IRIS BUSINESS SERVICES LIMITED



Risk Management Process Manual

Version 1.3

April – 2023

This document contains sensitive & confidential information, and should not be disclosed, transmitted, duplicated, used in whole or part other than for its intended purpose and intended recipients.

Document Information

Document Name	IBSL – Risk Management Process	**Version**	1.3
Date Created	28 August 2017	**Release Date:**	25th April 2023
Document No.	ISMS 14		
Classification	Internal		
Prepared By	Akshay Rane	**Document Owner**	Head-IT (CTO)
Reviewed By	Mahesh Tilave		
Approved By	P K X Thomas		

Distribution: To all employees and relevant consultants, contractors, vendors and third parties of the Iris Business Services Limited (IBSL).

Review history:

Sr.No.	Author	Date	Review details	Version Number
1	CISO	March 2018	No Change required	Ver 1.0
2	CISO	March 2018	No Change required	Ver 1.0
3	CISO	September 2020	Annual Review	Ver. 1.1
4	CISO	September 2021	Annual Review	Ver. 1.2
5	CTO	August 2022	Annual Review	Ver 1.2
6	CTO	April 2023	Annual Review	Ver 1.3

Summary of changes from the previous release

Sr. No.	Version	Brief Description of the change(s) made
1	1.0	Initial release
2	1.1	Changes according to change in scope from product specific to enterprise level certification ● Replaced IRIS GST Reference with IBSL, organization as a whole
3	1.2	Added: ● Asset Identification

		● Identification of Threat and Vulnerability ● Control Rating Table ● Control Implementation ● Residual Risk Value Threshold

Table of Contents

1.0 PROCESS SUMMARY **3**

2.0 REFERENCES **3**

3.0 DEFINITIONS AND ACRONYMS **4**

4.0 PROCESS INPUTS **4**

5.0 ENTRY CRITERIA **4**

6.0 PROCEDURE **4**

6.12 RESIDUAL RISK CALCULATION 10
6.13 RISK TREATMENT 11
RISK TREATMENT OPTIONS 11
RISK TREATMENT PRIORITY 12
6.14 MONITORING AND REVIEW 12
6.15 COMMUNICATION AND CONSULTATION 12
6.16 PREPARE STATEMENT OF APPLICABILITY 12

7.0 VALIDATION CRITERIA **12**

8.0 PROCESS DELIVERABLES **12**

9.0 EXIT CRITERIA **13**

10.0 ANNEXES **13**

1.0 Process Summary

This process details the steps involved in managing the risks from the stage of identifying the risks to closure.

2.0 References

ISO 27001:2013 - Clause 6.1, 6.2, 17.1.1

3.0 Definitions and Acronyms

CISO - Chief Information Security Officer

4.0 Process Inputs

- Knowledge of business and technical processes
- Knowledge in risks
- Incident / Weakness Reporting Form
- Contract
- Change Requests
- Statement of Applicability
- Business Continuity Plan test results
- Management Review Meeting
- Internal Audit
- Clients Audit
- Customer Feedback
- Security Incidents
- Internal Technical Vulnerability Assessment
- External Technical Vulnerability Assessment
- External Audits

5.0 Entry Criteria

- Risk Identification Meeting

6.0 Procedure

The Risk Assessment Process requires the involvement from all levels in the IBSL's Function and requires an understanding on the Information Security Risk, Service management system risks and the Quality system risks faced by IBSL's Function.

6.1 Establishing the context

IBSL's Function shall determine the internal and external context of the organization, in which the organization seeks to achieve its objectives and concerns of internal and external stakeholders, and shall be documented in the context of the organization document.

6.2 Asset Identification

All assets including hardware, software, information, non-IT assets and people in IBSL are identified and are appropriately valued. Following are the asset categories

Classification	Assets (illustrative only)

Information Assets	Databases, system documentation, training material, procedures, plans, quality records.
Software Assets	Application software, System Software, development tools and utilities.
Paper Documents	Contracts, Guidelines, Company Documentation.
Physical Assets	Desktops, laptops, Routers, Firewall, Servers Networking devices, Racks, Storage devices (tapes, hard disks), buildings, Surveillance, furniture etc.
People	Personnel, Customers, Subscribers, Sub-Contractors.
Services	Air-conditioning, Electricity Supply, Internet Connectivity.

6.3 Risk Identification

Risk owners shall identify the risks associated with the loss of confidentiality, integrity and availability of information and or which will impact the business objectives of the organization. Risk owners are the functional heads and these Risk owners will be identified / appointed by the Steering Committee.

Identification of risks will be done on yearly basis for existing processes and on an ad-hoc basis as required for new services/functions introductions, or changes contemplated to existing products or processes and IBSL's Function's business objectives.

IBSL's Function shall perform the risk assessments for any other process considering the following list of risk factors but may not be limited to;

- Changes to Legislations and Guidance
- Transition of Key Managers
- Change in the Database (Up gradation/New Change)
- Specific safety conditions (additional monitoring)
- Critical Audit Findings
- Missed Internal Audits
- Procedural Gaps
- Service Level Agreement Non compliances
- Environmental Threats
- Software and Link Failures
- Data Backup Failure
- Communication Failure
- Organizational Changes

6.4 Asset Confidentiality / Integrity / Availability Rating

Confidentiality

Definition: A concept that applies to organization's information assets that must be held in confidence and indicates a level of protection that must be provided to assets to prevent unauthorized disclosure.

If the confidentiality of asset is compromised, the impact on the organisation needs to be understood/estimated by asset owner. Based on the sensitivity of the asset, confidentiality characteristic of an asset has to be rated as low, moderate, high, and critical and mission critical.

Low/ Public (1) - unauthorized disclosure of the information asset result in negligible damage to its business objectives, financial performance or reputation.

Moderate/ Internal (2) - unauthorized disclosure of the information asset result in limited damage to its business objectives, financial performance or reputation.

High/ Sensitive (3) - unauthorized disclosure of the information asset result in high damage to its business objectives, financial performance or reputation.

Critical/ Restricted (4) - unauthorized disclosure of the information asset result in severe damage to business objectives, disruption of business activities and potential damage to the Business's reputation and revenue streams.

Mission Critical/ Secret (5) - unauthorized disclosure of the information asset result in severe or catastrophic damage to the Organization, its business objectives, significant disruption of business activities, danger on human life, and potential longer-term damage to the Organization's reputation and revenue streams.

Integrity

Definition: A characteristic applying to organization's information assets that provides assurance, under all conditions, that the asset has not been altered without authorization

If the integrity of asset is compromised, the impact on the organisation needs to be understood/estimated by asset owner. Based on the sensitivity of the asset, integrity characteristic of an asset has to be rated as low, moderate, high, and critical and mission critical.

Low (1) - Insignificant impact if the asset is compromised. Typically, this would include information which would not result in a financial / business loss to IBL, if made available publicly.
Moderate (2) - Some impact if the asset is compromised. It may result in some level of business / financial loss, if disclosed to unauthorized users.

High (3) - High impact if the asset is compromised. It would probably result in high business / financial loss to IBSL

Critical (4) - Significant impact if the asset is compromised. It would probably result in severe damage to the Organization, critical business / financial loss to IBL and potential damage to the Organization's reputation.

Mission Critical (5) - Very Critical impact if the asset is compromised. It would result in severe damage to the Organization, mission critical business / financial loss to IBL impacting the reliability of data and potential damage to the Organization's reputation.

Availability

Definition: A characteristic that ensures organization's information assets will be available to authorized users when required.

If the asset is not available, the impact on the organization needs to be understood/estimated by asset owner. Based on the sensitivity of the asset, availability attribute of an asset has to be rated as low, moderate, high, and critical and mission critical.

Low (1) - Non-availability of asset would have minimal / insignificant impact on IBL. For example, assets with Maximum Permissible Downtime greater than 5 working days.

Moderate (2) - Non-availability of asset may have some impact on IBL, if prolonged for a long period of time. For example, assets where Maximum Permissible Downtime is between 3 & 5 working days.

High (3) - Non-availability of asset would result in high impact to IBL. This would typically apply to assets where Maximum Permissible Downtime is between 3 & 1 working days.

Critical (4) - Non-availability of asset would result in critical impact to IBL. This would typically apply to assets where Maximum Permissible Downtime is 1 working day.

Mission Critical (5) - Non-availability of asset would result in high impact to IBL. This would typically apply to assets where Maximum Permissible Downtime is less than 1 working day.

6.5 Asset Classification Rating:

The asset classification value is the computation of the values assigned to Confidentiality, Integrity and Availability
The asset classification has to be rated as follows:
1 - Low value
2 - Moderate value
3 - High value
4 - Critical value
5 - Mission Critical value

6.6 Identification of Threat

Threat is any aspect that can exploit vulnerability, intentionally or accidentally, and obtain, damage, or destroy an asset. Such threats shall be identified for the several asset groups noted in previous section.

6.7 Identification of Vulnerability

Vulnerabilities are the weaknesses or gaps in an organisation's environment that can be exploited by threats to gain unauthorized access to an information asset. Vulnerabilities that can be exploited by threats shall be mapped for each group of information asset.

6.8 Risk Analysis

The risks can be categorized Low, Medium and High for the Likelihood and Impact. The following Matrix provided in tables shall be utilized for the Risk Analysis

Likelihood	
Probability is the measure of the chance that a threat will be able to exploit a given vulnerability. Probability values are assigned using the following matrix	
Value	**Criteria**
1(Low)	The probability of occurrence of potential event is very low, as all the control measures are in place to take care of the same. Hence there is very low chance of occurrence.
2(Medium)	The chances of occurrence of potential event is moderate, even though the control measures are in place and this occurrence may cause a moderate loss/impact on the process, deliverables and business.
3(High)	The chance of occurrence of potential event is high. In spite of having control measures like SOPs, checklists, the probability of occurrence is **high.**

Impact

Impact is the measure of the adversity of a security event that can be described in terms of loss or degradation of any, or a combination of any, of the three security goals - CIA (confidentiality, integrity and availability). Impact value shall be assigned as per matrix as follows:	
Value	**Criteria**
1(Low)	Capable or susceptible to potential event with minimal impact on the customer deliverables, where Customer will most likely not be able to detect the failure.
2(Medium)	Capable or susceptible to potential event with medium impact on the output, here the customer will more like able to detect the failure. Example-Not meeting the SLA, such things could lead to decrease in the performance level, having moderate effect on processes and deliverables.
3(High)	Capable or susceptible to potential event with severe impact on the output, where the customer shall not be satisfied with the failure and this may directly or indirectly impact on processes and deliverables. Example-Not following SOP, non-compliance to regulatory requirements.

Asset Rating – Asset rating will be derived by quantifying the level of confidentiality, integrity and availability of each asset. Assets will be rated from 1 to 5 wherein 1 being lowest and 5 highest.

Thus Asset rating will be the function of confidentiality, integrity and availability
Asset Value = Confidentiality x Integrity x Availability

From "Aggregate Asset Value"	To "Aggregate Asset Value"	Aggregate Asset Value	Final Asset Classification Rating
1	4	Low value	1
5	10	Moderate value	2
11	40	High value	3
41	64	Critical value	4
65	125	Mission Critical value	5

6.9 Risk Evaluation

Risk value will be calculated based on the Asset Rating, Risk Likelihood and Impact of Risk. Risk value is the multiplication of Asset Rating, Likelihood and Impact of Risk. Minimum value of the Risk value will be 1 and maximum value of the Risk value will be 27.

Inherent Risk Value = Asset Rating x Likelihood × Impact

Asset Rating	Likelihood	Impact	Risk Value	Risk Category

1	1	1	1	Low
1	1	2	2	Low
1	1	3	3	Low
2	1	1	2	Low
1	2	2	4	Medium
1	2	3	6	Medium
2	3	1	6	Medium
3	2	1	6	Medium
3	1	3	9	High
3	3	3	27	High
4	3	3	36	High
5	3	3	45	High

6.10 Control Rating

ISMS Controls put in place will be rated on the basis of effectiveness in mitigating the risk. Rating will be given from 1 to 5 wherein 1 being lowest and 5 highest.

Control Rating	Description	Definition
1	Very Low	Significant control deficiencies have been identified and no compensatory controls identified
2	Low	Several control deficiencies have been identified and some compensatory controls exist
3	Medium	Few low impact control deficiencies noted
4	High	Few low impact control deficiencies noted, compensatory controls exists
5	Very High	No/Minor control deficiencies which are acceptable by the organization

6.11 Control Implementation

Information security controls to mitigate inherent risks identified in previous stage shall be identified. These security controls shall derive from the Statement of Applicability within which the Company has identified controls that are applicable to it. Necessary implementation guidance shall be available in the Information Security Procedure document that contains descriptive activities and responsibilities for implementing every control mentioned in Risk Register Risk Treatment Plan and Statement of Applicability.

6.12 Residual Risk Calculation

Residual Risk is a remaining risk after considering the existing controls.

Residual Risk value will be calculated based on the Inherent Risk Value minus Control Rating.

Residual Risk value = Inherent Risk – Control Rating, is considered as a Residual Risk.

Residual Risk Value threshold are as follows;

Slab level	From "Residual Risk Value"	To "Residual Risk Value"	Classification of Residual Risk Value	Residual Risk Value Rating
1st	1	4	Very low risk value	1
2nd	5	14	Low risk value	2
3rd	15	24	Moderate risk value	3
4th	25	34	High risk value	4
5th	35	45	Very high-risk value	5

.

Residual Risk is a function of inherent risk – controls and it is termed as

- Low
- Medium
- High

6.13 Risk Treatment

For each identified risk, the risk owners will prioritize the risks in consultation with CISO and will establish and implement an appropriate "Risk Treatment" option within the agreed time frame.

Risk Treatment Options

Mitigate	Risk will be treated with immediate effect based on the priority of the risk. Periodic monitor and review will be carried out. Risk Owner to accept certain degree of risk
Transfer	Pass this risk to someone else (e.g. by insurance or by outsource / passing responsibility for the risk to a contractor) Take cost effective actions to reduce the risk
Accept	Accept the risk and live with it
Avoid	Agree that the risk is too high and do not proceed with the project or activity. You may decide not to proceed with the activity likely to generate the risk, where practical. Alternatively, you may think of another way to reach the same outcome.

- If the residual Risk value is ≥ Medium, the risks will be treated. Each risk and Risk Treatment Activities will be assigned to the risk owners.
- As part of the Risk Treatment Process, IBSL's Function management will determine and document what actions (prevention or detection) are necessary to manage the risk.
- Residual Risk value < medium is considered as an Acceptable Level of Risk or Residual risk. Risk owners will review those risk on a yearly basis and will take appropriate action to treat those risks if required. The results of the risk treatment options will be approved by the risk owner.

Risk treatment priority

- High Risk: Treated with high priority.
- Medium Risk: Treated within agreed time or compensating controls.
- Low Risk: No treatment or long range plan as decided by the Risk owner in consultation with CTO.

6.14 Monitoring and Review

The Risk Register will be reviewed on a yearly basis by the risk owner. The Risk review inputs will be sent to CISO for review. Also Risk Inputs and status will be presented to Management during Management Review Meetings.

Risks and risk response activities will be monitored by the responsible Risk owners to ensure that risks remain within acceptable risk levels, that emerging risks and gaps are identified and that risk response and control activities are adequate and appropriate.

6.15 Communication and Consultation

Communication and consultation is a continual and iterative process that an organization conducts to provide, share or obtain information and to engage in dialogue with stakeholders regarding the management of risk.

6.16 Prepare Statement of Applicability

List the control objectives and controls selected and implemented with the reasons for their selections. List the control objectives and controls excluded with justifications.

7.0 Validation Criteria

- Review Risk assessment and management plan

8.0 Process Deliverables

- Risk assessment and management plan
- Minutes of Meetings

9.0 Exit Criteria

- Approved Risk assessment and management plan

10.0 Annexes

Template for Statement of Applicability.