Risk Assessment and Treatment Process

Document Classification	[insert classification]
Document Reference	ISMS-Doc-06-2
Version	1
Dated	[insert date]
Document Author	[insert name]
Document Oner	[insert name/role]

Revision History

Version	Date	Revision Author	Summary of Changes

Distribution

Name	Title

Approval

Name	Position	Signature	Date

Contents

Figures

Tables

1 Introduction

The effective management of information security has always been a priority for [Organization Name] in order to manage risk and safeguard its reputation in the marketplace. However, there is still much to be gained by [Organization Name] in continuing to introduce industry-standard good practice processes.

The international standard for information security, ISO/IEC 27001, was first published by the ISO and IEC in 2005 and was revised in 2013. [Organization Name] has decided to adopt ISO/IEC 27001 as an effective way to put in place an information security management system (ISMS) to ensure that our objectives remain current and our processes, policies and controls are continually improved as part of this exercise it has decided to pursue full certification to ISO/IEC 27001 in order that the effective adoption of information security best practice may be validated by an external third party.

A key part of an ISMS is the management of risk. Risk is the happening of an unwanted event, or the non-happening of a wanted event, which affects a business in an adverse way.

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 organization policies and procedures or external legislation and regulation
- The resources of the business are not utilised in an efficient and effective manner
- The confidentiality, integrity and availability of information is not reliable

It is important that [Organization Name] 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.

The selection of controls to address identified risks will be made from Annex A of ISO/IEC 27001 but also from the expanded and additional controls laid out in ISO IEC 27017 and 1SO/IEC 27018

2 Risk assessment and treatment process

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

- ISO/IEC 27001- Information Security Management Systems
- ISO 31000 - Risk Management Guidelines

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

The process of risk assessment and treatment is shown in figure 1 and described in more detail in the following sections. 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.

2.1 Criteria for performing information security risk assessments

There are a number of criteria that determine when an information security risk assessment should be carried out within [Organization Name] 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 organization, the ISMS 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 organization which may invalidate the conclusions from previous risk assessments e.g. changes to relevant legislation, 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 organization should err on the side of caution and ensure that one is performed.

2.2 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 organization's 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.

2.3 Process diagram

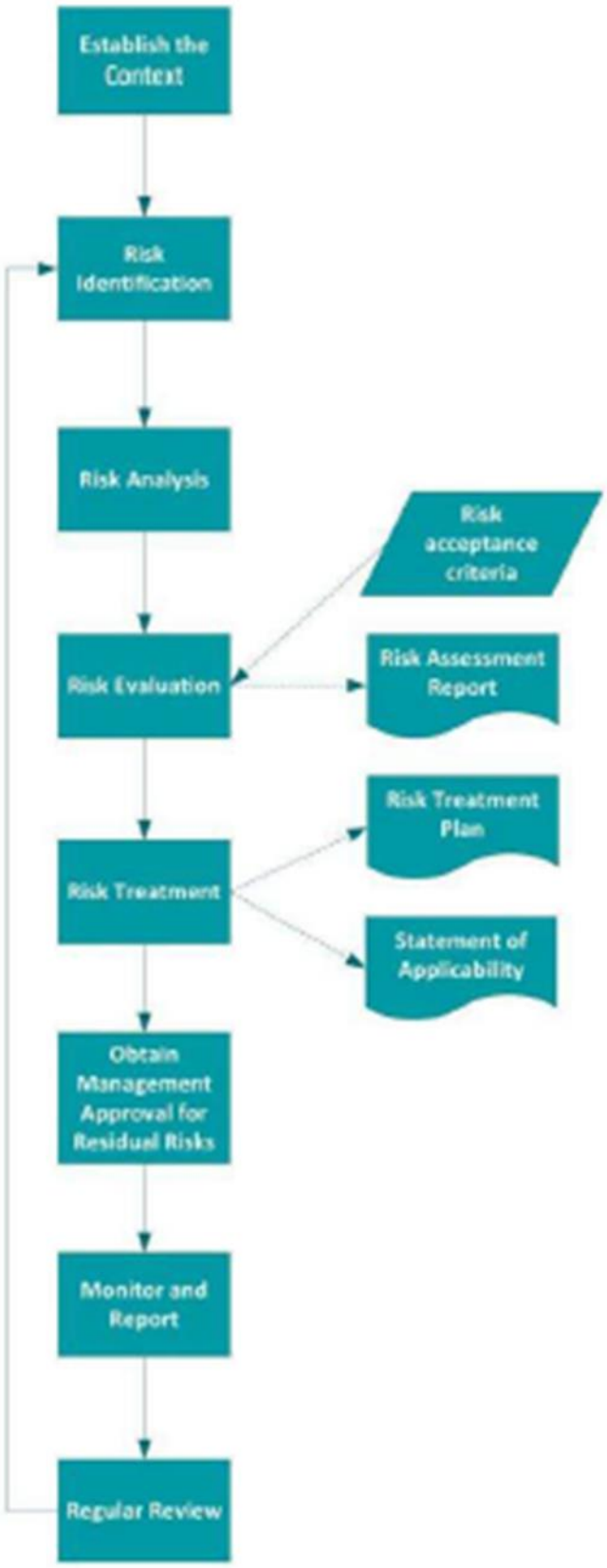

Figure 1: Risk Assessment and Treatment Process Diagram

2.4 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, organizational 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 organization's culture
- Standards, guidelines and models adopted by the organization
- Form and extent of contractual relationships
- The type(s) of cloud services provided

The external context may include:

- The cultural, social, political, legal, regulatory, financial, technological, economic, natural and competitive environment, whether international, national, regional or local
- Key drivers and trends having impact on the objectives of the organization
- 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
- Organizational units e.g. specific departments

- Business process(es)
- IT services, systems and networks
- Customers, products or services

2.5 Risk identification

The process of identifying risks to be assessed will consist of the following steps in line with the requirements of ISO/IEC 27001. Risks are identified to the confidentiality, integrity or availability of information within the scope of the ISMS.

[Note - there is a wide variety of risk identification approaches you could use (see ISO/IEC 27005 for a full list) and we do not list them all here. Instead, two common approaches are proposed; asset-based (usually more detailed) and scenario-based a high-level approach). The ISO/I EC 27001 standard does not specify a particular approach so either is acceptable or certification purposes.]

[Note - if you choose to conduct an asset-based risk assessment the following sections will apply:]

2.5.1 Compile/ maintain asset inventory

A full inventory of assets is compiled and maintained by [Organization Name]. The definition of an asset is taken to be "anything that has value to the organization" and is therefore worthy of protection. This will include customer data that [Organization Name] 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, organization structure

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.

2.5.2 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.

2.5.3 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).

[Note - if you choose to conduct a scenario-based risk assessment the following section will apply]

2.5.4 Identify risk scenarios

The identification of risks to the information security of the organization will be performed by a combination of group discussion and interview with interested parties.

Such interested parties will normally include (where possible):

- Manager(s) responsible for each business-critical activity
- Representatives of the people that normally carry out each aspect of the activity
- Providers of the inputs to the activity
- Recipients of the outputs of the activity
- Appropriate third parties with relevant knowledge
- Representatives of those providing supporting services and resources to the activity
- Any other party that is felt to provide useful input to the risk identification process

Identified risks will be recorded with as full a description as possible that allows the likelihood and impact of the risk to be assessed. Each risk must also be allocated an owner.

[Note - the rest of the document applies to both risk assessment approaches:]

2.6 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.

2.6.1 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 organization or similar organizations 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.

2.6.2 Assess the impact

An estimate of the impact that the loss of confidentiality, integrity or availability cou ld have on the organization must be given. This should consider existing controls that lessen the impact, as long as 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 organization
- Legal, contractual or organizational obligations

The impact of each risk will be graded on a numerical scale of 1 (low} to S (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 organization 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 subject of the risk assessment.

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

2.6.3 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

[Note -you may decide to change the definition of high, medium and low classifications based on your general risk appetite e.g. you may decide that only risks with a score of 16 or more will be classified as high.)

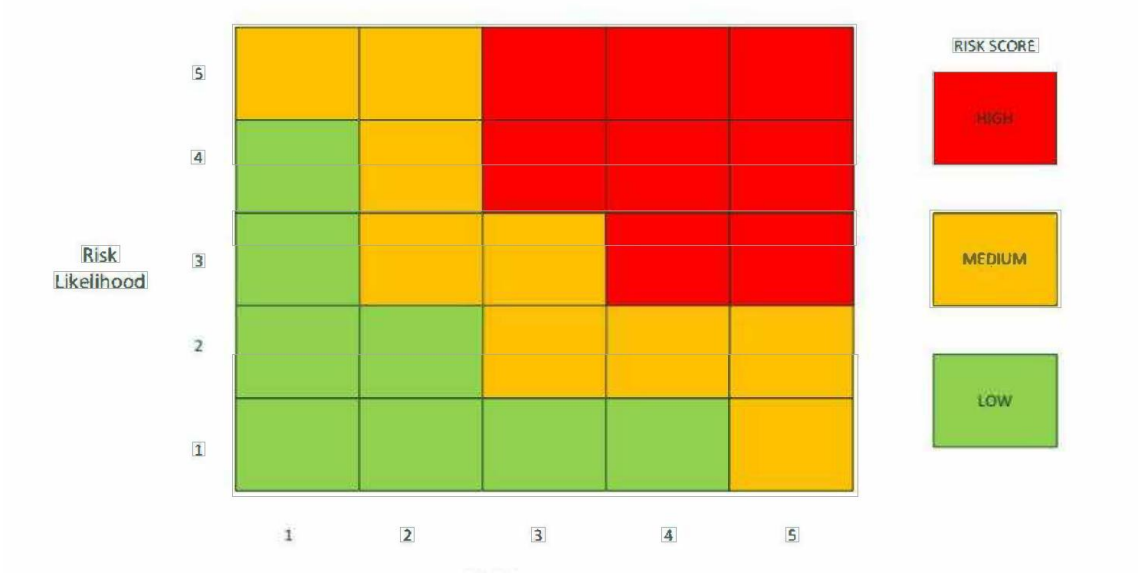

Figure 2: Risk matrix chart

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

2.7 Risk evaluation

The purpose of risk evaluation is to decide wh ich risks can be accepted and which ones need to be treated. This will take into account 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 organization.

2.7.1 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
- Risk Owner
- Whether the risk is recommended for acceptance or treatment
- Priority of risks for 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.

2.8 Risk treatment

For those risks that are agreed to be above the threshold for acceptance by [Organization Name], 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 organization may decide to accept these risks even though they remain at a medium rating. Such decisions must be recorded with a suitable explanation.

2.8.1 Risk treatment options

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

1. Modify the risk - apply appropriate controls to lessen the likelihood and/or impact of the risk
2. Avoid the risk by taking action that means it no longer applies
3. Share 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.

2.8.2 Select ion of controls

In accordance with [Organization Name]'s adoption of the 1S0/IEC 27001 standard, Annex A of that document will be used as the starting point for the identification of appropriate controls to address the risk treatment requirements identified as part of the risk assessment exercise.

The controls set out in Annex A will be supplemented by the extended and additional guidance set out in the following codes of practice:

- IS0/IEC 27002- Code of practice for information security controls
- IS0/IEC 27017 - Code of practice for information security controls based on 1S0/IEC 27002 for cloud services
- 1S0/IEC 27018 - Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors

The last two of these provide specific application of the Annex A controls to a cloud service provider scenario and address the area of the protection of PII more comprehensively than the 1S0/IEC 27001 standard on its own.

2.8.3 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
- Risk owner
- Recommended treatment option
- Control(s) to be implemented
- Responsibility for the identified actions

- Cost estimate for implementing the control(s)
- Timescales for actions
- Expected residual risk levels after the controls have been implemented

2.8.4 Statement of applicability

The Statement of Applicability will set out those controls from Annex A of the ISO/IEC 27001 standard that have been selected and the reasons for their selection. It will also detail those that have been implemented and identify any that have been explicitly excluded together with a reason for such exclusion.

2.9 Management approval

At each stage of the risk assessment process management will be kept informed of progress and decisions made, including formal signoff of the proposed residual risks. Management will approve the following documents:

- Risk Assessment Report
- Risk Treatment Plan
- Statement of Applicability

Signoff will be indicated according to [Organization Name] documentation standards. In addition to overall management approval, the acceptance or treatment of each risk must be signed off by the relevant risk owner.

2.10 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 review process of the ISMS.

2.11 Regular review

In addition to a full annual review, risk assessments will be evaluated on a regular basis to ensure that they remain current and the applied controls valid. The relevant risk assessments will also be reviewed upon major changes to the business such as office moves, mergers and acquisitions or introduction or new or changed IT services.

2.12 Roles and responsibilities

Within the process of risk assessment there are several key roles that play a part in ensuring that all risks are identified, addressed and managed. These roles are shown in the RACI table below, together with their relative responsibilities at each stage of the process.

2.12.1 RACI chart

The table below clarifies the responsibilities at each step using the RACI model, i.e.:

- R: Responsible
- A: Accountable
- C: Consulted
- I: Informed

Step	Information Security Manager	Risk Owners	Top Management
Establish the context	R	C	A
Risk identification	C	R	A
Risk analysis	C	R	A
Risk evaluation	C	R	A
Risk treatment	R	C	A
Management approval for residual risks	C	C	A/R
Monitor and Report	R	I	A
Regular Review	R	C	A

Table 3: RACI Chart

Further roles and responsibilities may be added to the above table as the risk assessment and treatment process matures within [Organization Name].

3 Conclusion

The process of risk assessment and treatment is fundamental to the implementation of a successful Information Security Management System (ISMS) and forms a significant part of the ISO/IEC 27001 standard. Only by fully understanding its risks can an organization hope to ensure that the controls it has in place are enough to provide an appropriate level of protection against information security threats.

For a cloud service provider, the regular assessment of risks and the application of comprehensive controls is vital to the continuing confidence of its cloud service customers and in meeting its obligations to protect PII from all-too-common threats.

By following this process [Organization Name] will go some way to ensuring that the risks that it faces in the day to day operation of its business are effectively managed and controlled.