INTERNAL AUDIT REPORT

INFORMATION SECURITY MANAGEMENT SYSTEM
ISO/IEC 27001

Organization:

ADDVOLT

Audit report date:

2nd December 2024

PGM CONSULTING

1.1 Audit objective

Evaluate compliance with the standard ISO/IEC 27001:2022, documentary support, policies and processes associated with the scope and boundaries of the ISMS.

1.2 Analysis criteria

The Criteria taken into account in implementing this IA (Internal Audit) were the degree of compliance of the Information Security Management System in relation to the reference standard, ISO/IEC 27001:2022.

The scope of the ISMS:

Information security related with the development, management and support related with ADDVOLT platform, software, and services" According with the Statement of Aplicability.

1.3 Date and Place

The IA took place on 21, 22 and 27 of November 2024, mainly held on-site in the ADDVOLT office (2 days) and 0,5 day remote, having analyses of processes and activities at the company's office in Águas Santas.
The audit lasted an effective duration of 2.5 day.

1.4 Audit Team

- Paulo Garcia Miguel (PM) – Lead Auditor

2. Summary

The Audit Plan was complied with and was subject to some adjustments to ensure the objectives of the audit were achieved.

The requirements and controls points of the standard have been audited, validating the application or not of such controls to the defined scope of the ISMS.

ISMS demonstrates that it is structured and documented, requiring more time to stabilise and integrate ADDVOLT's activity.

As strengths, the Audit Team points out:

- Dedication of the ISMS team
- Dedication of the IT and SW Development team
- Use of new tools in the operational management of the ISMS
- Technical knowledge of relevant elements of the Organization

ADDVOLT has demonstrated the necessary skills and means to overcome the findings presented in this report easily.

The audit team appreciates the participation and contribution given by the employees contacted.

The audit team recalls that an audit is a sampling evaluation process, so it recommends evaluating other situations that may bring constraints to the implemented management system.

3. Âmbito da AI

STANDARD CLAUSES (ISO/IEC 27001:2022)		AUDIT SCOPE (1)	NC (2)	IO
4.1	Understanding the organisation and its context (*)	PM		
4.2	Understanding the needs and expectations of stakeholders	PM		
4.3	Determine the scope of the information security management system	PM		
4.4	Information security management system	PM		
5.1	Leadership and commitment	PM		
5.2	Politics	PM		
5.3	Roles, responsibilities and authorities in the organization	PM	1	
6.1	Actions to address risks and opportunities	PM	2	8
6.2	Information security and planning objectives to achieve them	PM		
6.3	Planning of changes	PM		
7.1	Resources	PM		
7.2	Competence	PM		
7.3	Awareness	PM		
7.4	Communication	PM		
7.5	Documented information	PM		
8.1	Operational planning and control	PM		
8.2	Information security risk assessment	PM		
8.3	Information security risk treatment	PM		
9.1	Monitoring, measurement, analysis and evaluation	PM		
9.2	Internal audit	PM		
9.3	Management review	PM	3	
10.1	Non-compliance and corrective action	PM		
10.2	Continuous improvement	PM		
A	**Annexe A**			
5	**Organizational controls**			
A 5.1	Policies for information security	PM		
A 5.2	Information Security Roles & Responsibilities	PM		
A 5.3	Segregation of Duties	PM		
A 5.4	Management responsibilities	PM		
A 5.5	Contact with authorities	PM	4	
A 5.6	Contact with special interest groups	PM		
A 5.7	Threat Intelligence	PM		

STANDARD CLAUSES (ISO/IEC 27001:2022)		AUDIT SCOPE (1)	NC (2)	IO
A 5.8	Information security in project management	PM		
A 5.9	Inventory of information and other associated assets	PM		9
A 5.10	Acceptable use of information and other associated assets	PM		
A 5.11	Return of assets	PM		
A 5.12	Classification of information	PM		
A 5.13	Labelling of information	PM		10
A 5.14	Information transfer	PM		11
A 5.15	Access control	PM		
A 5.16	Identity management	PM		
A 5.17	Authentication information	PM		
A 5.18	Access rights	PM	5	
A 5.19	Information security in supplier relationships	PM		
A 5.20	Addressing information security within supplier agreements	PM		
A 5.21	Managing information security in the ICT supply chain	PM		
A 5.22	Monitoring, review and change management of supplier services	PM	6	
A 5.23	Information security for use of cloud services	PM		12
A 5.24	Information security incident management planning and preparation	PM		
A 5.25	Assessment and decision on information security events	PM		
A 5.26	Response to information security incidents	PM		
A 5.27	Learning from information security incidents	PM		
A 5.28	Collection of evidence	PM		
A 5.29	Information security during disruption	PM		
A 5.30	ICT readiness for business continuity	PM		13
A 5.31	Legal, statutory, regulatory and contractual requirements	PM		
A 5.32	Intellectual property rights	PM		
A 5.33	Protection of records	PM	7	
A 5.34	Privacy and protection of PII	PM		14
A 5.35	Independent review of information security	PM		
A 5.36	Compliance with policies, rules and standards for information security	PM		
A 5.37	Documented operating procedures	PM		

STANDARD CLAUSES (ISO/IEC 27001:2022)		AUDIT SCOPE (1)	NC (2)	IO
6	**People Controls**			
A 6.1	Screening	PM		
A 6.2	Terms and conditions of employment	PM		
A 6.3	Information security awareness, education and training	PM		
A 6.4	Disciplinary process	PM		
A 6.5	Responsibilities after termination or change of employment	PM		
A 6.6	Confidentiality or non-disclosure agreements	PM		
A 6.7	Remote working	PM		
A 6.8	Information security event reporting	PM		
7	**Physical Controls**			
A 7.1	Physical security perimeters	PM		
A 7.2	Physical entry	PM		
A 7.3	Securing offices, rooms and facilities	PM		
A 7.4	Physical security monitoring	PM		
A 7.5	Protecting against physical and environmental threats	PM		
A 7.6	Working in secure areas	PM		
A 7.7	Clear desk and clear screen	PM		
A 7.8	Equipment siting and protection	PM		
A 7.9	Security of assets off-premises	PM		
A 7.10	Storage media	PM		
A 7.11	Supporting utilities	PM		15
A 7.12	Cabling security	PM		
A 7.13	Equipment maintenance	PM		
A 7.14	Secure disposal or re-use of equipment	PM		
8	**Technological Controls**			
A 8.1	User endpoint devices	PM		
A 8.2	Privileged access rights	PM		
A 8.3	Information access restriction	PM		16
A 8.4	Access to source code	PM		
A 8.5	Secure authentication	PM		
A 8.6	Capacity management	PM		
A 8.7	Protection against malware	PM		
A 8.8	Management of technical vulnerabilities	PM		17
A 8.9	Configuration management	PM		

STANDARD CLAUSES (ISO/IEC 27001:2022)		AUDIT SCOPE (1)	NC (2)	IO
A 8.10	Information deletion	PM		
A 8.11	Data masking	PM		
A 8.12	Data leakage prevention	PM		
A 8.13	Information backup	PM		
A 8.14	Redundancy of information processing facilities	PM		
A 8.15	Logging	PM		
A 8.16	Monitoring activities	PM		
A 8.17	Clock synchronization	PM		
A 8.18	Use of privileged utility programs	PM		
A 8.19	Installation of software on operational systems	PM		
A 8.20	Networks security	PM		
A 8.21	Security of network services	PM		
A 8.22	Segregation of networks	PM		
A 8.23	Web filtering	PM		
A 8.24	Use of cryptography	PM		
A 8.25	Secure development life cycle	PM		
A 8.26	Application security requirements	PM		
A 8.27	Secure system architecture and engineering principles	PM		
A 8.28	Secure coding	PM		
A 8.29	Security testing in development and acceptance	PM		
A 8.30	Outsourced development	PM		
A 8.31	Separation of development, test and production environments	PM		
A 8.32	Change management	PM		
A 8.33	Test information	PM		
A 8.34	Protection of information systems during audit testing	PM		

(1) Include the acronyms of the EA element(s) that audited the clause or
(2) Indicate the sequential number assigned to the Non-Compliance(s) – NC or to the Opportunities for Improvement in the clauses in which they are verified.

4. Findings

N°.	Class.	ISO/IEC 27001	Findings
1	NC	5.3	It was not defined some critical job profiles or responsibilities. Ex. ISMS Manager,
2	NC	6.1	The identification of Risks and Opportunities as a result of the SWOT Analysis for Information Security was not carried out.
3	NC	9.3	The management review is not yet be done.
4	NC	A.5.5	Has not been formal defined who should communicate with legal entities.
5	NC	A.5.18	There was no evidence of digital access being reviewed.
6	NC	A.5.22	The suppliers of critical services are not yet evaluated.
7	NC	A.5.33	It is not clearly defined the protection time for the relevant information records.
8	IO	6.1.3	Complete the information in the SoA – Statement of applicability
9	IO	A.5.9	The assets Inventory should be reviewed to identify the relevant Information Assets.
10	IO	A.5.13	Clarify the process of classifying and labelling documents of external origin. All the documents should be lebelling,
11	IO	A.5.14	Clarify the transfer rules for use the MsTeams to transfer information and approve the policy.
12	IO	A.5.23	It must ensure that the Factorial HR answer to the cloud services qualification survey.
13	IO	A.5.30	It should be tested the Business Continuity Scenarios.
14	IO	A.5.34	It would be beneficial to define the data retention period for candidate applications in the privacy policy.

15	IO	A.7.11	A system for saving the communications system from power cuts must be implemented
16	IO	A.8.3	The information management process must allow for appropriate access management by user or group of users.
17	IO	A.8.8	It should be clarified in the policy that when we cannot resolve the vulnerability directly, it is planned in a ticket.

Matosinhos, 2 December 2024
Lead Auditor