Risk Methodology

Contents

Figures

Tables

Introduction

The effective management of information security has always been a priority for branch of Specialized Technical Services STS Holding Ltd in order to manage risk and safeguard its reputation in the marketplace. However, there is still much to be gained by branch of Specialized Technical Services STS Holding Ltd in continuing to introduce industry-standard good practice processes and take into consideration the Cybersecurity legislation and regulations in KSA such as the Essential Cybersecurity Controls (ECC-1:2018) and Cloud Computing Controls (CCC-1:2020) published by the National Cybersecurity Authority

Risk is realised when:

- The objectives of the business are not achieved
- The assets of the business are not safeguarded from loss
- There is non-compliance with branch of Specialized Technical Services STS Holding Ltd policies and procedures or Cybersecurity legislation and regulations
- The resources of the business are not utilised in an efficient and effective manner
- The confidentiality, integrity and availability of information is not reliable
- The continuity of the business was disrupted
- The need to activate the BCP or DRP

It is important that STS has an effective risk assessment and treatment process in place to ensure that potential impacts do not become real, or if they do, that contingencies are in place to deal with them.

It is important also that the process is sufficiently clear so that successive assessments produce consistent, valid and comparable results, even when carried out by different people.

The purpose of this document is to set out such a process. And to provide Cybersecurity requirements based on best practices and standards within Risk management to ensure the risks of the branch of Specialized Technical Services STS Holding Ltd are mitigated. And to ensure managing cybersecurity risks in a methodological approach in order to protect the CSP’s and CST’s information and technology assets as per organizational policies and procedures, and related laws and regulations.

This methodology aims to comply with cybersecurity requirements and related legislative and regulatory requirements, which is a legislative requirement in Control No. 1-5-1 of the NCA Essential Cybersecurity Controls (ECC-1:2018) and Control No. 1-2-P-1 of the NCA Cloud Computing Controls (CCC-1:2020) issued by the National Cybersecurity Authority. This document also aims to comply with the cybersecurity requirements issued by the legislative and regulatory authorities operating in the Kingdom, which may apply to the branch of Specialized Technical Services STS Holding Limited, such as:

- Requirements issued by the Communications, Space and Technology Commission (CST)

1 Risk assessment and treatment process

The process described in this document is aligned with the following:

ISO/IEC 27001 - Information Security Management Systems
ISO 31000 - Risk Management Guidelines
Cybersecurity legislation and regulations in KSA such as the Essential Cybersecurity Controls (ECC-1:2018) and Cloud Computing Controls (CCC-1:2020) published by the National Cybersecurity Authority

It is recommended that these documents be reviewed for a full understanding of the environment within which this risk assessment process operates.

In the Risk Assessment Process for the branch of Specialized Technical Services STS Holding Limited that includes all STS Risks and Assets along with the CSP's and CST's Risks and Assets, we include the following items in the risk assessment process:

- Defining acceptable risk levels for the branch of Specialized Technical Services STS Holding Limited assets and cloud services, and clarifying them to the CST if they are related to the CST (Please refer to Management Approval Section)
- Considering data and information classification in cybersecurity risk management methodology. (Please check the below paragraph)
- Developing cybersecurity risk register for branch of Specialized Technical Services STS Holding Limited Assets along with cloud services and monitoring it periodically according to the risks. (Please refer to the Risk Assessment & Treatment Plan sheet)

The process of risk assessment and treatment is shown in figure 1 and described in more detail in the following sections. The first step of the risk analysis process is started by collecting the branch of Specialized Technical Services STS Holding Limited Assets along with the CSP's and CST's Assets, and implementing data and information classification for all these assets based on the Confidentiality, Integrity and Availability of each asset to calculate the asset weight and asset evaluation level (High, Medium, Low) and identify the risks (Threats & vulnerabilities) for each level and add the mitigation controls accordingly. (You can refer to the Data and Information Protection Policy for more information on the data classification levels)

The process used is qualitative in nature in that it uses the terms high, medium and low to describe the relative classification level for each specific risk. In some circumstances it may be appropriate to also use quantitative techniques i.e., using numbers such as financial values within the process to provide a higher degree of detail in assessing risks. In all cases where quantitative techniques are used the criteria should be clearly stated so that the risk assessment is understandable and repeatable.

For High Risks (with score level of 12 and above), a treatment plan should be provided to the management for approval to be initiated within three months from the day they were reported. For medium and low risks (risk score is less than 12), the treatment plans should be initiated within 6 months. The security officer shall follow up to update the status of risk treatment every 6 months or in the event of changes in the relevant legislative and regulatory requirements issued by the legislative and regulatory authorities operating in the Kingdom, which may apply to the branch of Specialized Technical Services STS Holding Limited, such as the cybersecurity controls that are issued by the NCA (National Cyber Security Authority) and update the results in the risk register and the treatment plan accordingly.

The cybersecurity risk assessment procedures must be implemented at least in the following cases:

1. Early stages of technology projects through the following controls:
    a. Define and document the requirements of this ECC in the cybersecurity requirements document and approve them by the representative • Include cybersecurity requirements within the first phase of the information and technology projects lifecycle (Technical Project Lifecycle) within the organization.
    b. Implement cybersecurity risk assessment procedures at an early stage of technical projects to avoid events or circumstances that could compromise the confidentiality, integrity, and availability of information and technology assets, including, in particular, the identification of information and technology assets in technology projects, potential exposure to threats, and relevant vulnerabilities.
    c. Remediate all cybersecurity risks in accordance with the approved cybersecurity risk management methodology.

2. Before making major changes to technology infrastructure through the following controls:
    a. Define and document the requirements of this ECC in the cybersecurity requirements document and approve them by the representative.
    b. Include cybersecurity requirements within the IT Change Management lifecycle in the organization.
    c. Implement cybersecurity risk assessment procedures before making a material change in the technology architecture to avoid events or circumstances that could compromise the confidentiality, integrity, and availability of information and technology assets, including, in particular, the identification of information and technology assets in technology projects, potential exposure to threats, and relevant vulnerabilities. These changes include, but are not limited to: a basic and sensitive update to one or several systems in the network, such as database systems, or a radical change in network mapping
    d. Remediate all cybersecurity risks in accordance with the approved cybersecurity risk management methodology.

3. During the planning phase of obtaining third party services through the following controls:

a. Define and document the requirements of this ECC in the cybersecurity requirements document and approve them by the representative.
b. Include cybersecurity requirements within the third-party, contracts, and procurement management procedures in the organization.
c. Implement cybersecurity risk assessment procedures when planning to acquire services from a third party. to avoid events or circumstances that could compromise the confidentiality, integrity, and availability of information and technology assets, including, in particular, the identification of information and technology assets in technology projects, potential exposure to threats, and relevant vulnerabilities.
d. Remediate all cybersecurity risks in accordance with the approved cybersecurity risk management methodology.

1.1 Criteria for performing information security risk assessments.

There are several criteria that determine when an information security risk assessment should be carried out within branch of Specialized Technical Services STS Holding Ltd and these will vary in scope.

In general, the criteria are that a risk assessment will be performed in the following circumstances:

A comprehensive risk assessment covering all information assets as part of the initial implementation of the Information Security Management System (ISMS)
Updates to the comprehensive risk assessment as part of the management review process – this should identify changes to assets, threats and vulnerabilities and possibly risk levels
As part of projects that involve significant change to the branch of Specialized Technical Services STS Holding Ltd or its information assets
As part of the IT change management process when assessing whether proposed changes should be approved and implemented
On major external change affecting the branch of Specialized Technical Services STS Holding Ltd which may invalidate the conclusions from previous risk assessments e.g. changes to relevant legislation and regulations, mergers and acquisitions
When evaluating and selecting suppliers, particularly those that will play a part in the delivery of cloud services to customers

If there is uncertainty regarding whether it is appropriate to carry out a risk assessment, the branch of Specialized Technical Services STS Holding Ltd should err on the side of caution and ensure that one is performed.

1.2 Risk acceptance criteria

One of the options when evaluating risks is to do nothing i.e., to accept the risk. This is a valid approach but must be used with caution. The circumstances under which risks may be accepted must be fully agreed and understood.

Criteria for accepting risks will vary according to several factors which may change over time. These include the branch of Specialized Technical Services STS Holding Ltd general or cultural attitude to risk, the prevailing financial climate, legal and regulatory requirements, the current view of top management and the sensitivity of the specific assets or business areas within scope.

Before carrying out a risk assessment the criteria for accepting risks must be discussed by appropriate people with knowledge of the subject area and, if necessary, top management. This discussion should establish guidelines for the circumstances in which risks will be accepted i.e., not subjected to further treatment.

These criteria may be expressed in several different ways, depending on the scope of the risk assessment and may include situations where:

- The cost of an appropriate control is judged to be more than the potential loss.
- Known changes will soon mean that the risk is reduced or disappears completely
- The risk is at or lower than a defined threshold, expressed either as a level e.g. low or as a quantified amount e.g. a financial sum
- An area is known to be high risk but also high potential reward i.e. it is a calculated risk

These acceptance criteria must be documented and used as input to the risk evaluation stage of the assessment process.

1.3 Process diagram

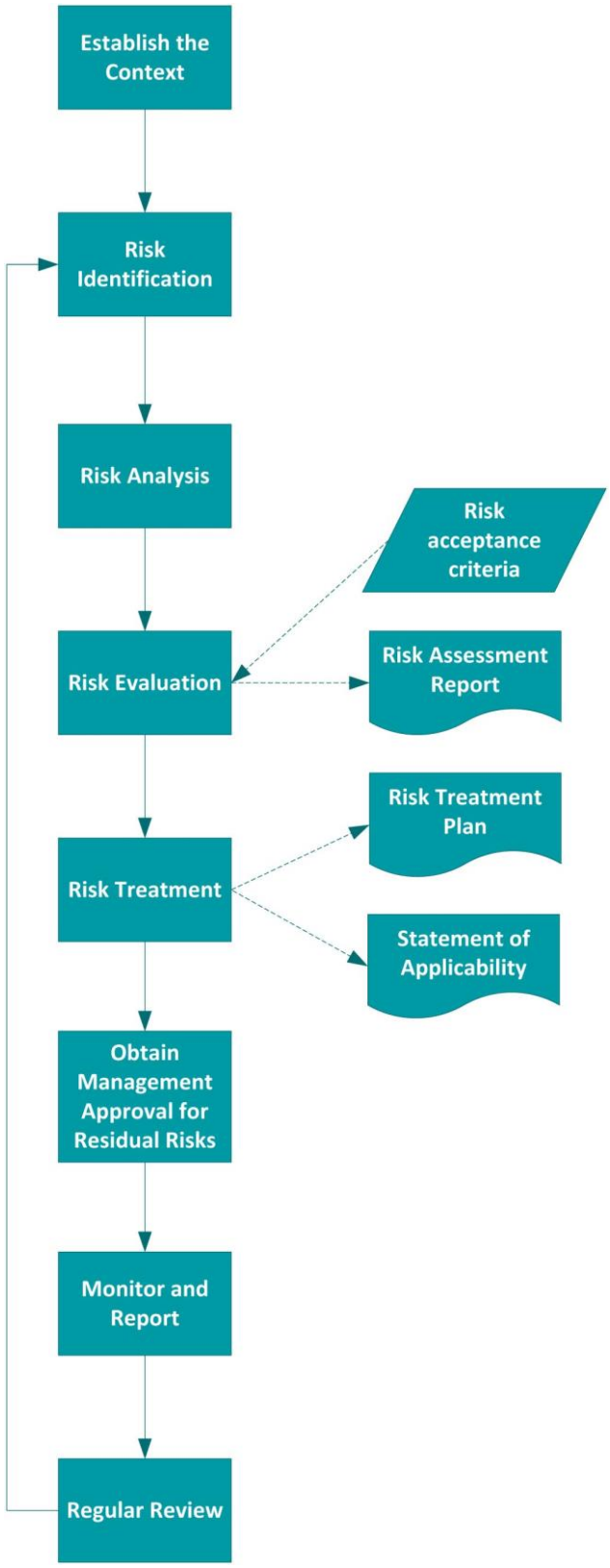

Figure 1: Risk assessment and treatment process diagram

1.4 Establish the context.

The overall environment in which the risk assessment is carried out must be described and the reasons for it explained. This should include a description of the internal and external context and any recent changes that affect the likelihood and impact of risks in general.

The internal context may include:

Governance, structure, roles and accountabilities
Policies, objectives, and the strategies that are in place to achieve them
The capabilities, understood in terms of resources and knowledge (e.g. capital, time, people, processes, systems and technologies)
Information systems, information flows and decision-making processes (both formal and informal)
Relationships with, and perceptions and values of, internal stakeholders
The branch of Specialized Technical Services STS Holding Ltd culture
Standards, guidelines and models adopted by the branch of Specialized Technical Services STS Holding Ltd
Form and extent of contractual relationships
The type(s) of cloud services provided

The external context may include:

The cultural, social, political, legislations and regulations, financial, technological, economic, natural, and competitive environment, whether international, national, regional or local

Key drivers and trends having impact on the objectives of the branch of Specialized Technical Services STS Holding Ltd
Relationships with, and perceptions and values of, external stakeholders
The prevailing market or industry view of the security of cloud service providers – this may be affected by any recent breaches involving the loss of personally identifiable information (PII)

The scope of the risk assessment must also be defined. This may be expressed in terms of factors such as:

Geographical location e.g. countries, offices, data centres
Branch of Specialized Technical Services STS Holding Ltd units e.g. specific departments
Business process(es)
IT services, systems and networks
Customers, products or services

1.5 Risk identification

The process of identifying risks to be assessed will consist of the following steps in line with the requirements of industry-standard good practice processes and the Cybersecurity legislation and regulations in KSA such as the Essential Cybersecurity Controls (ECC-1:2018) and Cloud Computing Controls (CCC-1:2020) published by the National Cybersecurity Authority. Risks are identified to the confidentiality, integrity, or availability of information.

1.5.1 Compile/maintain asset inventory.

A full inventory of assets is compiled and maintained by branch of Specialized Technical Services STS Holding Ltd. The definition of an asset is taken to be “anything that has value to the branch of Specialized Technical Services STS Holding Ltd” and is therefore worthy of protection. This will include customer data that branch of Specialized Technical Services STS Holding Ltd stores and processes in its role as a cloud service provider.

Two major types of assets are identified:

Primary assets – information and business processes and activities
Supporting assets – hardware, software, network, personnel, site

The list of assets is held in the document Information Asset Inventory as part of the ISMS. Within the inventory every asset is assigned a value which should be considered as part of impact assessment stage of this process. Each asset also has an owner who should be involved in the risk assessment for that asset. Where appropriate for the purposes of risk assessment, cloud customer data assets may be owned by an internal role and the customer consulted regarding the value of those assets.

For the purposes of risk assessment, it may be appropriate to group assets with similar requirements together so that the number of risks to be assessed remains manageable.

1.5.2 Identify potential threats.

For each asset (or asset group), the threats that could be reasonably expected to apply to it will be identified. These will vary according to the type of asset and could be accidental events such as fire, flood or vehicle impact or malicious attacks such as viruses, theft or sabotage. Threats will apply to one or more of the confidentiality, integrity and availability of the asset.

1.5.3 Assess existing vulnerabilities.

Attributes of an asset (or asset group) which may be exploited by any specific threat are referred to as vulnerabilities and will be detailed as part of the risk assessment.

Examples of such vulnerabilities may include a lack of patching on servers (which could be exploited by the threat of malware) or the existence of paper files in a data centre (which could be exploited by the threat of fire).

1.6 Risk analysis

Risk analysis within this process involves assigning a numerical value to the a) likelihood and b) impact of a risk. These values are then multiplied to arrive at a classification level of high, medium, or low for the risk.

1.6.1 Assess the likelihood.

An estimate of the likelihood of a risk occurring must be made. This should consider whether it has happened before either to this branch of Specialized Technical Services STS Holding Ltd or similar branch of Specialized Technical Services STS Holding Ltd in the same industry or location and whether there exists sufficient motive, opportunity, and capability for a threat to be realized.

The likelihood of each risk will be graded on a numerical scale of 1 (low) to 5 (high). General guidance for the meaning of each grade is given in table 1. When assessing the likelihood of a risk, existing controls will be considered. This may require an assessment to be made as to the effectiveness of existing controls.

More detailed guidance may be decided for each grade of likelihood, depending on the subject of the risk assessment.

GRADE	DESCRIPTION	SUMMARY
1	Improbable	Has never happened before and there is no reason to think it is any more likely now
2	Unlikely	There is a possibility that it could happen, but it probably won't
3	Likely	On balance, the risk is more likely to happen than not
4	Very Likely	It would be a surprise if the risk did not occur either based on past frequency or current circumstances
5	Almost certain	Either already happens regularly or there is some reason to believe it is virtually imminent

Table 1: Risk likelihood guidance

The rationale for allocating the grade given should be recorded to aid understanding and allow repeatability in future assessments.

1.6.2 Assess the impact.

An estimate of the impact that the loss of confidentiality, integrity or availability could have on the company must be given. This should consider existing controls that lessen the impact, if these controls are seen to be effective.

Consideration will be given to the impact in the following areas:

Customers
Finance
Health and Safety
Reputation
Knock-on impact within the branch of Specialized Technical Services STS Holding Ltd
Legal, contractual or branch of Specialized Technical Services STS Holding Ltd obligations

The impact of each risk will be graded on a numerical scale of 1 (low) to 5 (high). General guidance for the meaning of each grade is given in table 2.

GRADE	DESCRIPTION	CUSTOMER IMPACT	FINANCIAL IMPACT	HEALTH & SAFETY	IMPACT ON REPUTATION	LEGAL IMPACT
1	Negligible	No effect	Very little or none	Very small additional risk	Negligible	No implications
2	Slight	Some local disturbance to normal business operations	Some	Within acceptable limits	Slight	Small risk of not meeting compliance
3	Moderate	Can still deliver product/service with some difficulty	Unwelcome but could be borne	Elevated risk requiring immediate attention	Moderate	In definite danger of operating illegally
4	High	Business is crippled in key areas	Severe effect on income and/or profit	Significant danger to life	High	Operating illegally in some areas
5	Very High	Out of business; no service to customers	Crippling: the Company will go out of business	Real or strong potential loss of life	Very High	Severe fines and possible imprisonment of staff

Table 2: Risk impact guidance

More detailed guidance may be defined for each grade of impact, depending on the risk assessment.

The rationale for allocating the grade given should be recorded to aid understanding and allow repeatability in future assessments.

1.6.3 Risk classification

Based on the assessment of the grade of likelihood and impact, a score is calculated for each risk by multiplying the two numbers. This resulting score is then used to decide the classification of the risk based on the matrix shown in figure 2.

Each risk will be allocated a classification based on its score as follows:

High: 12 or more
Medium: 5 to 10 inclusive
Low: 1 to 4 inclusive

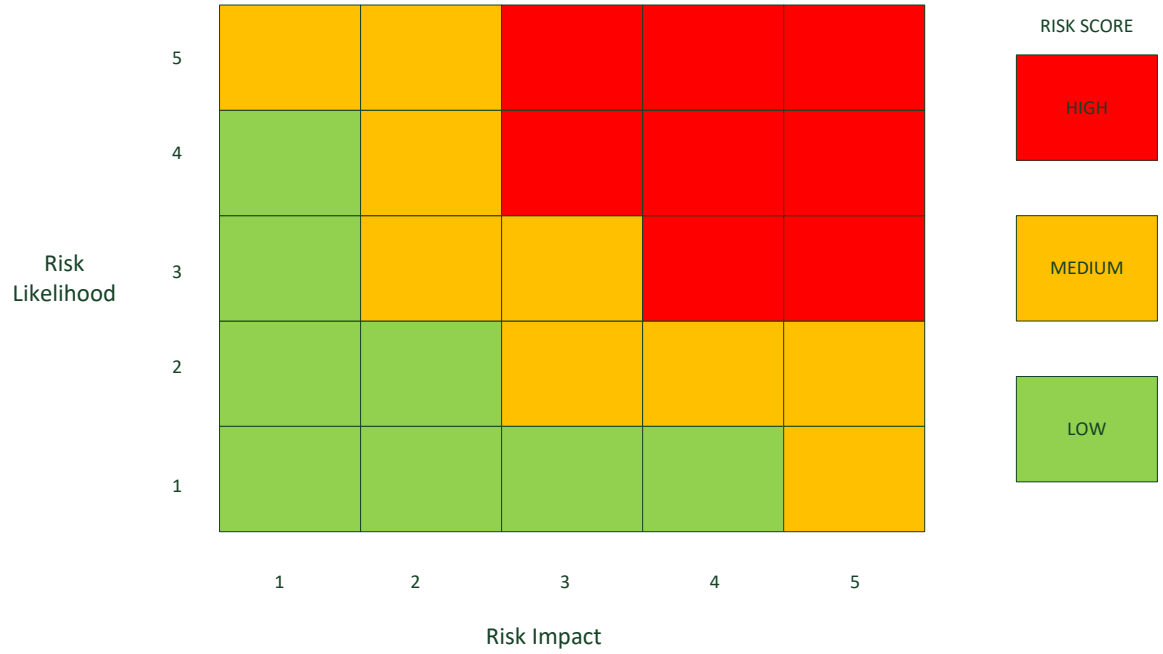

Figure 2: Risk matrix chart

The classification of each risk will be recorded as input to the risk evaluation stage of the process.

1.7 Risk evaluation

The purpose of risk evaluation is to decide which risks can be accepted and which ones need to be treated. This will consider the risk acceptance criteria established for this specific risk assessment (see Risk Acceptance Criteria, above).

The matrix in Figure 2 shows the classifications of risk, where green indicates that the risk is below the acceptable threshold. The orange and red areas generally indicate that a risk does not meet the acceptance criteria and so is a candidate for treatment.

Risks will be prioritized for treatment according to their score and classification so that very high scoring risks are recommended to be addressed before those with lower levels of exposure for the branch of Specialized Technical Services STS Holding Ltd.

1.7.1 Risk assessment report

The output from the risk evaluation stage is the risk assessment report. This shows the following information:

Assets [asset-based risk assessment only]
Threats [asset-based risk assessment only]
Vulnerabilities [asset-based risk assessment only]
Risk scenario descriptions [scenario-based risk assessment only]
Controls currently implemented
Likelihood (including rationale)
Impact (including rationale)
Risk Score
Risk Classification
Whether the risk is recommended for acceptance or treatment

This report is input to the risk treatment stage of the process and must be signed off by management before continuing, particularly in respect of those risks that are recommended for acceptance.

1.8 Risk treatment

For those risks that are agreed to be above the threshold for acceptance by branch of Specialized Technical Services STS Holding Ltd, the options for treatment will then be explored.
The overall intention of risk treatment is to reduce the classification of a risk to an acceptable level. This is not always possible as sometimes although the score is reduced, it remains in the same classification e.g. reducing the score from 8 to 6 means it remains a medium level risk. The branch of Specialized Technical Services STS Holding Ltd may decide to accept these risks even though they remain at a medium rating. Such decisions must be recorded with a suitable explanation.

1.8.1 Risk treatment options

The following options may be applied to the treatment of the risks that have been agreed to be unacceptable:

1. **Accept** the risk – acknowledge that the risk exists but apply no safeguard
2. **Mitigate** the risk - apply appropriate controls to lessen the likelihood and/or impact of the risk.
3. **Avoid** the risk by taking action that means it no longer applies.
4. **Transfer** the risk with another party e.g., insurer or supplier.

Judgement will be used in the decision as to which course of action to follow, based on a sound knowledge of the circumstances surrounding the risk e.g.

Business strategy
Regulatory and legislative considerations
Technical issues
Commercial and contractual issues

The Risk Manager will ensure that all parties who have an interest or bearing on the treatment of the risk are consulted, including the risk owner.

1.8.2 Risk treatment plan

The evaluation of the treatment options will result in the production of the risk treatment plan which will detail:

Risks requiring treatment
Recommended treatment option
Control(s) to be implemented
Expected residual risk levels after the controls have been implemented

1.9 Risk Appetite

At each stage of the risk assessment process for branch of Specialized Technical Services STS Holding Limited, CSP's and CST's, management will be kept informed of progress and decisions made, including formal signoff of the proposed residual risks. And if there are any risks related to the CST's, we ensure to informing them formally with these risks.

Management will approve the following documents:

Risk Assessment Report
Risk Treatment Plan
Signoff will be indicated according to branch of Specialized Technical Services STS Holding Ltd documentation standards. In addition to overall management approval, the acceptance or treatment of each risk must be signed off by the relevant risk owner.

The below criteria outlines the thresholds for accepting risk levels or treating identified risks for branch of Specialized Technical Services STS Holding Limited, Cloud services and CST's (if the risks related to them):

In accordance with this methodology, all risks classified as Medium and low will be accepted by the management. These risks are deemed to have an acceptable level of potential impact and likelihood, and therefore, no further action will be taken to mitigate them. However, in the case of risks classified as High and critical, a meeting will be conducted with the management and risk owners to thoroughly evaluate the potential consequences and likelihood of occurrence, and if there are any risks related to the CST's, we ensure to informing them formally with these risks. This meeting will facilitate informed decision-making regarding appropriate actions to treat the identified risks, ensuring that the branch of Specialized Technical Services STS

Holding Limited and Cloud services and CST's security postures are effectively maintained and aligned with its risk appetite.

1.10 Risk monitoring and reporting

As part of the implementation of new controls and the maintenance of existing ones, key performance indicators will be identified which will allow the measurement of the success of the controls in addressing the relevant risks.

These indicators will be reported on a regular basis and trend information produced so that exception situations can be identified and dealt with as part of the management committee meetings process.

All Risks that are related to the CST's, we directly report these risks to the tenants.

1.11 Acceptable Appetite for CSPs

In addition to the above criteria mentioned in the Management Approval Section that outlines the thresholds for accepting risk levels, kindly find the following points that outlines the risks for CSPs:

- Branch of Specialized Technical Services Holding Limited identifies the cloud computing services provided and analyse the business impact based on specific procedures to understand and evaluate the risks (for example: service outage, data leakage, unauthorized access, etc.) and the damages that they may cause.
- Work to determine risk levels for cloud computing services (for example Critical High Medium Low and determining the acceptable risk levels)
- Sharing acceptable risk levels with subscribers for the service provided (for example: sharing risk and threat assessment analysis for cloud computing services provided to subscribers)

1.11.1 Risk Categorization

As mentioned in this document, we utilize a risk matrix to quantify and qualify CSP's cybersecurity risks based on likelihood and impact. Risk levels are classified into low, medium, high, and critical categories, providing clear visibility into the severity of identified risks.

1.11.2 Acceptable Risk Levels:

At Branch of Specialized Technical Services Holding Limited, we recognize that not all risks can be completely eliminated, and therefore, we establish acceptable risk levels to guide our risk management efforts. These acceptable risk levels are determined through a comprehensive evaluation process involving key stakeholders,

including senior management, cybersecurity experts, and client representatives. The following principles govern our approach to acceptable risk levels:

Low and Medium Risks:

Risks classified as low and medium are deemed acceptable by Branch of Specialized Technical Services Holding Limited top management and the cloud department. These risks are assessed to have a relatively low likelihood of occurrence and a moderate impact on our cloud services and subscribers. As such, they are considered within the tolerance levels set forth by our risk management framework.

High and Critical Risks:

Risks classified as high and critical pose significant threats to the confidentiality, integrity, and availability of our cloud services and subscribers. As such, they are not deemed acceptable within our risk tolerance thresholds.

In instances where high or critical risks are identified, immediate action is taken to convene a meeting with all stakeholders from Branch of Specialized Technical Services Holding Limited and affected clients. This meeting serves as a forum for transparent discussion, risk analysis, and decision-making regarding appropriate risk response strategies.

During the meeting, stakeholders collaboratively assess the potential impact of the identified risks on business operations, regulatory compliance, and client relationships. This assessment includes an evaluation of risk likelihood, potential vulnerabilities, and available mitigation options.

Based on the outcomes of the discussion, stakeholders collectively determine the most suitable risk response options (mentioned in section 1.8.1 Risk Treatment Options).