Audit report

Management systems certification

1. Company information

Company name	POTENS PERFORACIJA D.O.O.		
Address	Bakionička 14, 31210 Požega, Serbia		
Other audited sites			
Company representative	Borko Pavlović	**E-mail**	office@potensperforacija.co.rs
Scope of certification	Manufacture of perforated sheet, grated metal steps. Manufacture and installation of spare parts for thermos-power plants, processing industry, light and heavy steel structures, steel elements for railways		

2. Audit information

Audit date	**Stage 1:**	**Stage 2:** 03/04.02.2025.	**until:** 05.02.2025.		Remote: no
Audit method: **Single audit**	**No. of employees:** 45		**No. of employees in scope:** 45		**Audit duration:**24h
Audit standard(s)	**Standard 1:**	**Standard 2:**	**Standard 3:**	**Standard 4:**	**Standard 5:**
	ISO 27001: 2022	Select	Select	Select	Select
Audit type per standard	**Audit type:** 2. Surveillance	**Audit type:** Select	**Audit type:** Select	**Audit type:** Select	**Audit type:** Select
Registration no.	TA420233016838				
Scope	☐ No changes ☒ Adjustment required	**EAC scope:** Select	**NACE code** (only for EMAS):	**Category (ISO 22003/ISO 13485/ISO 50003):**	
Lead Auditor		**Auditor**		**Expert**	
Ilija Šarac					

3. Audit objectives

The audit objectives are the following:

1. Determination of the conformity of the client's management system, or parts of it, with audit criteria within the scope of the Management System.
2. Determination of the ability of the management system to ensure the client organization meets applicable statutory, regulatory, and contractual requirements.
3. Determination of the effectiveness of the management system to ensure the client organization can reasonably expect to achieve its specified objectives.
4. As applicable, identification of areas for potential improvement of the management system.
5. Review of any management system's changes.
6. Validation that the management system was effectively applied in the previous period (valid for surveillance or recertification audits) and to verify its readiness for the coming period.

The audit was carried out according to the relevant applicable procedure for Management Systems Certification and the relevant Regulation for Certification of TÜV AUSTRIA. The basic information documenting the results of the audit are included into this report, and in total, into the audit questionnaire, the copies of documents and other evidence obtained during the audit.

*) RATING of audit findings:

1: Fully compliant
2: Opportunity for improvement
3: Minor nonconformity: Effectiveness of client's corrective action is reviewed during the next audit
4: Major nonconformity: Correction through submission of documents
5: Major nonconformity: Correction through Re-audit
NA: Not applicable or/and excluded

4. Detailed result of the audit

Result of Audit stage 1	**No audit stage 1 was planned for this year's audit procedure.**

Requirement	**Standard 1:**	**Standard 2:**	**Standard 3:**	**Standard 4:**	**Standard 5:**
	Select	Select	Select	Select	Select
A. Management system (Justification of any exclusion for ISO 9001)					
B. Management review					
C. Internal audit					
D. Legislative Requirements (License of Operation, Authorizations etc.)					
E. Infrastructure, basic requirements, HACCP/oPRP plans					
F. Miscellaneous					

LIST OF DEVIATIONS FOR STAGE 1				Time allowed to close deviations until maximum 6 months after the completion of stage 1		
No.	**Description of finding**	**Relevant standard**	**Clause of the standard**	**Corrective action**	**Correction evidence**	**Rating of corrective action**

			Completion of corrective actions
Place, date:		**Place, date:**	**Place, date:**
Lead auditor	**Company representative**	**Company representative**	**Lead auditor**
(Signature)	(Signature)	(Signature)	(Signature)
(Name)	(Name)	(Name)	(Name)

Audit conclusions	Audited	Rating *)
Mandatory requirements		
Compliance to all the requirements of the relevant management system standard (or other normative document related to the management system)	☒	1
Conclusion / Comment: The organization has demonstrated determination to comply with all requirements of information security management standards. The organization has ensured that the business activities take place in a consistent and efficient manner and in accordance with the Laws of the Republic of Serbia. This commitment to compliance has helped to establish trust between all its interested parties, to promote a culture of continuous improvement and reduce the number of threatening incidents to zero. Adhering to the standards set in information security procedures and policies, the organization has helped set its security objectives and ensure information security and privacy of personal data.		
Monitoring of the performance, measurement, reports, and reviews in comparison to the main goals and objectives (related to the expected outcomes that are resulted from the requirements of the applicable management systems standards)	☒	1
Conclusion / Comment: By monitoring and measuring performance, generating reports, and conducting reviews in accordance with its main objectives arising from the information security management system requirements, the organization has laid the foundation for continuous improvement and ensuring information security and data privacy. This process allowed the organization to identify areas for improvement, take corrective action, and adjust its information security and security strategy. With the metrics for monitoring the security objectives defined in the " Rulebook on internal organization and systematization of jobs and tasks " document, the organization evaluated the performance and effectiveness of its information security management system and personal data protection.		
Management system performance in relation to statutory / regulatory / contractual requirements	☒	1
Conclusion / Comment: The organization has defined all statutory, regulatory, and contractual requirements, policies, plans and procedures relevant to the purpose and strategic direction: • "Manual ISMS" version 4 from 01.07.2024. • "SWOT Analiza" - SWOT from 03.01.2025. for 2025. • "PR-03.01 – Goals IMS 2025 "dated 10.01.2025 for 2025. By creating these acts, the organization has perfected its relationship to external issues affecting service security.		
Monitoring of processes	☒	1

Conclusion / Comment: The organization begins to apply performance measurement and analysis activities to provide data and information on the compliance of the service characteristics with the advertised and demonstrate compliance to interested parties, as well as the smooth functioning of information security management system.		
Internal audit and management review	☒	1
Conclusion / Comment: Internal audits are done according to procedure PR 04, updated on 01.07.2024. Internal audit frequency and planning is documented in the program of internal audits PR 04.02 from 03.01.2025. Results are recorded in PR 04.03 Report on internal audits. Internal audits were conducted on January 8, 2025. Internal audits covered all organizational units of the company Potens Perforacija. Management reviews are done every year based on procedure PR 05 Review by man-agement, updated on 01.07.2024.Records of participants and issues discussed and decided recorded in record of the review PR 05.01. The most recent was done on 10.01.2025.		
Upper management responsibility for the stated policies	☒	1
Conclusion / Comment: Senior management has taken responsibility for the information and privacy data security policy and thereby demonstrated its commitment to the well-being of employees, clients, and other interested parties providing leadership and direction, the general director Mr Borko Pavlovic sets the tone for the organization's culture and values and ensures that its policies are aligned with its overall information security, and information security objectives.		
Management system effectiveness	☒	1
Conclusion / Comment: Senior management has taken responsibility for the information and privacy data security policy and thereby demonstrated its commitment to the well-being of employees, clients, and other interested parties providing leadership and direction, the general director Mr Borko Pavlovic sets the tone for the organization's culture and values and ensures that its policies are aligned with its overall information security, and information security objectives.		
The corrective actions from the previous audit (action list) were reviewed and their effectiveness was verified	☒	n/a
Conclusion / Comment: No non-conformities were observed during the audit and no corrective actions were initiated.		
Complaint management and handling	☒	1
Conclusion / Comment: Management and handling of complaints has been established, but there were no complaints in the previous period.		
Changes review	☒	1

Conclusion / Comment: All management documented information updated on 01.07.2024. Procedure PR 07 Management of documented information, by implementing the requirements of the ISO/IEC 27001:2022 standard and included requirements of impact of climate changes.		
Use of the logo and/or any reference to the certification	☒	1
Conclusion / Comment: The organization uses the certification logo in accordance with the rules.		

Information security specific requirements according to ISO 27001	
Locations	**Audited**
Headquarter: Bakionička 14, 31210 Požega, Serbia	☒
Location / Branch office 1: Address	☐
Location / Branch office 2: Address	☐
Data center 1: Bakionička 14, 31210 Požega, Serbia	☒
Data center 2: Address	☐
Statement of applicability (SoA) and exclusions	
The statement of applicability applies in **version 4 from 01.07.2024**	
The following measures of Annex A and/or Annex B are declared as "not applicable": • No measures of Annex A and/or Annex B are declared as "not applicable". All exclusions have been considered in detail, and the reasons given are plausible. The exclusions are accepted.	
Data protection and information security policies and information security objectives	
Conclusion / Comment: Information security policy is appropriately defined and documented as "Policy ISMS". Top management is committed to the implementation of the policy, which complies with organizational context and is appropriately communicated within the organization. Objectives PR-03.01, version for 2025. dated.	

03.01.2025. are defined at the process levels, prescribed measures, responsibilities, deadlines for their achievement, as well as the method of evaluating the results. Signed by the CEO mr Borko Pavlović

Risk management process

Conclusion / Comment: The organization has an appropriately defined risk management process which relies on documented risk management methodology "Metodologija za procenu rizika". The last risk assessment was conducted on 10.01.2025. and results are documented within Procedure for addressing risks and opportunities PR-02 version 3 from 01.07.2024. Risks and opportunities assessment documented in P0 02.01, edition 03 of.03. 01.2025, Concerning of financial, market share, product, human resources, brand etc.

Inspected requirements of the standard according to the audit plan			
Annex A of ISO 27001:2022	**CA / R**	**1. SA**	**2. SA**
Organizational information security	☒	☒	☒
Asset Management	☒	☒	☒
Customers and suppliers	☒	☒	☒
Access control	☒	☒	☒
Information security incidents	☒	☒	☒
Business Continuity	☒	☒	☒
Compliance	☒	☒	☒
Human resource security	☒	☒	☒
Physical security	☒	☒	☒
Devices and equipment	☒	☒	☒
IT operation	☒	☒	☒
Configuration- and data management	☒	☒	☒
Backup, Logging, Monitoring	☒	☒	☒
Network security	☒	☒	☒
Development	☒	☒	☒

LIST OF POSITIVE FINDINGS	
No.	**Description**

LIST OF FINDINGS / NONCONFORMITIES

No.	Relevant standard	Clause of the standard	Description of finding	Rating *)	Root cause and corrective action	Completion of corrective action until:	Correction evidence for nonconformities	Evaluation/Verification of corrective action

*) Rating: 1 = Fully compliant; 2 = Opportunity for improvement; 3 = Minor nonconformity; 4/5 = Major nonconformity; NA = not applicable or/and excluded

			Completion of corrective action
Place, date:		**Place, date:**	**Place, date:**
Lead Auditor	**Company representative**	**Company representative**	**Lead Auditor**
(Signature)	(Signature)	(Signature)	(Signature)
(Name)	(Name)	(Name)	(Name)

5. Recommendation of the audit team

The certification scope is appropriate	**Yes**	☒	**No**	☐
The audit objectives have been fulfilled	**Yes**	☒	**No**	☐

Standard(s)	**Audit team suggestion**				
ISO 27001	☐	Issue of the certificate	**AFTER**	☒	no other action
	☒	Maintenance of certificate		☐	Correction of nonconformities with the submission of documents
	☐	Renewal of certificate		☐	Correction of nonconformities with the Re-audit
	☐	Withdrawal of certificate			

Place, date:	Požega, 05.02.2025.		
Lead auditor	Ilija Šarac	**Auditor(s)**	
Signature		**Signature**	

Other Information / Disclaimer:

During the validity of the certificate, the certified company is obliged to inform the certification body about relevant changes in the management system and its documentation.
It should be noted that the audit is conducted based on sampling of available information, which may result in nonconformities in addition to those documented during the audit.
The result of the audit does not relieve the audited company of its responsibility for the control of the existing management system and for the maintenance and conformity with the requirements of the standard(s) for which the certificate(s) has/have been issued.
The certification body or the auditor shall under no circumstances replace the control carried out by the competent national authorities.

*) The audit involves assessing the performance of the management system in ensuring that the company fundamentally meets the applicable legal, regulatory, and contractual requirements. This evaluation is based on samples viewed and is not an assessment of compliance with legal requirements. The responsibility for enforcement and assessment of compliance with the relevant laws and regulations remains with the company in all cases.

6. Distribution list

- ✔ Client
- ✔ Certification body of TÜV AUSTRIA
- ✔ Audit team