Recertification & Transition Assessment Report

Pisys Ltd

Assessment dates	24/03/2025 to 27/03/2025 (Please refer to Appendix for details)
Assessment Location(s)	Aberdeen (000)
Report author	Kalpeshkumar Patel
Assessment Standard(s)	ISO/IEC 27001:2013

Table of contents

Executive summary

I would like to thank the audit participant for their assistance and co-operation which allowed the audit to run effectively.

This audit has been conducted remotely utilising Information and Communications technology, specifically Microsoft Team as permitted under this schemes requirement and fulfilling BSI GP145 and BSI GF058 risk criteria.

The audit followed the assessment agenda as communicated in Programme Management Report. The planned audit objectives have been achieved, there were no connectivity issues which adversely affected the audit.

A positive observation is hereby raised with regards the organisation implementing improvement initiatives and Management approach during this assessment

Minor NCRs
Clause 5.2 - Organisation has not demonstrate the methods of communication within Information Security Policy Statement
Clause 9.3.2 - Changes in the needs and expectations of interested parties has not been reviewed in the ISMS Management Review Meeting

Good Practice - # Network and Operational Security Documentation and Management

Overall, a positive demonstration was witnessed in respect to the organisations intent and commitment in implementing, maintaining and continual improvement of the ISMS to ensure it remains well established and aligned to their intent and objectives, including statutory and regulatory requirements.

Next year visit booked remotely for 1 days on 17th March 2026 with James Stewart

It is important to remember that assessment work is based on sampling techniques and is time constrained. Even though a problem may not have been identified in an area of activity, this does not necessarily mean that no problems exist. Throughout the assessment, the BSI auditors were well supported, with free access to any information requested, which enabled the achievement of the agreed audit plan.

Changes in the organization since last assessment

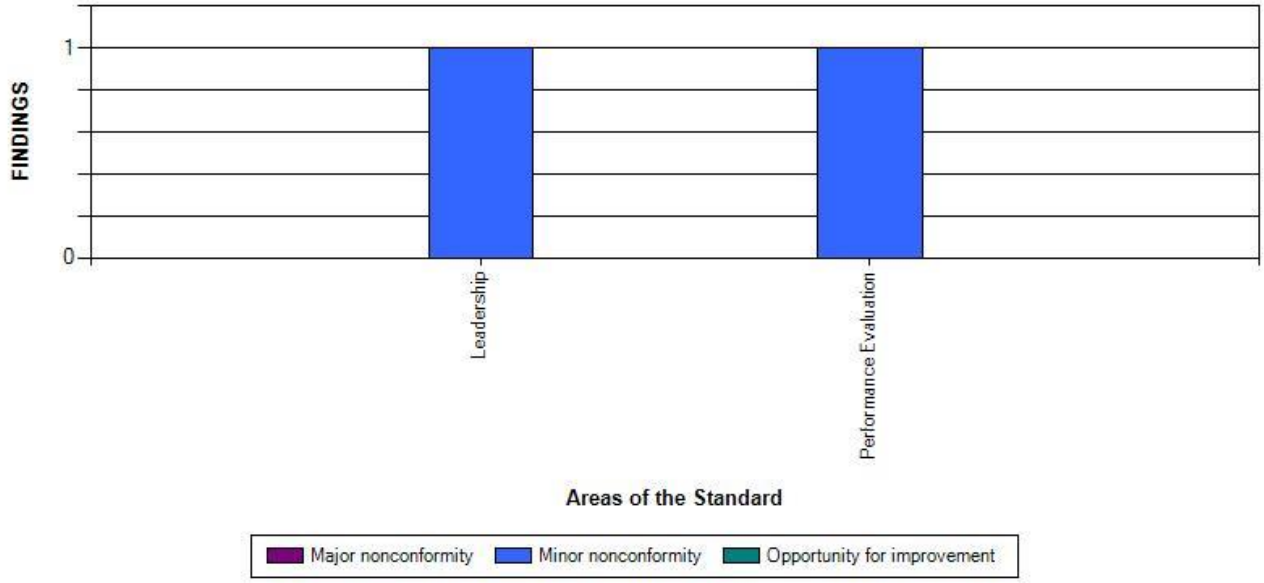
There is no significant change of the organization structure and key personnel involved in the audited management system.

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

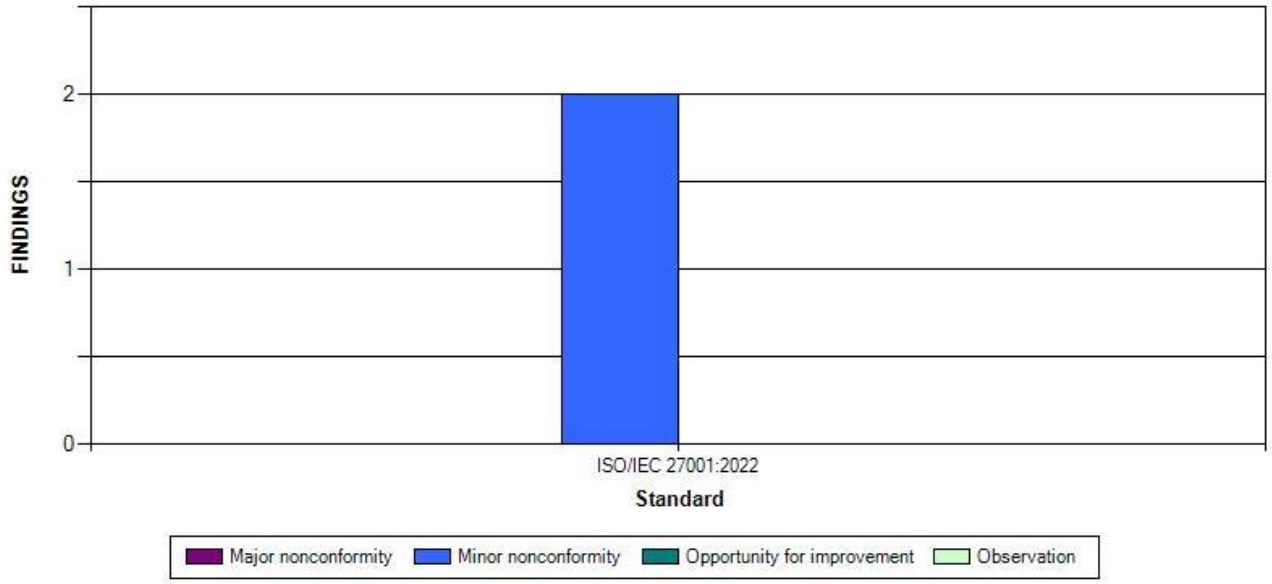
There was no change to the reference or normative documents which is related to the scope of certification.

NCR summary graphs

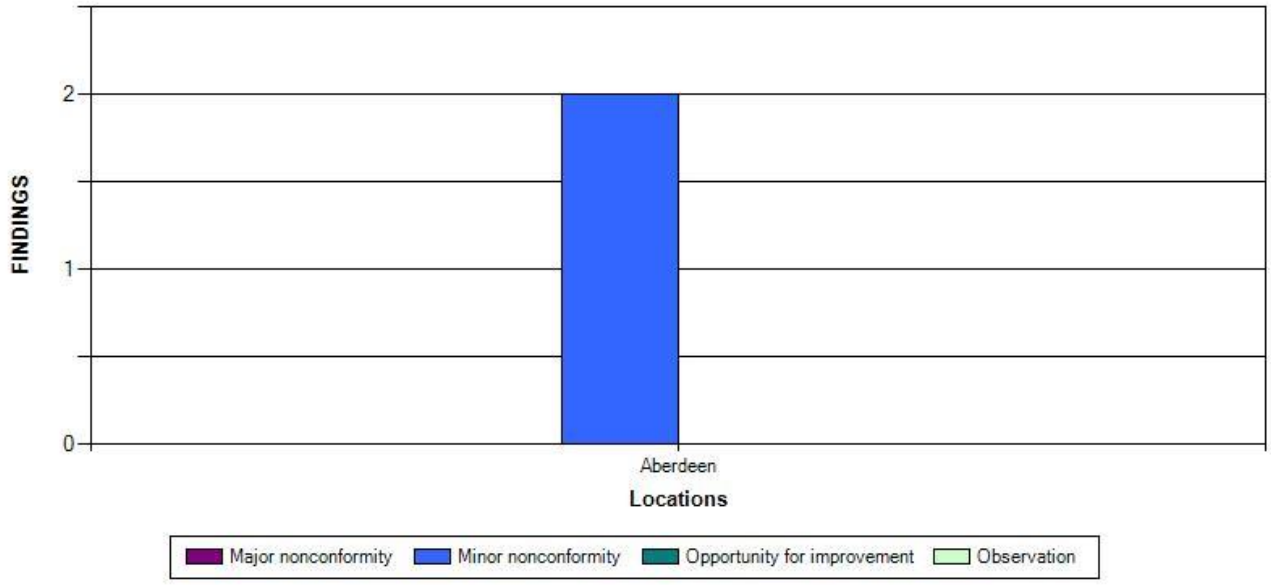
Areas of the standard(s) where BSI recorded findings



Which standard(s) BSI recorded findings against



Where BSI recorded findings



Your next steps

NCR close out process

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

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

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

Assessment objective, scope and criteria

The objective of the assessment was to conduct a reassessment of the existing certification to ensure the elements of the proposed scope of registration and the requirements of the management standard are effectively addressed by the organization's management system.

If this visit is part of a multi-location assessment, the final recommendation will be contingent on the findings from all assessments.

The scope of the assessment was defined in the plan provided in terms of locations and areas of the system and organization to be assessed.

The criteria of the assessment was ISO: 27001:2022 and Pisys Ltd's management system documentation.

Statutory and regulatory requirements

Statutory and regulatory requirements including legislation were seen to have been reviewed and updated on a regular basis. This has been effective.(Refer Section - Legal, Regulatory and Contractual Compliance)

Assessment participants

Name	Position	Opening meeting	Closing meeting	Interviewed (processes)
Peter Henderson	Director		X	X
Rowland Gault	Software Developer	X	X	X
Fiona Johnston	Contracts Manager			X
Akmal Muhammad	Software Developer - IT and Cloud Admin			X
Kyriaki Raizi- Cooke	Product Manager			X
Jim Emerson	Software Developer			X

Assessment conclusion

BSI assessment team

Name	Position
Kalpeshkumar Patel	Team Leader

Assessment conclusion and recommendation

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

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

Please submit a plan through the BSI Connect Portal detailing the nonconformity, the root cause, correction and your proposed corrective action, with responsibilities and timescales allocated. The plan is to be submitted no later than 11/04/2025. If the corrective action plan is not received by this date, you may be putting your certification status at risk.

For any questions please contact your local BSI office, referencing the report number 3991942, 30121028.

Use of certification documents, mark / logo or report

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

Findings from previous assessments

Finding Reference	2319113-202303-N1	**Certificate Reference**	IS 618522
Certificate Standard	ISO/IEC 27001:2013	**Clause**	6.2
Location reference	0047530525-000		
Assessment Number	3524643		
Category	Minor		
Area/process:	Planning		
Details:	The organisation has not determined how it plans to achieve its information security objectives.		
Clause requirements	Information security objectives and planning to achieve them The organization shall establish information security objectives at relevant functions and levels. The information security objectives shall: a) be consistent with the information security policy; b) be measurable (if practicable); c) take into account applicable information security requirements, and results from risk assessment and risk treatment; d) be communicated; and e) be updated as appropriate. The organization shall retain documented information on the information security objectives. When planning how to achieve its information security objectives, the organization shall determine: f) what will be done; g) what resources will be required; h) who will be responsible; i) when it will be completed; and j) how the results will be evaluated.		
Objective Evidence:	The organisations objectives are set at a high level. There was no evidence supplied during the audit that demonstrated that the organisation had determined how it was planning to meet its objectives as defined within ISO27001.		
Cause			
Maturity and understanding of the requirements.			
Correction/containment			
Objectives will be reviewed on a regular basis to ensure they align with defined performance metrics.			
Corrective action			
Current objectives will be reviewed and updated with alignment to performance measures.			

Closed?	
Yes	
Justification	04/03/24 JS * Information Security Policy V2.10: 1.2 How is this achieved. : new section added. * Whilst a descriptive paragraph has been added to the policy document, there is further work required to be able to close the finding. Two additional OFIs were raised at this finding around objectives and performance measurements. These will assist with progress towards closure of this finding. Planning to achieve the objectives is intended to create the required performance metrics. March 2025 KP - Objectives are listed in the Policy Documents in Section B.2.5 SMART objective with KPI, Delivery Methods, Annual / Monthly Targets **After review from this assessment, corrective action is deemed effective and allows this non-conformance to be closed out.**

Finding Reference	2464758-202403-N1	**Certificate Reference**	IS 618522
Certificate Standard	ISO/IEC 27001:2013	**Clause**	A.18.1.3
Location reference	0047530525-000		
Assessment Number	3760692		
Category	Minor		
Area/process:	Compliance (A.18)		
Details:	Information retention periods did not look to be fully documented		
Clause requirements	Protection of records Records shall be protected from loss, destruction, falsification, unauthorized access and unauthorized release, in accordance with legislative, regulatory, contractual and business requirements.		
Objective Evidence:	No evidence was available to illustrate documented retention periods.		
Cause			
Maturity and understanding of the ISO Standard Requirements			
Correction/containment			
Section A has been added to Data Retention Policy			
Corrective action			
# Data Retention Policy updated on 6th March 2024 # Section A stated the Data Retention periods with appropriate retention periods for Accounting & Tax, Immigration Checks, HMRC Approval Documents, Backup, Contractual, CVs & Interview notes for unsuccessful job applications, Personal files and Training records etc.			

Closed?	
Yes	
Justification	29/01/25 JS: Not reviewed at this assessment, will be updated in March 2025 March 2025 KP - Data Retention Policy has been updated **After review from this assessment, corrective action is deemed effective and allows this non-conformance to be closed out.**

Findings from this assessment

Opening Meeting:

The opening meeting was conducted and arrangements for the assessment were confirmed with representative's present. This included confirmation of the visit plan, employee numbers in scope, confidentiality, H&S, BSI standard assessment approach (open questions, sampling, recording, non-conformity definition), and visit purchase order reference entered.

No significant complaints have been received by the business.

No Significant security incidents have occurred resulting in any regulatory or legal action being taken against the business.

Business Update and Changes to the ISMS, Review of Previous Findings:

No significant changes in the Information Security Management System documentation, Organisation Structure / Key personnel and Product & Services
- Previous Non-conformities were effectively reviewed and closed during this audit.

Organisational Context, Interested Parties, Scope, and ISMS Documentation:

Documented Information / Evidence
Information Security Policy Rev 2.11 Dated 08/05/2024
https://www.pisys.co.uk

Context of the Organisation
founder of the organisation having an experience to worked on survey boats in some of the most hostile environments on the planet, developing and commissioning mission- critical systems to support he emerges upstream energy sector. which put them in a unique position to assist companies who require effective high-tech solutions to complex problem in any industry.

Pisys 360 Integrated HSEQ Software
> Permit to Work - A cloud based system for creating and managing Permits to Work across any type of business or work site.
> Action Tracking - Create and assign actions, manage approval with complete visibility on action

history
> Operations Training Simulator - Control Room Operator, Emergency Response, Stability, OIM Training MEM Training
> ESG Reporting - Record and Manage Environment, Social and Governance Data Quickly and accurately

- Context of the organisation has categories in the PESTLE Manners which stated the Risks in all areas including the capacity management and governance

Interested Parties & their expectations are listed for clients, staff, suppliers (AWS, Microsoft, Dell etc), Regulatory bodies (ICO, HSEQ, Environmental), shareholders, competitors, neighbours, senior management

Scope of Certification
The systems, processes and infrastructure involved in delivering Pisys' range of software products and services in accordance with Statement of Applicability 1.0 Dated 18/12/2024

ISMS Documentation Structured the Manual, Process / policies and relevant records templates with the consideration of the legal, regulatory, including Climate change and contractual requirements, stored in the company SharePoint Section Information Security, Policies and Procedures, which are utilised by all business unit as and when needed.

Process Interaction chart demonstrate the information life cycle between PISYS, Customers Vendors and Regulatory bodies

Climate Change Issues has been considered, Stated the Risk to Data Centre and ISMS from environmental factors like Natural Disaster e.g. Energy Usage, Remote Working and Carbon Footprint monitoring. organisation has implemented the DR and BCP within the ISMS to protect / mitigate the Potential data loss and down time in case of environmental disasters.

Conclusion
Planned activities have been fully realised.

Leadership and Commitment:

Organisational Control
5.1 ISMS Policies,
5.2 ISMS Roles & Responsibilities
5.3 Segregation of duties
5.4 Management Responsibilities
5.5. Contact with Authorities
5.6 Contact with Special Interest Group
5.7 Threat Intelligence

Documented Information / Evidence
Information Security Policy Rev 2.11 Dated 08/05/2024

> Top Management Interview (PH- Company Director)
A Leadership interview took place with PH- Company Director whose has demonstrate clear understanding

-Top Management demonstrate a clear commitment to information security, actively participating in the establishment, implementation, and maintenance of the ISMS.
- leadership ensures that the ISMS aligns with the Organisation's Strategic direction and business objectives, reinforcing a strong governance structure
- the organisation has implemented a framework for setting information security policies and objectives, providing a roadmap for the ISMS

> ISMS & Other Policies,
Information Security Statement Signed by PH - Company Director
-The ISMS Policy is well documented providing a clear and comprehensive framework for information security that is easily accessible to all relevant stakeholders.
- It is align with the organisation's overall objectives, ensuring that information security is an integral part of the business strategy e.g. Protecting the CIA, Unauthorised access to Pisys Information , Staff Awareness & Training
- The policy demonstrates a commitment to legal and regulatory compliance, outlining the organisation's responsibilities to adhere to application information security laws and standards
- The Information Security Statement has not demonstrate the methods of effective communicates aligns well with the ISO:27001:2022 standards *NCR Raised

> Roles and Responsibilities
- the organisation has established a well-defined structure for managing information security responsibilities. the distribution of roles aligns with ISO:27001:2022 requirements ensuring accountability and promoting a culture of shared responsibilities for information security
- The organisation has implemented mechanisms for regular reviews and updates of roles and responsibilities to adapt to changes in the organisational structure and information security landscape
- Key Personal (Management, ISMS Team & Staff) Including the Information Security Officers and Data Owners demonstrate a clear understanding of their respective roles and actively contribute to the effectiveness of the ISMS
ISMS Team Members Includes Director, Development Team Representative, Support Team Representative

 # 5.7 Threat Intelligence
- Microsoft Health Scoring
- Microsoft Defender Installed on End User Devices
- Information Security and Access Control Review Meeting carried out Monthly
- Annual Penetration Test and Cyber Essential Certificate
- Firewall and Encryption to safe guard of sensitive data and prevent unauthorised access
- Weekly Team Meeting for Staff Awareness

Email Notification received from Microsoft dated 22/03/2024 Stated the New Vulnerability Notification : PisysVulnerabilityNotificationRule - Vulnerability Name CVE-2025-2476 with High Severity,
Microsoft Defender Secure Score - 72.48%

Conclusion
Planned activities have not been realised - Non-conformance raised.

Planning & Operations:

Documented Information / Evidence
Risk Assessment Process Revision 6 Dated 22/04/2024

Risk Assessment & Treatment
Source of risk Identification - Introduction of New Assets , Product, Service Line and Teams
Key Document Review - Assets Register, SOA and Risk & Incident Register
Business Areas - Development, Support, Administration and Management
Risk Score = Likelihood x Impact (3 x 3 Matrix) - Low, Medium and High
Risk Treatment Options = Tolerate, Treat, Transfer or Terminate

 # Risk Register Template

> System ID	> Areas	> Due Date
> Outstanding On	> Risk description	> Date Created
> SOA Control Numbers	> Date Raised	> Response
> Project Name	> Date Completed	> Status
> Score Post Mitigation	> Action Description	> Priority

Total Number of Risk – 509, Open Risk - 4
Risk ID - 509 - Pisys DB1 data disk is exceeding IOPS investigate what's causing the High IOPS, Disk Might benefit from increased IOPS - 10/03/2025
Risk ID - 478 - Inadequate Consideration given to unsuccessful system logins- 09/09/2024
Risk ID 463 - Failure to review recommended actions on MS Secure Score - 10/06/2024
Risk ID 462 - Notification that base windows Intune policies have been deprecated - 10/06/2024

Statement of Applicability Ver 1.0 dated 18/12/2024 contained the reason for inclusion, and compliance Evidence
> ISO Control Number
> Control Description
> Status of Applicability
> Evidence Details

ISMS Objectives & Planning for Changes
Information Security Policy Rev 2.11 Dated 08/05/2024

Strategic Direction of the ISMS
> Protecting our system from Unauthorised Access
> Ensuring that out system are always available for use
> Ensuring that we complying with all current legislations
> Ensuring that Safety and comfort of our staff
> Ensuring that we continue to be accountable to the standard enforced by out ISO 27001 Security Certification

ISMS KPI
> Completion of ISMS Awareness Programme - 85% - Monthly Monitoring
> Completion of ISMS Audit Programme - 100% - Monthly Monitoring
> O365 Defender Score - 15% better performance than similar sized company score - Monthly
Monitoring
> 99.5% Availability of Key System- Monthly Monitoring
> 85% Resolutions of Penetration Test Risk Register Actions - Monthly Monitoring
> 90% Management of ISMS Risk Register Actions

Conclusion
Planned activities have been fully realised.

Performance Evaluation & Improvement:

Documented Information / Evidence

Objective / Performance Monitoring & Measurement
ISMS KPI are monitored on monthly basis
> Completion of ISMS Awareness Programme - 85% - Achieved - 100%
> Completion of ISMS Audit Programme - 100%
> O365 Defender Score - 15% better performance then similar sized company score - Pisys Score 5.59 % / Industries Average Score 46.11%
> 99.5% Availability of Key System - 99.995% (26 Mins down time in Since 2024
> 85% Resolutions of Penetration Test Risk Register Actions - Achieved 89%
> 90% Management of ISMS Risk Register Actions - 4 Open Risk in the Risk Register - Not Achieved

 # Internal Audit Schedule Contain the Clause 4 to 10 and SOA controls (Organisational, People, Physical and Technical)
IA Report - SOA control A.8.1 to 8.14
- IA Date -02/09/2024
- Internal Auditor - RG and KRC
- IA Scope - A8.1 to A8.14
- IA Findings - No Findings
- IA Score is 91.67%

IA Report - SOA Control A8.15 to A8.22
- IA Date - 07/10/2024
- Internal Auditor - RG and KRC
- IA Scope - A8.15 to A8.22
- IA Findings - No Audit Findings
- IA Score - 100%

IA Report - SOA Control A5.24 to A5.29
- IA Date - 15/05/2024
- Internal Auditor - RG and KRC
- IA Scope - A5.24 to A5.29
- IA Findings - No Audit Findings
- IA Score - 100%

Management Review
it is evident that organisation has followed a set framework for evaluating and enhancing the effectiveness of its information security practices. The MRM Process demonstrating a commitment to continual improvement and a proactive approach to managing information security

The MRM conducted at planned interval (Annually) on dated 17/12/2024, ensuring a systematic and timely assessment of the ISMS. Top Management actively participates in the MRM, providing strategic insights and demonstrating a strong commitment to information security Governance. the MRM Process address key aspects, including performance evaluation, risk management, incident response and compliance with legal, regulatory and contractual requirements, However, Changes in the needs and expectation of the interested parties has not been reviewed in the annual MRM dated 17/12/2024 * NCR Raised

Conclusion.
Planned activities have not been realised - Non-conformance raised.

Nonconformity, Incident and Complaints, Corrective Action, and Continual Improvement:

5.24 Information security incident management planning and preparation
5.25 Assessment and decision on information security events
5.26 Response to information security incidents
5.27 Learning from information security incidents
5.28 Collection of evidence
6.8 Information security event reporting

Documented Information / Evidence
Dealing with Security Incident Procedure Rev 7.0 Dated 22/04/2024

Process- Preparation - Identification - Evidence, Containment, Eradication - Recovery and Lesson Learned
- Incidents are reported to senior management or designated email box "support@pisys.co.uk"
- Evidence may be obtained from support team members, helpdesk, server logs, development team etc.
- Forensic Evidence are retained in the secure manner and link with incident records in the action tracker
- Relevant parties are informed by the authorised personnel, subject to severity and impact

Incident Log Template contained
> System ID
> Business Area
> Date
> Incident Description
> Priority
> Root Cause
> Action Required
> Response
> Comment

Evidence
System ID - 508
Date - 17/02/2025
Due Date 04/04/2025
Business Area - Infrastructure
Incident - SQL Time Cut (MOC 2791 Dated 15/01/2025, Shift heavy ATMS DBs to DB2) - Management of change
Priority - Medium
Date of Action 24/03/2025

Continual Improvement
Source - Management Review, Audit findings, Industry updates and employee feedback

Last Meeting dated 17/12/2024 Feedback evidence the following OFI and Actions for continual improvement
- Continue to Raise profile of ISMS (Team Meeting -Security Moment)
- Considering of the risk as part of development and release cycle - Action recorded in the Risk Register
- Servers updates regularly test failover but consideration is to be given to scheduling occasional out-of-the-blue server failover test
- Monthly Information Security and Access Control Meeting dated 30/01/2025 Actions as below

Review of MS Secure Score, Defender and End Point Portal, Rack space, Asset Register, Network Protocols and Cyphers, ESET Alerts, User Access
Ongoing Tickets - # 467 - Cloud Recovery, # 478- unsuccessful Logins, # 479 - Email Quarantine, # 480 - Removable Media Policy
Added # 490 - Backup Risk
Added & Close out # 496 - Increasing in Phishing email using @pisys.co.uk email from: address

Conclusion
Planned activities have been fully realised.

Resources; Physical and Environmental Security:

Physical & Environmental Security
7.1 Physical security perimeters
7.2 Physical entry
7.3 Securing offices, rooms and facilities
7.4 Physical security monitoring - New
7.5 Protecting against physical and environmental threats
7.6 Working in secure areas
7.7 Clear desk and clear screen
7.8 Equipment siting and protection
7.9 Security of assets off-premises
7.10 Storage media
7.11 Supporting utilities
7.12 Cabling security
7.13 Equipment maintenance
7.14 Secure disposal or re-use of equipment
8.1 User endpoint devices

Documented Information / Evidence
Acceptable User Policy
Remote Working Policy
Location - 7 Queen's Garden, Aberdeen AB15 4YD, United Kingdom

Note- This address is used for phone answering, Correspondence and team meeting purpose only, however currently organisation does not have and dedicated space on this location and all employees are working 100% remotely. Meeting rooms are available upon request, if needed.

- Network Infrastructure - Cloud Environment with Azure and AWS DC
- Spare IT Hardware are stored at the AM - Cloud Administrator's home address, which is authorised by the director
- Leavers assets are collected face to face meeting upon exit interview with relevant personnel
Secure WEEE disposal certificate obtained from the service provider
- Employees are followed the clear desk / clear screen policy, acceptable user policy

Conclusion
Planned activities have been fully realised.

Communication:

Documented Information / Evidence
Communication Policy Rev 1 dated 10/04/2024
Incident Response Procedure
Employee Handbook Rev 17 Dated 02/09/2024 (Section 2.10.7 social media)

Communication Process effectively convey the significance of information security throughout the organisation. training programs are in place to enhance awareness and competence among employees, ensuring they understand their roles in maintaining information security, aligned with ISO:27001:2022 requirements.

Key Elements
- Secure Electronic Communications
- Voice Communication
- Physical Communication
- Social Media and Online forums
- Training and Awareness
- Incident Response Reporting

Competency, Awareness and Training
Security Training Register Last Reviewed on dated 28/01/2025

Date	Training Description	Attended by
29/08/2024	SANS 2024 Cloud Sec Exchange	RAG, MAK and KRC
31/10/2024	Sensitive Data Logging	MAK, RAG, PM, BRS, ASH, GS, JEE
25/01/2024	ISC2 Certified in Cyber Security	KRC
28/01/2025	ISC2 Certified in Cyber Security	MAK
20/03/2025	Team Meeting to discuss the ongoing Security updates e.g. Fake Captcha, Amazon Kills, ISO Audits	

Conclusion
Planned activities have been fully realised.

Documented Information & Record Retention:

Documented Information / Evidence
Information Classification Policy Rev 1.0 Dated 22/04/2024
Information Classification Policy has considered the CIA requirements
Level - Confidentiality - Integrity - Availability
0 - Public - Low- Low
1- Internal Use- Medium - Medium
2- Confidential - High - High

ISMS Documentation Structured the Manual, Process / policies and relevant records templates with the consideration of the legal, regulatory and contractual requirements, stored in the Company SharePoint with Doc ID, Number, Title, Rev Number and Dates. ISMS Change are addressed in each policy (Change Request, Review and Approval) between the Owner, Reviewer and Approval Author on Company SharePoint Site.

Type of change - Elective and Emergency
Frequency of Doc Review - Annual

- Acceptable Use of Information and Assets Policy
- Access Control Policy
- Assets Management Process
- Audit Procedure
- Business Continuity Plan
- Capacity Management Plan for Mission Critical System
- Clear Scree and Clear Desk Policy
- Communication Policy
- Cryptography Policy
- Data Backup Policy
- Data Breach Procedure
- Data Protection Policy for Hosted Services
- Data Retention Policy
- Dealing with Security Incident Procedures
- Disaster Recovery Policy for Data Centres
- Employees Handbook
- File Sharing Policy
- Information Classification Policy
- Information Security Policy
- IS Roles and Responsibilities Policy
- IT Leavers Procedures
- IT Security Policy
- Logging Policy
- Maintain and Improve the ISMS
- Management of change Policy
- Management of Removable Media Policy
- Management Review
- Outsourcing Policy
- PISYS Information Security Policy Summary
- PISYS Service Delivery Model
- PISYS Testing Team
- User Authentication Guideline
- Privacy and Protection of PII Policy
- Protection of Intellectual Property Rights Policy
- Remote Working Policy
- Risk Assessment Process
- Risk Treatment Process
- Secure Development Policy
- Server checks
- Supplier Security Policy
- Use of cloud Services Policy
- Use of Endpoint Device Security Policy
- Vendor Review
- Vulnerability Disclosure Policy
- Work Station Build Procedures

 # Data Retention Policy Rev 1 Dated 06/03/2024

Section A stated the Data Retention periods with appropriate retention periods as below
Accounting & Tax - 3 Years
Immigration Checks - 2 Years
Expense Accounts - 6 Years
Wage and Salary Records - 6 Years
Annual Leave and Working Time Records - 2 years
National Insurance Returns - 3 Years
HMRC Approval Documents - Indefinite
Backup - as per Backup Policy
Contractual - Period as agreed
CVs & Interview notes for unsuccessful job applications - 6-12 Months
Personal files and Training records - 6 Years
Pensions - 12 Years

Conclusion
Planned activities have been fully realised.

Human Resource (Screening & Background Checks):

5.4 Management responsibilities
6.1 Screening
6.2 Terms and conditions of employment
6.3 Information security awareness, education, and training
6.4 Disciplinary process
6.5 Responsibilities after termination or change of employment
6.6 Confidentiality or non-disclosure agreements
6.7 Remote Working
6.8 Information security event reporting

Documented Information / Evidence
Acceptable User of Information Assets Rev 3.0 Dated 31/05/2024
Form 105 - Application Form
Form 106- Onboarding Checklist
Employment Contract
Employee Handbook
Procedure 021 - IT Leavers Procedures Rev 1.1 Dated 27/05/2023
Remote working Policy Rev 1 Dated 01/07/2024

- The Organisation implemented effective HR controls for managing the entire employment lifecycle including onboarding, changes in the roles and offboarding, ensuring a comprehensive approach to personnel security
Evidence
- HR Controls align cohesively with the organisation's business objectives underscoring a strategic integration of human resource practice into the broader information security framework.
- Intellectual Property Rights Policy Covers the Copyrights, Trademark, Patent, Trade Secret and Confidential Information
- Employee must follow the Acceptable Use of Information and Assets Policy
- Employee Hand Book,
> Appendix 1, Section 9.1 PISYS Disciplinary Procedure
> Section 2.10.6 Confidentiality
- ID Documents - Passport, Right To Work, Driving License
- Other Documents CV, P45 / P46, Education Certificate, Previous Work Experience, Personal References

Induction Training
- Employment Guide
- Information Security Management - ISO 27001 System
- IT Asset Allocation
- Incident Reporting

Remote Working Policy Stated the following
> Remote Access Approval
> Secure Remote Access
> Security of Device, Network, Data Working Environment, Communication, Physical,
> Incident Reporting
> Awareness and Training
> Employee Responsibilities for Remote Working

IT Leavers Checklist Contain the Responsibilities for the Office Manager and Technical support during the leavers event occurrence

Office Manager Ensure that PISYS IT Assets are returned / collected from the staff on the last working day and notify the Technical support team who are responsible for disable the network access, email forwarding and remove the user from bug system within 24 hours

 # Evidence
New Starters Employee - EM - Software Tester
Start Date - 17/02/2023
Police Scotland Check Ref # B01582192 Dated
UK Passport Ending with - 2753
Employment Contract - 07/04/2023
Regular Attendance in Weekly ISMS Awareness Meeting (Last dated 27th Feb 2025, 13th & 20th Mar 2025)
- Fake Captchas
- Amazon Kills on Device Alex Processing

Conclusion
Planned activities have been fully realised.

Access Control:

5.15 Access control
5.16 Identity management
5.17 Authentication information
5.18 Access rights
8.2 Privileged access rights
8.3 Information access restriction
8.4 Access to source code
8.5 Secure authentication
8.18 Use of privileged utility programs

Documented Information / Evidence
Acceptable User of Information Assets Rev 3.0 Dated 31/05/2024
Form 106- Onboarding Checklist
Procedure 021 - IT Leavers Procedures Rev 1.1 Dated 27/05/2023
Access Control Policy Rev 6 dated 12/04/2024
Microsoft Entra Admin Centre (User Management)

Access Control Principle - Least Privileged, Separation of Duties, Access Control Mechanisms, Access Review and Access Removal
Access to Pisys Information Assets, Network, Application and Data, which are access by all Supporting Assets including all Endpoint devices e.g. laptops, mobile devices, servers, cloud based services, software's and physical premises, if any
- Access request must be raised by the user's managers and Information Security Officer with justification of valid reason
- Access Request approval (data Owners and IS Officer) based on the job roles and responsibilities with users identity and authentication
- Unique user credential, password and MFA
- Access review rights are regularly reviewed to reflect the changes in the system architecture and user's job roles

IT Onboarding Checklist include allocation of Work Email, User Credential Network Access (Bug system, AWS, RACKSPACE, ESET, Server Domain, IMD, VPN Certificate, Public Calendar), IT Assets Allocation, SharePoint Access, Office 365 Account
- Use of Secure VPN or other approved secure methods are mandatory to connect with PISYS Network
- Employees are responsible to protect their password, MFA (Microsoft Authenticator) and up to date antivirus, software firewall and security patches
- Office Manager Ensure that PISYS IT Assets are returned / collected from the staff on the last working day and notify the Technical support team who are responsible for disable the network access, email forwarding and remove the user from bug system within 24 hours

User Access are recorded in the MS Entra Active Directory (22 User Account including Cloud Admin(2), Permit to Work, Pisys Support, Pisys Public, Mail@trackpipe.com

 # Evidence
EMP Name - EM
Start Date - 17/04/2023
Information Access - Work Email, PISYS Intranet, ISMS Policy and Procedure, Corporate Laptop Assigned
Last Login - 26/03/2025
Group Member Include following
> PisyswindowsDeviceCompliance
> PTW ProdUsers
>All Users,
> All Pisys Users
> ATMS DevUsers
>ATMProdControlPanelUsers
>ATMSProdUsers
>Developers
>Pisys
>PisysMFA
>PTWCControlPanelUsers
User Type - Member, Since 11/04/2023
Software Installed / Access - 1 Password, Microsoft Office 365, Adobe, Dell Standard Applications, MS Copilot, MS Defender, MS Intune Extension
Access to Testing Environment

Ticket # MOC2831
Dated 12/02/2025
Description - Add Fiona and Lynda to order email distribution
Approved by JE - Cloud Admin
Priority - Normal
Type - Standard Task
Closed by 12/02/2025

Ticket # MOC 2825
Dated - 10/02/2025
Description - Create Admin User for JIM to Access ESET Portal
Approved by - AM
Priority - Normal
Type - Standard Task
Closed - 10/02/2025

Conclusion
Planned activities have been fully realised.

Assets Management:

5.9 Inventory of information and other associated assets
5.10 Acceptable use of information and other associated assets
5.11 Return of assets
5.12 Classification of information
5.13 Labelling of information
7.10 Storage media
8.9 Configuration management - New
8.10 Information deletion - New
8.11 Data masking - New
8.12 Data leakage prevention - New

Documented Information / Evidence
Asset Management Process Rev 1.5 Dated 27/05/2024
Work Station Build Procedure Rev 2.0 Dated 17/03/2025
Privacy Protection of PII Policy Rev 2.0 Dated 17/06/2024

Information Assets Classification - Desktop, Monitor, Laptop, Printer/ Printer Hardware, Network Hardware, Servers, Power Related Hardware, Information (Internal / External), Facilities, Documentation, and Personnel
- Laptops are BitLocker Encrypted
- All Devices are built with latest Windows Operating System, Protected with Windows Defender XDR and enrolled in the Entra ID.
- Data Bearing Devices are cleaned by using Bit Raiser before recycled / disposal
- Each Laptop has the Unique Device TAG, which is listed in the assets register
- Pisys Staff trained and trusted their knowledge about Information security, however no DLP control has been placed on the end user devices. but annual review in placed
- Access to USB on the end user devices are available upon Approved MOC Request, Currently all developers are authorised to transmit the data via USB Slots, Risk has been address in the ISMS Risk Register
- Very Limited PII Data has been managed by the Pisys, which require to Mask during the Processing, e.g. User Password, Financial, Client confidential and HR Data
- Secure VPN, TLS 1.2 and above are used to protect the DLP during the Transit in Production Environment / Pisys Cloud Infrastructure
- IaaS, PaaS, and SaaS Service Provider is responsible to protect the DLP along with their services e.g. Azure / AWS

 # Evidence
Assets Register Content include, Title, Business Area, Assets Type, Specification, Tag No., Location, Status (Working/ Broken / Scrapped / Recycled), Comment, Purchase Date, Cost, Last PAT Test, Confidentiality, Integrity, Availability, Disposal Date, Disposal Destination, Disposal MOC
- Assets Register configured on the Company SharePoint Site
Total Laptops - 017 Working

Tag No. LAP028
Employee- AM
Device - Dell Precision 3530
Mfg- Dell
Purchase Date 11/11/2019
Status - Working

Tag Number - LAP025
Employee - JM
Device - XPS15
Mfg - Dell
Purchase Date 28/03/2019
Status - Working

TAG - LAP032
Employee Name - EM - Software Tester
Device -Vostro 7000Etido
Mfg - Dell
Purchase Date - 11/05/2021
Status - Working

Tag LAP017
Device - Latitude E6530
Mfg - Dell
Status - Disposed Dated 25/08/2021
Destruction Doc - Donated to Charity with Servers (See MOC 1722) AMIC collected the item on 29/04/2023

Ticket # MOC 2880
Dated 27/03/2025
Description - Hess ATMS DB Delete (Demo Version)
Priority - Normal
Task - Standard
Ticket Closed - 27/03/2025

Ticket # MOC2872
Dated 12/03/2025
Description - Delete Old DB Backups from DB1 and DB2
Priority - Normal
Task- Standard
Ticket Closed - 12/03/2025

Conclusion
Planned activities have been fully realised.

IT Operational Security, Network Security, Cryptography: Encryption Key Management & Regulation:

5.14 Information transfer
5.37 Documented operating procedures

6.6 Confidentiality or non-disclosure agreements
8.6 Capacity management
8.7 Protection against malware
8.8 Management of Technical Vulnerability
8.13 Information backup
8.14 Redundancy of Information Processing Facilities
8.15 Logging
8.16 Monitoring activities - New
8.17 Clock synchronization
8.19 Installation of software on operational systems
8.20 Networks security
8.21 Security of network services
8.22 Segregation of networks
8.23 Web filtering - New
8.24 Use of cryptography
8.31 Separation of development, test, and production environments
8.32 Change management
8.34 Protection of information systems during audit testing

Documented Information / Evidence
PISYS AWS Hosting Environment Rev 3 Dated 21/03/2025

> Subnet and Network Routing
> Access Control List
> Security Groups
> Load Balancers
> TLS Security
> Web Application Firewall
> Endpoint Protection
> Windows Firewall
> Identity and Access Management
> Data Encryption

Pisys AWS Architecture Documented Diagram has segregated e.g. SG- Pisys LB, SG Apps, SG - DB, SG - DC and SG- Pisys- CVPN
AWS Environment synchronised with AWS Cloud Watch
Clock Synchronisation - Windows NTP
Subnets are segregated public and private
AWS VPN, Load Balancer, Amazon Router53, S3 Storage, VPC End Point, Amazon Cloud Watch, NAT Gateway, Router, Internet Gateway, AWS Inbuilt features are in use
Two Private Database Server and Two Private Web Server, Two Load Balancer,

Six Access Control List
- ACL-Pisys-Private DC - Active Directory Domain Controller
- ACL-Pisys-Private DB -Associated with DB Server
- ACL-Pisys-Private Apps - Associated with Web Server
- ACL-Pisys-Public- LB- Associated with Load Balancer
- ACL-Pisys-Public - NAT- Associated with NAT Subnet
- ACL-Pisys-Private- CVPN - Associated with CVPN Subnet

AWS Client VPN Secure with 2048 RSA certificate and Encryption with AES256, Only Https traffic

allowed to App Servers and RDP & SSH Traffic to all servers with authenticated users through VPN
Microsoft SQL Server 2022 running in high configuration standards for availability, storage, CPU and log files
Five security groups serves as a stateful firewall for inside subnet resource
AD Authentication and authorisation process in placed to control remote access to servers for Pisys Staff connected to AWS VPN
TLS 1.2 and / or TLS 1.3 (ELB Security Policy - TLS13-1-2-Res-2021-06) secure all communication between webservers and browsers of whether sensitive data is being transmitted or not
Secure Development Practice and mitigate OWASP's top10 threat within the applications

 # End Point Protection includes
- Real-time file System protection from Virus and Malware
- Host intrusion prevention
- Advanced Memory Scanning to Protect from Obfuscated threats
- Exploit blocker to protect against exploits in applications
- Ransomware shield
- An intrusion detection system (IDS) provides network attack protection
- Botnet protection
- Web access protection
- Anti Phishing Protection
- Email client protection

Capacity and Event Log Management
Windows Servers 2022 OS installed with built in firewall enabled on all servers and configured
Pisys Staff are managed through Microsoft Entra ID Domain & Office365 Email address
AWS Servers access provided via 2048 -bit RSA Security certificate and server domain user account
Disks and AWS S3 Buckets are protected with AES256 encryption
Data Files (200GB) DB Logs (200GB) are stored in the AWS
Each Servers has an encrypted 600GB disks to store database backups.
Alert Notification in placed upon usage of 90% of resources e.g. CPU, Memory, Storage
Server Events Logs are linked with AWS and cloud Watch, every 5 mins (90 days retention)
MS Defenders running on the End User Devices (NO Malware Remediated, 6% noncompliant, and Secure Score 72.48%, No. of Active Devices - 23)
Servers are protected with ESET End Point Protection - No Vulnerability Found - No. of Active Servers & Computers - 14, 1 Alerts for Outdated WinRAR Ver 7.1.0 (New Version 7.1.1) running on End User Device.

Last Pen Test Date 17/01/2024,
Scope - Web Application Security for ATMS (https://atms.pisys.co.uk),
Conducted by AKIMBORCORE,
Pen Test Findings - 6 Low and 2 Medium
Current Status of findings - Closed (Refer Risk Register Actions - 542 to 552 and "YouTrack" Ref for Action Tracking)

Web Filtering
- All PISYS Work Stations managed through MS Intune, and Windows Defender
- Blocked Category - Cults, Gambling, Nudity, Pornography/Sexually Explicit, Sex Education, Tasteless Violence, Child Abuse Images, Criminal Activity, Hacking, Hate & Intolerance, Illegal Drug, Illegal Software
School Cheating, Self-Harm, Weapons

Data Backup Policy Rev 5.0 Dated 18/10/2024
- Automated incremental backup for Production, Testing and DevOps Environments running every hours between 24/7 365
- 30 Days SLA with customer
- 60 Days SLA with Pisys
- Monthly Full Snapshots

Pisys retain data for the last 30days, enabling Points in time recovery. Admin will inform the staff members about customer offboarding by raising MOC Tickets

BCP Test Ticket - MOC 2819
Dated - 05/02/2025
Description - Grab a Copy of the audits DB from QC sites
Methods - DB1 Files Copied from DB and Installed in to Local SQL Server, Delete the Backup from server
Results - Successful
Down Time - no Downtime

Client Data backed up in the datacentre and replicated to backup sites
Backup integrity test undertaken by the IT support Staff

Change Management
Ticket # MOC2749
Dated 18/11/2024
Description - Create Stanley Black & Decker PTW db - Trial
Priority - Normal
Completed - 18/11/2024

Ticket # MOC 2855
Dated 27/02/2025
Description - Delete Stanley Black & Decker PTW db - Trial
Priority - Normal
Completed 27/02/2025

Cryptographic Policy Rev 1.6 dated 16/12/2024
Key Management - AWS, Azure DevOps, Server Certificate (SSL and DB Server Encryption)
Authentication - TLS Certificate
Protection - AWS Certificate Manager
Certificates are backed up on the Secure Web Servers
Validity - 1 Year

Ticket - MOC2523
Dated - 01/05/2024
Description - Issue a New *.pisys.co.uk and update it on AWS Certificate Manager, IMD VPN and OTS Servers
Priority - Normal
Completed 02/04/2024

Conclusion
Planned activities have been fully realised.
Good Practice

Software / System Acquisition, Development and Maintenance & Project Management:

5.8 Information security in project management
8.25 Secure development life cycle
8.26 Application security requirements
8.27 Secure system architecture and engineering principles
8.28 Secure coding - New
8.29 Security testing in development and acceptance
8.30 Outsourced development
8.31 Separation of development, test and production environments
8.32 Change management
8.33 Test information

Documented Information / Evidence
Secure Development Policy Rev 3 Dated 12/11/2024
OWASP Guide Ver 4.05
Microsoft Integrated Security into DevOps Processes (DevSecOps)
PISYS Testing Team (SOP), Rev 1.6 Dated

- Information Security Risk address at any point of the development lifecycle e.g. Design, Coding, Build, Deploy and run
- Zero Trust Architecture and Governance followed and every stage of SDLC
- Each User Account has granted the information access followed by Need to know and least privileged principle

Information Security Objective followed, specified by Microsoft
> Established security standard, metrics and governance
> Require use of proven security features languages and frameworks
> Perform Security Design review and threat modelling
> Define and use cryptographic standard
> Secure the software supply chain
> Secure the engineering environment
> perform security testing
> Ensure operational platform security
> Implement security monitoring and response
> Provide security training

Sprint Management - You Track Portal (Open, In-Progress, To Verity and Done / Passed)
Dedicated Channel on the You Track for Each Pisys Software Product
Coding Platform - MS Visual Studio and Visual Studio Code
Developers are not allowed to ignore any Code Warning
Second Opinions are obtained for the design and threat model
Password Rotations is not mandate for user account, however regular rotation of the certificate is mandatory
Static and Dynamic Analysis Security testing adopted
Application Pen Test run annually e.g. Cyber Essential and External Pen Test
Existing and Potential Security Issues are reviewed / discussed in the weekly team meeting
Security moment shared via the shared blog post from Information security authorities
Testing Documentation - SharePoint, YouTrack and Qase

Testing Life Cycle - Requirement - Planning - Case Creation & Design - Execution and Cycle Closer
Type of Test - Automation & Manual
Test outcome logged an stored in the SharePoint with version control
Test Requirement Gathered and Defact Management - YouTrack
Test Case Management - Qcase
Automated Test Environment - Regression Testing using subset of Qase test cases & Robot Framework and Selenium

Evidence
PTW V 1.6.3.10 - Patch Release Test Plan Rev1 Dated 16/12/2025
PTW V 1.6.3.10 - Patch Release Rev1 Dated 15/01/2025
PTW Ver 1.6.3.10 Patch Release - Release Note Rev 1.0 dated 15/01/2025
Scope of Dev, Testing, and Release of following Tickets for above version of the Software product - PTW (Permit to Work)
1701 - Isolation Status
1703 - Improvements of Isolation
1709 - Permit List - Validation Between Filter
1708 - A user without admin rights for any of the general permit or isolation items is unable to edit any contractor documents
1705 - long term isolation improvement
1701 - isolation "Live Only" Checkbox
1702 - Isolation Rejects

Ticket - MOC2793 dated 15/01/2025 - Update PTW to V 1.6.3.10,
Priority - Normal
Type - Standard Task
Completed -15/01/2025 at 19:00
down Time - 15 Mins

- Technique Used - Blackbox Testing, Static Analysis, Data Injection (Positive & Negative), and Visual Inspection
- Test Deliverables - Test Script, Interval Progress Report, Release Test Report, Environmental Details, Detailed Software Test Tool Set, Regression Test Pack
- Test Conducted by - KRC and EM,
- Developer - GS
- Release between 16/12/2024 to 17/01/2025
- Objective Achieved

Conclusion
Planned activities have been fully realised.

Supplier Security (Selection / Review / Monitoring / NDA):

5.19 Information security in supplier relationships
5.20 Addressing information security within supplier agreements
5.21 Managing information security in the ICT supply chain
5.22 Monitoring, review and change management of supplier services
5.23 Information security for use of cloud services - New
6.6 Confidentiality or non-disclosure agreements

Documented Information / Evidence
Supplier Security Policy Rev 1.2 Dated 18/10/2024

- Suppliers are reviewed and approved by the director in consultation relevant Team members
- Supplier Agreements are mandatory along with SLA, NDA, Intellectual Property Rights and Termination T&Cs
- Contract owner is responsible to monitor the supplier performance and proposed any required changes
- Cloud Service Supplier Assessment Criteria Includes VPC, Compute, Storage, IAM, DNS Security, Geographical Location, and Data Encryption
- All Suppliers are listed in the Company SharePoint
- Access rights are managed in accordance with Pisys Access Control Policy

 # Documented Information Retained
- Supplier Contract
- Non Disclosure Agreement - Pisys Template Valid from 31/05/2024
- Supplier Performance Records

Evidence - List of Current Suppliers
- AWS
- BSI - https://bsigroup.com/en-GB/about-bsi/compliance-and-ethics-in-bsi/
- Dell
- Log me In
- Rackspace Technology
- Red Evolutions
- Microsoft Ireland
- Akimbo Core
- Google Cloud
- Twilio Ireland Ltd
- SAGE
- Shopify
- 3T Training
- Embarcadero - Contract DocuSign Envelop ID D9CD258DFFBB, Expire on dated 01/09/2025 (C++ Builder Professional Name User Support ESID PID 1032468, PO Number 12874 Dated 26/06/2024

Conclusion
Planned activities have been fully realised.

Business Continuity Management / ICT Readiness:

5.29 Information security during disruption
5.30 ICT readiness for business continuity - New
8.14 Redundancy of information processing facilities

Documented Information / Evidence
Business Impact Analysis Rev 2.0 Dated 18/03/2025
Business Continuity Plan Rev 1.5 Dated 12/06/2024
Disaster Recovery Policy for Data Centre Rev 2.0 Dated 19/03/2025

Strategy - Prevention - Detection - Response and Recovery
Prevention - Risk Assessment, Training, Access Control, Regular Backup and Physical Security

Detection - System Monitoring, Incident Response Team and Reporting Procedure
Response - Activation of the IRT, Containment, Eradication, Recovery and Posit Incident Review
Recovery - BCP, DRP, Testing and Exercise, Vendor Management and Insurance
RTO- Restore Operation within 2 Hrs during the normal office time between Mon - Fri 09:00 to 17:30 UK time

BCP Includes Incident Occurrence - First Hr Strategy - Incident Response Team - Critical System - Recovery - Data Backup - Recovery Objectives and Alternative Communication

BCP Commitment for Employee Awareness, regular review of BCP, Generic Response to DR, Emergency Contract, and ensure the information security during DR situation

BCP Responsibilities are assigned to Information Security Manager, Employees, Contractors, Vendors and Overall Day to Day Task

Key Business Function - Development, Finance, InfoSec, IT, People, Quality, Sales and Support
Info Assets - Client Data, Contracts, People, PO, System Spec, Source Code, System Documentation, Supplier Invoice, Marketing Materials, Phone / 1-1 Conversation, Account Info, SharePoint Site , Test Plan, Run cases

Impact area - Financial, Legal and Reputation

BCP Risk - Physical Damage, system Breakdown, Access Restriction Physical & Logical, Utility Outage, Supply chain interruption, Damage to loss or corruption of IT

 # Evidence
Currently 100% Remote Working in PISYS

BCP Test Ticket - MOC 2871
Dated 12/03/2025
Description - Copy Anasuria ATMS database to MAK Dev Machine to investigate visibility issues
Methods - Login to DB1 and restore backup files to MAKs Dev Machine
Results - successful
Down time - No Downtime

BCP Test Ticket - MOC 2755
Dated 25/11/2024
Description - Restore CLEAN Linen Services Backup to QC
Methods - follow Wizard at http://qcp.pisys.co.uk/PTW/
Results - successful
Down time - No Downtime

Conclusion
Planned activities have been fully realised.

Legal / Regulatory / Contractual Compliance:

5.31 Legal, statutory, regulatory, and contractual requirements
5.32 Intellectual property rights
5.33 Protection of records

5.34 Privacy and protection of PII
5.35 Independent review of information security
5.36 Compliance with policies, rules, and standards for information security
8.8 Management of technical vulnerabilities

Documented Information / Evidence
Privacy Protection of PII Policy Rev 2.0 Dated 17/06/2024
Data Retention Policy Rev 1 Dated 06/03/2024
Information Security Policy Section C.2. Legal regulatory and Contractual Compliance
Protection of Intellectual Property Rights Policy Rev 1.0 Dated 07/06/2024

- Intellectual Property Rights and Non Disclosures are address in the Relevant Contractual documents e.g. Supplier, Employees and Customers
- Sensitive and PII Data Records are retained and protected with standard encryption provided by the relevant service provider and in accordance with the data retention policy & Privacy Protection of PII Policy
- Source of Legislative Updates - Industry Forum, Workshop's, www.legislation.gov.uk and Direct Contact between the director and authorities
- Intellectual Property Rights Policy Covers the Copyrights, Trademark, Patent, Trade Secret and Confidential Information

 # Evidence
- The Data Protection Act 2018
- Copyright, Design and Patents Act 1988
- Computer Misuse Act 1990
- Regulation of Investigatory Power Act 2000
- Human Rights Act 1998
- Electronics Communications Act 2000
- The Copyrights and rights in Database Regulations 1997
- Requirements of Writing (Scotland) Act 1995
- The Electronics Documents (Scotland) Regulations 2014
- GDPR 2018
- The Intellectual Property Rights 2014
- WEEE Directive 2012 /19/EU
- Modern Slavery Act 2015

Employment Contract Template Section

Cyber Essential
Organisation - Pisys Limited
Scope - Whole Organisation
Profile Version - 3.1 Montpellier
Certificate Number - e8621ff1-d07c-4c48-a237-39748974a038
Certificate Date 27/02/2025
Re-Certificate Date - 27/02/2026

ICO Registration reference: Z5787765
Date registered: 20 September 2001
Registration expires: 19 September 2025
Payment tier: Tier 1
Data controller: Pisys Limited

Address: 7 Queen's Gardens, Aberdeen - AB15 4YD

Last Pen Test Date 17/01/2024,
Scope - Web Application Security for ATMS (https://atms.pisys.co.uk),
Conducted by AKIMBORCORE,
Pen Test Findings - 6 Low and 2 Medium
Current Status of findings - Closed (Refer Risk Register Actions - 542 to 552 and "YouTrack" Ref for Action Tracking)

Conclusion
Planned activities have been fully realised.

Competency, Awareness and Training (Staff Interview):

Documented Information / Evidence
- The Organisation demonstrate a clear understanding of the significance of employee awareness and education, as evidence by the information security awareness programs and regular training sessions.

Induction Training
- Employment Guide
- Information Security Management - ISO 27001 System
- IT Asset Allocation
- Incident Reporting

 # Remote Working Policy Stated the following
> Remote Access Approval
> Secure Remote Access
> Security of Device, Network, Data Working Environment, Communication, Physical,
> Incident Reporting
> Awareness and Training
> Employee Responsibilities for Remote Working

Regular Attendance in Weekly ISMS Awareness Meeting (Last dated 27th Feb 2025, 13th & 20th Mar 2025)
- Fake Captchas
- Amazon Kills on Device Alex Processing

Emp Name - KRC - Product Manager
- Join Pisys as QA Tester
- Internal and External Engagement via Email, Teams
- Weekly Product Meeting
- Security Risk for Test Data base needs to sanitised and cleaned
- Phishing email awareness demonstrated with observation of sender's email address, body part, signature panel
- Data sensation skills use as necessary
- No Testing Data Retention
- Test Cases are stored in the Qcase
- Test notes and release notes are stored in the Company SharePoint
- Password Change Every 90 days (12 Characters Length with Lower, upper, Numbers and Special Characters)

- Information Security Policy were shared onscreen

Emp Name - JE - Software Developer
- Internal Engagement
- Tools Use- You Track - Sprint Management
- Code Writing - Java Script, SQL Servers and Local Machine
- Code Review related Risk has been considered during merging, QA and Release process, if any
- Phishing email awareness demonstrated with observation of sender's email address, body part, signature panel
- Password Change Every 90 days (12 Characters Length with Lower, upper, Numbers and Special Characters)
- Information Security Policy were shared onscreen

Conclusion
Planned activities have been fully realised.

Closing Meeting:

The closing meeting was conducted, and the report findings summarised to those present. The BSI standard assessment approach including confidentiality, nature of sampling, appeals process (if required), and any forward actions following this assessment were confirmed. The next visit planning arrangements were reviewed and confirmed

Minor (2) nonconformities arising from this assessment.

Finding Reference	2630475-202503-N1	**Certificate Reference**	IS 618522
Certificate Standard	ISO/IEC 27001:2013	**Clause**	5.2
Location reference	0047530525-000		
Assessment Number	3991942		
Category	Minor		
Area/process:	Leadership and Commitment		
Statement of non-conformance:	Organisation has not demonstrated the methods of communication within Information Security Policy Statement		
Clause requirements	Policy Top management shall establish an information security policy that: f) be communicated within the organization; and g) be available to interested parties, as appropriate.		
Objective Evidence	Information Security Policy Statement		
Cause			
Correction/containment			
Corrective action			

Finding Reference	2630475-202503-N2	**Certificate Reference**	IS 618522
Certificate Standard	ISO/IEC 27001:2013	**Clause**	2022_9.3.2
Location reference	0047530525-000		
Assessment Number	3991942		
Category	Minor		
Area/process:	Performance Evaluation & Improvement		
Statement of non-conformance:	Changes in the needs and expectations of interested parties has not been reviewed in the ISMS Management Review Meeting		
Clause requirements	Management review inputs The management review shall include consideration of:		

	b) changes in external and internal issues that are relevant to the information security management system;
Objective Evidence	Annual Management Review Minutes Dated 17/12/2024
Cause	
Correction/containment	
Corrective action	

Next visit objectives, scope and criteria

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

The scope of the assessment is defined in the plan provided in terms of locations and areas of the system and organization to be assessed.

The criteria of the assessment was ISO: 27001:2022 and Pisys Ltd's management system documentation.

Please note that BSI reserves the right to apply a charge equivalent to the full daily rate for cancellation of the visit by the organization within 30 days of an agreed visit date. It is a condition of registration that a deputy management representative be nominated. It is expected that the deputy would stand in should the management representative find themselves unavailable to attend an agreed visit within 30 days of its conduct.

Next visit plan

Date	Auditor	Time	Area/process
			CAV1
17/03/2026	James Stewart	09:00	Opening Meeting Introduction, attendees, programme, visit criteria, scope, confidentiality, methodology, sampling, limitations, findings, H&S, issues, plan, Q&A.
		09:15	Business update and Review of the ISMS
		09:30	Context and Policy (4,5) : Change/Update, Leadership, Roles/Responsibilities, Context/Scope, Core policy Changes to Org Context, Needs / expectations of interested parties, Scope Statement validation, Management System Policies/Processes, Roles Responsibilities & Authorities
		10:00	Leadership & Commitment (5) Leadership Interview
		10:30	Planning and Operations (6,8) : SOA, Risk Assessment/Treatment, Objectives, Change
		11:00	Evaluation and Improvement (9,10) : Internal Audit, Corrective Actions, Performance, Management Review, Improvement
		11:30	Organisational: information assets (A.5.9 - 5.14)
		12:00	Lunch & Report Writing
		13:00	Organisational: information security incident management (A.6.8, 5.24 - 5.28)
		13:30	Technological: use of cryptography (A.8.24)
		14:00	Technological: information deletion, masking & data loss prevention (DLP) (A.8.10 - 8.12)
		14:30	Technological: networks incl segregation, web filtering & redundancy (A.8.20 - 8.23, 8.14)
		15:00	Daily Review & Updates
			Closing Meeting
		15:30	Report Writing & Audit Trails

Appendix: Your certification structure & ongoing assessment programme

Scope of certification

IS 618522 (ISO/IEC 27001:2022)
The systems, processes and infrastructure involved in delivering Pisys' range of software products and services in accordance with Statement of Applicability 1.0 Dated 01/03/2025

Assessed location(s)

The audit has been performed at Central Office.

Aberdeen / IS 618522 (ISO/IEC 27001:2013)

Location reference	**0047530525-000**
Address	Pisys Ltd 7 Queen's Gardens, Aberdeen AB15 4YD United Kingdom
Visit type	Re-certification Audit (RA Opt 2)
Assessment number	3991942
Assessment dates	24/03/2025
Deviation from audit plan	No
Total number persons within scope of certification across ALL locations	15
Total number of persons within scope of certification at THIS location	15
Scope of activities at the site	The systems, processes and infrastructure involved in delivering Pisys' range of software products and services in accordance with Statement of Applicability 1.0 Dated 18/12/2024
Assessment duration	3 day(s)

Aberdeen / IS 618522 (ISO/IEC 27001:2022)

Location reference	**0047530525-000**
Address	Pisys Ltd 7 Queen's Gardens Aberdeen AB15 4YD United Kingdom
Visit type	Transition Audit
Assessment number	30121028
Assessment dates	27/03/2025
Deviation from audit plan	No
Total number persons within scope of certification across ALL locations	15
Total number of persons within scope of certification at THIS location	15
Scope of activities at the site	The systems, processes and infrastructure involved in delivering Pisys' range of software products and services in accordance with Statement of Applicability 1.0 Dated 18/12/2024
Assessment duration	1 day(s)

Certification assessment programme

Certificate number - IS 618522
Location reference - 0047530525-000

		Audit 1	Audit 2	Audit 3	Audit 4	Audit 5	Audit 6	Audit 7
Business area/location	**Date (mm/yy):**	01/25	03/25	03/25	03/26	01/27	01/28	03/28
	Duration (days):	1	3	1	1	2	0.5	3
RR		X						
PM		X					X	
TR				X				
CAV					X	X		
RAV			X					X
Opening Meeting Introduction, attendees, programme, visit criteria, scope, confidentiality, methodology, sampling, limitations, findings, H&S, issues, plan, Q&A.		X	X	X	X	X		X
Business update and Review of the ISMS			X		X	X		X
Context and Policy (4,5) : Change/Update, Leadership, Roles/Responsibilities, Context/Scope, Core policy Changes to Org Context, Needs / expectations of interested parties, Scope Statement validation, Management System Policies/Processes, Roles Responsibilities & Authorities			X		X	X		X
Leadership & Commitment (5) Leadership Interview			X		X	X		X
Planning and Operations (6,8) : SOA, Risk Assessment/Treatment, Objectives, Change			X		X	X		X
Evaluation and Improvement (9,10) : Internal Audit, Corrective Actions, Performance, Management Review, Improvement			X		X	X		X
Support (7) : Resources, Competency, Awareness, Communications,			X			X		X

Document Management							
.							
Organisational: policies, responsibilities, contacts, threat intelligence (A.5.1 - 5.7)		X	X				X
Organisational: information assets (A.5.9 - 5.14)		X		X			X
Organisational: suppliers including use of cloud services (A.5.19 - 5.23)		X			X		X
Organisational: information security incident management (A.6.8, 5.24 - 5.28)		X		X			X
Organisational: legal, statutory, regulatory requirements, data privacy, review (A.5.31 - 5.36)		X			X		X
Organisational: information security during disruption including ICT readiness (A.5.29, 5.30)		X					X
People: starters & leavers, awareness training incl. remote working (A.6.1 - 6.7)		X			X		X
Physical: perimeter, facilities, monitoring, protection, cabling, maintenance (A.7.1-7.8, 7.11-7.13)		X					X
Technological: operational procedures & management (A.5.37, 8.6, 8.17, 8.18)		X			X		X
Technological: IT asset management (A.8.1, 7.9, 7.10, 7.14)		X	X		X		X
Technological: use of cryptography (A.8.24)		X		X			X
Technological: identity & access management (IAM) (A.5.15 - 5.18, 8.2 - 8.5)		X			X		X
Technological: anti-malware protection & vulnerability management (A.8.7, 8.8)		X			X		X
Technological: information deletion, masking & data loss prevention (DLP) (A.8.10 - 8.12)		X		X			X
Technological: information backup & test restores (A.8.13)		X			X		X

Technological: logging & monitoring incl. security information event management (SIEM) (A.8.15, 8.16)		X			X		X
Technological: networks incl segregation, web filtering & redundancy (A.8.20 - 8.23, 8.14)		X		X			X
Technological: secure development - requirements, design, coding & testing (A.8.25- 8.34)		X			X		X
Technological: IS in project management, change & configuration management (A.5.8, 8.32, 8.9, 8.19)		X			X		X
Business Function sample: Operations/Awareness [4-10, A.X]							
Local ISMS controls and Processes (9.2, 8.2, A.5.29-30, A.5.24-28, A.5.9-14)							
Lunch & Report Writing	X	X	X	X	X	X	
Report Writing & Audit Trails	X	X	X	X	X	X	
Daily Review & Updates	X	X	X	X	X	X	
Closing Meeting	X	X	X	X	X	X	

Mandatory requirements – recertification

Review of assessment finding regarding conformity, effectiveness and relevance of the management system:

The organization has shown a positive approach to improving the ISMS. However, two minor NCRs were identified during the assessment. Root cause analysis and corrective actions will be provided within the agreed timeframe

Management system strategy and objectives:

During the assessment, top leadership showed a positive approach by providing strategic direction and committing to legal, regulatory, and contractual SLAs, along with technical and training resources provisioning

Review of progress in relation to the organization's objectives:

Software developers monitor ISMS objectives and review them with senior leadership every month.

Review of assessment progress and the recertification plan:

The three-year plan was reviewed during this audit to ensure it fits the number of employees and meets the scheme's requirements.

BSI client management impartiality and surveillance strategy:

Auditor does have all P, T and S Codes as require over the Certification Cycle and impartiality has been maintained in accordance with BSI Processes and procedures.

Continue with the current total assessment days/cycle.

Expected outcomes for accredited certification

What accredited management system certification means?

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

In particular, it is to be expected that the organization

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

What accredited management systems certification does not mean?

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

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

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

Definitions of findings:

Nonconformity:

Non-fulfilment of a requirement.

Major nonconformity:

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

Minor nonconformity:

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

Opportunity for improvement:

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

How to contact BSI

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

Should you wish to speak with BSI in relation to your certification, please contact your local BSI office – contact details available from the BSI website:

https://www.bsigroup.com/en-GB/UK-office-locations/

Notes

This report and related documents are prepared for and only for BSI's client and for no other purpose. As such, BSI does not accept or assume any responsibility (legal or otherwise) or accept any liability for

or in connection with any other purpose for which the Report may be used, or to any other person to whom the Report is shown or into whose hands it may come, and no other persons shall be entitled to rely on the Report. If you wish to distribute copies of this report external to your organization, then all pages must be included.

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

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

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

Regulatory compliance

BSI conditions of contract for this visit require that BSI be informed of all relevant regulatory non-compliance or incidents that require notification to any regulatory authority. Acceptance of this report by the client signifies that all such issues have been disclosed as part of the assessment process and agreement that any such non-compliance or incidents occurring after this visit will be notified to the BSI client manager as soon as practical after the event.