ISMS Surveillance Audit Report

Information Security Management System ISO27001:2022

Client Ref. No.	
Organization Name	
Address	
Site Address (If any)	
No. of Employees	
No. of Users	
No. of Server	
No. of work stations	
No. of Application Development and Maintenance staff	
E mail id	
Name of MR	
Telephone/Fax	
Scope	
Exclusions	
Date of Audit	
Audit Team	Team Leader: Auditor : Technical Expert :
Audit Man day	
Brief about the Client (Legal Entity, Characteristics of businessareas, Information assets andTechnology used)	
Audit Objective	Audit Objectives • Ensure your Management System has continued to fulfill requirements between Audits • Ensure Internal Audits and Management Review have been performed to programme • Review actions taken on nonconformities identified during previous Audits • Evaluate your handling of any complaints • Evaluate the continued effectiveness of the management system, regarding achieving your objectives • Evaluate your legal compliance and performance • Evaluate your progress of planned activities aimed at continual improvement • Ensure continuing operational control • Review any changes to your organisation since the previous Audit

	• Ensure that BCI and the Accreditation Body marks are being used correctly Identify any areas for potential Improvement of the Management System

Verification of the Audit Duration:		
1.	Audit Duration for Surveillance	
2.	Are quoted man-days adequate?	
3.	Is there any change in employee details since Stage-1 Audit?	
4.	Is there any change in Scopesince previousaudit?	
5.	Is there any information or Event accrued after the previous Audit date which may affect the Man-days?	

***Status:** C – Complies, O – Observation, N – Nonconformity, N/A – Not Applicable

Clause	ISO 27001-2022 ISMS Requirements	Comments (Manual Procedures or Documents reference)	Status* C/N/O/ NA
4	**Context of the organisation**		
4.1	**Understanding the Organisation and its context**		
	A. Has the external and internal issues relevant to the information security management system been identified?		
	B. Has the organization's context been identified to establish its information security management system (ISMS)		
	C. Has the internal issues that are relevant to the organization'spurpose been identified and the influence these issues could have on its ability to achieve the outcomes that its ISMS intends to achieve been documented?		
	Has the organization :-		
	a) Determined the influence the *internal stakeholders* could have?		
	b) Determined the influence the approach to *governance* could have?		
	c) Determined the influence the organization's *capabilities* could have?		
	d) Determined the influence the organization's *culture* could have?		

Clause	ISO 27001-2022 ISMS Requirements	Comments (Manual Procedures or Documents reference)	Status* C/N/O/ NA
	e) *Determined the influence the organization's contracts could have?*		
	f) Identified the *external* issues that are relevant to the organization's purpose and considered the influence these issues could have on its ability to achieve the outcomes that its ISMS intends to achieve?		
	g) Determined the influence environmental conditions could have?		
	h) Determined the influence *key trends and drivers* could have?		
	i) Determined the influence *external stakeholders* could have?		
4.2	**Understanding the needs and expectations of interested parties**		
	a) Has the organization determined all the parties that have an interest in the organization's ISMS?		
	b) Has the organization identified the requirements of the parties including their needs and expectations?		
4.3	**Determining the scope of the information security management system**		
	a) Determined boundaries and applicability of the ISMS?		
	b) Is ISMS Policy available as documented information?		
	c) Has the Organisation considered; external and internal issues, requirements of interested parties, interface and dependencies between activities performed by the Organisation and those performed by other organizations?		
4.4	**Information security management system**		

Clause	ISO 27001-2022 ISMS Requirements	Comments (Manual Procedures or Documents reference)	Status* C/N/O/ NA
	Has the organisation documented the process to establish, implement, maintain and continually improve the ISMS?		
5	**Leadership**		
5.1	**Leadership and commitment**		
	Has the Management:-		
	a) Established policy and objectives in line with strategic direction?		
	b) Ensured integration with organizations processes?		
	c) Ensured resources?		
	d) Communicated importance of management and conformity?		
	e) Ensured ISMS achieves intended outcomes?		
	f) Directed and supported persons involved in the ISMS?		
	g) Promoted continual improvement?		
	h) Supported other relevant managers?		
5.2	**Policy (Verify Documented ISMS Policy)**		
	a) Is the policy appropriate to the purpose of the Organisation?		
	b) Does the policy includesinformationsecurity objectives or provides the framework for setting information securityobjectives?		
	c) Does the policy includesacommitmenttosatisfyapplicablerequirementsrelatedtoinformationsecurity?		
	d) Does the policy includeacommitment to continual improvement of the information security management system?		
	e) Isthe policy availableasdocumentedinformation? (Give reference of Policy Number)		
	f) Is the policy communicated within the organization?		

Clause	ISO 27001-2022 ISMS Requirements	Comments (Manual Procedures or Documents reference)	Status* C/N/O/ NA
	g) Is the policy Available to interested parties?		
5.3	**Organizational roles, responsibilities and authorities**		
	a) Are Rolesandauthoritiesassignedandcommunicated?		
	b) Has top management assigned responsibilities for; ensuring the ISMS which conform to the standard, reporting on the performance to top management?		
6	**Planning**		
6.1	**Actions to address risks and opportunities**		
6.1.1	General		
	a) Has the managementconsidered; context of the Organisation, needs and expectations of interested parties?		
	b) Determined the risks and opportunities that need to be addressed; ISMS achieves intended outcomes, prevents or reduces undesired effects and achieves continual improvement?		
	c) Has theorganizationplanned;actions toaddressrisksand opportunities and how to;integrateandimplementactions into its ISMS and evaluatetheeffectiveness?		
6.1.2	**Information security risk assessments(Verify Documented Information on the Risk Assessment Process)**		
	a) Has theorganizationdefinedandappliedariskassessmentapproachthat;establishesandmaintainsriskacceptancecriteriaandcriteriaforperformingriskassessments?		

Clause	ISO 27001-2022 ISMS Requirements	Comments (Manual Procedures or Documents reference)	Status* C/N/O/ NA
	b) Ensuredrepeatabilityproducingconsistent,validandcomparableresults?		
	c) Have thesecurityrisksassociatedwithlossofConfidentiality,IntegrityandAvailability along with RiskOwners identified?		
	d) Has the risks analysis been done and potentialconsequences,realisticlikelihood,levelsofrisk been identified?		
	e) Have the risks been evaluated, comparedandpriorities been assigned?		
	f) Has the documentedinformation been retained by the organization?		
6.1.3	**Information security risk treatment(Verify Documented Information on the Risk Treatment Process& the Statement of Applicability)**		
	a) Has theorganizationdefinedandappliedInformationsecurityrisktreatmentprocessto;selecttreatmentoptions?		
	b) Determinedcontrols“from any source”?		
	c) Compared controls with Annex A?		
	d) ProducedaStatementofApplicability?		
	e) Formulatedatreatmentplan?		
	f) Obtainedownersapprovaloftreatmentsandresidualrisks?		
	g) Retaineddocumented information?		
6.2	**Information security objectives and planning to achieve them(Verify Documented Information on the Information Security Objectives)**		

Clause	ISO 27001-2022 ISMS Requirements	Comments (Manual Procedures or Documents reference)	Status* C/N/O/ NA
	a) Has the organization establishedobjectives***"atrelevant functionsandlevels"***?		
	b) Are these objectives consistent,measurable(where practicable), takeintoaccountrequirements, assessmentandtreatments,communicated,updated?		
	c) Has theOrganisationretaineddocumentedinformation such as whatwillbedone,whatresourceswillberequired,whowillberesponsible,whenitwillbecompleted andhowresultswillbeevaluated?		
7	**Support**		
7.1	**Resources**		
	Has the Organisation provided enough resources to achieve information security?		
7.2	**Competence(Verify Documented Information for the Evidence of the Competence)**		
	Has the organizations determined the necessary competence and ensure it, take actions to acquire, retain documentation?		
7.3	**Awareness**		
	a) PersonsshallbeawareofitheISMSpolicy,theircontributionstotheISMS,consequenceofnot conforming		
	b) Make sure that the people who work for the organization understand and are aware of its information security policy.		
	c) Make sure that the people who work for the organization understand how they can support and help enhance the effectiveness of the ISMS.		
7.4	**Communication**		

Clause	ISO 27001-2022 ISMS Requirements	Comments (Manual Procedures or Documents reference)	Status* C/N/O/ NA
	Has the organisation determined the need for internal and external communication?		
7.5	**Documented information**		
7.5.1	General		
	a) Has the organizations ISMS included the documentedinformationrequired bythestandard?		
	b) Information defined by the Organisation as required		
7.5.2	Creating and updating		
	When creating documented information; has the Organisation ensured appropriateness; identification and description, format, review and approval requirement?		
7.5.3	Control of documented information		
	a) Has the documented information controlled to ensure; availability		
	b) Has the Organisation addressed; distribution		
	c) Has the External documents, Documented Information of External Origin controlled as other Documented Information?		
8	**Operation**		
8.1	**Operational planning and control(Verify Documented Information "evidencingProcess Execution" as Planned)**		
	a) Has the Organisation planned, implemented and controlled all the processes?		
	b) Has the Organisation implemented plans to achieve objectives?		
	c) Has the Organisation controlled planned changes and review consequences of unplanned changes?		

Clause	ISO 27001-2022 ISMS Requirements	Comments (Manual Procedures or Documents reference)	Status* C/N/O/ NA
	d) Has the Organisation ensured that the out sourced processes are determined and controlled?		
8.2	**Information security risk assessments (Verify Documented Information on Risk Assessment)**		
	a) Has the Organisation performed risk assessments at planned intervals or at significant changes?		
	b) Has the Organisation retained documented information		
8.3	**Information security risk treatment (Verify Documented Information on Results of Risk Treatment)** Has the Organisation implemented risk treatment plan and retain documentation?		
9	**Performance evaluation**		
9.1	**Monitoring, measurement, analysis and evaluation(Verify Documented Information on Evidence of Monitoring and Measuring)**		
9.2	**Internal audit(Verify Documented Information on Internal Audit Program & result)**		
	Has the Organisation conducted internal audits and auditors selected to conduct audits "that ensure the objectivity and impartiality of the audit process"?		
9.3	**Management review(Verify Documented Information on the result of Management Review)**		
	Has the Top management reviewed the ISMS at planned intervals and recorded the actions which include		
	a. Statusofactionsfrom previous meetings		
	b. Externalandinternalchanges		
	c. Feedbackonperformance		
	d. Non-conformitiesandcorrective actions		
	e. Monitoringandmeasurement		

Clause	ISO 27001-2022 ISMS Requirements	Comments (Manual Procedures or Documents reference)	Status* C/N/O/ NA
	f. Auditresults		
	g. Fulfillmentofobjectives		
	h. Feedbackfrominterested parties		
	i. Resultsofriskassessments andtreatmentplans		
10	**Improvements**		
10.1	**Nonconformity and corrective actions(Verify Documented Information on non-conformance& corrective action)**		
	a) Has the Organisation reacted to nonconformities, evaluated the need for actions and implemented actions?		
	b) Does the documented procedures for corrective actions define requirements for:		
	i. Identifying non-conformities		
	ii. Determining the causes of non-conformities		
	iii. Evaluating the need for actions to ensure that non-conformities do not recur		
	iv. Determining and implementing the corrective action needed		
	v. Recording results of action taken and Reviewing of corrective action taken		
10.2	**Continual improvement**		
	Does the organisation continually improve the effectiveness of the ISMS through the use of the:		
	• Information security policy & objectives		
	• Audit results & analysis of monitored events		
	• Corrective & preventive actions		
	• Management review?		
*	**Use of Logo**		

Table A.1 Control Objectives and Controls of ISO/IEC 27001:2013

*** Status:** C – Complies, O – Observation, N – Nonconformity, N/A – Not Applicable

A.5	Information Security Policies (Management direction for information security)	Applicable	Adequate	
A.6	Organisation of Information Security (Internal Organisation, Mobile Devices & Teleworking)			
A.7	Human Resource Security (Prior to employment, during employment, Termination & Changes of employment)			
A.8	Asset Management (Responsibility for Assets, Information Classification, Media Handling)			
A.9	Access Control (Business requirements of access control, user access management, user responsibility, system & application access control)			
A.10	Cryptography (Cryptographic Controls, Key management for cryptographic controls)			
A.11	Physical and Environmental Security (Secure areas, Equipment, Physical entry controls, Protecting against external and environmental threats)			
A.12	Operations Security (Operational procedures and responsibilities, protection from malware, Back up, Logging and Monitoring, Control of operational software, Technical Vulnerability Management, Information system audit considerations)			
A.13	Communications Security (Network security management, Information transfer)			
A.14	System Acquisition, Development and Maintenance (Security requirements of information systems,			

	Security in development and support processes, Test data)			
A.15	Supplier Relationships (Information security in supplier relationships, Supplier service delivery management)			
A.16	Information Security Incident Management (Management of information security incidents and improvements)			
A.17	Information Security aspects of Business Continuity Management (Information security continuity, Redundancies)			
A.18	Compliance (Compliance with legal and contractual requirements, Information security reviews)			

Observations (Areas Of Concerns Which May Be verified During Next Audit)	

Non Conformities Raised	
Total	
Major	
Minor	
Above Nonconformance (s) identified in the Stage 2Audit, to be given to the Client in theSpecifiedFrom (BCI-F11) and accepted separately. *Client need to respond by using their Corrective Action Form comprising the Root Cause Analysis with Systemic Corrective Action **(AFAR)**. Failing to whichmaylead"ClientResponses"being rejected by Lead Auditor*	

SUMMARY OF AUDIT	
Stage of Audit	
☐	Stage 2
☐	Surveillance 1
☐	Surveillance 2
☐	Modification
☐	Renewal
☐	Upgrade From

☐	Other
Recommendation	
☐	Continuation of Certificate
☐	Refusal of the Certificate
☐	Follow Up audit
☐	Modification of the current certificate (registration no. and expiration date remain unchanged)
☐	other :
Reason for Recommendation	
☐	**Auditee complies with the requirements of the reference standard:** Congratulations, on the basis of the above summary, Lead Auditor is pleased to put forward a recommendation for Continuation of Certificate.
☐	**Minor NC:** Congratulations, Lead Auditor is pleased to put forward a recommendation for Continuation upon off-site verification of closure of all issues, the NC closure need to be submitted along with the Corrective Action Plan and objective evidence with 15 days from the surveillance audit but not later than 60 days from the date of surveillance audit. If all non-conformances are not closed within 60 days, a full reassessment may be required.
☐	**Major NC:** Organization is not recommended for Certification. A follow-up assessment will be scheduled to allow for on-site verification and closure of all issues within 60 days from the date of surveillance audit. If all non-conformances are not closed within 60 days, a full reassessment may be required.
☐	**Not Recommended:** Organization is not recommended for certification, a surveillance audit will be required. To progress your Continuation, please respond to each non-conformances, with a plan showing proposed actions, timescales and responsibilities for resolution. The organization should consider the root cause of the non-conformance and the potential for related issues in other parts of your system.
	***Proposed Audit Date for Surveillance Audit* on or Before (mm/yyyy)**

Acceptance of the Report

Signature		**Signature**	
Name of the Auditor		Name of the Representative	
Date		Date	