Assessment Report

IRIS Business Services Limited

Assessment dates	18/10/2021 to 19/10/2021 (Please refer to Appendix for details)
Assessment Location(s)	Navi Mumbai (000)
Report Author	Sujit Kumar Verma
Assessment Standard(s)	ISO/IEC 27001:2013



...making excellence a habit.™

Table of contents

Executive Summary 3
Changes in the organization since last assessment 6
NCR summary graphs 7
Your next steps 9
NCR close out process 9
Assessment objective, scope and criteria 10
Statutory and regulatory requirements 10
Assessment Participants 11
Assessment conclusion 12
Findings from previous assessments 13
Findings from this assessment 15
ISMS Framework & Top Management:: 15
Legal: 16
Software Development, Implementation & Support: 16
Physical Security & Admin: 17
IT Infrastructure: 18
Minor (2) nonconformities arising from this assessment. 20
Next visit objectives, scope and criteria 22
Next Visit Plan 23
Appendix: Your certification structure & ongoing assessment programme 24
Scope of Certification 24
Assessed location(s) 24
Certification assessment program 25
Expected outcomes for accredited certification. 25
Definitions of findings: 26
How to contact BSI 27
Notes 27
Regulatory compliance 27

Executive Summary

Information Security Management System (ISMS) is implemented effectively at IRIS Business Services Limited with focus on strategic direction to create secured environment and follow the security practices. IRIS Business Services Limited management system demonstrated that it is aligned with the strategic direction of the organization to deliver intended results, particularly in providing trusted services to their customers.

Strengths:
Management Commitment.
Internal Audit Mechanism.
Well Documented Risk Management Process.

There are scope for further improvement in some areas, accordingly Opportunities for Improvement and minor non-conformities have been raised in following areas.

Opportunity for improvements are identified for the Software Development, Implementation & support and IT Infrastructure departments while the following minor non-conformities are raised.

Minor non-conformity:
1. Background verification of the persons deployed by Housekeeping agency not evident.
2. Monitoring and review of the STPI ISP service provider is not evident.

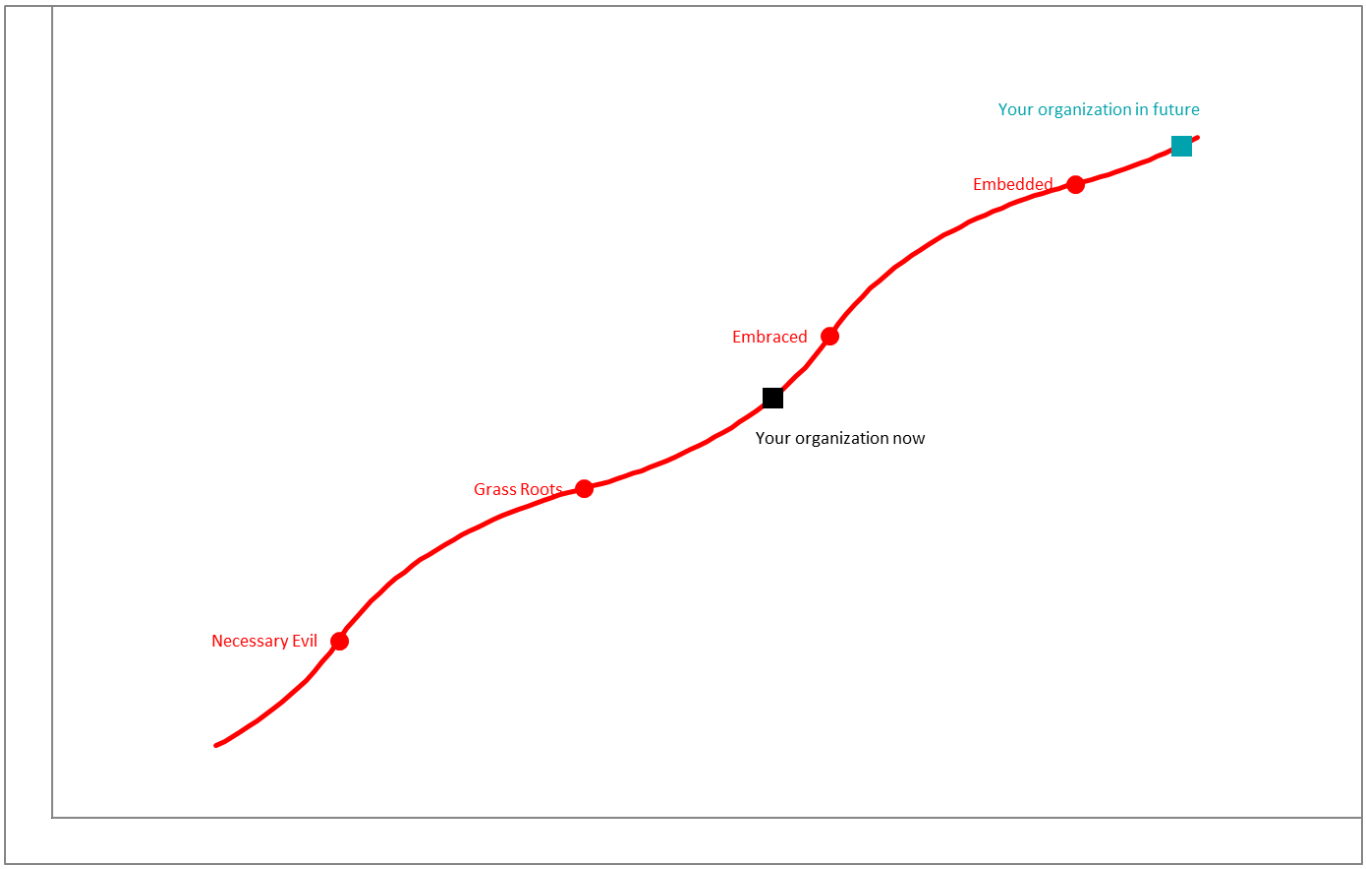
Please find the detail in the report below.

Audit was conducted remotely and participation of team is good. Internet based solution, Google meet is used for interview and sharing evidences. There was no interruption due to technical issues. The communication tool was effective, and not once did it interrupt the audit process. No connectivity issues were encountered. The audit client was comfortable with the remote audit, as the information security threat was nil. The shared documents could not be accessed by the auditor other than being able to read them and the complete control was lying with the audit client.

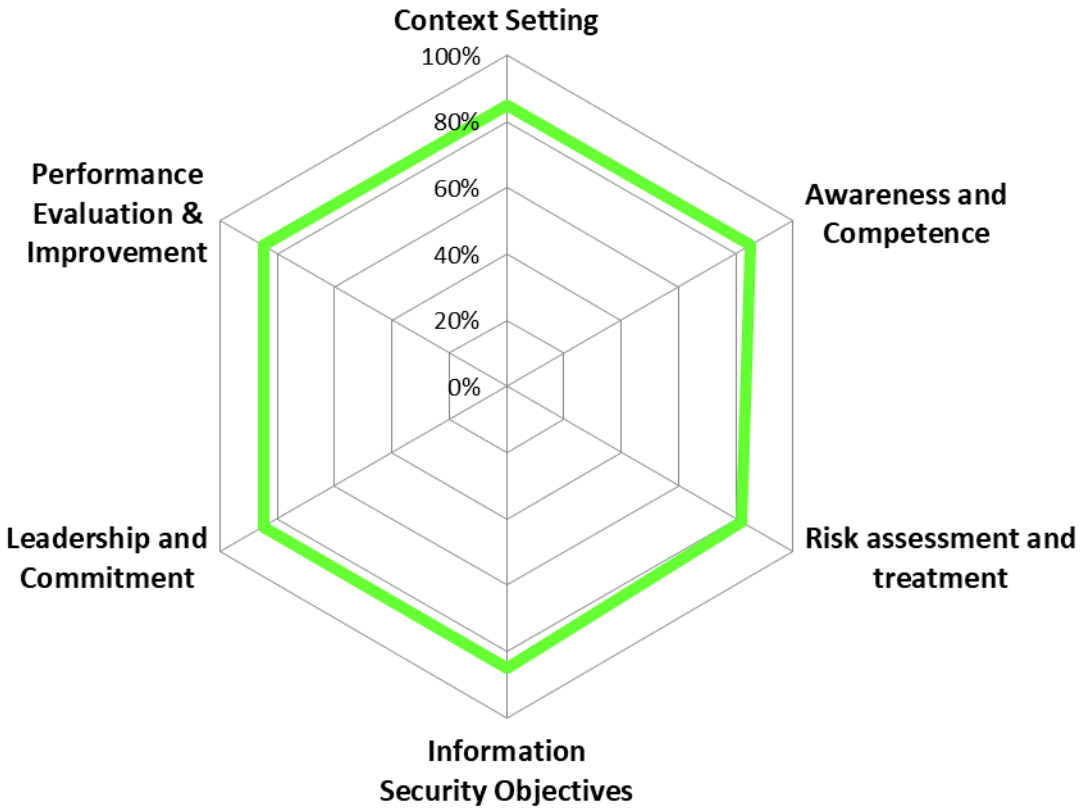
Planned Audit objectives have been achieved. The communication tool is effective and enabled smooth audit process

...making excellence a habit.™

BSI Continuum



Excellerator - Information Security Management.



Changes in the organization since last assessment

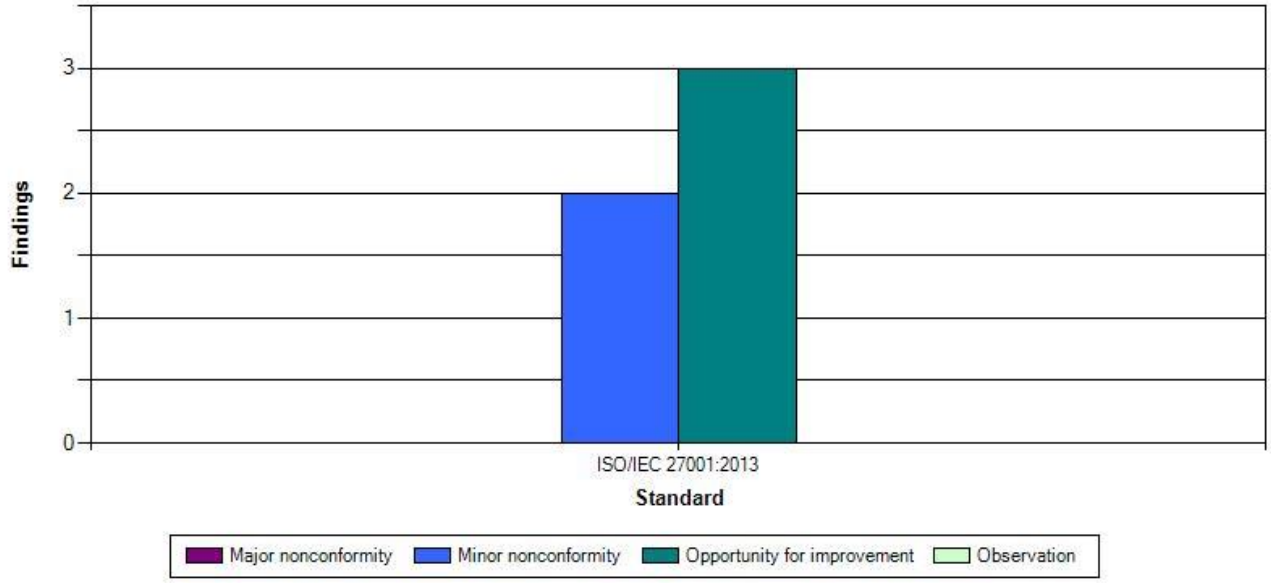
There is no significant change of the organization structure and key personnel involved in the audited management system.

No change in relation to the audited organization's activities, products or services covered by the scope of certification was identified.

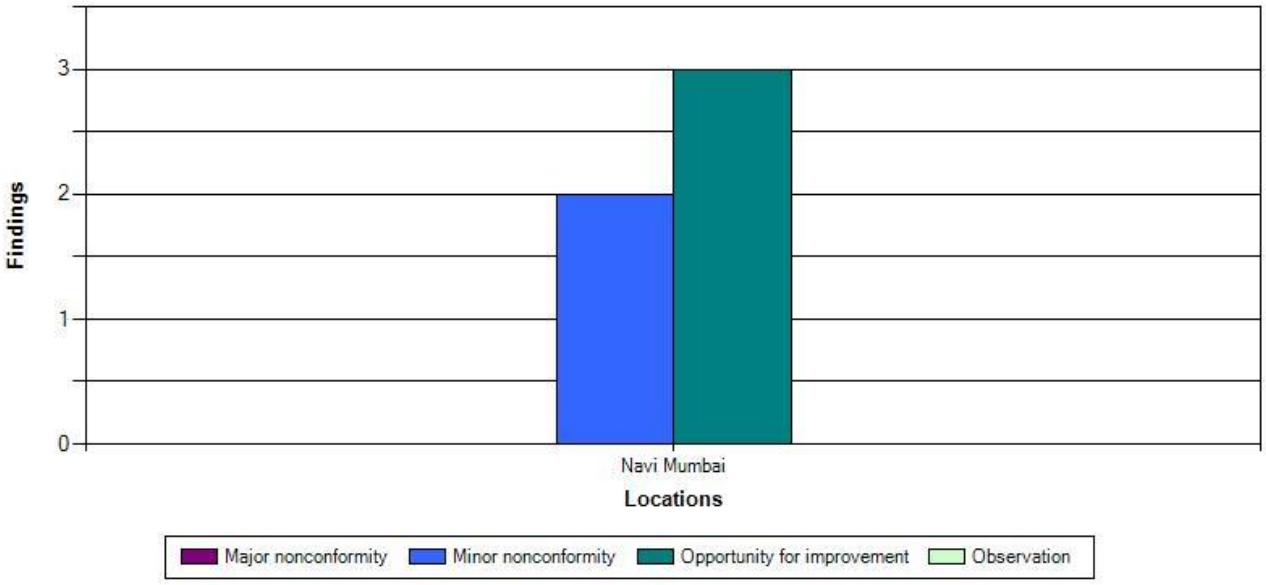
There was no change to the reference or normative documents which is related to the scope of certification.

NCR summary graphs

Which standard(s) BSI recorded findings against



Where BSI recorded findings



Your next steps

NCR close out process

Corrective actions with respect to nonconformities raised at the last assessment have been reviewed and found to be effectively implemented.

2 nonconformities requiring attention were identified. These, along with other findings, are contained within subsequent sections of the report.
A nonconformity relates to a single identified lapse, which in itself would not indicate a breakdown in the management system's ability to effectively control the processes for which it was intended. It is necessary to investigate the underlying cause of any issue to determine corrective action. The proposed action will be reviewed for effective implementation at the next assessment.

Please refer to Assessment Conclusion and Recommendation section for the required submission and the defined timeline.

...making excellence a habit.™

Assessment objective, scope and criteria

The objective of the assessment was to conduct a surveillance assessment and look for positive evidence to ensure that elements of the scope of certification and the requirements of the management standard are effectively addressed by the organization's management system and that the system is demonstrating the ability to support the achievement of statutory, regulatory and contractual requirements and the organization's specified objectives, as applicable with regard to the scope of the management standard, and to confirm the on-going achievement and applicability of the forward strategic plan and where applicable to identify potential areas for improvement of the management system.

The scope of the assessment is the documented management system with relation to the requirements of ISO27001:2013 Standard and the defined assessment plan provided in terms of locations and areas of the system and organization to be assessed.

ISO27001 Standard
IRIS Business Services Limited management system documentation

Statutory and regulatory requirements

Statutory and regulatory requirements are in place.

Assessment Participants

Name	Position	Opening Meeting	Closing Meeting	Interviewed(processes)
Rajendra Patil	Architect - Cloud & System	X	X	X
Akshay Rane	Security Analyst	X	X	X
Sachin Pandhare	Senior Manager - Information Security	X	X	X
Gayathri Chandrasekar	Senior Officer - Information Security	X	X	X
Santosh Sharma	Head - Legal		X	X
Sabu Ouseph	Senior System Administrator		X	X
Mayank Sharma	Project Lead - GST		X	X
Gautam Mahanti	Vice President		X	X
Sujit Acharya	Admin Manager		X	X

Assessment conclusion

BSI assessment team

Name	Position
Sujit Kumar Verma	Team Leader

Assessment conclusion and recommendation

The audit objectives have been achieved and the certificate scope remains appropriate. The audit team concludes based on the results of this audit that the organization does fulfil the standards and audit criteria identified within the audit report and it is deemed that the management system continues to achieve its intended outcomes.

RECOMMENDED - Corrective Action Plan Required ('Minor' findings only): The audited organization may be recommended for certification / continued certification, based upon the acceptance of a satisfactory corrective action plan for all 'Minor' findings as shown in this report. Effective implementation of corrective actions will be reviewed during the next surveillance audit.

Please submit a plan through the BSI Connect Portal detailing the nonconformity, the root cause, correction and your proposed corrective action, with responsibilities and timescales allocated. The plan is to be submitted no later than 25/10/2021. If the corrective action plan is not received by this date you may be putting your certification status at risk.

For any questions please contact your local BSI office, referencing the report number 3230691.

Use of certification documents, mark / logo or report

The use of the BSI certification documents and mark / logo is effectively controlled.

...making excellence a habit.™

Findings from previous assessments

Finding Reference	2005128-202012-N1	**Certificate Reference**	IS 683782
Certificate Standard	ISO/IEC 27001:2013	**Clause**	A13.2.4
Location reference	0047662924-000		
Category	Minor		
Area/Process:	Facility, Administration and Physical Security:		
Details:	Service agreement and NDA is not identified for UPS vendor.		
Objective Evidence:	Service agreement and NDA not evidenced for UPS service provider M/s Sendure		
Cause			
Inadequate awareness towards Information Security compliance during vendor management			
Correction/containment			
Forming a Service Agreement and NDA is initiated.			
Corrective action			
Administration Team member will be retrained on maintaining valid SLAs and NDAs of all third party service providers hired for administration function.			
Closed?:			
Yes			
Justification	NDA with confidential, Non-disclosure clause signed with the Sandures solutions dated 10Apr2021 evident. Also, NDA with the Security guard evident.		

Finding Reference	2005128-202012-N2	**Certificate Reference**	IS 683782
Certificate Standard	ISO/IEC 27001:2013	**Clause**	A18.2.3
Location reference	0047662924-000		
Category	Minor		
Area/Process:	IT Infra		
Details:	Patch update is not found reviewed for laptops available for remote working as per compliance requirements		
Objective Evidence:	HR Laptop GEN-LAP-00244 found last OS security patch updated on 16/01/2020		
Cause			

...making excellence a habit.™

Operational gap in patch management process	
Correction/containment	
Respective HR Laptop "GEN-LAP-00244" has been updated with latest patches on 30-12-2020	
Corrective action	
Endpoints will be configured to auto download OS patches and deploy from the OEM website. ITSS Team member will be retrained on the Patch Management control information security.	
Closed?:	
Yes	
Justification	Auto patch update enabled in EUS devices. Auto update for laptop host name HPFS-LAP-0005 and GEN-LAP-00274 evident.

Findings from this assessment

ISMS Framework & Top Management::

Top management has shown commitment to the ISMS deployed and are fairly satisfied with it. They have conveyed that they were able to smoothly handle the COVID related operational information security challenges because of ISMS processes already in place. They have demonstrated continual improvement with regular MRM meeting and improvement measures taken.

Statement of Applicability created and only single control A.14.2.7 excluded with justification.

Documented Information Security Policy maintained. Information Security Policy statement is mentioned, ISMS Scope statement, interested parties with need and expectations, Segregation of Suppliers, PDCA model etc. in included in it.

ISMS Roles and Responsibility of Senior management and member of Information Security committee defined in Information Security procedures document.

Function wise Information Security objectives are set & assessed on monthly basis as per IT Audit & Cybersecurity project status. This audit is carried out by external agency RSM consulting. Function wise observation is given in their audit report.

Risk management process maintained. Risk Assessment and Risk Treatment is included in it. Risk assessment excel sheet is maintained. It is common risk assessment sheet for all the processes and is updated Bi-annually. Asset identification and Asset classification is part of this document. Risk mitigation plan is made for risk with moderate and above rating. Action plan for each risk evident. Currently, moderate risks- 4 no's out of Total risk 139 is there but it is treated.

Document control procedure is available and followed. They have total ISMS policy 15 nos. and Infosec procedure manual 13 nos.

Internal Audit conducted for year 2021-2022 and findings recorded, and CAP is available in it. Management response towards corrective action plan recorded. There are 3 Minor NC s recorded for IT Infra, 1 Minor NC for HR and 1 Minor NC for SLA monitoring.

MRM meeting is conducted twice. Checked Minutes of meeting dated 30Sep2021. Review of documented policies & procedure, Internal audit result, Observations with respect to Information security objectives, Improvement identified are Migration of IT infrastructure into cloud, Phasing out EOL Systems, Implementation of new MIS for HR.

Evidenced:
Interview o Gautam Mahanti, Vice President.
Statement of Applicability version 1.1 Created Date 28Aug2017 Released Date 21.09.2021.
Information Security Management Policy Version 1.4 Date 21Sep2021.
Information Security Management Procedures /Standards / Guidelines.
IT Audit & Cybersecurity project status – September 2021.
IBSL_Risk Management Process version 1.1 Dated 21Sep2021.
Document control procedure version 1.2 Dated 21Sep2021.
IRIS-Information Security (IS) Audit Report 2021-2022 Report date 15Sep2021.
Minutes of meeting dated 30Sep2021 version 1.0

...making excellence a habit.™

Finding Reference	2119288-202110-I1	**Certificate Reference**	IS 683782
Certificate Standard	ISO/IEC 27001:2013	**Clause**	
Location reference	0047662924-000		
Category	Opportunity for Improvement		
Area/Process:	ISMS Framework & Top Management:		
Details	Information Security objectives are tracked as part of the monthly audit but record in detail could be maintained		

Legal:

Legal department takes care of compliance related to company Act, SEBI, RBI etc.
Legal agreement is executed by CS and approved by CFO. All the statutory compliances like Company related compliance report, SEBI Compliance related report (Quarterly), Financial compliances, HR related compliances, Legal related compliances trademark, patent etc. are reviewed and approved by the board of director on half yearly basis. Information related to the compliances are kept in the CS laptop and backed up in the desktop under his custody in office. Checked Anti-virus and Patch update of Laptop of company secretary Santosh Sharma.

Evidenced:
Notice of Board meeting No. 04 of 2021-22.
Agenda- Statutory compliance report for the period of Apr'10, 20210 to June 30, 2021.
Anti-virus update of laptop of Santosh Sharma Hostname GEN-LAP-00293 and found updated on 18Occt2021.
Verified Windows Security Patch Update KB5006670 of laptop of Santosh Sharma Hostname GEN-LAP-00293 and found updated on date 15Oct2021.

Software Development, Implementation & Support:

This team works in developing products, its enhancement and supporting it. Agile KANBAN model, Product backlog, User stories, Information security requirement by infosec team, Adherence to INVEST (Independently Negotiable Valuable Estimable Small Testable), Development, KANBAN Board, Testing Repositories, Publishing is included in the change management procedure. Product Manager monitoring of project, Client Manager provides support, Rollback plan, UAT Sign off, change request form, Exception based on the business justification is also included in this procedure.

Quick Scrum is project development software. Checked project flow of ST#106 (PO SO Movement changes) which is InProgress product and Completed project ST#103 GSTR1 ENB Recon Enhancement. They are major category project. Checked sample CR. Implementation plan & date, Deployment time, Enhancement, Rollback plan, Coding review, Testing. CICD is the feature in Jenkins tool used for deployment.

Checked information security awareness training completed by Project manager Mayank Sharma.

Documented Security Development Guidelines available.

Checked Application Security test report for Onyx application.

All codes are kept in code repository GIT LAB and its user access review evident.

Evidenced:
Change management procedure version 1.2 dated 12Oct2021.
ST#106 (PO SO Movement changes) Project
ST#103-ENB Recon Enhancement Project
Change Request Number S202109-CRF-2
Email from Communication IRIS dated 02Sep2021 received by Mayank Sharma regarding infosec training.
Information Security Quiz record maintained and infosec training of Mayank Sharma evident.
Security Development Guidelines Apr 2021.
ONYX Application Security Test Report for IRIS business Services Ltd. May 2021 with 1 High, 1 Medium, 5 Low finding)
User control review dated 16Sep2021.

Finding Reference	2119288-202110-I2	**Certificate Reference**	IS 683782
Certificate Standard	ISO/IEC 27001:2013	**Clause**	
Location reference	0047662924-000		
Category	Opportunity for Improvement		
Area/Process:	Software Development, Implementation & Support		
Details	Secure Coding review report should be documented although review is evident in project flow.		

Physical Security & Admin:

Verified Address which is as in Assessment Plan.

IRIS is owner of this office evident vide Registration document with Navi Mumbai Municipal Corporation dated 12Oct2021 purchased from TRACMAIL INDIA PVT LTD.
Verified shop & Establishment certificate which is valid till 08.09.2021.

Modern Security Agency provides the Security Guards. Checked Service agreement dated 10May201 and valid till 31.03.2024. Police verification report dated 06.05.2019 of security guard Arvind Tatkare evident and dated 02.12.2019 of security guard Pushparaj Singh evident. Checked MSF Onsite training record for Security guards Arvind Tatkare, Bablu Ali Syed, Surendra Yadav.

...making excellence a habit.™

Housekeeping service is provided by agency Sanjay Maintenance Pvt Services Ltd.. Checked Service agreement dated 01Dec2012 & is valid till agreement is terminated.

Fire drill not conducted due to covid. Fire Extinguishers are deployed in the office. Service report of Fire Extinguisher done by Sigma Fire Services dated 30Aug2021 evident. Service report of smoke detector done by ACG telecom dated 04May2021 evident.

UPS is maintained by the Sandures Solutions. Checked PO Copy dated Apr 10,2021 valid up to one year. Service report of Sandures dated 16.08.2021 evident. DG is deployed On Call basis.

Video round of office conducted. Checked presence of security guard, visitor register, vendor register, material inward register, material outward register, COVID guidelines followed like temperature check, availability of Sanitizer, Access management system is presently disabled due to COVID so separate register is kept for employee entry. Checked Fire cylinder expiry date kept at reception. Smoke detector, fire extinguisher is installed in reception, within office, Fire exit door is open. Entry needs to be made in Server room register to access server room. Fire extinguisher, smoke detector installed in the server room. UPS with batteries installed in separate UPS room.

IT Infrastructure:

Team responsible for maintenance of IT servers, endpoint, Network, Helpdesk. IRIS has developed multiple products and there is daily meeting conducted between IT infrastructure and various teams for new requirements or to solve technical or operational issues. Most of the production servers are on cloud while Servers for UAT & Production servers are on premise. Firewall is deployed on premise. IRIS own team maintain IT Infrastructure.

Asset inventory with EUS devices, models, Asset TAG, location, allocated to, allocated date, last allocated user, OS etc. evident. Physical server inventory with owner, license status, purchase date etc. evident. Virtual machine inventory with owner, VMServer name, role, department, type of license, OS version also evident. All Software are part of VM inventory.

Checked monthly IT infrastructure report for September month. It included Server information, Decommissioned server, Storage Status, Network, AWS account with instance, Azure project account detail, Backup server report, Issue tracker & GLPI Ticketing tool, SSL certificate Status, Windows patch status etc.

Checked the process to decommission server. Approval from server owner taken, Back Up of Server taken and then they keep it in shutdown condition, Subsequently Decommission it and management is informed in MRM meeting.

Checked patch management process. Change request(CR) is raised before carrying out the patch update. Implementation plan, OS Type, Rollback plan, Approvals etc. is included in CR. Patch status update is part of monthly performance sheet.

Sophos anti-virus software is deployed, and Secure IT is being used for windows 7.

Checked Network Diagram. Primary Internet links are provided by the STPI and Secondary is of SSV-ION. Fortinet firewall is installed.

VAPT using NESSUS and NMAP is done by RSM consulting pvt. ltd. There were 2 High, 2 Medium and 4 Low finding. IRIS management response of finding closure is evident in VAPT report excel.

AD user access review evident. CACTI tool provided by the STPI is used to monitor network utilization.

Evidenced:
Asset inventory sheet
Server inventory sheet
IRIS VM Inventory version 1.4
Email dated Jul 28, 2021 of Prasanna for decommissioning of server SRINIDCIKFKOHA.
Approval from project lead evident.
CR No. IRIS / IT / 2021 /09/ 001 for windows server patching.
Sophos End Point Protection Dashboard
Sophos Central Dashboard for Server.
Network Diagram
External VAPT report of IRIS business services ltd. May 2021.
VAPT report excel.
AD Access review vide Email dated Oct 4, 2021 of Sabu Joseph (IT) to Poonam Sharma (HR) and reversion of Poonam Sharman and subsequent reversion by Sabu regarding correction done.
AD Access review vide Email dated Aug 4, 2021 of Sabu Joseph (IT) to Poonam Sharma (HR) and reversion of Poonam Sharman and subsequent reversion by Sabu regarding correction done.

Finding Reference	2119288-202110-I3	**Certificate Reference**	IS 683782
Certificate Standard	ISO/IEC 27001:2013	**Clause**	
Location reference	0047662924-000		
Category	Opportunity for Improvement		
Area/Process:	IT Infrastructure		
Details	Change request of addition and decommissioning of servers done on Email should be integrated with existing change management tool.		

Minor (2) nonconformities arising from this assessment.

Finding Reference	2119288-202110-N1	**Certificate Reference**	IS 683782
Certificate Standard	ISO/IEC 27001:2013	**Clause**	A7.1.1
Location reference	0047662924-000		
Category	Minor		
Area/Process:	Physical Security & Admin		
Statement of non conformance:	Background verification of the persons deployed by Housekeeping agency not evident.		
Clause requirements	Screening Background verification checks on all candidates for employment shall be carried out in accordance with relevant laws, regulations and ethics and shall be proportional to the business requirements, the classification of the information to be accessed and the perceived risks.		
Objective Evidence	Background verification of the persons deployed by Housekeeping agency not available		
Cause			
Correction/containment			
Corrective action			

Finding Reference	2119288-202110-N2	**Certificate Reference**	IS 683782
Certificate Standard	ISO/IEC 27001:2013	**Clause**	A15.2.1
Location reference	0047662924-000		
Category	Minor		
Area/Process:	IT Infrastructure		
Statement of non conformance:	Monitoring and review of the STPI ISP service provider is not evident.		
Clause requirements	Monitoring and review of supplier services		

...making excellence a habit.™

	Organizations shall regularly monitor, review and audit supplier service delivery.
Objective Evidence	Monitoring and review report of the STPI ISP service provider is not available
Cause	
Correction/containment	
Corrective action	

Next visit objectives, scope and criteria

The objective of the assessment is to conduct a surveillance assessment and look for positive evidence to ensure the elements of the scope of certification and the requirements of the management standard are effectively addressed by the organization's management system and that the system is demonstrating the ability to support the achievement of statutory, regulatory and contractual requirements and the organizations specified objectives, as applicable with regard to the scope of the management standard, and to confirm the on-going achievement and applicability of the forward strategic plan.

The scope of the assessment is the documented management system with relation to the requirements of ISO27001:2013 and the defined assessment plan provided in terms of locations and areas of the system and organization to be assessed.

ISO27001:2013
IRIS Business Services Limited management system documentation

Please note that BSI reserves the right to apply a charge equivalent to the full daily rate for cancellation of the visit by the organisation within 30 days of an agreed visit date.

Next Visit Plan

Date	Auditor	Time	Area/Process	Clause

Appendix: Your certification structure & ongoing assessment programme

Scope of Certification

IS 683782 (ISO/IEC 27001:2013)

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 2021

Assessed location(s)

The audit has been performed at Permanent Locations.

Navi Mumbai / IS 683782 (ISO/IEC 27001:2013)

Location reference	**0047662924-000**
Address	IRIS Business Services Limited T-231, International Infotech Park Vashi Navi Mumbai Maharashtra 400 703 India
Visit type	Continuing assessment (surveillance)
Assessment reference	3230691
Assessment dates	18/10/2021
Deviation from Audit Plan	No
Total number of Employees	34
Total persons doing work at this site	34
Scope of activities at the site	Software development, Implementation, after sales service , Human Resource, Administration, IT Infrastructure Management, Legal & Finance
Assessment duration	2 day(s)

...making excellence a habit.™

Certification assessment program

Certificate Number - IS 683782
Location reference - 0047662924-000

		Audit1	Audit2	Audit3
Business area/Location	**Date (mm/yy):**	10/21	10/22	10/23
	Duration (days):	2	2	4.5
ISMS Frame work & Top Management		X	X	X
Software Development and Maintenance		X	X	X
IT Infra		X	X	X
Human Resources			X	X
Physical Security & Administration		X	X	X
Legal		X	X	X
Finance			X	X
Recertification				X

Expected outcomes for accredited certification.

What accredited management system certification means?

To achieve an organization's objectives related to the Expected Outcomes intended by the management systems standard, the accredited management system certification is expected to provide confidence that the organization has a management system that conforms to the applicable requirements of the specific ISO standard.

In particular, it is to be expected that the organization

- has a system which is appropriate for its organizational context and certification scope, a defined policy appropriate for the intent of the specific management system standard and to the nature, scale and impacts of its activities, products and services over their lifecycles, is addressing risks and opportunities associated with its context and objectives;
- analyses and understands customer needs and expectations, as well as the relevant statutory and regulatory requirements related to its products, processes and services;
- ensures that product, process and service characteristics have been specified in order to meet customer and applicable statutory/regulatory requirements;
- has determined and is managing the processes needed to achieve the Expected Outcomes intended by the management system standard;
- has ensured the availability of resources necessary to support the operation and monitoring of these products, processes and services;
- monitors and controls the defined product process and service characteristics;
- aims to prevent nonconformities, and has systematic improvement processes in place including the addressing of complaints from interested parties;
- has implemented an effective internal audit and management review process;

• is monitoring, measuring, analysing, evaluating and improving the effectiveness of its management system and has implemented processes for communicating internally, as well as responding to and communicating with interested external parties.

What accredited management systems certification does not mean?

It is important to recognize that management system standards define requirements for an organization's management system, and not the specific performance criteria that are to be achieved (such as product or service standards, environmental performance criteria etc).

Accredited management systems certification should provide confidence in the organization's ability to meet its objectives related to the intent of the management system standard. A management systems audit is not a full legal compliance audit, and does not necessarily ensure ethical behaviour or that the organization will always achieve 100% conformity and legal compliance, though this should of course be a permanent goal.

Within its scope of certification, accredited management systems certification does not imply or ensure, for example:
• that the organization is providing a superior product and service, or
• that the organization's product and service itself is certified as meeting the requirements of an ISO (or any other) standard or specification.

Definitions of findings:

Non-conformity:

Non-fulfilment of a requirement.

Major nonconformity:

Nonconformity that affects the capability of the management system to achieve the intended results. Nonconformities could be classified as major in the following circumstances:
- If there is a significant doubt that effective process control is in place, or that products or services will meet specified requirements;
- A number of minor nonconformities associated with the same requirement or issue could demonstrate a systemic failure and thus constitute a major nonconformity.

Minor nonconformity:

Nonconformity that does not affect the capability of the management system to achieve the intended results.

Opportunity for improvement:

It is a statement of fact made by an assessor during an assessment, and substantiated by objective evidence, referring to a weakness or potential deficiency in a management system which if not improved may lead to nonconformity in the future. We may provide generic information about industrial best practices but no specific solution shall be provided as a part of an opportunity for improvement.

Observation:

It is ONLY applicable for those schemes which prohibit the certification body to issue an opportunity for improvement.
It is a statement of fact made by the assessor referring to a weakness or potential deficiency in a management system which, if not improved, may lead to a nonconformity in the future.

How to contact BSI

Visit the BSI Connect Portal, our web-based self-service tool to access all your BSI assessment and testing data at a time that's convenient to you. View future audit schedules, submit your corrective action plans and download your reports and Mark of Trust logos to promote your achievement. Plus, you can benchmark your performance using our dashboards to help with your continual improvement journey.

Should you wish to speak with BSI in relation to your certification, please contact your local BSI office – contact details available from the BSI website:
https://www.bsigroup.com/en-IN/Contact-us/

Notes

This report and related documents are prepared for and only for BSI's client and for no other purpose. As such, BSI does not accept or assume any responsibility (legal or otherwise) or accept any liability for or in connection with any other purpose for which the Report may be used, or to any other person to whom the Report is shown or in to whose hands it may come, and no other persons shall be entitled to rely on the Report. If you wish to distribute copies of this report external to your organisation, then all pages must be included.

BSI, its staff and agents shall keep confidential all information relating to your organisation and shall not disclose any such information to any third party, except that in the public domain or required by law or relevant accreditation bodies. BSI staff, agents and accreditation bodies have signed individual confidentiality undertakings and will only receive confidential information on a 'need to know' basis.

This audit was conducted through document reviews, interviews and observation of activities. The audit method used was based on sampling the organization's activities and it was aimed to evaluate the fulfilment of the audited requirements of the relevant management system standard or other normative document and confirm the conformity and effectiveness of the management system and its continued relevance and applicability for the scope of certification.

As this audit was based on a sample of the organization's activities, the findings reported do not imply to include all issues within the system.

Regulatory compliance

BSI requires to be informed of all relevant regulatory non-compliance or incidents that require notification to any regulatory authority. Acceptance of this report by the client signifies that all such issues have been disclosed as part of the assessment process and agreement that any such non-

compliance or incidents occurring after this visit will be notified to BSI as soon as practical after the event.