IRIS BUSINESS SERVICES LIMITED



Information Security Management Policy

Version 1.6

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	Information Security Policy	**Version :**	1.6
Date Created	28th August 2017	**Released Date**	25th April 2023
Document No.	ISMS 01		
Classification	Internal		
Prepared By	Akshay Rane	**Document Owner**	Head-IT (CTO)
Reviewed and Approved By	Mahesh Tilave PKX Thomas		

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

Review history:

	Author	Date	Review details	Version Number
1	CISO	March 2018	Annual Review	Ver 1.1
2	CISO	March 2019	Annual Review	Ver 1.2
3	CISO	September 2020	Annual Review	Ver 1.3
4	CISO	September 2021	Annual Review	Ver 1.4
5	CTO	August 2022	Annual Review	Ver 1.5
6	CTO	April 2023	Annual Review	Ver 1.6

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	Change in team members
3	1.2	Change in team members – Removed Madhavi Dhomse and added Nisha Rai as HR Representative
4	1.3	Changes according to change in scope from product specific to enterprise level certification Changes in process owners Changes in Service Providers Changes in email domain Change in diagram
5	1.4	Updated Stakeholder Details
6	1.5	Annual Review
7	1.6	Change in 7.4 Stakeholder identification and analysis--Removed Sabu O and added Mahesh Tilave as IT Head

Table of Contents

1. ISMS Scope Statement	6
2. Normative References	6
3. Terms and definitions	6
4. Context of the organization	7
4.1 Understanding the organization and its context	7
4.2 Understanding the needs and expectations of interested parties	8
4.3 Determining the scope of the Information Security Management System	10
5. Leadership	16
5.1 Leadership and Commitment	16
5.2 Policy	16
6. Planning	21
6.1 Actions to address risks and opportunities	21
6.2 Information security objectives and planning to achieve them	22
7. Support	22
7.1 Resources	22
7.2 Competence	23
7.3 Awareness	23
7.4 Communication	24
7.5 Documented information	27
8. Operation	28
8.1 Operational planning and control	28
8.2 Information security risk assessment	28
8.3 Information security risk treatment	28
9. Performance evaluation	29
9.1 Monitoring, measurement, analysis and evaluation	29
9.2 Internal audit	29
9.3 Management review	30
10. Improvement	30
10.1 Nonconformity and corrective action	30
10.2 Continual improvement	31

INFORMATION SECURITY MANAGEMENT SYSTEM

Introduction

Information is an asset, like other important business assets has value to an organization and consequently needs to be suitably protected. Information security protects information from a wide range of threats in order to ensure business continuity, minimize business losses and maximize return on investments and business opportunities.

Information security consists of preserving the following elements:

- **Confidentiality**: Ensuring that information can only be accessed by those with the proper authorization.
- **Integrity**: Safeguarding the accuracy and completeness of information and the ways in which it is processed.
- **Availability**: Ensuring that authorized users have access to information and associated assets whenever required.

Information security is achieved by implementing a suitable set of controls, which could be policies, practices, procedures, organizational structures and software.

ISO 27001:2013 is a standard specification for an Information Security Management Systems (ISMS). ISO 27001:2013 provides conditions for information security management. Comprised of the 14 Domain, 35 control objectives and 114 controls of the ISO 27001:2013 standard, this reference applies to the development, implementation and maintenance stages of an information security system. Organisations applying for certification are evaluated according to this document.

An ISMS is the means by which Senior Management monitor and control their security, minimizing the residual business risk and ensuring that security continues to fulfill corporate, customer and legal requirements. It forms part of an organization’s internal control system.

An ISMS is designed to ensure adequate and proportionate security controls of information assets in IBSL. It will maintain and improve competitive edge and provide secure and uninterrupted utilization of information technology to reduce organization’s overall business risk.

Purpose of the ISMS Manual:

The purpose of this ISMS manual is to:

- Define the Information Security Policy and to adequately describe the ISMS required to implement the Information Security policy,
- Incorporate ISMS Procedures commonly applicable throughout the business unit
- Serve as a reference for the executives of the company and third parties regarding the ISMS adopted by the company.

1. ISMS Scope Statement

"Information Management System applies to software development, implementation, after sales service, IT Infrastructure, Administration, Human Resource, Legal and Finance functions of IRIS Business Services Limited"

This is in accordance with Statement of Applicability, Version 1.1, dated 21st September 2020.

Following are the associated services.

- Product Teams
- IT Infrastructure Management
- Human Resource
- Administration
- Finance
- Legal

2. Normative References

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO/IEC 27000, Information technology — Security techniques — Information security management systems — Overview and vocabulary

ISO22301 Business Continuity planning

ISO31000 Risk Management

3. Terms and definitions

For the purpose of the Standard, the following terms and definitions apply.

a. Availability: Ensuring that authorized users have access to information and associated assets when required.

b. Confidentiality: Ensuring that information is accessible only to those authorized to have access.

c. Integrity: Safeguarding the accuracy and completeness of information and processing methods.

d. Information Security: Security preservation of confidentiality, integrity and availability of information.

e. Information Security Management System: ISMS is the part of the overall management system, based on business risk approach, to establish, implement, operate, monitor, review, maintain and improve information security.

f. Risk Acceptance: Decision to accept a risk.

g. Risk Analysis: Systematic use of information to identify source and to estimate the risk.

h. Risk Assessment: Overall process of risk analysis and risk evaluation.

i. Risk Evaluation: Process of comparing the estimated risk against given risk criteria to determine the significance of risk.

j. Risk Management: Coordinated activities to direct and control an organization with regard to risk.

k. Risk Treatment: Treatment process of selection and implementation of measures to modify risk.

l. Statement of applicability: Document describing the control objectives and controls that are relevant and applicable to the organization's ISMS based on the results and conclusions of risk assessment and risk treatment processes.

4. Context of the organization

4.1 Understanding the organization and its context

COMPANY PROFILE

IRIS Business Services Limited is one of the first provider of full professional XBRL products and solutions to organizations globally. The company headquartered in Mumbai, India with international offices in United States, Singapore, United Kingdom, and the UAE.

IRIS is a direct member of XBRL International and XBRL US. The Company has over eighteen years of proven expertise in the financial information management space, providing customized technology solutions for data and content management, for the dissemination of information to investors and stock exchanges, and for effective content management to institutional clients.

Over the last eight years, IRIS has been very closely involved in the XBRL space, in taxonomy creation, software solutions and in the conversion of structured and

unstructured data into XBRL for SEC filing in the US. IRIS has multidisciplinary skills in XBRL as well as in technology. Taxonomy experts, software engineers, business analysts and accountants come together to provide a complete range of products and services across the XBRL supply chain.

IRIS' XBRL based solutions and services include:

Software products, tools and services for authoring and consumption of XBRL data,

Data conversion services from structured and unstructured data into XBRL

It enables workflow based e-filing solutions for Regulators in Capital Markets and Banking, XBRL Consulting and Training Services, Taxonomy development and testing services

IRIS offers solutions for:

Enterprises, Business Registers, Central Banks, Stock Exchanges, BFSI, Governments/ Regulators

IRIS supports content requirements for institutional clients as well as retail clients both in the Indian and global markets. The content solutions range from raw data provision, to newsletter creation and research support. Our digitization division undertakes a large volume digitization of financial content. Our financial training division offers programs both to retail and institutional clients

Company's Objective through ISMS

An ISMS is designed to ensure adequate and proportionate security controls of information assets in IBSL. It will maintain and improve competitive edge and provide secure and uninterrupted utilization of information technology to reduce organization's overall business risk.

IBSL has developed, implemented, maintained and continually improve documented ISMS within the context of the organization's overall business activities and risk.

The policy document is divided into

- **ISMS Policy Manual**

  The policy manual will include the security policy statement from the management. The mandatory controls and the applicable control objectives.

- **ISMS Procedure Manual**

  The procedure manual will give the detailed procedures for achieving the control objectives.

- **ISMS Forms and Templates**

  The relevant forms and templates to the procedures are attached here.

4.2 Understanding the needs and expectations of interested parties

The interested parties that are relevant to the ISMS of IBSL have been determined below:

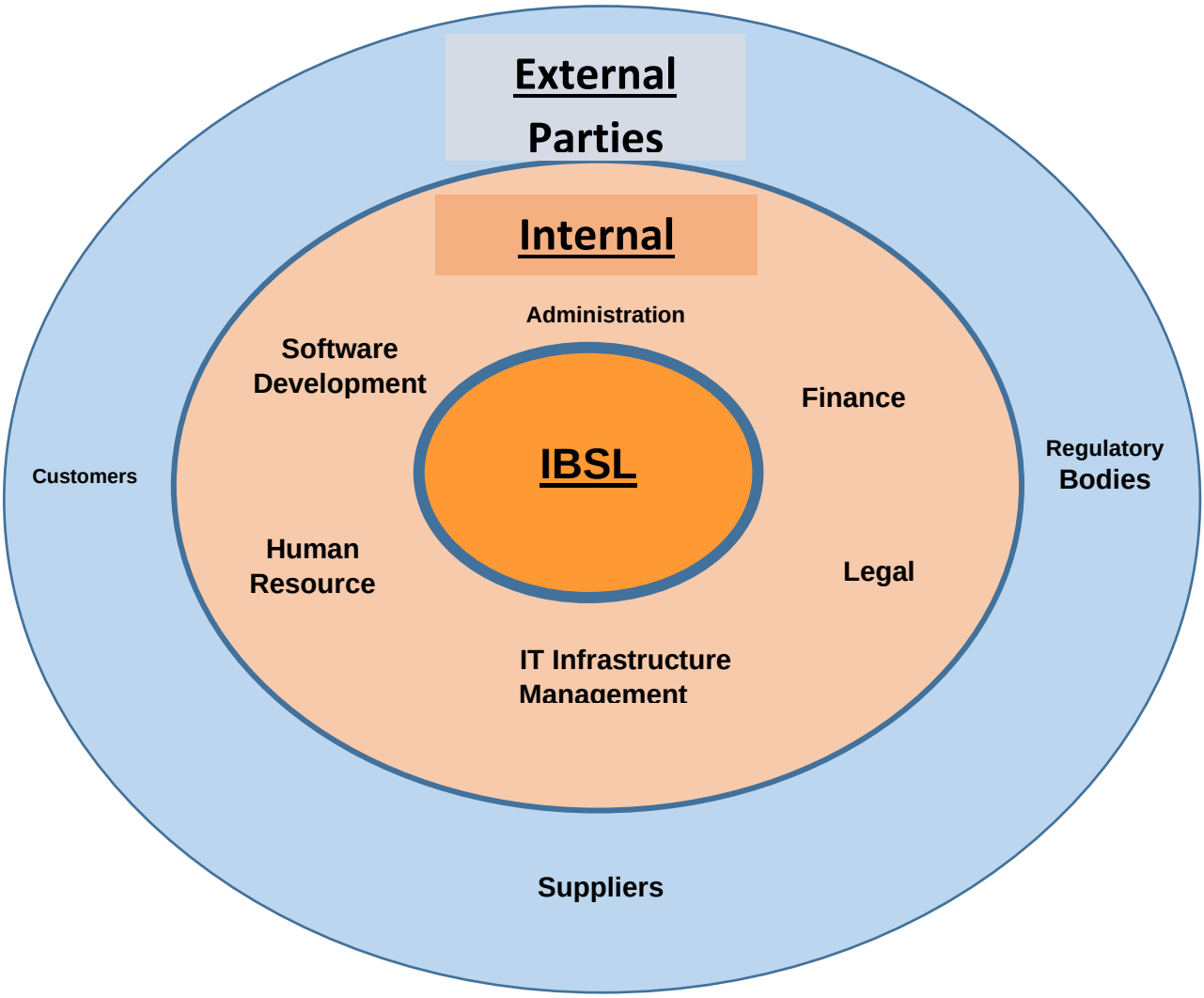
Internal Parties	Needs	Expectation	Issues occurring to achieve needs & expectations
Product Team	People, Technology, Training	Product stability and continuous improvement	Disrupted development, Lack of skilled workforce
Human Resource	People, Training	Adequate resourcing and training of resources	Attrition, inadequate hiring
IT Infrastructure Management	People, Technology, Training	Robust IT infrastructure management	Technical glitches, outdated systems, Vendor non-performance
Administration	People, Training, Technology	Security and maintenance of facilities	Safety hazards, Vendor non-performance
Finance	People, Training	Maintain strong financials	Inadequate financial controls
Legal	Compliance	Maintain compliance with legal authorities	Non-Compliance to legal authorities
Customers	Stability & continuous improvement of the product	Timely and excellent quality business services	Resources, Competency & Disruption in services
Regulatory Bodies	On time filling of returns, payment of dues, compliance to regulations	Continued compliance	Continuous change in the compliance eco-system
Supplier (Tata, AWS, STPI, Azure, I-ONE)	Continued business relationship	On time supply, timely delivery of product & services	Pricing, disruption in business relationship

Following is the department-wise segregation of suppliers;

- ITSS – Amazon Web Services, Azure - Data Center Services
- ITSS – Tata Tele Services Ltd, STPI and I-ONE. – Internet Service Provider
- Administration – Sigma Fire Equipment - Fire Fighting Equipment,
- Administration – Safepro Center for Training and Consultancy - Emergency Drill Conductor
- Product Teams - On-Contract Developers (Consultants)

4.3 Determining the scope of the Information Security Management System

"Information Management System applies to software development, implementation, after sales service, IT Infrastructure, Administration, Human Resource, Legal and Finance functions of IRIS Business Services Limited"

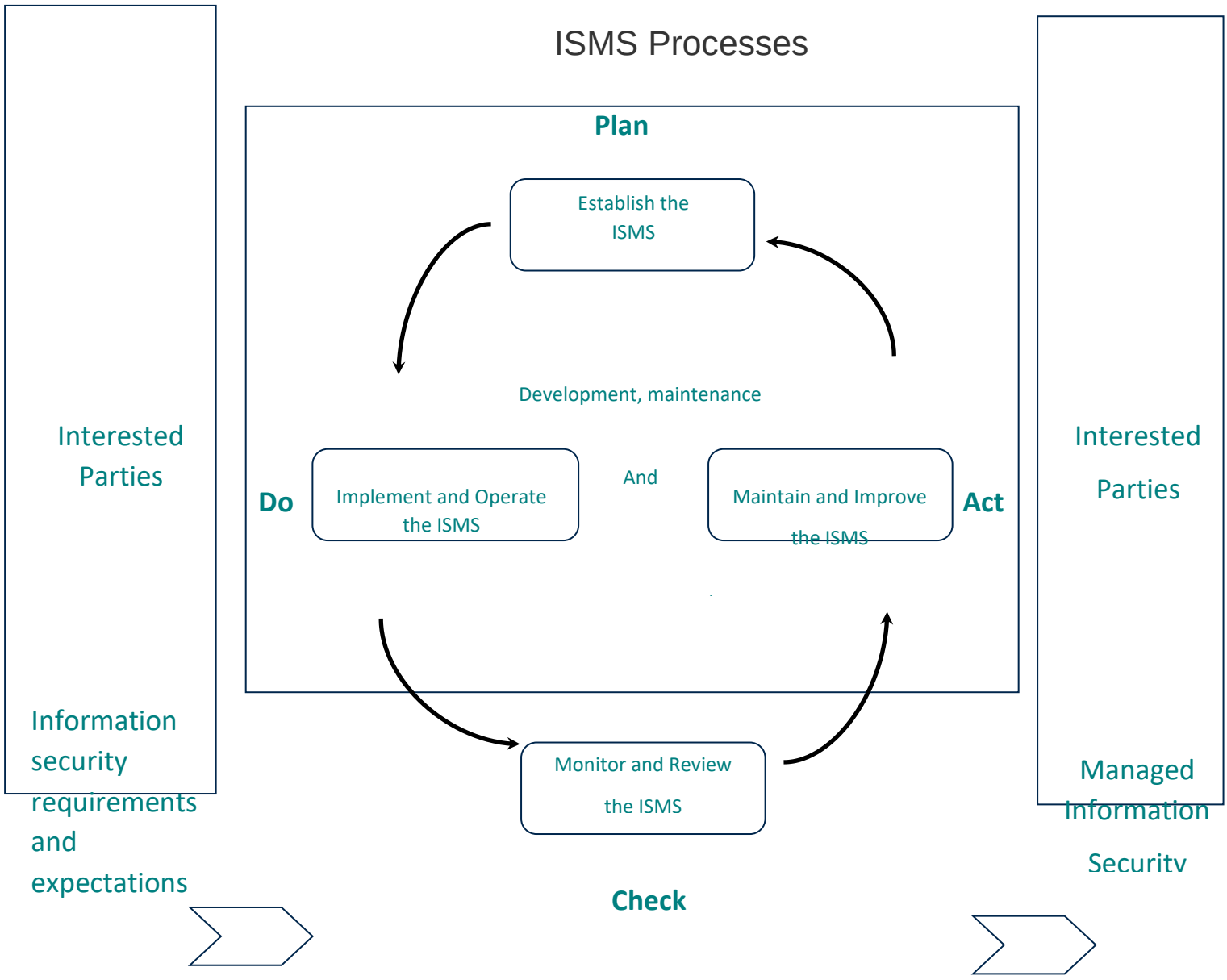


4.4 Information security management system

The organization shall establish, implement, maintain and continually improve an information security management system, in accordance with the requirements of this International Standard.

PDCA MODEL

For the purpose of this standard the process used is based on the PDCA model.



Plan (establish the ISMS): Establish security policy, objectives, targets, processes and procedures relevant to managing risk and improving information security to deliver results in accordance with an organization's overall policies and objectives.

Do (implement and operate the ISMS): Implement and operate the security policy, controls, processes and procedures.

Check (monitor and review the ISMS): Assess and, where applicable, measure process performance against security policy, objectives and practical experience and report the results to management for review.

Act (maintain and improve the ISMS): Take corrective and preventive actions, based on the results of the management review, to achieve continual improvement of the ISMS.

STAGE	STEP
PLAN	**ESTABLISH ISMS** **1. ISMS Scope** ▪ The process used to establish the scope ▪ Strategic and Organizational context ▪ Approach to Information Security Risk Management ▪ Criteria for information security risk evaluation ▪ Degree of Assurance ▪ Identification of information assets **2. ISMS Policy** ▪ Define the information security policy ▪ Framework for setting its objectives and targets ▪ Establish an overall sense of direction and principles **3. Risk Identification and Assessment** ▪ Appropriate process based Risk Assessment approach ▪ Impact and likelihood of threats ▪ Calculation of risk based on the assessment ▪ Identification of residual risks **4. Risk Treatment Plan** ▪ Method selected for treating of risk ▪ Controls in place for treatment of risk ▪ Additional controls to be implemented ▪ Time frame for implementing the proposed controls ▪ Identification of Acceptable level of risk **5. Statement of Applicability** ▪ Selection of control objective and controls ▪ Preparation of Statement of Applicability

DO	**IMPLEMENT AND OPERATE ISMS** **1. Formulate a Risk Treatment Plan** ▪ Accept the risk, or ▪ Transfer the risk, or ▪ Reduce the risk to an acceptable level **2. Implement the Risk Treatment Plan** ▪ Controls to be implemented in line with Risk Treatment Plan ▪ Assign responsibility and individual accountability for actions ▪ Monitor them against specified criteria ▪ Approval from Management for acceptable risk and residual risk **3. Training and Awareness** ▪ Conducting Awareness program on Information Security on semiannual basis. ▪ Security Training wherever necessary ▪ Monitoring of training and awareness program to ensure continuous effectiveness **4. Manage Resources** ▪ Adequate Resources to be allocated for ISMS operations ▪ Monitoring of resources

CHECK	**MONITOR AND REVIEW ISMS** **1. Regular Reviews of ISMS effectiveness** ▪ Execute the monitoring procedures ▪ Identify inadequate controls ▪ Take corrective actions ▪ Record action and event having an impact on ISMS **2. Conduct ISMS Internal Audit** ▪ To ensure Information Security Policy effectiveness and in line with business requirements ▪ Ensure appropriate risk assessment methodology is used ▪ Procedures are being followed and controls are in placed ▪ Residual risk have been assessed correctly and are acceptable to the management ▪ Agreed actions from previous audits and reviews have been implemented ▪ Compliant with standards **3. Management Reviews** ▪ Check periodically for ISMS effectiveness ▪ Identify improvements needed and implement the same
ACT	**MAINTAIN AND IMPROVE ISMS** ▪ Implement Identified Improvements ▪ Take appropriate corrective and preventive actions ▪ Communicate the results and actions and agree with all interested parties ▪ Improvement achieving intended objectives

5. Leadership

5.1 Leadership and Commitment

Management has established, implemented, operates, monitors, reviews, maintains and improves ISMS by formation of Security Forum and issuance of a Policy statement on information security through Company Directive dated Sept. 07, 2017.

The Security Forum is formed to ensure the following:

1. Information security objectives and the plans are established and integrated with processes
2. Roles and responsibilities for information security requirements have been established
3. Importance of meeting Information security objectives and conforming to the information security policy, its requirements and the need for continual improvement are communicated.
4. Sufficient resources are provided and sufficient direction has been provided to develop, implement, operate and maintain the ISMS effectively.
5. Ensures ISMS achieves its intended outcome
6. Acceptable level of risk are identified
7. Periodic reviews of ISMS are conducted.

5.2 Policy

Building Transparency. Driving Growth.

IRIS BUSINESS SERVICES LIMITED

INFORMATION SECURITY POLICY STATEMENT

Information is a valuable corporate asset and it should be protected from all threats, whether internal or external, deliberate or accidental. Information security management ensures uninterrupted business, prevents and minimizes damages due to security incidences using best practices and standards. The objective of this policy is to ensure:

a. **Confidentiality, integrity and continuous availability of information for business needs**

b. **Implementation of security controls by Information Security Management System (ISMS) through policies and procedures.**

c. **Reporting of security breaches for appropriate, timely and corrective actions.**

d. **Maintaining all relevant records and documents supporting the security controls in compliance with statutory, regulatory and procedural requirements.**

e. **Reviewing and monitoring of controls and conducting periodical audits.**

Chief Information Officer

5.3 Organizational roles, responsibilities and authorities

Management has ensured by establishing Information security forum the responsibilities and authorities for roles relevant to Information Security are assigned and communicated. This cover:

Ensuring that ISMS confirms to the requirements of ISO 27001:2013 and reporting on the performance of the information security management system to management.

(Please Refer IBSL - Information Security Procedure document)

5.4 Security Objective Metrics

Functions	Objectives	Metrics	Target	Owner	Frequency	Domain Reference
Product Teams	**Systems Acquisition, Development and Maintenance**	Application security assessment at system acquisition. Bi-annual control self-assessment	95% bug free. All changes should be authorized.	Product Owner	Annual	14.0

		of change controls, system acquisition process, information security requirement during development, Regression testing, user acceptability and integration testing	Zero high security vulnerability in the application			
IT Infrastructure Management	**Information Security Policy**	Every function should attend the semi-annual Training & Awareness. Annual Review to be conducted	95% IS Policy Awareness All review points should be addressed	CISO	Semi-Annual	5.0
	Access Control	Semi-annual access review is conducted	100% corrective action on the review points identified. Timely review	CISO and Business Owners	Semi-Annual	9.0
	Physical and Environmental Security	Semi-annual physical access review is conducted	95% corrective action on the review points identified. Timely review	CISO and Business Owners		11.0

	Asset Management	Review of asset register and risk register. Annual Control Self-assessment of asset management process	95% corrective action on the review points identified.	Business Owners	Semi-Annual	8.0
	Communication & Operations Security	Annual Control Self-assessment of communications and operations security controls such as Antivirus and malware compliance Firewall and security device configuration review SLA monitoring of IT providers	100% compliance towards antivirus and malware 100% corrective action on the review points identified.	CISO	Daily monitoring of Anti-virus and Firewall. SLA monitoring on annual basis	12.0 and 13.0
	Information Security Incident Management	Semi-annual review of critical security incidents	Non-occurrence of repeatable critical incidents	CISO	Semi-Annual	16.0
	Information Security Aspects of Business Continuity Management	Annual BCP Drill	95% corrective action on the review points identified.	CISO and business owner	Annual	17.0

Human Resource	**Implementation of Human Resource Security**	HR security effectiveness is measured through semi-annual Training & Awareness, Annual control self-assessment focused on HR information security. Background Check of all onboarding employees.	98% corrective action on the review points identified. Every function should attend the training 100% corrective action on the review points identified for onboarding employee BG Check.	HR Head	Semi-Annual	7.0
Admin	**Physical and Environmental Security**	Semi-annual physical access review is conducted	95% corrective action on the review points identified. Timely review	Admin and Business Owners	Semi-Annual	11.0
Finance	**Compliance**	Annual Self-assessment of internal financial controls	100% corrective action on the review points identified. 100% compliance of	Head - Finance	Annual	18.0

			critical financial controls			

6. Planning

6.1 Actions to address risks and opportunities

. **6.1.1 General**

When planning for the information security management system, the organization has considered the issues referred to in 4.1 and the requirements referred to in 4.2 and determine the risks and opportunities that need to be addressed. Additionally, Management reviews the ISMS at planned intervals of once a year to ensure its continuity, suitability and effectiveness. Management also ensures that a review takes place in response to any changes affecting the basis of the original risk assessment, e.g. significant security incidents, new vulnerabilities or changes to the organizational or technical infrastructure. The results of the review are clearly documented and the records maintained accordingly

6.1.2 Information security risk assessment

Define a Systematic approach to Risk Assessment

Method of risk assessment is identified and in accordance with business information security, legal and regulatory requirements. Policies and objective has been defined to reduce risk to acceptable levels. Criteria for accepting the risk and identifying the acceptable level of risk have been determined.

Identify the Risk

IT processes and associated information have been identified in accordance with the scope and the owners of these processes. Risk is identified based on impact and likelihood of losses of confidentiality, integrity and availability on these processes.

Assess the Risk

The business harm that might result from a security failure, taking into account the potential consequences of loss of information have been assessed along with the realistic likelihood of such a security failure occurring

Estimation has been done for the level of risk and also determined, whether, the risk is acceptable or requires treatment using the criteria established.

6.1.3 Information security risk treatment

Identify and evaluate options for the treatment of Risk

Appropriate controls have been applied for accepting the risk, which satisfies the organization policy. The reduction of risk is also done by transferring the associated business risk to other parties like insurance, suppliers etc.

Select control objectives and controls for the treatment of Risks

Appropriate control objective has been selected based on the risk assessment carried out and a risk treatment plan has been framed.

Risk assessment is carried out once a year to produce consistent, valid and comparable results

6.2 Information security objectives and planning to achieve them

Management has ensured by establishing Information security forum that ISMS confirms to the objectives of ISO 27001:2013 comprises of 35 security objectives and 114 security controls contained in 14 domains. Applicable controls are listed separately in Statement of Applicable. The following is a brief overview of each of these domains:

- **Information Security Policy** - Provide guidelines and management advice for improving information security.
- **Organizational Information Security** – Facilitate information security management within the organization.
- **Human Resource Security** – Facilitate HR services
- **Asset Management** – Carry out an inventory of assets and protect these assets effectively.
- **Access Contro**l - Control access to information.
- **Cryptography** – Inscriptions.
- **Physical and Environmental Security** - Prevent the violation, deterioration or Disruption of industrial facilities and data
- **Operations Security** - Ensure the adequate and reliable operation of information processing devices.
- **Communication Security** - Ensure the adequate and reliable operation of information processing devices.
- **Systems Acquisition, Development and Maintenance** - Ensure that security is incorporated into information systems.
- **Supplier relationship** – Procurement, SL
- **Information Security Incident Management**- Incident, Change & problem management.
- **Information Security Aspects of Business Continuity Management** - Minimize the impact of business interruptions and protect the company's essential processes from failure and major disasters.
- **Compliance** - Avoid any breach of criminal or civil law, of statutory or contractual requirements, and of security requirements.

7. Support

7.1 Resources

Provision of resources

Resources are provided:

1. To establish, implement, operate and maintain ISMS.
2. To ensure that information security procedures support the business requirements.
3. To Identify and address legal and regulatory requirements and contractual security obligations.
4. To maintain adequate security by correct application of all implemented controls.
5. To carry out reviews when necessary, and to react appropriately to the results of these reviews.

7.2 Competence

The Security Forum ensures the following:

1. The necessary competencies for personnel performing work effecting the ISMS are determined
2. Information Security Awareness training are provided and, if necessary, employing competent personnel to satisfy these needs.
3. The effectiveness of training provided and actions taken are evaluated
4. Maintaining records of training, skills, experience and qualifications.

The Security Forum also ensures that all relevant personnel are aware of the relevance and importance of their information security activities and their contribution to the overall achievement of the ISMS objectives.

7.3 Awareness

The following training and awareness programs are being conducted on a continuous basis:

- Training is being given to the Facility Management Team on information security and the requirements of ISO27001:2013 standards
- Training is also given to the relevant personnel of Support team on best practices and ISO27001:2013 standards
- Induction training program to newly joined personnel includes a session on information security

- Training on ISO27001:2013 certification process and Internal Audit of ISMS has been provided to the information security team.
- Training will be given on a continuous basis to all the relevant personnel involved in the ISMS process
- Information Security awareness is created through posters display of instructions, screen savers etc.
- Feedback from attendees is taken to assess the effectiveness of the training program

The procedure for Information Security Awareness is as per IBSL available in IBSL - Information Security Procedure Manual

7.4 Communication

The organization shall determine the need for internal and external communications relevant to the information security management system including:

a) On what to communicate;

b) When to communicate;

c) With whom to communicate;

d) Who shall communicate; and

e) The processes by which communication shall be effected.

Communication Plan:

Purpose of Communications Management Plan

The overall objective of a Communications Management Plan is to promote the success of an IBSL by meeting the information needs of IBSL stakeholders. The IBSL Communications Management Plan (CMP) defines the IBSL structure and methods of information collection, screening, formatting, and distribution and outline understanding among project teams regarding the actions and processes necessary to facilitate the critical links among people, ideas, and information that are necessary for IBSL success.

The intended audience of the IBSL CMP is the CIO as Service Delivery Head, CTO/HRM/CISO as Head IT, Head-compliance as IT Operations Lead, PM/Business Owner, and IT Infra Team.

Stakeholder identification and analysis

Name	Title	Contact	Communication	Vehicle
S.Swaminathan	Director/CEO	s.swaminathan@irisbusiness.com	Management Communication (Strategic Communication)	*Email* *Verbal*
K.Balachandran Vineet Kandoi	Director-Finance	k.balachandran@irisbusiess.com vineet.kandoi@irisbusiess.com	Financial Announcements	*Email*
Deepta Rangarajan	Director-Operations	deepta.rangarajan@irisbusiness.com	Internal communication	*Email*
P K X Thomas	(CTO)	pkx.thomas@irisbusiness.com	Internal communication to PM/Business Owner	*Email* *Phone*
Mahesh Tilave Akshay Rane	IT-Lead Information Security Coordinator ITSS Team	mahesh.tilave@irisbusiness.com akshay.rane@irisbusiness.com ITsupport@irisbusiness.com	Security Awareness mails IT Announcements IS Overall communication with Risk Management related communication	*Email* *Phone*
Nisha Rai / Sujit Acharya	HR/Administration	nisha.rai@irisbusiness.com sujit.acharya@irisbusiness.com	HR & Administration Announcements & communication	*Email* *Phone* *Verbal*

Communications Vehicles and Communications Matrix

Vehicle	Target	Description Purpose	Frequency	Owner	Distribution Vehicle	Internal/ External
Business Announcements	All Employees	One page communication of project progress and deliverable status & Current affairs	Monthly	CEO	Email Verbal	Internal
Communication to Media	Media	Organization related announcements & declaration	As & when require	CEO	Verbal	External
Financial Announcements	PM/Business Owner	Approval of budgets	As & when required	Director – Finance	Email	Internal
Internal communication to PM/Business Owner	PM/Business Owner	Existing & New project updates	As per project schedule	Service Delivery Head (CIO)	Email	Internal
Security Awareness mails	All employee	IT IS related information/communication	As & when required	CTO (Head IT)	Email	Internal
IT Announcements	All employee	IT specific announcements	As & When require	CTO (Head IT)	Email	Internal
HR & Administration Announcements & communication	All employee	People information Physical Security	As & when require	HR/Administration	Email Verbal	Internal

7.5 Documented information

7.5.1 General

ISMS documentation includes the following:

- Documented statement of the security policy and control objective
- The scope of ISMS and procedures and controls in support of the ISMS
- Risk assessment report and risk treatment plan
- Documented procedures needed by IBSL to ensure effective planning, operation and control of its information security processes.

Please refer **IBSL - Master List for ISMS Documents**

7.5.2 Creating and updating

When creating and updating documented information the organization shall ensure appropriate:

a) Identification and description (e.g. a title, date, author, or reference number);

b) Format (e.g. language, software version, graphics) and media (e.g. paper, electronic); and

c) Review and approval for suitability and adequacy.

7.5.3 Control of documented information

Documented information required by the information security management system and by this International Standard shall be controlled to ensure:

a) It is available and suitable for use, where and when it is needed; and

b) It is adequately protected (e.g. from loss of confidentiality, improper use, or loss of integrity).

For the control of documented information, the organization shall address the following activities, as applicable:

c) Distribution, access, retrieval and use;

d) Storage and preservation, including the preservation of legibility;

e) Control of changes (e.g. version control); and

f) Retention and disposition.

Documented information of external origin, determined by the organization to be necessary for the planning and operation of the information security management system, shall be identified as appropriate, and controlled.

NOTE: Access implies a decision regarding the permission to view the documented information only, or the permission and authority to view and change the documented information, etc.

The procedure for control of documents is as per IBSL - Information Security Procedure Manual

8. Operation

8.1 Operational planning and control

The organization shall plan, implement and control the processes needed to meet information security requirements, and to implement the actions determined in 6.1. The organization shall also implement plans to achieve information security objectives determined in 6.2. Applicable controls are listed separately in Statement of Applicability and the same is leveraged for implementation of processes required to meet IS requirements

Statement of Applicability document covers following aspects:

1. All the applicable control objectives
2. Reasons for exclusion of any control objectives
3. Relevant documents and records related to the selected objectives

The detailed statement of applicability is available in **ISMS 01**

Management approval has been obtained for proposed residual risks and authorization for implementation

The organization shall keep documented information to the extent necessary to have confidence that the processes have been carried out as planned.

The organization shall control planned changes and review the consequences of unintended changes, taking action to mitigate any adverse effects, as necessary.

The organization shall ensure that outsourced processes are determined and controlled.

8.2 Information security risk assessment

The organization shall perform information security risk assessments at planned intervals or when significant changes are proposed or occur, taking account of the criteria established in 6.1.2 a).

The organization shall retain documented information of the results of the information security risk assessments.

8.3 Information security risk treatment

The organization shall implement the information security risk treatment plan.

The organization shall retain documented information of the results of the information security risk treatment.

Refer IBSL - Risk Management Process Manual for Procedure on Risk Assessment and Methodology

9. Performance evaluation

9.1 Monitoring, measurement, analysis and evaluation

The organization shall evaluate the information security performance and the effectiveness of the information security management system.

The organization shall determine:

a) What needs to be monitored and measured, including information security processes and controls;

b) The methods for monitoring, measurement, analysis and evaluation, as applicable, to ensure valid results;

NOTE: The methods selected should produce comparable and reproducible results to be considered valid.

c) When the monitoring and measuring shall be performed;

d) Who shall monitor and measure;

e) When the results from monitoring and measurement shall be analysed and evaluated; and

f) Who shall analyse and evaluate these results.

The organization shall retain appropriate documented information as evidence of the monitoring and measurement results.

Please refer performance measurement matrix in section 5.4 of this document for details.

9.2 Internal audit

The organization shall conduct internal audits at planned intervals once in six months to provide information on whether the information security management system:

a) Conforms to

1) The organization’s own requirements for its information security management system; and

2) The requirements of this International Standard;

b) Is effectively implemented and maintained.

The organization shall:

c) Plan, establish, implement and maintain an audit programme(s), including the frequency, methods and responsibilities, planning requirements and reporting. The audit programme(s) shall take into consideration the importance of the processes concerned and the results of previous audits;

d) Define the audit criteria and scope for each audit;

e) Select auditors and conduct audits that ensure objectivity and the impartiality of the audit process;

f) Ensure that the results of the audits are reported to relevant management; and

g) Retain documented information as evidence of the audit programme(s) and the audit results.

Please refer **IBSL - IA procedure for details**

9.3 Management review

Top management has established information security forum which shall review the organization's information security management system at planned intervals to ensure its continuing suitability, adequacy and effectiveness.

The management review shall include consideration of:

a) The status of actions from previous management reviews;

b) Changes in external and internal issues that are relevant to the information security management system;

c) Feedback on the information security performance, including trends in:

1) Nonconformities and corrective actions;

2) Monitoring and measurement results;

3) Audit results; and

4) Fulfilment of information security objectives;

d) Feedback from interested parties;

e) Results of risk assessment and status of risk treatment plan; and

f) Opportunities for continual improvement.

The outputs of the management review shall include decisions related to continual improvement opportunities and any needs for changes to the information security management system.

The organization shall retain documented information as evidence of the results of management reviews.

The Management Review Procedure is as per IBSL available in IBSL - Information Security Procedure Manual

10. Improvement

10.1 Nonconformity and corrective action

When nonconformity occurs, the organization shall:

a) React to the nonconformity, and as applicable:

1) Take action to control and correct it; and

2) deal with the consequences;

b) Evaluate the need for action to eliminate the causes of nonconformity, in order that it does not recur or occur elsewhere, by:

1) Reviewing the nonconformity;

2) Determining the causes of the nonconformity; and

3) Determining if similar nonconformities exist, or could potentially occur;

c) Implement any action needed;

d) Review the effectiveness of any corrective action taken; and

e) Make changes to the information security management system, if necessary.

Corrective actions shall be appropriate to the effects of the nonconformities encountered.

The organization shall retain documented information as evidence of:

f) The nature of the nonconformities and any subsequent actions taken, and

g) The results of any corrective action.

10.2 Continual improvement

Information Security Forum has implemented and identified improvements in the ISMS. Appropriate corrective and preventive action in accordance with the learning from security incidents are taken. The results and actions to all interested parties are communicated by Security Forum. Security Forum ensures that the improvements are implemented to achieve their intended objectives. Annual internal audits would identify process improvements and the same would be addressed accordingly. Annual Risk Assessment would review the risk portfolio and would make necessary synchronization needed to maintain agility of business operations. Performance evaluation would assess the adequacy and effectiveness of ISMS controls and would remediate shortfalls if any so as to achieve the planned objectives of ISMS.

End of Document