Audit Type:	Remote Stage Two 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:	68
Site(s) audited:	As Above
Date of Audit:	07 October 2024 (4) 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

Stage 2 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	0	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), Jacob Foster (External Consultant at CompliancePath) and Shirin Bascombe, Lead Auditor at British Assessment Bureau. Philippe (PB) is accountable for the ISMS. There were 15 Major NCs raised from the ST1 audit conducted on 09 November 2023; 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's 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. INS Global works with businesses of all sizes, and across different industries Clients have included AGA Benefit Solution, AIMA, and Anora Group plc. INS HQ is based in Shanghai, China, and has circa 65 employees located worldwide.

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

A sample of Interested Parties evidenced 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. The 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

The interested parties register could be expanded to include suppliers and further consideration of how the requirement(s) will be addressed through the information security management system could be improved; this was identified as an opportunity for improvement.

Internal/external issues have been defined and documented 01-ISMS Scope of the ISMS document observed 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 identified.

It was suggested to review the new ISO amendment related to climate change to consider if climate change is relevant to their ISMS in relation to external and internal issues and or defined interested parties; this was identified as an opportunity for improvement.

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, including 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)
Other interested parties/stakeholders (optional) The ISMS Governance Council are responsible for ensuring the ongoing maintenance of the Information Security Management System and the ISMS communicated to the wider organisation through their team meetings, ISMS policies and employee handbook are 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.
Confirmed with the interview(s) with the following to ascertain commitment and awareness to the ISMS:
WH – CEO
YL – HR Manager
PB – Head of Product Development and Information Security Manager
OH – Global Business Manager
HS – Assistant Product Manager
RL – Senior Business Global Manager

A good level of commitment and engagement was demonstrated during the audit with the participation of the external audit this was evidenced from all those who participated in the audit and at all levels within the organisation.

Additional cited: all staff email comms 18/03/2024 adoption of password manager and ISMS, 23/09/2024 email comms all staff ISO27001 update.

The 02-ISMS Information Security Management System (ISMS) Policy, Information Security Policy and associated policies 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 Vanta platform. Leadership is committed to the development, implementation, continual improvement and the management of the ISMS. This includes the internal audit programme, management reviews, client feedback, and assessing risks and opportunities.

The Information Security Policy is in place and provides a framework for the ISMS and setting objectives. cited as 02-ISMS Information Security Policy v1 May 2024, approved by the CEO (WH) and published internally using Vanta and is made available externally upon request.

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 'Roles, Responsibilities, and Authorities' documents in place observed in Vanta;

these include well-defined roles and responsibilities for the ISMS. Job descriptions are in place which are further explored in Clause 7 of this report.

Clause 6: Planning

A Risk Management has been referred 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 will be assessed as to its likelihood and impact. Both impact and likelihood are assessed 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) and the associated typical/likely threats have been assessed based on their potential effects on Confidentiality, Integrity and Availability (CIA attributes) also.
Risks sampled:
Risk #: R-67 - Failure to define, review, approve, publish, share, or communicate Information Security Policies. Therefore, personnel don't understand information security requirements.
CIA Category: C, I, A
Risk Owner: PB
Likelihood: 4 - Likely
Impact: 4 - Likely
Inherent Risk Score: 16
Risk Treatment: Mitigate – details observed within Vanta
Residual Likelihood: 1 - Very unlikely
Residual Impact: 4- Likely
Treatment Status: 20/08/2024 - approved

Risk #: R-59 - Subject access and deletion requests are not addressed within required timeframes.
CIA Category: C,
Risk Owner: PB
Likelihood: 4 - Likely
Impact: 4 - Likely
Inherent Risk Score: 16
Risk Treatment: Mitigate – details observed within Vanta
Residual Likelihood: 1 - Very unlikely
Residual Impact: 4- Likely
Treatment Status: 25/06/2024 - approved
Risks are to be reviewed 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 Sept 2024 is in place. Controls have been established along with the selected controls and reasons for selection and an overview of implementation. It was observed the organisation have not utilised the new Information Security Attributes within their SoA.
The controls were reviewed and 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
5.2 Information security roles and responsibilities – Responsibilities are defined 03-ISMS Roles, Responsibilities, and Authorities v1 Jan-2024
5.3 Segregation of duties – defined as per roles, and 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
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

5.6 Contact with special interest groups – Regular updates from Security Agency newsletters

5.7 Threat intelligence – Feeds and manual checks from key sources to identify potential vulnerabilities and threats and established Operations Security Policy v1 Apr-2024 in place. Krebs on security.

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. YL is responsible for managing and maintaining the asset register through Vanta and exported Asset tracker s/s. Sampled: RL-Asset DESKTOP-2RLL79V, OH Asset OUMI-LAPTOP

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 – 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 March 1, 2024 and Security in Azure App Service

5.15 Access control – Established an Access Control Policy v1 Dec-2023 mandates access control procedures. Regular review of permissions and access undertaken.

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 platform used; observed with (device security)

5.17 Authentication information – Password Policy is in place mandated through the access control policy. Password manager records on employee workstations (XFA).

5.18 Access rights – User Access Management Administrators shall perform access rights reviews of user, administrator, and service accounts on a quarterly basis to verify that user access is limited to systems that are required for their job function. Access reviews shall be documented. Cited New Access Request Ticket – #GVS-657 18/02/2024 YL reviews the access rights quarterly automated review observed within Vanta – ‘planned access reviews’

5.19 Information security in supplier relationships – Third Party Management Policy; 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

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 practices, 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.

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 – Above plan tested at least annually Cited: Business Continuity Test Report 02 Oct 2024 Cited: Tabletop Disaster Recovery Exercise Meeting Minutes

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) – All HR information is deemed strictly confidential, and as such only approved members of the senior management team have access.
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 policies 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 sampled: Client: STAFIMY NDA dated 02/02/2024 cited
6.7 Remote Working – Established Information Security Policy (AUP)
6.8 Information security event reporting - Part of training includes reporting of infosec events and the addressing/management of those events. Incident Response Plan; sampled later within this report.

A7 physical security controls – Virtual tour undertaken of INS Global Consulting HQ located at 3904-3905, Tower 2, Grand Gateway Centre, No. 3 Hongqiao Road, Xuhui District, Shanghai, China. verified the following controls.
7.1 Physical security perimeters – 7.2 Physical entry – 7.3 Securing offices, rooms and facilities – 7.4 Physical security monitoring – Mandated as per Physical Security Policy and Third-Party Management Policy, the grand gateway is a commercial complex comprising of twin office towers, multi-tenanted service managed offices, secure main entrance observed includes secure turn stylize and secure lifts the organisation utilise is an access management application downloaded to staff based at this location. Visitors are managed through the same app as observed with YL; CCTV observed in place maintained by building management and internal INS CCTV in place in the office maintained by 3rd party IT supplier, Admin Manager and HR Manager responsible for reviewing applications for access and small comms cabinet maintained by 3rd party provider
7.5 Protecting against physical and environmental threats – mandated through the Physical Security Policy v1 May 2024. Fire hose located on each floor and drill performed by building management on 21/09/2024.
7.6 Working in secure areas – Visitors, delivery personnel, outside support technicians, and other external agents shall not be permitted access to secure areas without escort and/or appropriate oversight. Third parties in secure areas shall sign in and out on a visitor log and shall be escorted or monitored by INS Global personnel.
7.7 Clear desk and clear screen - Users shall not leave confidential materials unsecured on their desk or workspace, and will ensure that screens are locked when not in use as per the AUP in place.
7.8 Equipment siting and protection – Mandated as per Physical Security Policy and Third-Party Management Policy – 3rd party managed – Microsoft.
7.9 Security of assets off-premises – All staff who are in possession of a work laptop are automatically allowed to remove them. policies in accordance with the Asset Management Policy and Information Security Policy (AUP) along with the XFA agent installed on all devices.
7.10 Storage media – As per Data Management Policy and Asset Management Policy.
7.11 Supporting utilities – Mandated as per Physical Security Policy and Third-Party Management Policy – 3rd party managed – Microsoft.
7.12 Cabling security – Mandated as per Physical Security Policy and Third-Party Management Policy – 3rd party managed – Shanghai Hongkou District Hanying Electronic and Grand Gateway Center
7.13 Equipment maintenance for – Company devices purchased and maintained from Shanghai Hongkou District Hanying Electronic in the vendor list on Vanta
7.14 Secure disposal or re-use of equipment - in accordance with the Asset Management Policy and Information Security Policy (AUP) None since implementation of the ISMS. Crosscutting shredder observed in the office for disposal of potential confidential paper waste.

A8 Technological Controls

8.1 User endpoint devices – all employees with the Vanta Agent installed have screen lock correctly configured; Microsoft Defender and enrolled on XFA as observed

8.2 Privileged access rights - Granting of administrative rights shall be strictly controlled, and requires approval from the asset owner sampled Zoho CRM user list and planned access review

8.3 Information access restriction – Applications must restrict access to program functions and information to authorized users and support personnel in accordance with the defined access control policy. Request for new access observed. Completed access review s/s cited 01/08/2024

8.4 Access to source code – Access to program source code and associated items, including designs, specifications, verification plans, and validation plans shall be strictly controlled in order to prevent the
introduction of unauthorized functionality into software, avoid unintentional changes, and protect intellectual property. Account Administrator users and permissions as observed in Vanta

8.5 Secure authentication – As per the Access Control Policy; all accounts for which a password has been created have MFA enabled. Network diagram observed

8.6 Capacity management – Established Operations Security Policy. monitoring observed in Azure sampled: Autoscaling screenshots observed and linked in Vanta

8.7 Protection against malware – Malware detection on employee workstations (XFA) installed; as observed.

8.8 Management of technical vulnerabilities – Vulnerabilities Azure scanning in place; as observed. Microsoft Defender in place and Global View vulnerabilities use of SonarCloud's branches observed with a sample of remediation actions observed uploaded to Vanta

8.9 Configuration management – Systems and Network Configuration, Hardening, and Review as per Operations Security Policy; Codebase Cloud Infrastructure - changes that affect the codebase or configuration of software products developed by INSGlobal. Codebase changes managed in JIRA software - 'GlobalView Development (GV)'. Cloud infrastructure changes are also documented within Confluence - 'Product Development / Cloud Infrastructure' Provisioning and Securing Laptops and Desktops v1 May 2024 Development Environments Baseline v1 Oct-2024 Restoring the Production Environment from. Azure Backups v1 Oct-2024

8.10 Information deletion – Established Data Management Policy Appendix B Data Retention Matrix in place. None to date

8.11 Data masking – Data is restricted to appropriate audiences and data is non-accessible or encrypted as appropriate through Third-Party. Cloudflare is only used for website where there is no personal data held

8.12 Data leakage prevention – Hard disk encryption on employee workstations (XFA) as per Data Management Policy. Verifies that Cloudflare provides encryption for the rest of all data stored within Cloudflare Workers KV by default. Managed through XFA as observed with PB

8.13 Information backup – Mandated as per Operations Security Policy - Information Backup
Backups are configured to run weekly on in-scope systems. The backup schedules are maintained within the backup application software. Cited Azure backup screenshot 08/04/2024, Restore Server, latest back storage logs observed with PB

8.14 Redundancy of information processing facilities – third-party providers/tools have backups and have secondary systems in place should something go down. Cited: Geo-redundant backup

8.15 Logging – As per the Operations Security Policy; Storage accounts with Activity Logs have access logs enabled (Azure)

8.16 Monitoring activities – Alerts are set up to trigger communications if unexpected behaviours are registered and then investigated. Sampled Operational alert dashboard and Vanta

8.17 Clock synchronization - This feature is built into the Internet Time Server.

8.18 Use of privileged utility programs – As per Microsoft Active Users observed and Global View admin accounts observed.

8.19 Installation of software on operational systems – Rules governing the installation of software by users shall be established and implemented in accordance with the INS Global Information Security Policy

8.21 Security of network services - Any service is subject to strict service level agreements, and restrictions in place. Cloudflare notifications enabled.

8.22 Segregation of networks – evidence within Vanta includes Network diagram and network segregation (GV development, GV production and GV staging observed)

8.23 Web filtering - AV protection in place. Policy regarding Configuration and Hardening Standards mandated with the operations policy

8.24 Use of cryptography – All data is encrypted (at rest and in transit). Appropriate SSLs are in place to aid the process. An approved Cryptography Policy v1 Apr-2024 is in place to mandate control. Observed evidence in Vanta

8.25 Secure development life cycle – Established Secure Development Policy v1.1 Sept 2024 in place

8.26 Application security requirements – Established Secure Development Policy mandates control evidence and development

wiki in Confluence Application code should be scanned prior to deployment. Patches to address application vulnerabilities that materially impact security should be deployed within 90 days of discovery. SonarCloud
8.27 Secure system architecture and engineering principles - Established Secure Development Policy and Confluence wiki - Secure Engineering Principles and Planning
8.28 Secure coding – Accordance with the Secure Coding Guidelines and Code Review and Quality Control
8.29 Security testing in development and acceptance – Established Quality Assurance and Code Review in place; observed SonarCloud scripts sample uploaded to Vanta
8.30 Outsourced development – Established Secure Development Policy - in-house only.
8.31 Separation of development, test and production environments – All development and testing is done in a secure virtual environment; As observed test data only, Global view testing environment.
8.32 Change management – Change management procedure within Vanta. Sampled Change ticket # GV-1154 29/09/2024. Link to Quotation feature change – tested and QA 30/09/2024 production 30/09/2024 HS resolved. Support activity observed with Jira included release logs sampled v2.8.3. Release management tool observed with the global view platform includes realise announcement.
8.33 Test information - Established Secure Development Policy mandates control production data not used for dev or test; as observed. Global View.
8.34 Protection of information systems during audit testing – All verification of operational systems as per established Risk Management Policy, Procedure for Internal Audits, and Operations Security Policy.

Exclusions
There were no exclusions applied within the SOA.

The Statement of Applicability (SOA) – Version 1, Sept-2024

Process for planning of changes has been added to satisfy the new requirement of the standard; and exists as per the Operations Security Policy - Change Management. Changes to the organization, 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 once approved these will be tracked using the Jira.

The Information Security Objectives are well detailed in the 10-ISMS Information Security
Objectives Plan v1 Jul-2024 was published on Vanta and Confluence for all employees and has been planned by the designated members of the ISMS Governance Council. Evidence was seen which aligns the company's business model and strategies, these 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 noted below as:
1. Implement, maintain, and improve and information security management system (ISMS) that conforms to the requirements of ISO 27001
Owner: Head of Product Development
2. Comply with applicable laws/regulations and customer contractual obligations
Owner: CEO
3. Data minimization
Owner: Head of Product Development

Measurement Metrics and Criteria for the period of Jan -Dec 2024 are in place and observed within Vanta and Confluence
Sampled:
Objective 1
KPI: Percentage of audits passed per year
Target: 100% of audits passed – 31/12/2024
Performance (Status): ST1-Passed, Internal Audit Passed, ST2 not started yet

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 including Product Development, Global Mobility, Recruitment Services, HR, Account Management, Finance and Payroll; Marketing Including Web Development and Content Translators.
Job descriptions in place roles and documented. Noted JDs for the role of:
Developer – Inc's Key Responsibilities
Graphic Designer – Inc.'s Company intro, role profile requirements

The department manager will initially identify a people resource need which will be approved by the CEO and Management and 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: YS
Role: Global Mobility Specialist
Contract signed and dated: 26 03 2024
Start date: 25 Mar 2024
Background Check Verification Document completed by HR Manager
Induction process: through Vanta

Name: SS
Role: Software Developer
Contract signed and dated: 04 Dec 2024
Start date: due to 04 Dec 2024
Background Check Verification Document completed by HR Manager
Induction process: through Vanta

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

A disciplinary process exists referred to within HR Policy v1 Apr-2024 and AUP.

Employee exit process in place.
Evidence observed in Vanta.
Sampled Leaver:
GZ – last day 25/04/2024 – office 365 and Vanta disabled 25/04/2024
offboarding checklist cited completed 10/05/2024

Vanta is used to promote and track information security training. Vanta checklist 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:
HS - 03/04/2024 Completed Security training, Secure code training Info and GDPR training
OH – 20/11/2023 Completed GDPR training and Security training
RL – 02/07/2024 Completed GDPR training and Security training

Role-related training will be found on Confluence; observed Course Catalog

Appraisal and review process performed on an annual basis.
Yearly performance review within Vanta.
Cited: Employee Performance Review Form
Topics include characteristics rating against assessment of Excellent, Good, Satisfactory or Unsatisfactory, and goals.

Record cited for:
HS – Assistant Product Manager – completed 30-Jan-24 Line Manager: PB (Head of Product Development)
DZ – Software Developer – completed 08-Sep-23 Line Manager: PB (Head of Product Development)

Specifies communication methods to ensure employees, contractors, and others (as applicable) are aware of:
• Company Policies and Objectives
• Their contribution to the effectiveness of the Management System (including legal and contractual responsibilities as well as information security control measures that must be complied with)
• Implications of not meeting the requirements of the Management System
• Company performance and progress on actions to achieve objectives
• Changes to the Management System and the importance of (continual) improvement
The internal and external communication of information relevant to company performance and the Management System are planned and reviewed at management reviews.
Key elements of the Management System are communicated to all employees at their Induction and updates are provided to all employees via Management System Briefings and training.
As evidenced within this report.

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 policies 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.
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 the Access Control Policy, Operations Security Policy, and Secure Development Policy. 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, this includes all documents referred to within section 6 of this report.

The Risk Assessment Process is clearly defined for the ISMS and the risk links with the SoA, Risk Register; the most significant risk was identified and noted earlier in this report, the organisation has clearly demonstrated that they have planned, established and implemented the controls and procedures necessary to meet the requirements of the ISO 27001:2022 Standard, this included 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 by observing each part of the service provision; monitoring cited 'feature spotlight and feedback workshops' run monthly observed sample evidence held on 09/09/2024 and 01/10/2024. Vanta will be used to monitor the effectiveness of the ISMS 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, concerns, problems, and 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 have been 1 data breach reported sampled from Jira security incidents:-
Data Breach
Ticket #ISS-762
Raised 05/10/2024

Label: Security
Priority: Medium
Issue: laptop and corporate credit card stolen
Action: Reported to PB and accounts disabled
Status: awaiting; new registration to systems.

Security Incident
Ticket #ISS-727
Raised 28/06/2024
Label: Security
Priority: Medium
Issue: RL – employee account hacked - can't receive client emails.
Action: Assigned and investigated 28/06/2024 – The client involved contacted and account strengthened implementation of 2FA
Actioned and resolved on the 28/06/2024

Sampled NC and Improvement Log, no open non-conformances observed; sampled:
#25 Date Raised: 9 Sep 2024
Source: Internal Audit Minor Nonconformity
Finding: mNC-01: Nonconformities weren't ticketed, logged or documented in any location to track to completion within accordance with the standard
Cause: Non-Conformities and Improvements tracker not finalized.
Owner: Philippe BARTHELEMY
Corrective Action: Non Conformities and Improvements tracker was finalized and reviewed during the ISMS management review.
Target Date: 04 Oct 2024
Status: CLOSED
Status Date: 27 Sep 2024

#32 Date Raised: 19 Sep 2024
Date Raised:
Source: Internal Audit Finding: OFI-8: A.8.19 Installation of software on operational systems Evidence: Operations Security Policy OFI-8: No software is controlled , and users can install any software at their leisure
Cause: BYOD prevents INS from strictly control software installation on staff devices.
Owner: Philippe BARTHELEMY
Corrective Action: Risk discussed and accepted by the ISMS Council.
Target Date: 04 Oct 2024
Status: Closed
Status Date: 27 Sep 2024

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's 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 (Governance and Assurance Specialist - CompliancePath) - Lead Auditor
Date: September 16th - September 23rd 2024
Scope of ISMS: INS Global entire legal entity
Full scope of ISO27001:2022 standard clauses and information security controls as identified in the Statement of Applicability
The audit findings: 1 Minor NC and 8 OFIs

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 all the mandatory inputs and outputs of the management system. The minutes of the review meeting held on Date: 27th Sept 2024 were evidenced.
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; and referred to earlier with this report for more detail. As such INS Global Consulting has 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, 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 lawyer John Tang DeHeng Law 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 Registers and supporting documents cited 12-ISMS Relevant Laws, Regulations, and Contractual Requirements v1.1 Jun-2024; and 01-ISMS scope of ISMS; detail 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 Inc. Cyber Insurance Certificate Policy Number: DRSA006085 Expiry date: Friday, 13 July 2024, from Superscript
The organisation has had no enforcement orders since they were incorporated.

Use of the Certification Mark

The ‘Certification Mark’ of ISO 27001 is not currently being used; this is a ST2 assessment.

Closing Meeting

The closing meeting was remotely attended by Philippe Barthelemy (Head of Product Development /Information Security Manager), and Jacob Foster (External Consultant at CompliancePath). The findings of the audit were presented with the 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 penciled 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 around the 7 Oct 2025.

Non-Conformities and Opportunities for Improvement

	Type	Clause	Summary
No Non-Conformances Found			
OFI-1	OFI	4	(27001) It was suggested to review the new ISO amendment related to climate change to consider if climate change is relevant to their ISMS concerning external and internal issues and or defined interested parties;
OFI-2	OFI	4.2	(27001) The interested parties register could be expanded to include suppliers and further consideration of how the requirement(s) will be addressed through the information security management system could be improved

= 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 to 3)

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