

BLUEPRINT

Security Audits

Do you know how secure you really are?

Security policies and technical controls tend to grow over time and often look fine on paper. An audit independently checks whether they are actually followed, whether they still match today's threats, and whether they meet regulatory requirements such as the NIS2 Directive, the Czech Cybersecurity Act or ISO/IEC 27001.

What we review

- security policies, procedures and how they work in practice
- access and privilege management, identities and passwords
- configuration of key systems – network, firewalls, servers, Active Directory and cloud
- backup, recovery and resilience to outages
- compliance with NIS2, the Cybersecurity Act and ISO/IEC 27001 (gap analysis)

How we work

- 1 We agree on the scope and objectives together.
- 2 We review documentation, talk to the people responsible and verify technical settings.
- 3 We assess every finding by the risk it poses to your organisation.
- 4 We present the results and recommend next steps.

What you get

- a clear report for both management and the technical team
- findings ranked by severity
- a prioritised remediation plan with concrete recommendations
- a solid basis for security investment decisions

AI

AI in practice AI helps us work through extensive documentation and configurations faster; conclusions and recommendations come from our auditors.

Who it's for companies and institutions that want to know where they really stand, are preparing for certification or need to meet regulatory requirements.

Want to know where your weak spots are?

info@anomalis.cz · +420 603 106 456 (24/7 for urgent cases) · www.anomalisit.cz

Anomalis IT s.r.o. · Korunní 2569/108, 101 00 Prague 10, Czech Republic · Company ID 09717404 · VAT ID CZ09717404