

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	borko.pavlovic@potensperforacija.com
Scope of certification	Manufacture of perforated sheet, steel gratings. 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: 17.01.2026.	until: 22.01.2026.	Remote: no	
Audit method: Single audit	No. of employees: 119		No. of employees in scope: 45	Audit duration: 40h	
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: Re-certification	Audit type: Select	Audit type: Select	Audit type: Select	Audit type: Select
Registration no.	TA420233016838				
Scope	<input type="checkbox"/> No changes <input checked="" type="checkbox"/> 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

Audit report

Management systems certification



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					

Audit report

Management systems certification



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)	(Signature)	
(Name)	(Name)	(Name)	(Name)	(Name)	

Audit report

Management systems certification



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 the applicable information security management system standards. The organization has ensured that 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 establish trust between all interested parties, promote a culture of continuous improvement, and reduce the number of threatening incidents. In accordance with established information security procedures and policies, the organization has set its information security objectives and ensured 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 ISMS/IMS requirements, the organization has laid the foundation for continuous improvement and for ensuring information security and data privacy. This process enables identification of areas for improvement, implementation of corrective actions when needed, and adjustment of the information security strategy. With the defined objectives and KPIs (PR-02.01 – IMS Objectives 2026 and PR-02.03 – KPI, dated 05.01.2026), the organization evaluates the performance and effectiveness of its management system and personal data protection.		
Management system performance in relation to statutory / regulatory / contractual requirements	☒	1
Conclusion / Comment: The organization has defined statutory, regulatory, and contractual requirements, as well as policies, plans, and procedures relevant to its purpose and strategic direction. Evidence includes: <ul style="list-style-type: none">• "Poslovnik IMS" (IMS Manual), v5, dated 05.01.2026;• "Kontekst i zainteresovane strane" (Context and Interested Parties), dated 05.01.2025 (+ ISMS 04.01, dated 05.01.2025);• "SWOT analiza" (SWOT Analysis, ISMS 04.02), dated 05.01.2026;• "PR-10 – Zakonski i drugi zahtevi" (Legal and Other Requirements, PR-10, dated 05.01.2026.);• "PR-10.01 – Registar zakonskih i drugih zahteva" (Register of Legal and Other Requirements, PR-10.01, dated 05.01.2026.);• "PR-07.01 – Knjiga evidencije ugovora" (Contract Register, PR-07.01, dated 05.01.2026.). By maintaining these acts and records, the organization ensures systematic compliance and a structured relationship with external issues affecting information security.		

Audit report

Management systems certification



Monitoring of processes



1

Conclusion / Comment: The organization applies performance measurement and analysis activities to provide data and information on the conformity of process characteristics with defined requirements and to demonstrate compliance to interested parties, as well as the smooth functioning of the information security management system. Process monitoring is supported through documented objectives and KPIs and review through internal audits and management review records.

Internal audit and management review



1

Conclusion / Comment: Internal audits are performed according to the documented internal audit procedure and planning is defined through the annual program and audit plan. Evidence includes:

- PR-03.01 – Annual Internal Audit Program, dated 05.01.2026;
- PR-03.02 – Internal Audit Plan, dated 05.01.2026;
- PR-03.03 – Report on Conducted Internal Audit, dated 13.01.2026.

Management reviews are conducted according to procedure PR-02 – Management Review, dated 05.01.2026, and recorded in the latest management review record PR-02.02, dated 14.01.2026, including review of objectives, KPIs, risks/opportunities, and improvement actions.

Upper management responsibility for the stated policies



1

Conclusion / Comment: Top management has taken responsibility for the information security and personal data protection policies and thereby demonstrated commitment to the well-being of employees, clients, and other interested parties. Leadership and commitment are defined through "PR-33 – Liderstvo i posvećenost" (Leadership and Commitment, PR-33, dated 05.01.2026.), and supported by established roles and governance based on "ODLUKA O FORMIRANJU ODBORA ZA ISMS I IMENOVANJU PREDSTAVNIKA RUKOVODSTVA ZA ISMS" (Decision on Establishment of ISMS Committee and Appointment of ISMS Management Representative, dated 01.09.2025.). The General Manager/CEO Mr. Borko Pavlović sets the tone for the organization's culture and values and ensures that policies are aligned with information security objectives and organizational context.

Management system effectiveness



1

Conclusion / Comment: The organization has established and maintained an effective IMS/ISMS framework supported by updated documentation (IMS Manual, policies, procedures) and evidence of planned and performed activities (risk assessment, objectives/KPIs, internal audits, management review). The effectiveness of the system is evaluated through PR-02.03 – KPI and confirmed through the completed internal audit (PR-03.03, dated 12/13.01.2026) and management review (PR-02.02, dated 14.01.2026).

The corrective actions from the previous audit (action list) were reviewed and their effectiveness was verified



1

Conclusion / Comment: No non-conformities were observed during the audit and no corrective actions were initiated.

Audit report

Management systems certification



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: Documented information is managed and kept up to date in line with the requirements of the applicable standards, including ISO/IEC 27001:2022. Control of documented information is ensured through PR-01 – Management of Documented Information and PR-01.01 – Document and Record List (dated 05.01.2026), including distribution records. Changes to legal and other requirements are monitored through PR-10 / PR-10.01 (dated 05.01.2026). Where applicable, the organization considers external changes (e.g., regulatory, contractual, interested parties' needs, climate change impacts) within the context review and planning activities.

Use of the logo and/or any reference to the certification



1

Conclusion / Comment: The organization uses the certification logo and references to certification in accordance with the applicable rules.

Audit report

Management systems certification



Information security specific requirements according to ISO 27001

Locations

Audited

Headquarter: Bakionička 14, 31210 Požega, Serbia



Data center 1: Bakionička 14, 31210 Požega, Serbia



Statement of applicability (SoA) and exclusions

The statement of applicability applies in **version 5** from **05.01.2026**.

The following measures of Annex A and/or Annex B are declared as "not applicable":

- A.8.11 - Data masking
- A.8.14 - Redundancy of information processing facilities
- A.8.25 - Secure development life cycle
- A.8.27 - Secure system architecture and engineering principles
- A.8.28 - Secure coding
- A.8.29 - Security testing in development and acceptance
- A.8.31 - Separation of development, test and production environments

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 and personal data protection policies are appropriately defined and documented (IMS Policy and ISMS Policy, dated 05.01.2026). Top management is committed to implementation of the policies, which comply with organizational context and are communicated within the organization. Objectives for 2026 are defined at process level with prescribed measures, responsibilities, and deadlines (PR-02.01 – IMS Objectives 2026, dated 05.01.2026), as well as the method of evaluating results (PR-02.03 – KPI, dated 05.01.2026). The policies are approved/signed by the CEO/General Manager Mr. Borko Pavlović.

Risk management process

Conclusion / Comment: The organization has an appropriately defined risk management process supported by documented risk management methodology and records. Risks and opportunities are identified and assessed in accordance with PR-06 – Risks and Opportunities and PR-06.02 – Identification and Assessment of Risks and Opportunities (dated 05.01.2026), considering internal/external context and interested parties (Context documents dated 05.01.2025 and SWOT analysis

Audit report

Management systems certification



ISMS 04.02, dated 05.01.2026). The selection of information security controls is justified through the Statement of Applicability (SoA), version 5, dated 05.01.2026, and is aligned with assessed risks and objectives.

Audit report

Management systems certification



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	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Asset Management	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Customers and suppliers	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Access control	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Information security incidents	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Business Continuity	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Compliance	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Human resource security	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Physical security	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Devices and equipment	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
IT operation	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Configuration- and data management	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Backup, Logging, Monitoring	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Network security	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Development	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Audit report

Management systems certification



LIST OF POSITIVE FINDINGS

No.	Description
1.	The organization has demonstrated a high level of commitment to maintaining and improving its IMS/ISMS through timely updates of key documentation (IMS Manual v5, policies, procedures, risk management documents, and objectives for 2026). The integration of risk management, objectives (PR-02.01), and KPIs (PR-02.03) supports effective performance monitoring and continuous improvement.
2.	Internal audit and management review activities were conducted in a structured and systematic manner (PR-03.03 dated 13.01.2026 and PR-02.02 dated 14.01.2026), ensuring that system performance, risks, opportunities, and compliance obligations are regularly evaluated. This demonstrates strong leadership involvement and effective governance of the information security management system.
3.	The Statement of Applicability (SoA), version 5 dated 05.01.2026, has been refined and aligned with the results of the updated risk assessment process. Controls have been clearly justified in relation to identified risks, organizational context, and the needs of interested parties, demonstrating a mature and well-structured approach to information security management.

Audit report



Management systems certification

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

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

Audit report



Management systems certification

5. Recommendation of the audit team

The certification scope is appropriate	Yes	<input checked="" type="checkbox"/>	No	<input type="checkbox"/>
--	-----	-------------------------------------	----	--------------------------

The audit objectives have been fulfilled	Yes	<input checked="" type="checkbox"/>	No	<input type="checkbox"/>
--	-----	-------------------------------------	----	--------------------------

Standard(s)	Audit team suggestion				
ISO 27001:2022	<input type="checkbox"/>	Issue of the certificate	AFTER	<input checked="" type="checkbox"/>	no other action
	<input type="checkbox"/>	Maintenance of certificate		<input type="checkbox"/>	Correction of nonconformities with the submission of documents
	<input checked="" type="checkbox"/>	Renewal of certificate		<input type="checkbox"/>	Correction of nonconformities with the Re-audit
	<input type="checkbox"/>	Withdrawal of certificate			

Place, date:	Požega, 22.01.2026.		
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