Audit Type:	Remote Surveillance Audit
Organisation:	INS Global Consulting
Address:	3904-3905, Tower 2, Grand Gateway Center , No. 3 Hongqiao Road, Xuhui District , Shanghai
Standard(s):	ISO 27001:2022
Client Representative(s):	Mr Philippe Barthelemy
Total number of employees:	67
Site(s) audited:	As Above
Date of Audit:	30 October 2025 (3) days
Lead Auditor:	Shirin Bascombe
Full Audit Team:	Shirin Bascombe
This report is confidential and distribution is limited to the audit team, client representative and the British Assessment Bureau (BAB) office.	

Section A: Audit Objectives

Surveillance Audit

- to confirm that the management system conforms with all of the requirements of ISO 27001:2022;
- to confirm the Scope statement; represents the organisation's certified activities on the Certificate of Registration;
- to confirm that the organisation has effectively implemented ISO 27001:2022;
- to confirm that the Management System is capable of achieving the organisation's policies and objectives;
- to review links between the internal audits, management reviews and continuous improvement

Section B: Scope(s) of certification

The provision of business consultancy and growth solution to commercial clients Worldwide

Section C: Current audit findings and conclusions

The BAB Audit Team conducted a process-based audit, focussing on significant aspects, risks and objectives as required by ISO 27001:2022.

The audit methods used were interviews, observation of activities and review of documentation and records.

The structure of the audit was in accordance with the audit plan and audit planning process.

Number of nonconformities identified	0	Major	2	Minor
Number of opportunities for improvement identified	2			

Based on the results of this audit and the system's demonstrated state of development and maturity, management system certification is recommended. This recommendation will be independently verified by the British Assessment Bureau Head Office.

Section D: Audit Findings

Clause 1: Opening Meeting

This Audit is being completed using a remotely based on the complexity of the business in line with UKAS guidelines. A risk assessment has been carried out to ascertain the complexity of this audit and all evidence has either been seen electronically or via a video link and interviews have been carried out with Top management and Employees either at site or via digital platforms where required. The full audit has been completed within the allotted timeframe.

The opening meeting was attended by Philippe Barthelemy (Head of Product Development /Information Security Manager) and Shirin Bascombe, Lead Auditor at British Assessment Bureau. Philippe (PB) is accountable for the ISMS. There were 2 OFIs raised from the ST2 audit conducted on 07 October 2024, against the requirements of the ISO 27001:2022 Standard. No specific health and safety issues that may have affected the audit process were reported. It was established that the client has access to the requirements of ISO 27001:2022 through the Vanta security and compliance platform.

Clause 4: Context of the Organisation

INS Global Consulting was founded in 2006. INS Global offers services to assist businesses with international expansion, covering employment, payroll management, and company setup. INS Global provide streamlined solutions for seamless entry into global markets, aiming to simplify operations and reduce expansion challenges. INS Global comprehensive support is designed to cater to all aspects of international business growth. The scope of INS Global ISMS includes the assets, technologies and processes for the secure provision of HR services, including internally developed GlobalView, a Software as a Service (SaaS) platform aimed at simplifying HR management. GlobalView tool connects clients, employees, and the PEO provider, INS, creating streamlined HR processes.. Additionally, the scope is defined with consideration of the external and internal context of the organisation. Working with businesses of all sizes and across different industries, clients have included Temu, Weisstechnik and BP. INS HQ is based in Shanghai, China. There are circa 67 employees located Worldwide. No significant changes impacting the ISMS since the last audit.

Interested Parties and the information needs, and expectations requirements linked to how these will be addressed through the ISMS have been combined within the 01-ISMS Scope of the ISMS document.

A sample of Interested Parties includes but is not limited to:
• Customers - External
Protection of customer information (confidentiality, integrity, availability, and privacy) and compliance with contractual agreements
Addressed by ISMS: Yes, this requirement is addressed by the ISMS as per our SOA

• Management and Board of Directors - Internal
Protection of customer information (confidentiality, integrity, availability, and privacy) and compliance with contractual agreements and external regulations. Integrity of financial reporting
Addressed by ISMS: Yes, this requirement is addressed by the ISMS as per our SOA

• Employees - Internal
Information security training and awareness that can help employees align their daily operations with INS Global's information security goals and objectives
Addressed by ISMS: Yes, this requirement is addressed by the ISMS as per our SOA

Internal/external issues have been defined and documented 01-ISMS Scope of the ISMS document – Appendix E; observed:
• External
Financial and macroeconomic - Inflation, volatility of exchange rates.
Technological - Inability to keep pace with hacking tools. Insufficient use of cryptography. Third-party vendor changes or decommissions their services
Natural - Risk of disasters such as fire, flood and earthquakes.
• Internal
Physical infrastructure and environment - Insufficient IT infrastructure to support operations Information systems, information flows and decision making processes (both formal and informal) - Lack of IT direction and governance
Previous audits and previous risk assessment results. - Lack of remediation and oversight of findings arising from internal and external audits and assessments

Climate change is not considered relevant to the ISMS currently; however, the risk management policy in place states that any risks identified will be classified according to specific categories, which include an Environment and Sustainability category; none have been identified.

The context of the organisation has been defined within the 01-ISMS Scope of the ISMS version 1.1, Sept 2024. The Scope: 'The provision of business consultancy and growth solution to commercial clients Worldwide.' has been confirmed during the audit and accurately reflects the boundaries and applicability of the ISMS from both an internal and external perspective. It was noted that the ISMS included scope details and documented processes with clearly identified inputs and outputs throughout.

The Information Security Management System is well structured and reflects the operational processes through documented procedures included in the company's online security compliance platform, Vanta, with clearly identified inputs and outputs throughout.

Clause 5: Leadership

Leadership is clear at INS Global and has been well defined for the ISMS which includes the Leadership Team (ISMS Governance Council) who are committed to the development and implementation of the ISMS Policy and the Information Security Management System as a whole, to include continual review, improvement processes such as risk management and internal audit and effective communication such as the Management Review process. The ISMS Governance Council is overall accountable for the ISMS. The ISMS Governance Council members are:
CEO
Head of Operations
Head of Finance
HR Manager
Head of Product Development (Information Security Manager)
The ISMS Governance Council are responsible for ensuring the ongoing maintenance of the Information Security Management System and the ISMS is communicated to the wider organisation through their team meetings, ISMS policies and the employee handbook stored in Vanta. Comms, through Google Meets and Teams and company emails. ISO awareness would be introduced at onboarding through the induction process and security training. Comms cited: staff email comms 19/09/2025, audit comms cited and 18/09/2025 escalation to completed training and ISMS policy acceptance. Confirmed with the interview(s) with the following to ascertain commitment and awareness to the ISMS:
YL – HR Manager
DG – Global Mobility Specialist
IK – Global Mobility Specialist
PB – Head of Product Development and Information Security Manager

The 02-ISMS Information Security Management System (ISMS) Policy, Information Security Policy and associated policies are in place and are regularly reviewed and maintained by the ISMS Governance Council as per the documented information procedure. ISMS Policies are available for the organisation on the Vanta platform. Leadership is committed to the development, implementation, continual improvement and management of the ISMS. This includes the internal audit programme, management reviews, client feedback, assessing risks and opportunities.

An Organisation Chart is in place and is available internally through Vanta. In addition, there is a well-documented 'Information Security Roles and Responsibilities Policy' and '03-ISMS Roles, Responsibilities, and Authorities v1 Jan 2024' documents in place; these include well-defined roles and responsibilities for the ISMS, observed in Vanta; links to OFI in Clause 7. These roles remain unchanged from the last assessment. Job descriptions are in place, which are further explored in Clause 7 of this report.

Clause 6: Planning

A Risk Management was observed within to within Vanta and supporting Risk Management Policy v1 May-2024 and Risk Assessment and Risk Treatment Process v1 May-2024 outlines risk assessment methodology how they are planned and documented and any changes that may impact the ISMS; Risk Management is supported by the Risk Register within Vanta which links the Statement of Applicability (SOA) controls where relevant, each risk is assessed as to its likelihood and impact on a scale of 1-5. Impact can range from 1 (Very low impact) to 5 (Very high impact) and likelihood can range from 1 (Very unlikely) to 5 (Very likely) to produce an Inherent and Residual Risk Score. The associated typical/likely threats have been assessed based on their potential effects on Confidentiality, Integrity and Availability (CIA attributes).
Risks sampled were:
Risk #: R-92 - Third-party AI integration exposure.
CIA Category: C

Risk Owner: PB
Inherent Risk Score: 8
Risk Treatment: Mitigate – details observed within Vanta A5.20
Residual Risk Score: 4
Last reviewed: 29/10/2025

Risk #: R-93 - Data-loss protection gaps.
CIA Category: C,
Risk Owner: PB
Inherent Risk Score: 12
Risk Treatment: Mitigate – details observed within Vanta A8.12
Residual Risk Score: 4
Last reviewed: 29/10/2025

Risks are to be reviewed at least annually as part of the ISMS governance meetings and discussed at the Management Review.

The Risk Treatment Plan has been defined within the ISMS. The definition includes reference to the required headings within Annex A of the ISO 27001:2022 Standard and a documented Statement of Applicability (SOA) – v1 Aug 2025 is in place. Controls have been established along with the selected controls and reasons for selection, and an overview of implementation. All applicable controls have been selected for best practices and risk assessment activity.
The controls were reviewed, noted were:
A5 Organisational Controls
5.1 Policies for information security – A set of ISMS policies are held on Vanta. Cited: 02-ISMS Information Security Management System (ISMS) Policy v1 May-2024 and Information Security Policy (AUP) v1.2 Sep 2024
5.2 Information security roles and responsibilities – Responsibilities are defined 03-ISMS Roles, Responsibilities, and Authorities v1 Jan-2024 and Information Security Roles and Responsibilities Policy observed in place; the policy observed not versioned controlled within the document, suggested to review the policy to determine if valid and requires an update to the version or if retired as captured within the 03-ISMS Roles, Responsibilities, and Authorities document. Linked to OFI in clause 7.
5.3 Segregation of duties – defined as per roles, responsibilities; in accordance with Access Control Policy and Human Resource Security Policy; all GitHub repositories have protection rules enforced for administrators on the default branch (or production branch, if explicitly specified) observed in Vanta
5.4 Management responsibilities – Roles and Responsibilities including those of management, are stated for the ISMS. Established approved Information Security Roles and Responsibilities and Information Security Policy (AUP) documents in place
5.5 Contact with authorities – 03-ISMS Roles, Responsibilities, and Authorities and Incident Response Plan v1.1 Sep 2024
5.6 Contact with special interest groups – Regular updates from Security Agency newsletters; observed: sans newsletter 11/09/2025
5.7 Threat intelligence – Mandated as per Operations Security Policy v1 Apr-2024 - Threat Intelligence in place. Feeds and manual checks from key sources to identify potential vulnerabilities and threats; observed and sampled Microsoft Defender alert 30/08/2024
5.8 Information security in project management – As per the established Risk Management Policy in place.
5.9 Inventory of information and other associated assets – An approved Asset Management Policy v1 Oct-2023 is in place. PB is responsible for managing and maintaining the asset register through Vanta and XFA. Sampled Assets: PB and IK using own devices logged on XFA, DG - Company Asset DESKTOP-HJPIM69 logged on XFA, AR - password manager and antivirus observed not active on device, YK - HR Manager – only 1 company device logged on Vanta and XFA 2nd company device not known to PB and logged on the XFA or Vanta. Review of the asset inventory showed incomplete entries and missing updates for certain devices and information assets, as an incomplete or outdated asset inventory may result in insufficient protection of information assets and ineffective application of corresponding security controls. The organisation to ensure the inventory of assets is fully maintained and up to date; this was identified as a minor non-conformance.
5.10 Acceptable use of information and other associated assets – All policies and procedures for acceptable use are documented and stored on Vanta. Observed Information Security Policy (AUP) v1.2 Sept-2024
5.11 Return of assets – Leaver's policy/procedure in place for any form of termination, including resignations - all equipment is returned either on the day of termination or at a mutually agreed date with access/password permissions removed/changed on the last day of employment; refer to clause 7 of this report.
5.12 Classification of information – The Data Management Policy v2 Jun-2024 defines the levels of classification in use
5.13 Labelling of information – The Above Policy specifies the approach to classification.

5.14 Information transfer – As per Third-Party Management Policy v1 Apr-2024; sample agreements observed in Vanta Service Level Agreement for Microsoft Online Services May, 2025 and ING MSA Jun 2024 sampled.
5.15 Access control – Established an Access Control Policy v1 Dec-2023 mandates access control procedures. Cited: Access Matrix Regular review of permissions and access undertaken. Planned access review evidence uploaded to Vanta
5.16 Identity management – On joining, the hiring manager confirms what the new starter should and should not have access to based on their role. Monitored through Vanta and XFA platforms used, as observed
5.17 Authentication information – All end-user devices, including personal (BYOD) and company-owned devices, used to access INS Global information systems must be enrolled in the XFA MDM system. XFA verifies that a password manager is in use on the device for secure password storage. XFA agent observed in Vanta
5.18 Access rights – INS Global shall determine the type and level of access granted to individual users based on the 'principle of least privilege'. Access reviews shall be documented. Sampled: New Access Request Ticket – #ISS-921 02/07/25. YL reviews the access rights quarterly, observed within Vanta – 'planned access reviews ticket refs# ISS-886 01/08/2025
5.19 Information security in supplier relationships – Mandated by Third Party Management Policy, Apr 2025; Inventory of supplier types and associated risks will be tracked on Vanta, as observed.
5.20 Addressing information security within supplier agreements – Vendors assigned risk levels defined within Vanta as observed. Sampled: Supplier – Access Point signed MSA cited, New supplier observed within Vanta, sampled: NA Law – contract start 01/07/25, risk score: high – data classification observed considered. Cited: DSA signed 25/09/2025, T and Cs, INS Global Vendor Security Questionnaire 2025
5.21 Managing information security in the information and communication technology (ICT) supply chain – The agreements with suppliers include requirements regarding information security measures to be taken/adhered to. The suppliers are established entities with their own information security accreditations in line with best practice, legislation, and guidelines for information security practices relating to services provided.
5.22 Monitoring, review and change management of supplier services – INS shall regularly monitor, review, and audit supplier service delivery. Supplier security and service delivery performance shall be reviewed at least annually; observed Vanta vendor register. No issues reported.
5.23 Information security for use of cloud services – Mandated within AUP and Third Party Management Policy; sampled: Contractual agreements with Cloud service suppliers within Vanta
5.24 Information security incident management planning and preparation - approved Incident Response Plan v1.1 Sep-2024 in place.
5.25 Assessment and decision on information security events – refer to clause 9 of this report
5.26 Response to information security incidents – refer to clause 9 of this report
5.27 Learning from information security incidents – refer to clause 9 of this report for any further review
5.28 Collection of evidence – refer to clause 9 of this report
5.29 Information security during disruption – Established Business Continuity and Disaster Recovery Plan v1.2 Oct-2024
5.30 ICT readiness for business continuity – The Above plan is tested at least annually. Cited: 2025-09-03 Annual ISMS Incident Response and Business Continuity Test outcome cited successful test with 4 Actions. The organisation could consider implementing formal tracking of recommendations and actions resulting from continuity tests to enhance traceability and ensure effective follow-up; this was identified as an opportunity for improvement.
5.31 Legal, statutory, regulatory and contractual requirements – Legal register; referred to later within this report
5.32 Intellectual property rights – Any agreements entered into that require any form of compliance with legislative, regulatory and contractual requirements related to intellectual property rights and use of proprietary software products will be agreed between parties in line with compliance and contracts as observed in agreements.
5.33 Protection of records – mandated as per Control of Documented Procedure, Access Control and Data Management Policy observed with Vanta
5.34 Privacy and protection of personal identifiable information (PII) – Mandated as per Data Management Policy and Privacy Compliance Policy v2. Link OFI to review version control within Vanta. No requests since the implementation of the ISMS.
5.35 Independent review of information security – Compliance audited annually by external accreditation bodies for: ISO 27001
5.36 Compliance with policies, rules and standards for information security – 07-ISMS Procedure for Internal Audits and MR; referred to later with this report
5.37 Documented operating procedures – an approved Operations Security Policy is in place within Vanta

A6 People controls
6.1 Screening - Background checks are carried out, sampled and observed in clause 7
6.2 Terms and conditions of employment - Employee contracts in place; sampled and observed in clause 7
6.3 Information security awareness, education and training - Security training and acknowledgement of information security-related polices is mandatory for new employees as well as mandatory refreshers annually through Vanta; sampled and observed in clause 7
6.4 Disciplinary process – referred to in clause 7

6.5 Termination or change of employment responsibilities - observed in clause 7
6.6 Confidentiality or non-disclosure agreements – Contracts and NDAs in place; contracts of employment, agreements with suppliers and customers where requested/appropriate; sampled and observed in clause 7
6.7 Remote Working – Established Information Security Policy (AUP)
6.8 Information security event reporting - Part of the training includes reporting of infosec events and the addressing/management of those events. Incident Response Plan; sampled later within this report.

Exclusions
There were no exclusions applied within the SOA.

The Statement of Applicability (SOA) – Version 1, Aug 2025

Process for planning of changes exists as per the Operations Security Policy - Change Management. Changes to the organisation, business processes, information processing facilities, production software and infrastructure, and systems that affect information security in the production environment and financial systems shall be tested, reviewed, and approved prior to production deployment. There have been no major changes since implementing the ISMS. Any potential major changes will be identified and discussed in the ISMS Council, and once approved, these will be tracked using Jira.
Cited: Management Review ISMS, which records proposed changes.
Sampled proposed change: XFA: Include/exclude mobile devices

The Information Security Objectives are well-detailed in the 10-ISMS Information Security Objectives Plan v1 Jul-2024, reviewed on 04/01/2025 and have been planned by the designated members of the ISMS Governance Council. Shared via Vanta and Confluence for all employees. Evidence was seen that aligns the company's business model and strategies, which are further discussed at internal audits and at management reviews. The designated Information Security Team will oversee the Vanta platform, ensuring responsibility for timely reviews. The objectives documented include 3 ISMS objectives, which are aligned in accordance with the Information Security Policy and have been sampled below:
No.3: Data Minimization
Owner: ISMS Governance Council Information Security Team Head of Product Development
Action Plan to Achieve:
• Only collect PII needed for a business purpose
• Ensure PII collection and processing are limited to that which PII Principles are informed of, have consented 2 to, and/or are in accordance with a legitimate business purpose
• Securely delete PII when no longer needed
• Ensure SAR process is in place
• Ensure data breach and complaint process is in place
When: Q4 each year

Measurement Metrics and Criteria
Objective 3
Number of data breaches
Target of 0

Objective 3
Percentage of SARs responded to
Target of 100%

Evaluation of Q4 results for 2024 observed within Confluence – ISMS KPI
Q4 2025 to be evaluated and documented in the Dec 2025 Review.

Information Security objectives are reviewed and discussed at Management Review.

Clause 7: Support

Resources are made up of: Top Management (CEO, VP of Operations and Head of Finance), SMT functions include Global Business Department, including Sales and Business Development; Operations Department including Product Development, Global Mobility, Recruitment Services, HR, Account Management, Finance and Payroll; Marketing Including Web Development and Content Translators.
Job descriptions are in place and documented within the Employee Contracts
Cited: INS Global Organisation Chart_2025

The department manager will initially identify a people resource need, which will be approved by the CEO and Management, that will allow the HR manager to begin sourcing potential candidates via LinkedIn or a local job board. The restricted SharePoint folder is used to store employee records; restricted access only. Background checks are performed by HR as per the employee background check form observed in Vanta.

Employees sampled:
Name: CC
Role: Global Mobility Specialist
Contract signed and dated: 21/04/2025
Start date: 13/05/2025
Background Check Verification Document completed by HR Manager – 20/05/2025
Induction process: through Vanta

All employee contracts included, but not limited to, Confidentiality, Data Protection and IP clauses.

Disciplinary process exists, referred to within HR Policy v1 Apr-2024 and AUP.

Employee exit process in place.
Evidence observed in Vanta.
Sampled Leaver:
LVDH – Contractor - last day 29/08/2024 – office 365 and Vanta disabled
Asset: Personal Computer

Vanta is used to promote and track information security training. Vanta cited, which includes policy acceptance with default requirements set relevant to the role. Vanta records acknowledgement of read and understood. Vanta onboarding page observed completed mandatory security training provided by Vanta. Required to be refreshed on an annual basis.
Completed Security training sampled:
DD – Security training and GDPR training – Completed 15/09/2025
IK – Security training and GDPR training – Completed 03/05/2025
YL – Security training and GDPR training – Completed 28/03/2025
PB – Security training – Completed 28/03/2025 and GDPR training – Completed 02/06/2025

Role-related training will be found on Confluence; observed GlobalView Connect. Held monthly for every department, as observed with PB.
Appraisal and review process performed on an annual basis.
Cited: Employee Performance Review Form
Topics include characteristics rating against assessment of Excellent, Good, Satisfactory or Unsatisfactory, and goals.
Record cited for:
DZ – Software Developer – Review Date: 16/12/2024 Line Manager: PB (Head of Product Development)

Documented information and control methods were evidenced and in place and supported by the 05-ISMS Procedure for the Control of Documented Information v1 Jan-2024 using a Document Register ‘00-ISMS Master List of Documents’. Documents are effectively controlled by the Vanta platform and monitored by ISM. All polices include but are not limited to version history table, document title, classification, date and version within the document. ISMS documents must be reviewed by the ISMS Governance Council at least annually, with review dates held with Vanta as observed. Information Security Roles and Responsibilities Policy and Privacy Compliance would benefit from a review to give assurance of the validity of the documents; this was identified as an opportunity for improvement.
Sample of some of the documents evidenced:
01-ISMS Scope of the ISMS
02-ISMS Information Security Policy
Access Control Policy
Statement of Applicability
And all other documents referred to within this report.

Clause 8: Operation

The organisation has a register of documents implemented for the ISMS that includes a sample noted in section 6 of this report and additional supporting documents also include but are not limited to, Access Control Policy, Operations Security Policy, and Information Security Policy (AUP). Policies and processes are all controlled by the ISMS Governance Council and will go

through the necessary approval. The organisation has demonstrated that they have planned, established and implemented the controls and procedures necessary to meet the requirements of the ISO 27001 Standard, which includes all documents referred to within section 6 of this report.

Clause 9: Performance Evaluation

Performance Evaluation (Monitoring, Measuring and Analysing) has been established and defined and is tied in with the Risks, Objectives and Targets. Continuous monitoring is undertaken observing each part of the service provision; additional monitoring sampled: Cloud Audit Log Review – Entra Log Review Oct 2025. Vanta will be used to monitor the effectiveness of the ISMS, Confluence and tickets raised within Jira. The Non-Conformities and Opportunities for Improvement Log was evidenced at the audit, and is designed to document both internal and external audit actions and opportunities for improvement who is responsible for the management of each individual issue. There is an Incident Response Plan v1.1 Sept-2024, which outlines the process for managing any security occurrences; there has been 1 security incident reported and logged with Jira. There have been no data breaches.
Jira Security Incident Sampled:
Event: Email service interrupted - AWS Account suspended
Jira ticket #ISS-963 observed to include all investigation and supporting evidence
Status: Comms email to all staff stating resolved cited 04/09/2025

Sampled NC and Improvement Log, no open non-conformances observed; sampled:
#29 Date Raised: 09/10/2024
Source: Internal Audit Major Nonconformity
Finding: MNC-01: Audit Logging and Monitoring of cloud networks should be done. Even though you outlined that it sends alerts, there should be more manual reviews of the Cloud environments Audit Logs and monitoring.
Cause: Lack of automated extraction
Owner: PB
Corrective Action: Created Log Review SOP: Cloud Audit Log Review SOP - and created an automation to query logs and create a report in Confluence. Performed first Log Review (child level of the SOP)
Target Date: 24/10/2025
Status: Closed
Status Date: 30/10/2025

#30 Date Raised: 09/10/2024
Source: Internal Audit Opportunity for improvement
Finding: OFI-1: Implementation of a Standalone DLP Tool- Whilst there are minor controls in place such as Role Based security within Global View web application and policies to mitigate this, the best practice would be to implement a standalone data leakage prevention tool.
Cause: Cost - requires a higher tier of our O365 Subscription
Owner: PB
Corrective Action: Planned improvement under evaluation. Evaluating Microsoft Purview or equivalent DLP solutions for future implementation, pending cost analysis and feasibility for mixed-device environments.
Target Date: 24/10/2025
Status: In Progress
Status Date: 30/10/2025

The internal audit procedure has been defined within the 07-ISMS Procedure for Internal Audits v1 Jan-2024. An Internal Audit Plan cited within Jira next internal audit planned ticket ref IMR-59 was observed to cover an annual cycle in place. This is used to ensure that all the requirements of the standard are covered over the year. An internal audit of the ISMS has been conducted by the external consultant; the following audit report(s) have been sampled:
Auditor: Gerrick Bynoe @ CompliancePath
Date: October 9th 2025
Scope of ISMS: INS Global Full scope of ISO27001:2022 standard clauses and information security controls as identified in the Statement of Applicability
Summary of Findings:
Major nonconformities 1
Minor nonconformities 0
Opportunities for Improvement 3

The ISMS Management Review plan is cited within Confluence.

Management reviews have been referred to within the 08-ISMS Procedure for Management Review v1 Jan-2024, with meetings that are scheduled quarterly to discuss the ISMS. There is a set agenda in place which is covering the requirements of clause 9.3 of the ISO 27001, including the mandatory inputs and outputs of the management system. The minutes of the review meeting held on September 19, 2025, were evidenced: 2025-09-19 Quarterly ISMS Management Review
Participants:
CEO WH
Head of Operations RM
Head of Finance TH
HR Manager YL
Head of Product Development PB

Clause 10: Improvement

The organisation is fully aware that when non-conformities are identified, further review and analysis will be conducted. These may be identified through the management review, internal and external audits or service provision incident. The organisation has established how they address any issues that arise either internally or externally, using the Non-Conformities and Opportunities for Improvement Log, referred to earlier in this report for more detail. As such, INS Global Consulting have demonstrated and evidenced commitment to continuous improvement.

Legal Compliance

The CEO is ultimately accountable for ensuring the business is kept up to date with any legislation that could affect the organisation, and the Information Security Manager is responsible for ensuring the business is kept up to date with any relevant ISMS-related legislation that could affect the organisation. External legal counsel from Lawyer John Tang DeHeng Law, who is responsible for reviewing the legal register and informing Management of any relevant updates. As such management team is deemed competent to identify relevant legislation for the organisation. Information security subscriptions and tech news updates and feeds are also received, as observed in Vanta. The ISM is responsible for maintaining the Legal Register cited 12-ISMS Relevant Laws, Regulations, and Contractual Requirements v1.1 Jun-2024, last review Aug 2025; and 01-ISMS scope of ISMS; details the relevant compliance requirements. The following entries were sampled:
• Personal Information Protection Law PIPL, 2021 (China)
• General Data Protection Regulation (GDPR)
• Federal Law on Protection of Personal Data Held by Private Parties (Mexico)

Sample of company insurance:
The Employers Liability Insurance was requested, however was not available during the audit; as such unable to verify that appropriate company insurances are in place to meet statutory and organisational requirements; this was identified as a minor nonconformance. Links to A5.31.

The organisation has had no enforcement orders since they were incorporated.

Use of the Certification Mark

The ‘BAB Certification Mark’ of ISO 27001 is being used correctly.

Closing Meeting

The closing meeting was remotely attended by Philippe Barthelemy, Head of Product Development. The findings of the audit were presented with the 2 Minor Nonconformances and 2 opportunities for improvement fully explained, which the client accepted these findings as an accurate representation of the audit. The audit objectives were concluded in line with the ‘audit plan’ and all information requested was supplied and form as part of the above detail in terms of the requirements. The client was satisfied that the audit duration was a true reflection of the entire process-based activity. As part of the closing meeting, a discussion was held in regard to the date of the next audit by BAB in line with the Certification cycle. The client was advised that the date suggested was to be considered a pencilled-in date and not a formal booking. This date and audit duration (ie number of days) would be confirmed by the audit booking team closer to the date of the audit. The suggested date for the next audit was the 2 November 2026.

Non-Conformities and Opportunities for Improvement

	Type	Clause	Summary
NC-1	Minor	6.1.3	(27001) Finding: The organisation to ensure the inventory of assets is fully maintained and up to date Evidence: Review of the asset inventory showed incomplete entries and missing updates for certain devices and information assets; Linked to A5.9
NC-2	Minor	6.1.3	(27001) Finding: The organisation was unable to fully demonstrate adherence to legal and contractual obligations. Evidence: The Employers Liability Insurance was requested; however was not made available during the audit, as such, unable to verify that appropriate company insurances are in place to meet statutory and organisational requirements.
OFI-1	OFI	6.1.3	(27001) The organisation could consider implementing formal tracking of actions resulting from continuity tests to enhance traceability and ensure effective follow-up; links to A5.30.
OFI-2	OFI	7.5	(27001) Information Security Roles and Responsibilities Policy and Privacy Compliance would benefit from a review to give assurance of the validity of the documents.

= Major Non-Conformity
= Minor Non-Conformity
= Opportunity for Improvement

If non-conformances have been raised throughout this assessment, you are required to provide the following to assist in the closure of these to **compliance@british-assessment.co.uk**.

Major Non-conformance (Recertification Assessment) - Provide evidence within 10 days of the assessment
Major Non-Conformance (Surveillance Assessment) - Provide evidence within 28 days of the assessment
Minor Non-Conformances - Provide a corrective action plan within 28 days detailing how you intend to rectify in preparedness for the next assessment together with a root cause analysis.
Important Note: If this assessment represented a "Stage 2" (Initial) assessment, certification cannot be granted until such time that the corrective action plan has been received.

Certification Cycle Assessment Plan (from 2024 to 2027)

Business function/Process	Stage Two Audit	1st Surveillance Audit	2nd Surveillance Audit	Recertification Audit
Context of the organisation	✓	✓	P	P
Leadership	✓	✓	P	P
Planning	✓	✓	P	P
Support	✓	✓	P	P
Operation	✓	✓	P	P
Performance Evaluation	✓	✓	P	P
Improvement	✓	✓	P	P
Client Site Visit	tbc	tbc	tbc	tbc

P = Planned, ✓ = Done, ✗ = Excluded

Plan for next Assessment

Time	Assessment Activity
09.00	Arrive on site
	Opening Meeting
	Overview of Company Review:- Context of the Organisation Review non-conformities, observations, recommendations from previous audit.
	Leadership
	Planning for the management systems including risk
	Support
	Operation
	Performance Evaluation
	Improvement
	Performance Evaluation
	Customer Communication
	Internal Audits
	Legal Compliance
	Use of Certification Mark (where applicable)
	Auditor collating information and preparing for closing meeting.
	Closing Meeting

Assessment Notes

a. The assessment was based on sampling and therefore non-conformities may exist which have not been identified.

b. If you wish to distribute copies of this report external to your organisation then all pages must be included.

c. The British Assessment Bureau, its staff and agents shall keep all information relating to your organisation confidential and secure 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. The British Assessment Bureau staff agents and accreditation bodies have signed individual confidentiality undertakings and will only receive confidential information on a 'need to know' basis.

d. This report and related documents have been prepared for and only for the British Assessment Bureau client and for no other purpose. As such the British Assessment Bureau 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.

e. The management system documentation included the necessary policies, procedures, process descriptions etc, required by the standard.

The audit criteria applicable to this assessment are clearly outlined within the specific audit plan and the three-year programme. For further information on the audit scope and audit criteria, please refer to the accompanying audit plan and three-year programme.