

AUDIT REPORT



Project number: HU21841/25

Client name:	ConfigCat Kft.
Client address:	1136 Budapest, Tátra u. 5/A
Client's management representative:	Dávid Zoltán
Examined site(s) during the audit:	1136 Budapest, Tátra u. 5/A
Examined temporary locations during the audit ¹ :	-
Audit date:	2026. 05. 07.; 2026. 05. 08.
Lead auditor:	Németh László
Co-auditor(s):	-
Expert(s):	-
Other accompanying persons (eg.: observers, interpreters):	
Audit type:	Első felügyeleti audit/First surveillance audit
Audit method ² :	remote audit
Standard(s):	ISO/IEC 27001:2022 (MSZ ISO/IEC 27001:2023) Information Security Management System

1 The objective of the audit is:

- to define if Client's management system complies with audit criteria
- to evaluate if client is able to ensure compliance with applicable statutory, regulatory and contractual requirements
- to evaluate management system's effectiveness
- to define any area for potential improvement (if applicable)

2 Client scope

Scope of certification:	ConfigCat feature management rendszer tervezése, fejlesztése, telepítése és üzemeltetése Design, development, deployment, and operation of the ConfigCat feature management system
-------------------------	---

¹ A temporary site is established by the organization to perform a specific work or provide a service for a limited period of time and not intended to function as a permanent site (eg construction site, service site).

² If an Information and Communication Technology (ICT) method is applied during the audit, its evaluation is required in section 7.

AUDIT REPORT



Project number: HU21841/25

Changes in the scope of certification:	no changes
Statement of Applicability (date, version):	SoA 2025.05.23.
Not applicable controls and their justification:	A7.1 Physical security perimeter - Company does not have a physical office. Server hosting providers compliant with requirement. A7.2 Physical entry controls - Company does not have a physical office. Server hosting providers compliant with requirement. A7.3 Securing offices, rooms, and facilities - Company does not have a physical office. Server hosting providers compliant with requirement. A7.4 Physical security monitoring - Company does not have a physical office. Server hosting providers compliant with requirement. A7.5 Protecting against physical and environmental threats - Company does not have a physical office. Server hosting providers compliant with requirement. A7.6 Working in secure areas - Company does not have a physical office. Server hosting providers compliant with requirement. A7.11 Supporting utilities - Company does not have a physical office. Server hosting providers compliant with requirement. A7.12 Cabling security - Company does not have a physical office. Server hosting providers compliant with requirement. A7.13 Equipment maintenance - Company does not manage physical assets. Server hosting providers compliant with requirement. A8.20 Network controls - Company does not have any networks it manages. Datacenters are certified to meet these requirements. A8.21 Security of network services - Company does not have a physical office and server hosting is done by certified datacenter that meets these requirements according to contractual agreement. Requirements on networks are included in business continuity plan. A8.22 Segregation in networks - Company does not have any networks it manages. Datacenters are certified to meet these requirements. The justifications are acceptable.

3 Result of the audit

	Yes	Partly	No
The organization has properly adopted and operated its management system in accordance with standard requirements.	☒	☐	☐
The organization presented its ability to provide compliance of a product/service with agreed requirements in accordance with the organisation's policy and objectives.	☒	☐	☐
Scope of the management system is properly determined.	☒	☐	☐
Objective of the audit was achieved during the organization's management system's revision.	☒	☐	☐

Project number: HU21841/25

4 Summary of the audit

Introduction of the organization / Changes in certified scope (audit criteria, headcount, activity, personal changes):	The company has been operating for 8 years, providing service in SaaS form. The staff is 11 people. All employees continue to work from home. They only use cloud-based technology, but they also use their own devices. The migration to AWS has been completed. There was no change in headcount, but there were personnel changes. AI has been implemented, and its governance is currently being established. Development of the KPI system has begun. The incident management process has been improved. Headquarters: 1136 Budapest Tátra utca 5/A – provides only headquarters service.
Evaluation of corrective actions for previous year's nonconformities:	There were no nonconformity.
Unexamined activities and standard requirements during this audit:	On the first surveillance audit according to the Audit program the unexamined standard requirements: 4.4., 5.3., 7.2., 7.3., A5.1-5.8., A5.19.5.23, A5.24-5.30., A6., A8.25-8.34.
Use of CERTOP certification logo:	The organization uses the Certop logo on the Homepage. The Certificate can be downloaded from the homepage: https://configcat.com/iso/
Strengths of the system:	Strategic thinking, SWOT, management commitment Cloud based information management system (GDrive GITHUB, Trello) Security week in every two month. Monitoring – public feedback to customers. Documentation system (short policies but a lot of them).
Possibilities for development:	It is advisable to align information security objectives with those defined in the Mission and with the KPIs. Currently, data is not being tagged—the risk associated with this should be assessed in the risk analysis. It is advisable to back up data stored on Google Drive as well. The risk associated with the lack of backups should be assessed in the risk analysis.

5 Recorded Nonconformities³

Number	Description of nonconformities	Standard requirement	Category ⁴
1	Dániel Major was granted access to the company's ConfigCat on April 24, 2026, but there is no record of a request or authorization at audit@configcat.com	A.5.18	minor
-	-	-	-

³ Each nonconformities have to be recorded in a new row.

⁴ Major nonconformity – submission of proving documents of the introduced corrective action is mandatory

Minor nonconformities – the supporting documents for the corrective action must be presented at the next audit.

Project number: HU21841/25

6 Operation of the system/Findings of the audit⁵

Evaluation of compliance:	Yes	Partly	No
Context of the organization The organization has determined and monitored external and internal issues that are relevant to its purpose and strategic direction, the requirement of interested parties that are relevant to the information security management system, the boundaries and applicability of MS, documented its processes and made it available for the interested parties.	☒	☐	☐
Comment on the standard requirement: The organization maintains a clear and consistently updated understanding of its internal and external context, supported by the 2025 SWOT analysis and the integrated Mission documentation, which now includes linked historical versions. Stakeholder expectations remain well-defined and aligned with updated MAR risks, and the ISMS scope continues to be appropriate and justified, particularly regarding non-applicable physical controls. The ISMS is maintained effectively. Opportunities for improvement relate to strengthening the integration between the Mission, KPIs, and information security objectives.			
Leadership Leadership and commitment are ensured regarding the operation and development of information security management system. The policy complies with the strategic direction, the appropriate organizational roles, responsibilities and authorities are determined.	☒	☐	☐
Comment on the standard requirement: Management commitment to the ISMS remains clearly demonstrated through the maintained Information Security Policy (2026.04.02), the regular management review (2025.04.08), and the continued provision of resources and strategic direction. The appointment of Dániel Tóth as ISMS Officer remains effective, and leadership consistently supports the integration of ISMS requirements into organizational processes.			
Planning The management system is planned, the risks and opportunities related to the business activities are defined and evaluated, the information security risk assessment process is applied and documented, its goals are defined and the changes are managed in a planned manner.	☒	☐	☐

⁵ The objective evidences reviewed at the audit to support compliance or non-compliance are detailed in the Audit Note.

AUDIT REPORT



Project number: HU21841/25

Comment on the standard requirement:

Risk assessment and treatment continue to be effectively regulated through the updated Risk Management Plan (2026.04.23) and documented in the Risk Management.xlsx file, applying the established likelihood × impact methodology and the defined risk thresholds. The risk treatment plan remains integrated into Trello-based workflows and is approved during management review. Information security objectives are documented and monitored; however, an improvement opportunity was identified to better align these objectives with the Mission and KPIs. Additional recommendations include assessing risks related to untagged data and the lack of Google Drive backups. Overall, planning processes remain structured, consistent, and aligned with the ISMS requirements.

	Yes	Partly	No
Support The necessary resources needed for the establishment, implementation, maintenance and improvement of the management system are available. The competence and awareness of the staff is proven. The organization has determined the need for internal and external communication relevant to the information security management system. Documented information required by the management system and the organization is available.	☒	☐	☐

Comment on the standard requirement:

The organization maintains adequate resources for the ISMS, supported by cloud-based infrastructure and a stable staffing level. Communication processes remain effective through structured Slack channels and the bi-monthly Security Week, ensuring regular information flow. Documentation control is well-managed through GitHub/Wiki with pull-request-based approval and proper versioning, and external compliance documentation is collected and maintained. An opportunity for improvement remains in assessing risks related to missing Google Drive backups, which should be incorporated into the documentation and risk management processes.

	Yes	Partly	No
Operation The organization has planned, implemented and controlled the processes needed to meet the requirements and achieve the goals of the management system. Documented information is available. Control of externally provided processes, products and services is appropriate and well documented. (if applicable) Control of nonconforming outputs is documented and appropriate.	☒	☐	☐
The information security risk assessment has been performed and the organization has implemented the information security risk treatment plan. Documented information is available.	☒	☐	☐

Comment on the standard requirement:

Operational ISMS processes remain well-regulated through the organization's policies stored in GitHub/Wiki, with documented change management and clear version control. Risk assessment and treatment activities are consistently executed and recorded in the Risk Management.xlsx file, with treatment actions tracked through Trello tickets and approved during management review. Evidence confirms that planned processes are followed, changes are controlled, and outsourced activities are properly identified and overseen. Overall, operational control of the ISMS is effective and aligned with the standard's requirements.

AUDIT REPORT



Project number: HU21841/25

	Yes	Partly	No
Performance evaluation The organization regularly evaluate the effectiveness and performance of the management system. Monitoring, measurment and analyzing methods are determined; planning and implementing of internal audits and management review are effective, verified and documented.	☒	☐	☐

Comment on the standard requirement:

Performance evaluation processes remain effective, supported by the Security Objectives Measurement and Review Plan (2026.04.27) and continuous monitoring through tools such as Site24x7, with availability data publicly accessible at status.configcat.com. Internal audits were conducted in April 2026 with appropriate involvement of new team members, and the management review (2025.06.08) continues to evaluate ISMS effectiveness and drive improvements. An opportunity for improvement remains in expanding KPI coverage—particularly linking objectives more closely to Mission and access-review-related metrics—to further strengthen performance measurement.

	Yes	Partly	No
Improvement Improvement of the management system is verified, the organization determines and implements the selected opportunities for improvement, handling of nonconformities and corrective actions are efficient and properly documented.	☒	☐	☐

Comment on the standard requirement:

Continuous improvement of the ISMS remains well-supported through the organization's strategic planning activities, SWOT analysis, and regular management reviews, which together provide a structured basis for identifying and prioritizing enhancements. Internal audit findings from 2026 were handled appropriately, and corrective actions are tracked and implemented through Trello.

Annex A – Information security controls

	Examined during current audit	Conformity assessment	
		Yes	No
A5.1-5.8 ISMS roles/responsibilities	☐	☐	☐

Comments on the controls:

	Examined during current audit	Conformity assessment	
		Yes	No
A5.9-5.14 Assets	☒	☒	☐

Comments on the controls:

Inventory of assets policy, Access control policy controls. Currently, data is not being tagged—the risk associated with this should be assessed in the risk analysis.

AUDIT REPORT



Project number: HU21841/25

	Examined during current audit	Conformity assessment	
		Yes	No
A5.15-5.18 Access control	☒	☒	☒

Comments on the controls:

Regulated by the Access Control Policy. Password rules in Cyber Hygiene policy. There were a minor nonconformity: Dániel Major was granted access to the company's ConfigCat on April 24, 2026, but there is no record of a request or authorization at audit@confogcat.com-on

	Examined during current audit	Conformity assessment	
		Yes	No
A5.19-5.23 Supplier relationships	☐	☐	☐

Comments on the controls:

	Examined during current audit	Conformity assessment	
		Yes	No
A5.24-5.30 Incident management	☐	☐	☐

Comments on the controls:

	Examined during current audit	Conformity assessment	
		Yes	No
A5.31-5.37 Legal requirements, documentation	☒	☒	☐

Comments on the controls:

Compliance regulation. Vulnerability assessments: February 25, 2025 – Scheduled for 2026. Documented operational procedures: Collected on GITHUB/WKI, e.g., Operation Policies

	Examined during current audit	Conformity assessment	
		Yes	No
A6.1-6.8 HR processes	☐	☐	☐

Comments on the controls:

AUDIT REPORT



Project number: HU21841/25

	Examined during current audit	Conformity assessment	
		Yes	No
A7.1-7.14 Physical security, controls	☒	☒	☐

Comments on the controls:

A7.1 , A7.2, A7.3, A7.4, A7.5, A7.6, A7.11, A7.12, A7.13 controls aren't applicable, because the company does not manage physical assets. Server hosting providers compliant with requirement. Remote working is common.

	Examined during current audit	Conformity assessment	
		Yes	No
A8.1-8.19 IT	☒	☒	☐

Comments on the controls:

Technological controls remain effectively implemented and supported by well-defined operational policies, including Change management, Virtual Private Servers, Backup Plan, Logging and Monitoring Policy, and cloud-based infrastructure practices. Monitoring and security tooling (e.g., Sentry.io, Intruder.io, Grafana, Site24x7) continue to provide structured oversight of system performance and security events, while strong authentication practices such as GitHub 2-factor authentication are consistently applied. An improvement opportunity was identified regarding the need to assess risks related to missing Google Drive backups, which should be incorporated into the backup strategy and risk analysis.

	Examined during current audit	Conformity assessment	
		Yes	No
A8.20-8.24 Network security	☒	☒	☐

Comments on the controls:

A8.20, A8.2, A8.22 controls aren't applicable, because the company does not have any networks it manages. Datacenters are certified to meet these requirements. Web filtering: Browser Settings for Safe Browsing.

	Examined during current audit	Conformity assessment	
		Yes	No
A8.25-8.34 Development	☐	☐	☐

Comments on the controls:

7 Evaluation of the Information and Communication Technology (ICT) Method (if applicable)

ICT technology used during the audit:	google meet			
Areas affected by the use of ICT (e.g. sites, processes, standard clauses, interviews):	all, because it was a full remote audit.			
		Yes	Partly	No

AUDIT REPORT



Project number: HU21841/25

The ICT method used during the audit was appropriate.	☒	☐	☐
Confidentiality, information security and data protection were ensured.	☒	☐	☐
Reviewing of the planned processes, activities, sites, and the availability of the planned employees were ensured. The remote assessment did not affect the effectiveness of the audit.	☒	☐	☐
Required audit time was fulfilled.	☒	☐	☐

Any identified risks, other comments regarding the nature of the remote audit:

no

8 Comments

Identified, unresolved issues during the audit (if applicable):	-
Deviation from the audit plan and its reasons (if applicable):	-

The suggestion of the audit team concerning the issue / maintenance of the Certificate is included in the Certificate of performance that was filled out during the closing meeting of the audit.

We kindly ask to **report any changes concerning the certified management system**, in accordance with the General Terms and Conditions at our website (<https://hu.certop.com>).

The audit was based on a sampling procedure.

The Audit report contains confidential information.

9 Planned date of the following year's audit

Execution of the annual surveillance procedures in time is the condition of the certificate to stay in force.

Due surveillance audits have to be implemented within 12 to 24 months after the recertification audit's/initial audit's certification decision, recertification audit and the related certification decision has to be conducted before the expiry of a validity deed!

The following audit's planned date: 2027. 05. 30.

Date: 2026. 05. 08.

Lead auditor