTMobitel is Sri Lanka's main mobile service provider. Sri Lanka Telecom, which was established in 1993, bought the network in October 2002. SLTMobitel currently provides GSM, UMTS, LTE Advanced, and 5G-Demonstration-Level service. On the SLTMobitel 4G+ trial network, uplink and downlink rates of up to 150 Mbit/s are feasible. SLTMobitel provides international services, including as GSM roaming in more than 200 countries and GPRS roaming in more than 120 countries. These characteristics make SLTMobitel one of Sri Lanka's biggest and most well-known suppliers of telecommunications services.

The Information Security Management System (ISMS) for ISO/IEC 27000 often begins with a separate implementation project to define, design, build, and deploy it (ISMS). Once it is up and running, the ISMS continues to manage information security by using the governance and management procedures that make up the management system.

The goal of this document is to give advice on how to handle SLT Mobitel's information security, hence its scope encompasses all information relevant to that company. The emphasis of this ISO standard is on all sorts of information, organizational rules, systems in place, required users or parties, and all technologies used by the company.

The financial effects of deploying an ISO27k ISMS in the SLT Mobitel organization are identified and categorized in this study as a set of typical or standard benefits and expenses. Being that we are unaware of your unique information security scenario or dangers, it is obviously general.

Cost Benefit Analysis

Implementing ISO 27001 has its own financial ramifications in addition to a variety of advantages in terms of operating expenses and costs associated with costs. An enterprise must do a cost-benefit analysis before moving forward with the project in order to have a clear understanding of what will happen to the company after it is implemented.

Are determined by how much risk the business is willing to bear, as well as risk perception.
Management should weigh the following four costs:

1- Internal resources

2- External resources

3- Certification

4- Implementation

ISMS Benefits

SLT Mobitel will often gain from an ISO/IEC 27000 Information Security Management System in the methods listed above.

Risk minimization for information security

• Risk reduction - By reassessing corporate information security control requirements, information security controls are reinforced. Current information security policies and controls are updated, and information security controls are encouraged to be regularly evaluated and improved as required..

• Reducing risk - A thorough, organized approach enhances the chance that all relevant information security risks, vulnerabilities, and effects will be found, evaluated, and dealt with logically.

• Cost-cutting - The adoption of organizational guidelines for information security fundamentals, which will simplify administration within the SLT Mobitel Work environment and increase productivity.

• Risk mitigation - A professional, standardized, and rational risk management approach manages information security risks in accordance with their respective priority in addition to ensuring consistency across various information security-related and business operations throughout time.

• Cost-cutting - As critical controls are implemented and managed, the ability to selectively shift some risks to insurers or other third parties increases, which may open the door to negotiating cheaper insurance premiums.

• Risk mitigation - Through practices in awareness and security training, managers and employees become more acquainted with information security concepts, dangers, and controls.

The advantages of uniformity

• Offers a method for monitoring results and gradually improving information security status over time, resulting in cost savings and risk reduction

• Creates a comprehensive set of information security rules, processes, and guidelines that are customized for the firm and explicitly authorized by management - long-term advantages

Benefits of certification

formal proof that the organization's ISMS complies with ISO/IEC 27001 - risk reduction standards from an impartial, knowledgeable assessor.

• A company's information security management capabilities (and therefore its information security status) may be guaranteed to its employees, owners, business partners, regulators, auditors, and other stakeholders. - Risk mitigation and cost savings

• Standardization establishes a solid base of fundamental information security controls that are almost always necessary and on which particular supplemental measures may be constructed as necessary. - Cutting costs

• Saves money by not having to repeatedly explain the same core workplace laws in every situation.

• Economical because it can be used by many different departments, functions, business units, and organizations because it is broadly applicable.

• Permits the business to focus its resources and efforts on the extra security requirements necessary to safeguard specific information assets. - Cutting costs

• based on security standards that are generally recognised and approved - brand value

• To meet emerging security challenges (such BYOD and cloud computing) and brand value, the standards bodies are continuously developing and maintaining the ISO27k standards package.

• Formally specifies technical terms, allowing cost-effective discussion, analysis, and resolution of information security challenges by a variety of stakeholders at various times.

• Can be loosened or deleted affordably without jeopardizing important information assets, allowing for the removal of excessive, unsuitable, or superfluous restrictions.

•The ISO27k strategy reduces costs because it can be applied to any business more readily than stricter, more prescriptive standards like PCI-DSS. It is risk-based, which is why.

One of the benefits of an organized approach is that:

• It provides a framework or structure that is logically consistent for different information security methods, which lowers costs.

• Serves as a catalyst for the review of systems, data, and information flows with the potential to reduce costs related to redundant and other unnecessary systems, data, and processes, as well as to improve the quality of information (business process re-engineering) - cost-saving
• Promotes the company as a reliable, trustworthy, and well-run business partner (similar to the ISO 9000 stamp for quality assurance) - Brand equity

• Management has clearly proved its commitment to information security via corporate governance, compliance, or due diligence. - Risk mitigation and cost savings

The following are some advantages of compliance:

• ISO27k offers a comprehensive framework for information security management that incorporates a wide variety of both internal and external standards, leveraging the common features. - Risk mitigation and cost savings

In order to do business or to comply with privacy and other requirements, stakeholders or authorities may at some time need ISO27k compliance; nevertheless, it is likely to be more cost-effective to implement ISO27k on our own terms and - Cost-cutting

• Adopting commonly recognized best practices offers a strong defense in the event that legal or regulatory enforcement measures are taken in response to information security events. - Risk mitigation and cost savings

ISMS costs

These are the key expenses related to an ISO27k ISMS for SLT Mobitel's management system components.

Project management expenses for implementing an ISMS

• Pick a competent project manager (typically, but not always, the person who will eventually hold the position of CISO or Information Security Manager).

• Create a thorough information security management strategy that is connected with other business goals and requirements in addition to ISO27k.

Employ/assign, manage, direct, and monitor different project resources within the company.

Obtain management authorization to assign the resources necessary to assemble the implementation project team.

• Request their attendance at regular project management meetings.

• Continually compare real progress to the plans by include progress reports and updates.

• Identify and address project risks, ideally in advance.

• If required, get in touch with other parties who could be interested, such as people working on related projects at the same time, managers, or business partners.

Other costs related to implementing ISMS

• Make a list of the information assets;

• Determine the severity of security risks to information assets.

• create the security architecture and security baseline with the goal of reducing information risks by using the proper security controls, avoiding, shifting, or accepting those risks.

• Conduct training and awareness campaigns for the ISMS, such as by offering updated security guidelines;

• Review/update/reissue current information security policies, standards, procedures, guidelines, contract conditions, etc.; prepare/issue new ones. Justify the implementation of new security measures, as well as any upgrades, supplements, or retirements of current ones.

Costs of certification
Any component that malfunctioned would present unacceptably high information security risks; incomplete certification is more likely to occur; consider your options and select an appropriate certification body;

pre-certification visits; certification audit/inspection by an accredited ISO/IEC 27001 certification body; staff/management time spent during annual surveillance visits.

• ISMS internal audits.

• Examinations of SLT Mobitel branch security.

• Recertification every three years (more thorough review and hence wider impact, but still relatively minor)

• All of these costs will be decreased if we are successful in implementing the solution to a high standard through our own efforts.

Costs of ongoing ISMS upkeep and operation

Regular internal audits of the ISMS are conducted to ensure that the policies are being followed, and corrective and preventative measures are taken to address future and existing problems.

• Regular evaluation and upkeep of information security policies, standards, guidelines, and contract provisions, etc.

Combining ISO/IEC 27001 with ISO 9000 certification might potentially save minor registration expenses (a few thousand dollars).

Controls

Included in ISO 27001 are several control areas. There are 133 controls and 39 control goals listed under these areas.

The list of all control sections is provided below:

- Information Security policy
- Organizational Security
- Asset Management
- Human Resources Security
- Physical and Environmental security
- Communications and operations management
- Access control
- Systems development and maintenance
- Information Security Management and Incident Reporting
- Business continuity management
- Compliance

Methodology

The goal is to make sure that a business adheres to the ISO 27001-described information management structure. It will eventually increase the structure and security of its handling and organization.

The following are the two primary activities needed to standardize ISO 27001:-

1. Gap Analysis in comparison to ISO 27001's specified controls

2. Organizing the creation of an ISMS

1. Gap Analysis

Finding the gaps between the present procedures and ISO 27001 criteria is the first step.

133 controls are categorized into Il control areas according to ISO 27001. Each ISO 27001 control must be studied and evaluated against the following four criteria in order to meet the goal: -

(a) Applicability: Indicates whether or not our company is inside the purview of the control.

(b) Implementation: Whether or not the control is put into practice inside the organization.

(c) Fulfillment: According to ISO, a control must meet a certain requirement level in order to pass. Here, we determine whether or not the criterion level is met.

(d) Criticality Index: - You should also evaluate work based on its level of criticality, whether it is low, medium, or high.

In order to construct a gap priority index (GPI), multiply the values supplied to the four parameters as follows:

Applicability * Implementation * Fulfillment * Criticality Index = Gap Priority Index (GPI).

The focus regions may be quickly identified once gap priority index (GPI) calculations have been performed for all of the controls. This index may take on the following values: O, l, 2, 3, 4, or 6. the organization must arrange controls in accordance with GPI.

The GPI values may be used to make the following conclusions:-

1. The key emphasis areas must be sorted out first, starting with the controls with GPI values greater than

2. If there are 25 or more controls with a GPI > 2, the organization's processes are not in place, and significant adjustments are needed.

3. All GPI values for controls must be O in order to get the ISO certificate.

Finally, for all controls whose GPI is not zero, gaps may be found and the following suggestion report can be told to prepare:

(According to ISO) Gaps = Need for Processes — Processes implemented (currently in place)

2. Implementation of an ISMS

Information security is directed and regulated by the ISMS, or Information Security Management System, which is the entire management system made up of governance, rules, procedures, etc. In essence, it serves as a framework for handling and organizing information.

Generally speaking, the ISMS implementation is split into two phases:

1. Planning phase
The first five phases in the steps below come under the planning phase. Here, we primarily pinpoint the gaps in our information security system and make plans on how to remedy them.

2. Implementation phase:
After planning has been done to close the gaps and the holes have been discovered, it is time to take corrective action and begin the auditing process.

Steps are outlined for this.

I. Create an implementation plan for the ISMS
2. Define the ISMS scope
3. Information Assets in the Inventory
4. Explain risk assessment techniques
5. Prepare your statement of relevance
6. Create a risk management plan
7. Create and Implement an ISMS
8. Putting ideas into action and establishing an ISMS
9. Compliance Review
10. Remedial measures (which involves PDCA cycle)
11. Pre-certification Evaluation
12. Certificate Inspection

Risk Assessment (RA) and Risk Treatment plan (RTP)

The Failure mode Effect analysis (FMEA) approach is used for the RA and RTP. We essentially determine RPN (Risk Priority number) in this FMEA technique, which is defined as:

RPN stands for Risk Potential Negligibility.

The risks are evaluated, RPNs are computed, and then risks are ordered by RPN in accordance with the FMEA technique.

Process stages include the following ones:

-

1.List the companies or services the department provides that are within the purview of RA.

2. Determine the assets that provide or support the stated company or service.

3. Note the asset's number (to avoid duplication).

4. Describe how the asset helps to sustain or run the specified company or service.

5. After that, determine the potential failure scenarios for the chosen function. Please be aware that any function may have more than one failure mode.

6. Next, determine the outcome if the failure mode was correctly determined. What would happen to the company or service if the stated failure mode occurred?

7. Now look at the severity table and choose the number that best represents the failure mode's impact.

8. Next, determine what led to the failure mode. Please be aware that there may be several causes for each failure mode.

9. Now look at the probability table and choose the number that best reflects how often the cause will occur.

10. Now, identify the controls that are in place. Please classify the controls as either preventative or investigative. Put each control in its own row.

I l. Now look at the list of detectable abilities and choose a number that reflects how well the controls work.

12. You may now view the Risk Priority Number determined for a potential asset function failure scenario.

13. The risk status now reads "HIGH RISK," and recommendations to reduce each of these HIGH RISKS must be put down if the RPN is not below the permitted number. Please list each control in its own row.

14. Next, determine who will implement the suggested control and when that implementation is expected to occur.

15. If the RPN is now below the permissible level, the risk status will read "LOW RISK." Otherwise, HIGH RISK is indicated. The procedure must be redone from step one if it is HIGH RISK.

16. Calculation of the new RPN. If it falls short of the accepted standards, compare it to the standards and repeat the procedure.

The prioritized list of risks gives management a justification for choosing the amount of resources to devote to risk reduction: if more resources are committed, the cutoff point should go lower down the list, and vice versa.

The following criteria are used to choose the risks for the risk treatment plan once the risks have been sorted according to RPN:

l. All dangers with RPN values higher than 125.

2. Risk mitigation A plan is created that accounts for at least 5% of all potential hazards.

Statement of Applicability (SOA)

The document in which we specify which rules apply to our company is known as the Statement of Applicability. Basically, this is produced utilizing the results of the Risk Assessment (RA) and Risk Treatment Plan (RTP).

The RA and RTP texts themselves outline the relevant restrictions. Here, further details are provided. The SOA lists the relevant controls as well as the justifications for their application.

The following factors make the controls potentially applicable:

LR: legal specifications
CO: contractual responsibilities
Business needs and accepted best practices are referred to as BR/BP.
RRA: the findings of the risk analysis
TSE: in a limited sense.

A proper explanation is given as to why a certain regulation is not relevant. The company may then concentrate on matters that are important to them.

Conclusion

Only a small number of businesses worldwide have ISO 27001 certification. According to one of AC Nielson's survey findings, there are 5797 people. Being an ISO 27001 certified company may significantly boost an organization's reputation and serve as a point of differentiation. It is preferable to identify the flaws inside so that they may be rectified before someone takes advantage of them, rather than waiting for third parties to call them out.

Asset Register

1. **Index**

Asset Register	
SLT Mobitel	
Version Number 1.0	29.09.2022
Document Number	AR001
Document Owner:	CISO
Periodic Review:	Six Monthly
Last Review Date:	29.09.2022
Document Prepared by:	IT20627928-Herath H.M.T.D
Scope:	ISMS PROJECT
Audience:	Board Members and the Stake holders of SLT Mobitel

Index
Digital Assets
Business Databases
Source Code
Softwares
Non Digital Assets
People Assets
Servers
Network Devices
Desktops
Laptops
Media
Support Utilities

1. **Digital Asset**
   - **Asset 01**

SLTMOBITEL
The Connection

List of Digital assets and Valuation of Digital Assets

SLT Mobitel

Version Number 1.0 29.09.2022

#	Asset Title	Asset Details		Value
1	SLT Mobitel Website	**Asset ID**	1	8
		Owner	SLT Mobitel	
		Custodian	SLT Mobitel	
		Users	Staff, Customers, Employees	
		Location	202.129.235.65	
		Storage Details	Database Records	
		Classification	Public	
		Life Cycle	Every 4 hours	
		Disposal Method	Deletion of Database Records	
		Backup Schedule	Weekly	
		Backup Location	SLT Mobitel Head Office	
		Confidentiality Requirements		M
		Integrity Requirements		H
		Availability Requirements		H

- **Asset 02**

SLTMOBITEL The Connection

List of Digital assets and Valuation of Digital Assets

SLT Mobitel

Version Number 1.0 — 29.09.2022

#	Asset Title	Asset Details		Value
1	SLT Mobitel Billing Machine	Asset ID	2	9
		Owner	SLT Mobitel	
		Custodian	SLT Mobitel	
		Users	Staff, Customers, Employees	
		Location	Galle Road, Colombo 03	
		Storage Details	Customer Database Records	
		Classification	Public	
		Life Cycle	Every 24 hours	
		Disposal Method	Destroying the Machine	
		Backup Schedule	Weekly	
		Backup Location	SLT Mobitel Head Office	
		Confidentiality Requirements		H
		Integrity Requirements		H
		Availability Requirements		H

2. Software

- **Asset 03**

SLTMOBITEL The Connection

List of Softwares and Valuation of Softwares

SLT Mobitel

Version Number 1.0 — 29.09.2022

#	Description	Details		Value	
	SLT Mobitel Selfcare App	Owner	SLT Mobitel	3	9
		Custodian	SLT Mobitel		
		Users	SLT Mobitel Customers		
		Classification as per IT Dept.	Software Department		
		Asset ID	3		
		Serial Number	1122467		
		Type	Utility		
		Location [Server / Desktop ID]	202.129.234.66		
		Version	3.1.0		
		License Details	Updated Annually		
		No. Of Licenses	1		
		Application / Business Specific requirements	Registered Customers of SLT Mobitel		
		Technical Contact [SA/NA/DBA]	SA		
		Vendor	SLT Mobitel		
		Expected Life	Lifetime		
		Expired Life	Updated Annually		
		Maintenance Status	29th September 2022		
		Purpose / Service / Role	Maintanence and managing all the mobitel connections		
		Dependency	SLT Mobitel Server		
		Redundency Requirenebts			
		Confidentiality Requirements for data Processed		L	H
		Integrity Requirements for data Processed		L	H
		Availability Requirements for data Processed		L	H

- Asset 04

SLTMOBITEL
The Connection

List of Softwares and Valuation of Softwares

SLT Mobitel

Version Number 1.0 — 29.09.2022

#	Description	Details		Value	
	SLT Mobitel mCash APP	Classification as per IT Dept.	Software Department		
		Asset ID	4		
		Serial Number	N/A		
		Type	Utility		
		Location [Server / Desktop ID]	202.129.234.66		
		Version	2		
		License Details	Updated Annually		
		No. Of Licenses	1	3	9
		Application / Business Specific requirements	Registered Customers of SLT Mobitel		
		Technical Contact [SA/NA/DBA]	SA		
		Vendor	SLT Mobitel		
		Expected Life	Lifetime		
		Expired Life	Updated Annually		
		Maintenance Status	29th September 2022		
		Purpose / Service / Role	Maintanence and managing all the mobitel connections cashing service		
		Dependency	SLT Mobitel Server		
		Redundency Requirenebts			
		Confidentiality Requirements for data Processed		L	H
		Integrity Requirements for data Processed		L	H
		Availability Requirements for data Processed		L	H

1. Non-Digital Assets
   - Asset 05

SLTMOBITEL
The Connection

List of Non Digital assets and Valuation of Non Digital Assets

SLT Mobitel

Version Number 1.0 — 29.09.2022

#	Asset Title	Asset Details		Value
1	Documents and files	Asset ID	5	8
		Owner	SLT Mobitel	
		Custodian	SLT Mobitel	
		Users	Customers, Employees	
		Location	Document Storage Room	
		Storage Details	Storage Boxes and file cabinets	
		Classification	Internal	
		Life Cycle	Every 6 months	
		Disposal Method	Shredding the documents and files	
		Backup	Every 6 months	
		Backup Location	Backup center Colombo 03	
		Requirements		H
		Integrity Requirements		H
		Availability Requirements		M

- Asset 06

SLTMOBITEL The Connection

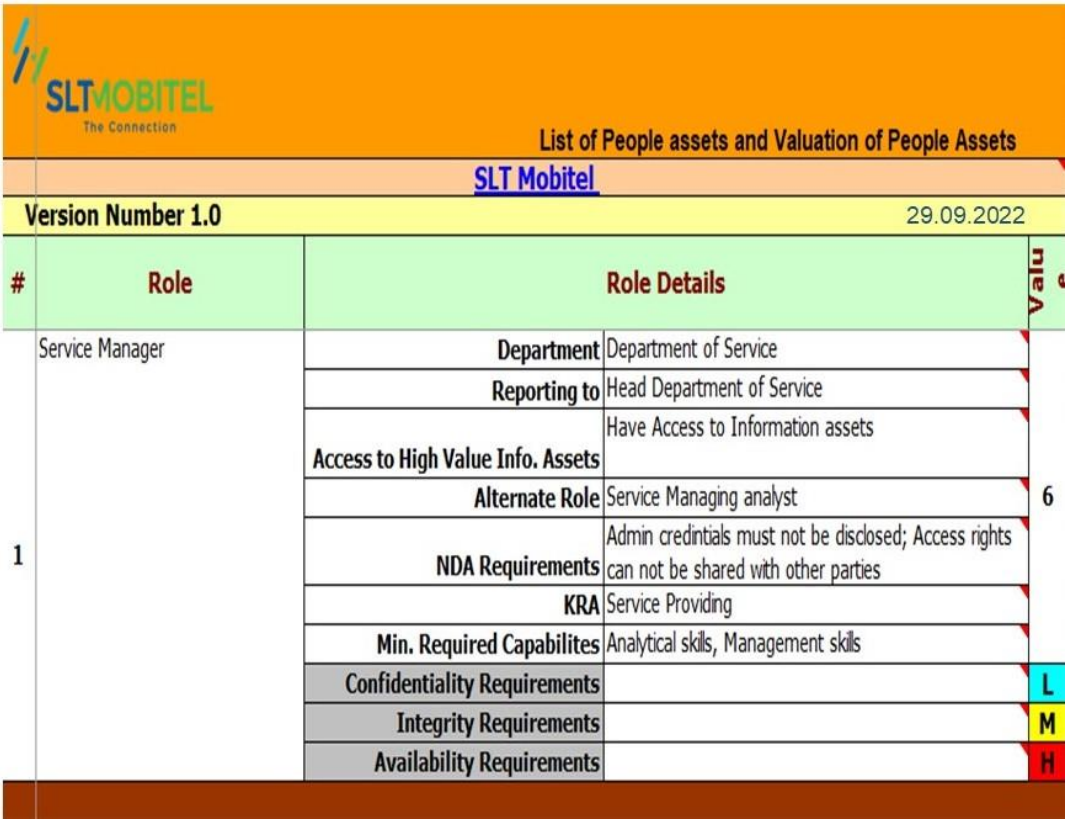
List of Non Digital assets and Valuation of Non Digital Assets

SLT Mobitel

Version Number 1.0 29.09.2022

#	Asset Title	Asset Details		Value
1	SLT Mobitel Head Office	Asset ID	6	5
		Owner	SLT Mobitel	
		Custodian	SLT Mobitel	
		Users	Customers, Employees	
		Location	Galle Road, Colombo 03	
		Storage Details	N/A	
		Classification	Public	
		Life Cycle	N/A	
		Disposal Method	N/A	
		Backup	N/A	
		Backup Location	N/A	
		Requirements		L
		Integrity Requirements		L
		Availability Requirements		H

3. People Assets
    - Asset 07



SLTMOBITEL The Connection

List of People assets and Valuation of People Assets

SLT Mobitel

Version Number 1.0 29.09.2022

#	Role	Role Details		Valu
1	Service Manager	Department	Department of Service	6
		Reporting to	Head Department of Service	
		Access to High Value Info. Assets	Have Access to Information assets	
		Alternate Role	Service Managing analyst	
		NDA Requirements	Admin credintials must not be disclosed; Access rights can not be shared with other parties	
		KRA	Service Providing	
		Min. Required Capabilites	Analytical skills, Management skills	
		Confidentiality Requirements		L
		Integrity Requirements		M
		Availability Requirements		H

- Asset 08

SLTMOBITEL The Connection

List of People assets and Valuation of People Assets

SLT Mobitel

Version Number 1.0 29.09.2022

#	Role	Role Details		Valu
1	Customer Service Receptionist	Department	Department of Human Resource	
		Reporting to	Manager of Department of Human Resource	
		Access to High Value Info. Assets	No Access to Information Assets	
		Alternate Role	Call center Operator	5
		NDA Requirements	System Login Credentials must not be disclosed	
		KRA	Customer Handling	
		Min. Required Capabilites	Analytical skills, Management skills, Communication Skills	
		Confidentiality Requirements		L
		Integrity Requirements		L
		Availability Requirements		H

1. Desktop
   - Asset 09

SLTMOBITEL

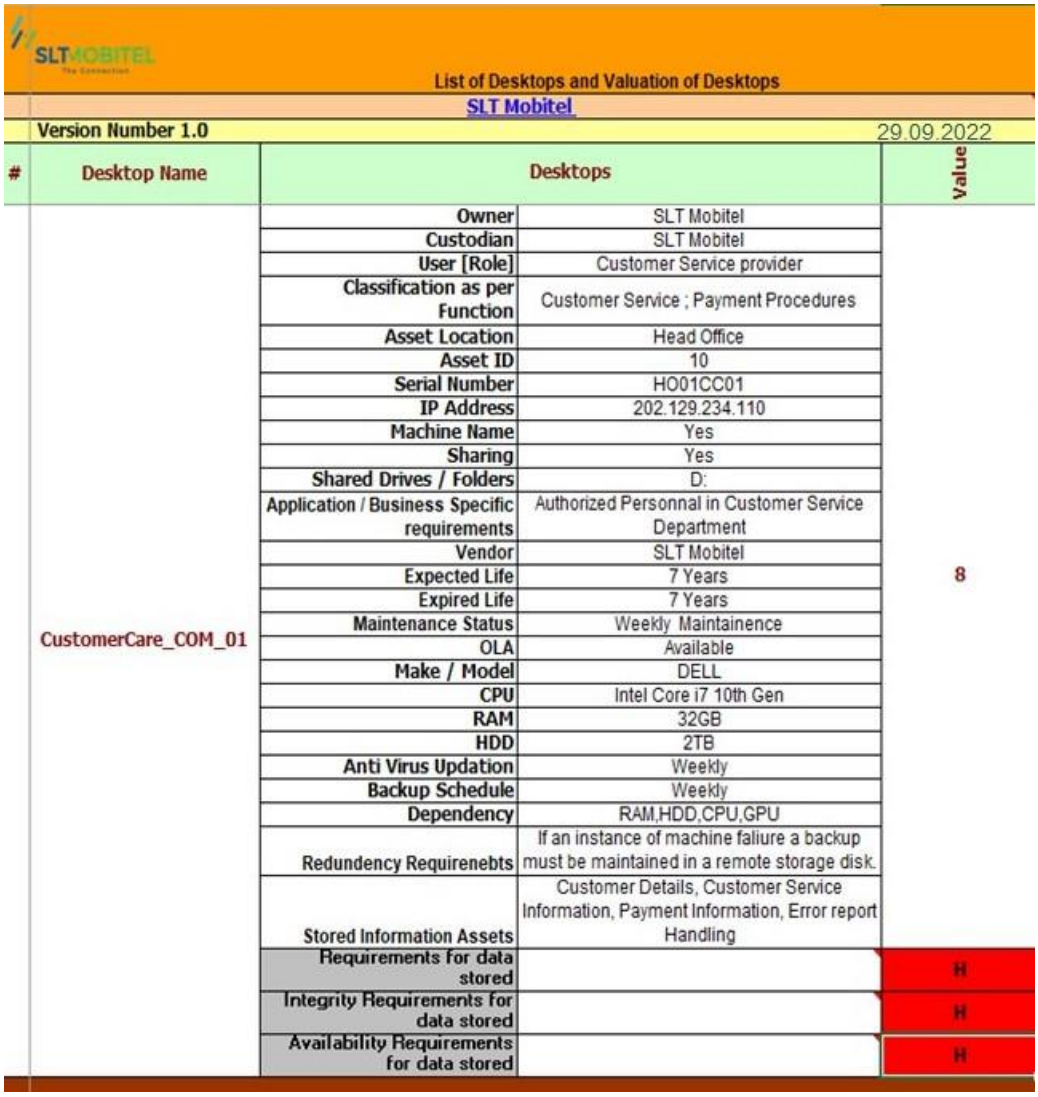
List of Desktops and Valuation of Desktops

SLT Mobitel

Version Number 1.0 29.09.2022

#	Desktop Name	Desktops		Value
	Marketing_COM_01	Owner	SLT Mobitel	7
		Custodian	SLT Mobitel	
		User [Role]	Marketing Consultant	
		Classification as per Function	Marketing ; Sales	
		Asset Location	Head Office	
		Asset ID	9	
		Serial Number	HO06M01	
		IP Address	202.129.234.100	
		Machine Name	Yes	
		Sharing	Yes	
		Shared Drives / Folders	D:	
		Application / Business Specific requirements	Authorized Personnal in Marketing Department	
		Vendor	SLT Mobitel	
		Expected Life	7 Years	
		Expired Life	7 Years	
		Maintenance Status	Weekly Maintainence	
		OLA	Available	
		Make / Model	DELL	
		CPU	Intel Core i7 10th Gen	
		RAM	32GB	
		HDD	2TB	
		Anti Virus Updation	Weekly	
		Backup Schedule	Weekly	
		Dependency	RAM,HDD,CPU,GPU	
		Redundency Requirenebts	If an instance of machine faliure a backup must be maintained in a remote storage disk.	
		Stored Information Assets	Marketing Posters, Marketing strategy documents, Sales reports, Project details	
		Requirements for data stored		M
		Integrity Requirements for data stored		M
		Availability Requirements for data stored		H

- Asset 10



List of Desktops and Valuation of Desktops

SLT Mobitel

Version Number 1.0 — 29.09.2022

#	Desktop Name	Desktops		Value
	CustomerCare_COM_01	Owner	SLT Mobitel	
		Custodian	SLT Mobitel	
		User [Role]	Customer Service provider	
		Classification as per Function	Customer Service ; Payment Procedures	
		Asset Location	Head Office	
		Asset ID	10	
		Serial Number	HO01CC01	
		IP Address	202.129.234.110	
		Machine Name	Yes	
		Sharing	Yes	
		Shared Drives / Folders	D:	
		Application / Business Specific requirements	Authorized Personnal in Customer Service Department	
		Vendor	SLT Mobitel	
		Expected Life	7 Years	8
		Expired Life	7 Years	
		Maintenance Status	Weekly Maintainence	
		OLA	Available	
		Make / Model	DELL	
		CPU	Intel Core i7 10th Gen	
		RAM	32GB	
		HDD	2TB	
		Anti Virus Updation	Weekly	
		Backup Schedule	Weekly	
		Dependency	RAM,HDD,CPU,GPU	
		Redundency Requirenebts	If an instance of machine faliure a backup must be maintained in a remote storage disk.	
		Stored Information Assets	Customer Details, Customer Service Information, Payment Information, Error report Handling	
		Requirements for data stored		H
		Integrity Requirements for data stored		H
		Availability Requirements for data stored		H