qualityaustria
Certification

Organization	**Core Experience d.o.o.,** Croatia/10000/Zagreb/Rim 21C
Auditee representative:	Maksimilijan Žagar
Order number:	246852/A7-24/000938
Audited sites:	Office: Croatia/10000/Zagreb/Florijana Andrašeca 18a

AUDIT-/ASSESSMENT REPORT

Year: 2025

Customer Service Center: A-4020 Linz, Am Winterhafen 1
Phone: +43 732 34 23 22, Fax: +43 732 34 23 23,
www.qualityaustria.com E-Mail: office@qualityaustria.com

AUDIT

Audit/Assessment date:	24.10.2025.	**Reporting date:**	31.10.2025.
Standard(s)/Regulation(s):		**Kind of audit/Assessment:**	
ISO 9001:2015		Surveillance audit	
ISO 27001:2022		Surveillance audit	
Audit objective:		**Start:**	**End:**
Evaluation of conformity		24.10.2025.	24.10.2025.
Documentation of evidence of conformity:		CL_27_01_101e, CL_27_01_187e	

AUDIT TEAM

1. Auditor (Lead):	Igor Stevkovski	Mobil: +389 78475570	E-Mail: igor.stevkovski@cis-cert.com
2. Auditor:	Siniša Tarailo	**Observer:**	-
Audit language:	Croatian	**Translator: (if required)**	-

APPLICATION

Application for issuing of certificate for the following standards:	**Application for continuing certification for the following standards:**
/	ISO 9001:2015, ISO 27001:2022

NONCONFORMITIES

Number of major nonconformities:	0	**Number of minor nonconformities:**	0

NEXT PLANNED AUDIT

☐ CA ☒ SA ☐ RA ☐ FA ☐ other	**Planned audit date:**	10/2026

CA = Certification audit, SA = Surveillance audit, RA = Recertification audit, FA = Follow-up audit

Auditing is based on a sampling process of the available information. The disclaimer of liabilities in point VI of the **quality**austria Terms and Conditions applies.

Customer Service Center: A-4020 Linz, Am Winterhafen 1
Phone: +43 732 34 23 22, Fax: +43 732 34 23 23,
www.qualityaustria.com E-Mail: office@qualityaustria.com

Content:

Customer Service Center: A-4020 Linz, Am Winterhafen 1
Phone: +43 732 34 23 22, Fax: +43 732 34 23 23,
www.qualityaustria.com E-Mail: office@qualityaustria.com

1 General

1.1 Scope of the Management System

Scope of the company is: The activity of business process outsorcing.

Declaration of applicability

Non-applicable standard requirements from ISO 9001:

- List the non-applicable standard requirements

The following declaration of applicability is valid at the time of the audit:

File name, version number, release date

In principle, all actions from Annex A of ISO / IEC 27001:2022 are relevant. Exceptions to this are:

- List the non-applicable standard requirements

Sites covered by the scope

Included sites/locations and subsidiaries:

Sites/locations within the Scope		Most recently audited / audited in this audit (YYYY)
Site 1 / A	Office:Florijana Andrašeca 18a, 10000 Zagreb	2025
Site 2 / B	-	-
Site 3 / C	-	-

System Technology and Application Statistics

For an appropriate audit planning and implementation, the system technology applied, and the organizational application statistics were dealt with. The following table documents the status at the time of the audit.

Customer Service Center: A-4020 Linz, Am Winterhafen 1
Phone: +43 732 34 23 22, Fax: +43 732 34 23 23,
www.qualityaustria.com E-Mail: office@qualityaustria.com

Information Security Relevant Data	
Total number of employees in the company:	41
Total number of employees within the scope of the certificate (employees, freelancers, etc.):	51
Total of locations within the scope of the certificate:	1
Number of ICT workplaces:	51
Number of servers (virtual plus physical):	2 virtual
Number of system administrators:	2
Number of internal software developers:	2
Number of teleworkers/remote access:	49
Number of different security zones:	1
Number of external IT suppliers /service providers:	4
(Cloud services, software, hardware, data center operator):	5
Number of business-critical applications:	4
Maximum tolerated period of disruption in hours (MTPD):	8
Company-critical data in general:	☐ few ☒ some ☐ many
Use of data encryption:	☒ yes ☐ no
e-commerce:	☐ yes ☒ no
e-cash:	☐ yes ☒ no

1.2 Current Situation – Developments since the last audit

There are no significant changes since last audit.

1.3 Audit Objectives as seen by the Organization

The objective of this audit is the determination of conformity with audit criteria and the evaluation of the ability and effectiveness of the management system.

Furthermore, areas for potential improvement of the management system (hints) should be detected.

2 Overall Impression

2.1 Strategic Direction

In the course of the audit, the following strategic objectives, programs or projects were displayed:

- Primary market focus is on Germany, while also expressing ambitions to expand further across the region
- Acquisition of new projects

Customer Service Center: A-4020 Linz, Am Winterhafen 1
Phone: +43 732 34 23 22, Fax: +43 732 34 23 23,
www.qualityaustria.com E-Mail: office@qualityaustria.com

- Expansion of the workforce up to 100 employees
- Integration of automation initiatives
- Change of the model toward greater AI support and less employees

2.2 Assessed Strengths

The Information Security Management System under consideration stands out due to the following features:

- Effective IMS
- Clear strategic orientation
- Systematic approach to managing objectives and risks
- Functional organizational structure
- IMS documentation management

2.3 Opportunities / Potentials

- Improve of interested parties needs and expectations
- Add pre-contract project management to existing processes
- Clarify risk evaluation criteria more clearly
- Present resources more clearly in the objectives
- Improve Approved supplier list
- Clearer definition of threat sources
- Unified IS asset inventory
- More precise rules for handling documents
- Clearer access rights matrix
- Linking legal requirements to practice
- Publishing privacy policy
- Clearer rules for USB usage
- Conducting external vulnerability testing

Customer Service Center: A-4020 Linz, Am Winterhafen 1
Phone: +43 732 34 23 22, Fax: +43 732 34 23 23,
www.qualityaustria.com E-Mail: office@qualityaustria.com

3 Specific Statements on Capability and Effectiveness of the Management System

3.1 Statements on the Management System's Performance

The company remains in a phase of steady growth, expanding both its workforce and presence across new regional markets. This development has introduced new systems, tools, and data flows, which are progressively being integrated into the ISMS. Governance processes and responsibilities remain clearly defined, and management demonstrates ongoing commitment to maintaining and improving information security practices. In the past year, company has signed five new contracts.

The context of the organization is described in the Excel document "Ulaz u Sustav upravljanja_Core_Experience_2025". The identification and review of external and internal issues are explained in the sheet "Kontekst". Both external and internal issues are covered.

External issues:

- Are there legal requirements the company must meet to perform its activities? Impact importance: High
- Who are our main competitors? Impact importance: Medium
- What kind of cultural environment are we operating in? Impact importance: Low

Internal issue: Are our employees satisfied with their jobs?

Assessment methodology: For all questions, answers are defined using SWOT analysis, and the impact importance is rated as neutral, or low, medium, or high.

Interested parties are described in the same Excel document "Ulaz u Sustav upravljanja_Core_Experience_2025", in the sheet "Zainteresirane strane".

The following interested parties have been identified: Customers/clients, partners, suppliers, process owners, competitors, company owners.

Example: Customers/Clients; Needs: Service quality tailored to current needs, availability, expertise, fair price, delivery quality. Expectations: Fair price for high service quality with proper safety level. Requirements: Service quality, deadline compliance, fair pricing. Impact: Critical. Ability to meet expectations: Fully.

Understanding and reviewing the needs and expectations of interested parties is built into the organization's processes and the company continuously adapts to their requirements. There is a documented procedure available: "Customer Support Process" (Proces korisničke podrške), dated 20.07.2024., code KP-1.

Customer Service Center: A-4020 Linz, Am Winterhafen 1
Phone: +43 732 34 23 22, Fax: +43 732 34 23 23,
www.qualityaustria.com E-Mail: office@qualityaustria.com

The scope is defined in the document „Izjava o obuhvatu sustava upravljanja" (Statement of the Management System Scope), dated 03.07.2024.

There have been no changes to the processes. The following processes have been reviewed and documented:

- „Proces korisničke podrške" (Customer Support Process) with focus on client onboarding, document reference KP-1, dated 20.07.2024.
- „Proces upravljanja ljudskim potencijalima" (Human Resources Management Process), document reference KP-02, dated 20.09.2024.

There have been no changes to the Quality and Information Security Policy. The document „Integrirana politika kvalitete i sigurnosti informacija" (Integrated Quality and Information Security Policy), dated 20.09.2024, is available to interested parties in English and Croatian on the organization's website.

Due to the presence of foreign employees, the system documentation is mostly prepared in bilingual format. For all other employees, the policy is available through the COREX SharePoint site.

Roles and responsibilities within the organization are defined through formal appointments and employment contracts. On 16.09.2024, a Decision on the appointment of the Chief Information Officer was made.

Responsibilities are further described in the Responsibility Matrix (RACI matrix), documented from 25.09.2024.

Example: The CEO is responsible for risk management, while the team leader is responsible for their team regarding project implementation.

Strategic and operational risks are defined in the organization Excel document: "QMS_ISMS_Rizici_Core_Experience", last update 09/2025.

There are two separate risk registers:

- Quality Management System (QMS) Risk Register
- Information Security Management System (ISMS) Risk Register

Risk assessment is carried out using the defined methodology:

Likelihood of occurrence: High (3) 71% – 100%, Medium (2), Low (1)

Severity of impact: High (3), Medium (2), Low (1)

Influence of impact: High (3), Medium (2), Low (1)

Risks are ranked by combining these dimensions (likelihood × impact x influence).

Risks are assessed in two phases – first, the inherent risk is defined and evaluated, and then the residual risk is assessed after mitigation measures are implemented.

Example: Risk – Lack of qualified workforce, recorded on 30.09.2025 as an operational risk within the human resources management process. Responsible

Customer Service Center: A-4020 Linz, Am Winterhafen 1
Phone: +43 732 34 23 22, Fax: +43 732 34 23 23,
www.qualityaustria.com E-Mail: office@qualityaustria.com

person: D.M. Type of objective: Operational. Interested parties: All. Inherent risk assessment: 2, 3, 3 (likelihood, impact, influence). Total score: 18.

Risk management strategy: Hiring in regions with surplus workforce, implementation of internal training programs, and employee development. Responsible person for implementing measures: D.M. Residual risk assessment: 2, 1, 1. Total score: 2. Conclusion: The risk has been successfully mitigated, and the measure is considered effective.

Information security risks are reviewed regularly, and updates are recorded within the risk register. No high or critical risks were identified during the reporting period. Management acknowledges that certain risks may remain unmitigated due to resource limitations and accepts them within an agreed tolerance level. This risk-based approach ensures that security decisions are proportionate to the company's context and operational capacity.

Access to systems continues to be managed via Microsoft Azure AD and Entra ID, applying the principle of least privilege. Multi-factor authentication remains in use for all relevant accounts. There is possibility for implementation of advanced technical controls such as conditional access policies and extended Defender for Endpoint, but due to budget limitations these options are not used. Nonetheless, existing baseline protections and Microsoft cloud security features provide a sufficient level of control for current operational needs.

During the audit, an Excel document with goals defined for the periods 2024/2025 and 2025/2026 was reviewed. The goals include both strategic and operational. For each goal, the interested parties, resources, responsible persons, implementation and monitoring methods, monitoring frequency, deadlines, achievement status, and risk of non-achievement are defined.

Example: Goal for the period 2024/2025 (Line 4) refers to achieving revenue in the amount of EUR 500.000. The responsible person is M. Ž., with a deadline set for 30.06.2025. The interested parties are the owners, employees, and the state, and the listed resources include employees, clients, financial resources, and infrastructure. The monitoring method is defined through a business case simulation, with weekly monitoring. The goal has been achieved, and the closing date is 31.08.2025.

Example: Goal in the area of information security for the period 2025/2026 refers to maintaining employee satisfaction at a level of ≥ 80%. The responsible person is P.Ć., and the deadline for goal completion is 31.06.2026. The interested parties are the owners, clients, and employees. Required resources include employees, financial resources, HR tools, and infrastructure. The monitoring method is based on a satisfaction survey and the internal platform CoreX Feedback Corner, with annual monitoring. The risk of not achieving the goal is assessed as medium.

Example: Goal in the area of service level management (SLA) is defined for the period 2025/2026: to ensure an average SLA of ≥ 90%. The responsible person is P.Ć., with a deadline of 31.03.2026. The interested parties are the owners and clients. Resources include employees, infrastructure, IT support,

Customer Service Center: A-4020 Linz, Am Winterhafen 1
Phone: +43 732 34 23 22, Fax: +43 732 34 23 23,
www.qualityaustria.com E-Mail: office@qualityaustria.com

and SLA monitoring tools. Monitoring is conducted through SLA reports, with a monthly frequency. The risk of not achieving the goal is assessed as medium.

Documents are maintained within the centralized document management system, accessible through Microsoft 365. Roles, responsibilities, and approval processes are defined and communicated to all relevant personnel.

The organization predominantly uses cloud-based services provided by reputable and globally recognized vendors. This approach contributes positively to the overall security posture, as the selected providers ensure compliance with industry standards and offer advanced protection mechanisms. Cloud services such as Microsoft 365, SharePoint, and OneDrive are leveraged for secure collaboration, data storage, and backup.

The asset register includes information about hardware, software, people, and information assets. Classification levels are applied according to established policy, defining protection and access requirements. During 2025, development began on a new centralized Employee Database to improve personnel tracking and ensure consistent lifecycle management of employee information.

Information transfer is managed through secure channels such as SharePoint, Teams, and encrypted email. Only authorized users have access to information classified above public level. Employees are instructed to use approved tools for all internal and client-related exchanges. Regular reminders and awareness initiatives reinforce compliance with information handling rules.

Microsoft Teams is widely used as internal communication tool. With addition of Planner this tool could be used for documenting and tracking ISMS-related records, including objectives, operational risks, incidents, nonconformities, and improvement actions.

Core activities can continue under remote or hybrid working arrangements supported by cloud collaboration tools. Backup and recovery measures remain in place via Microsoft 365 services and the infrastructure of contracted partners, ensuring availability and integrity of information.

Within the sales process, daily tasks are managed for clients, depending on the process stage. The process starts with the interest stage – after the client responds to the initial contact, they are entered into the CRM system. In the information exchange stage, the client is validated (fit check). Further communication, as well as tracking of activities and tasks, continues in the CRM (this can also include regular e-mail communication).

The sales process includes five key stages: Showing interest, Validation, Sending an offer, Downselect phase – if the client has launched a tender process (includes sensitive negotiations), Verbal confirmation – information that the job has been won, Contracting, which takes around one month; during

Customer Service Center: A-4020 Linz, Am Winterhafen 1
Phone: +43 732 34 23 22, Fax: +43 732 34 23 23,
www.qualityaustria.com E-Mail: office@qualityaustria.com

this period, project preparation activities begin (such as integration with the client's systems, information security, and other tasks).

Clients in the CRM are categorized as: Won (successfully acquired), Lost (not acquired), Future (potential future clients).

Project documentation may include processes and elements such as: Timeline, Prospecting process, Campaigns, Message Matrix, References.

All activities are tracked chronologically and documented by date within the CRM system.

Example of contractual documentation for the Tibber and CoreX project (MSA & SOW), dated 17.03.2025, was reviewed. The agreement is standardized (a base contract used for all clients), while the project approach differs depending on the scope and type of engagement. The service billing is based on engagement, for example, a full-time employee, and the contract includes defined elements such as required equipment, human resources, materials, and access to the knowledge base.

For the Tibber project, an invoice calculation matrix is used – an example document is "Invoice calculation Tibber 202509." The calculation includes total hours spent on training, productive work, and weekend work. CoreX uses a working hours plan that includes the total monthly and weekly hours, with sick leave considered (especially during the winter period), and is based on weekly and daily planning. The plan is further broken down in detail and includes time for meetings, breaks, and productive work. It is created in line with the client's marketing and sales department activities.

Based on this plan, the client can see detailed analytics about worker engagement in the CRM system – for example, the number of received and answered emails, chats, and similar. The client checks the service delivery based on the invoice matrix received from CoreX. The quality of delivered service is defined by the agreement. The documentation is stored on the SharePoint site coreexperience.sharepoint.

Communication within project teams is managed through internal communication channels. Within the project team, the Team Leader coordinates communication via Microsoft Teams, while at the operational level, the client's communication system or email is used.

In case of changes in requirements (for example, a reduced number of people working on the project), the client communicates this by sharing Excel spreadsheets, through Slack or email. An example of a change: in the case of a new market, the client Tibber sent an email with an Excel file containing the price calculation ("Tibber & CoreX commercial model"), and the change was confirmed by email sent on 25.06.2025 to the person V.K.

After the project is completed, the contract with the client is terminated.

Systems and devices are protected through a combination of built-in OS security features and antivirus software. Network protection includes firewall,

Customer Service Center: A-4020 Linz, Am Winterhafen 1
Phone: +43 732 34 23 22, Fax: +43 732 34 23 23,
www.qualityaustria.com E-Mail: office@qualityaustria.com

device control, and password-protected Wi-Fi separation for internal and guest access. Development and production environments remain segregated, and source code is securely stored and managed via GitHub. Internal testing and code inspection tools such as SonarQube continue to support secure development practices.

The organization maintains a Privacy Policy consistent with GDPR and other relevant data protection requirements. Personal data is processed only for legitimate business purposes and under appropriate contractual and technical safeguards. Data masking and role-based access are applied to limit exposure of sensitive information.

Procurement of equipment, such as laptops, is done through leasing. For remote agents, suppliers provide instructions for setting up the device, a list of required software, and details of what needs to be installed, along with onboarding guidelines on where and to whom the equipment should be sent.

The document "Supplier Classification CoreExperience 2025" contains a list of suppliers and information such as client name, delivered goods or services, evaluation based on criteria including deadline compliance, quality, number of complaints, price, payment method, frequency of price changes, communication, and presence of certified management systems (ISO 9001, ISO 27001). It also includes the date of the last evaluation (30.09.2025) and the planned next review (30.09.2026).

The document also lists the risk level for each supplier and the person responsible for supervision. The total score is based on the sum of evaluation points. The evaluation system includes a recommendation to avoid suppliers marked in red, and if possible, to define an alternative supplier. Supplier risk is categorized as low, medium, or high. Currently, there are no suppliers with high risk. Microsoft is classified as a irreplaceable supplier.

Example of communication with a supplier: email dated 16.10.2025 with the company CRATIS regarding license ordering, sent by M. Ž.

Regarding supplier-owned equipment, each employee signs an equipment handover form when signing the employment contract. The form defines what equipment was received, confirms that the employee will take care of the equipment, and includes a note about the right to request return of the equipment and possible sanctions in case of non-compliance.

Example: Equipment handover form dated 26.06.2025, signed by A. L. and M. Ž. as the director. The document is sent via the Docusign system.

The list of suppliers, can be improved with listing of all the cloud services used, like the CRM system.

Recruitment, onboarding, and offboarding processes remain aligned with HR procedures and include confidentiality clauses within employment contracts. The new Employee Database, once implemented, will further enhance traceability of employee records and compliance with access management requirements. Regular awareness sessions and communication of information security responsibilities are maintained.

The onboarding process is carried out through the Recruitment Client Overview, where the hiring conditions are defined (for example, required

Customer Service Center: A-4020 Linz, Am Winterhafen 1
Phone: +43 732 34 23 22, Fax: +43 732 34 23 23,
www.qualityaustria.com E-Mail: office@qualityaustria.com

language and previous work experience). Based on these conditions, the type of job ad is created and published on platforms such as Moj Posao, LinkedIn, and Facebook. Candidates apply through a link that leads them to the system, and each candidate is then assigned to a specific pool. The candidate is contacted, and an interview is scheduled via Teams, where job requirements are discussed in detail.

The team leader contacts the candidate and conducts the interview in the agreed language. In the next interview, the candidate receives additional information, and the hiring decision is usually made. The candidate is contacted via email.

Example email: Madeleine & Corex_Onboarding documents_23.09.2025. The employment contract was signed on 24.09.2025 by M.H.

For each employee, the HR department creates a personal storage space for documentation, and the new employee is registered in the employee database. The accounting department has access to certain documents. Data is later entered into tools such as Microsoft Planner and Cloud.

Employee documentation is stored at the following SharePoint location: SharePoint > Documents > Human Resources – L0 > Employment Documentation – L0 > Employee Documents Storage.

Each employee attends basic training delivered by the team leader or trainer, which includes key information about internal processes, who to contact, and relevant documentation. The second part of the training is focused on project-specific tasks, especially how to use the system for handling customer inquiries.

The organization provides proof of completed training through document records.
Example document: CoreX_Education – Excel sheet, dated 22.10.2025. Topic: Information Security – Basics and Threats, participant: R.L., trainer: F.L., position: Customer Care Representative.

Example training material: PowerPoint presentation – COREX – GDPR & Personal Data.

Example of offboarding: An email dated 23.10.2025 outlines the employee's last working day, the reason for leaving, and required actions such as returning company property (laptop, keys, ID badges) and deactivating access to systems and accounts effective from 23.10. The email was addressed to the Management group, read by F.G., and the accounting department was informed by D.M.

As a system improvement starting from the April 2025, the organization collects onboarding feedback. An onboarding survey is conducted 30 days after the employee starts and completes training. Data is collected in an Excel document titled Onboarding feedback. Formally defined onboarding process has been introduced.

Customer Service Center: A-4020 Linz, Am Winterhafen 1
Phone: +43 732 34 23 22, Fax: +43 732 34 23 23,
www.qualityaustria.com E-Mail: office@qualityaustria.com

The process of handling nonconforming outputs in the organization is carried out through the improvement program. As part of this process, the person is invited to a meeting, the identified mistakes are explained, and areas for improvement are pointed out. The person is then supported in correcting the issue, and after a certain period, the situation is evaluated and feedback is provided.

During the audit, the Excel document "Ulaz u Sustav upravljanja_Core_Experience_2025," sheet "Nesukladnosti" (Nonconformities), was reviewed.

Example: Nonconformity N-002 from 12.04.2025 – the agent did not complete the identity verification of the user according to the internal process "User Verification." The nonconformity was identified by the internal auditor. Corrective action: An additional discussion was held with the Team Leader regarding the verification rules, and additional information was added to the onboarding materials. Correction: The client was contacted, and the verification was completed afterwards. Responsible person: Team Leader. Completed: 14.04.2025.

During the audit, an example of a client complaint, R-001, received on 12.03.2025, was reviewed. The client submitted a complaint due to a delayed agent response time of 48 hours. The complaint was reported directly by the client. The identified cause was a temporary reduction in the number of available agents. The responsible person for recording the complaint was the Team Leader, while the person responsible for resolving the complaint was the Head of Customer Success. The client was answered on 13.03.2025. In the response, an apology was given, the situation was explained, and the processing of requests was accelerated. The complaint was officially closed on 13.03.2025. As a preventive measure, an automatic alert was introduced in the ticket system to trigger after 24 hours for all unanswered requests.

The organization maintains its commitment to continuous improvement while balancing business growth, available resources, and security priorities.

3.2 Statements regarding Internal Audits and Management Review

The internal audit is planned to be conducted once a year (integrated for both quality and information security).

The internal audit was carried out according to the document "Program audita za 2025. godinu", dated 01.09.2025. The criteria and scope were defined in line with ISO 9001 and ISO 27001 standards. Responsible persons were appointed, including the audit team leader and members of the management. The audited areas included Management, Sales, Customer Support, and Information Security.

The document "Plan audita 2025", dated 09.10.2025, was also reviewed. Type of audit: internal. Criteria: ISO 9001 and ISO 27001. Audit team leader: D.M., team members: M.Ž. and F.G.

Customer Service Center: A-4020 Linz, Am Winterhafen 1
Phone: +43 732 34 23 22, Fax: +43 732 34 23 23,
www.qualityaustria.com E-Mail: office@qualityaustria.com

In the internal audit report no. 01/2025 from 10.10.2025, two opportunities for improvement were identified:

(1) Review the need for a written audit program procedure – consider simplifying the documentation by using only the annual internal audit program form instead of a separate procedure.

(2) Optimize documentation by removing or reducing unnecessarily documented information to improve clarity and document management efficiency.

Internal audit conclusion: The internal audit confirmed that CoreX has an effective and mature integrated management system and shows ongoing improvement and strong readiness for the upcoming surveillance audit.

Management review "Ocjena uprave o sustavu upravljanja – 2025" for both systems was conducted on 15.10.2025. The review covers the period from 10/2024 to 10/2025.

The conclusion of the management review is that the system is effective and appropriate. The review included all relevant input and output data, including the analysis of the achievement level of the defined objectives.

As an example of an objective, the implementation of USB rules was mentioned (use is forbidden except in exceptional cases with encryption and approval, and with proper record keeping). Additionally, an awareness program is planned with the goal of holding at least two thematic training sessions per year.

3.3 Action Taken based on Hints and Recommendations resulting from Previous Audits

All hints and recommendations were taken into consideration.

4 Audit Results / Major and Minor Nonconformities / Further Procedure

According to audit findings, there were neither Major nor Minor NCs detected. Hints for improvements will be given in chapter 5 of this report.

Based on the audit results, the auditors come to following conclusion:

Continuation of a certificate for an implemented and verified Information Security Management System (ISMS) according to ISO 27001:2022 and Quality System management according to ISO 9001:2015 for company:

CORE EXPERIENCE d.o.o.
Rim 21c, 10000 Zagreb, Croatia

Customer Service Center: A-4020 Linz, Am Winterhafen 1
Phone: +43 732 34 23 22, Fax: +43 732 34 23 23,
www.qualityaustria.com E-Mail: office@qualityaustria.com

5 Hints and Recommendations ISO 9001:2015 / ISO 27001:2022

Clause 4 – Context of the Organization

- HIN-01: The organization conducts the review of the needs and expectations of interested parties using the Excel document "Ulaz u Sustav upravljanja_Core_Experience_2025," sheet Interested Parties. It is recommended that, during the review, the requirements of interested parties related to information security are also taken into consideration.

- HIN-2: It is recommended to consider adding the project management process, which covers activities before signing a contract with the client, as one of the main processes in the management system, together with the existing ones.

Clause 5 – Leadership / Leadership and worker participation

- No hints or recommendations

Clause 6: Planning

- HIN-03: The Excel document "QMS_ISMS_Rizici_Core_Experience" is used for risk ranking. It includes the risk register for the Quality Management System (QMS) and the Information Security Management System (ISMS). A risk treatment methodology has been defined. It is recommended to more clearly define and explain the meaning of the listed percentages, for example, the 71% to 100% range for high likelihood.
- HIN-04: In the Statement of applicability - Controls are identified as mitigation actions, but it is recommended to refer to specific control - documented information and not to define control in descriptive way.
- HIN-05: All the identified risks are evaluated as low, or acceptable level. Some risks could remain in higher level, due to the lack of technical controls implemented on the platforms (for ex. In MS 365,no conditional access, no labeling, no DLP policy due to budget limitations) and even with high level management can accept and acknowledge those risks.
- HIN-06 Risks should be identified and during operational events, incidents, or identified opportunities. Those risks can be evidenced and tracked in the task management tools (for ex. MS Teams – Planner).
- HIN-07: The Excel document with goals defined for the periods 2024/2025 and 2025/2026 includes both strategic and operational objectives. A methodology for goal setting and tracking is defined. In the part related to required resources, it is recommended to more clearly show the needed

Customer Service Center: A-4020 Linz, Am Winterhafen 1
Phone: +43 732 34 23 22, Fax: +43 732 34 23 23,
www.qualityaustria.com E-Mail: office@qualityaustria.com

resources, for example by indicating financial amounts, in cases involving investments in infrastructure.

- HIN-08: It is recommended to define for the following objectives, more specific targets and their measurability, like actual number of incidents, testing of BCM plans, etc., all based on risk mitigation decisions.
- HIN-09: MS teams with Planner could be used for evidence, monitoring and measuring the fulfilment of the objectives instead of the current excel file. This will provide more visibility, traceability and evidence of the activites taken to fulfill those objectives.

Clause 7: Support

- No hints or recommendations

Clause 8: Operation

- HIN-10: Iako postoji popis odobrenih dobavljača pod nazivom „Supplier Classification CoreExperience 2025", preporučuje se da se isti nadopuni svim odobrenim dobavljačima kojima se vrši plaćanje, primjerice dobavljačem CRM sustava / Although there is an approved supplier list called "Supplier Classification CoreExperience 2025", it is recommended to update the list to include all approved suppliers who receive payments, for example, the CRM system supplier.

Clause 9: Performance evaluation

- No hints or recommendations

Clause 10: Improvement

- No hints or recommendations

Annex A: Clause 5 – Organizational Controls

- A.5.7 – Threat Intelligence: Threat intelligence policy from 02.07.2024., v.1.0. It is recommended to review threat intelligence policy and to define clear sources for collecting those information
- A.5.9 - Inventory of information and other associated assets: It is recommended to define one list of all IS assets in the company and not to have two separate lists. Also it is needed to identify data and information as

Customer Service Center: A-4020 Linz, Am Winterhafen 1
Phone: +43 732 34 23 22, Fax: +43 732 34 23 23,
www.qualityaustria.com E-Mail: office@qualityaustria.com

IS assets, besides hardware, software and people and to link it with relevant processes and asset owners.

- A.5.12 - Classification of information: It is recommended to define more specific description on rules what can be done with documented information on different levels - e.g. sending attachment in mail and/or encrypted.
- A.5.18 – Access rights: It is recommended to create table with specific access rights with reference to locations which can be seen by each employee, in order to have easier review of access rights
- A.5.22 - Monitoring, review and change management of supplier services: It is recommended to include the CRM system in the list of suppliers.
- A.5.31 - Legal, statutory, regulatory and contractual requirements: It is recommended to refer in the list of legal requirements to specific paragraphs which relates to the company.
- A.5.34. - Privacy and protection of PII : There is new version of the Privacy Policy in the organization. This version should be published on the company's web page.

Annex A: Clause 6 – People Controls

- No hints or recommendations

Annex A: Clause 7 – Physical Controls

- A.7.10 – Storage media: It is recommended to consider more specific rules for usage of USB in the company.

Annex A: Clause 8 – Technological Controls

- A.8.8 - Management of technical vulnerabilities: It is recommended to conduct external pen test.

Distribution list	Enclosures
■ CORE EXPERIENCE d.o.o. ■ **quality**austria Customer Service Center ■ Igor Stevkovski, Siniša Tarailo	Audit plan Action plans (in case of nonconformities)

Sincerely
Quality Austria
Certification GmbH

The commissioned auditor
Igor Stevkovski

Customer Service Center: A-4020 Linz, Am Winterhafen 1
Phone: +43 732 34 23 22, Fax: +43 732 34 23 23,
www.qualityaustria.com E-Mail: office@qualityaustria.com