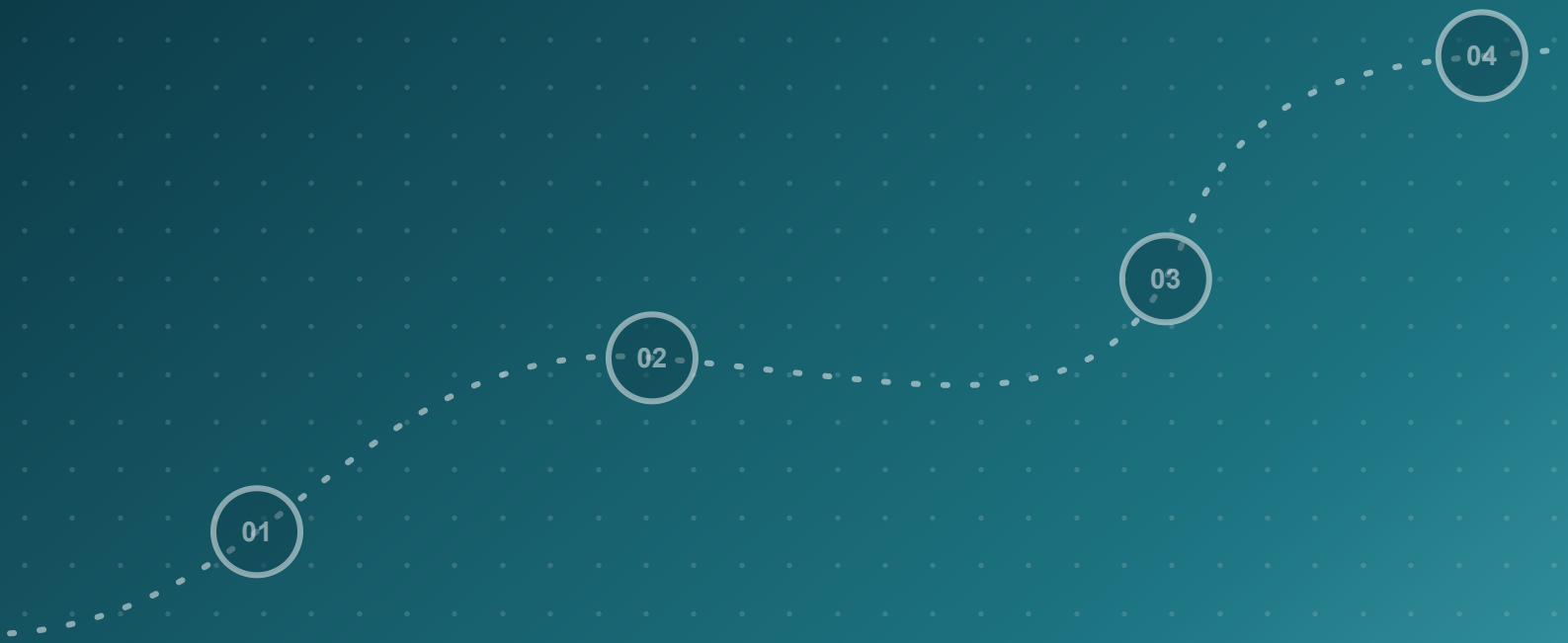
Thermic GRC
SEITENSTETTENGASSE 5/37, 1010 WIEN

GOVERNANCE · RISK · COMPLIANCE

Service Catalogue



EDITION
8 November 2026

VERSION
1.0

CLASSIFICATION
PUBLIC

COMPANY ID
ATU83687805

About Thermic GRC

Who We Are

Thermic GRC is an independent Information Security Governance, Risk and Compliance (GRC) and Virtual CISO (vCISO) advisory practice based in Vienna, to help European organisations navigate an increasingly complex regulatory landscape.

I founded Thermic GRC because I saw firsthand the challenges organisations face when struggling to translate complex European regulations into pragmatic, risk-based business decisions.



CISSP CGRC* CIPM CIPP/E CIS LI

About Me

My information security journey is deeply rooted in a European academic foundation, including a BSc and an MSc in Cyber Security and Management, alongside a minor in European Policing.

I've spent my career navigating the diverse information security landscapes of Western and Central Europe, growing from a GRC security consultant into a Chief Information Security Officer for a global enterprise, where I led multinational implementations of ISO 27001, NIS2, and the Cyber Resilience Act.

Mission Statement

Working towards a stronger, more secure Europe by supporting organisations implementing integrated, risk-based operational security governance frameworks and bridging the compliance gap.

LET'S TALK

Book a virtual coffee

Let's connect for a quick chat to talk about what's on your desk.

Schedule a meeting



SERVICES

Our services

4 modular services. Start where you stand

The Roadmap of Services

Whether you need a clear baseline of your compliance status, continuous operational governance, strategic management-level leadership, or targeted expertise for a specific project, our modular services meet you at the right point on the road.



FIGURE 1: SERVICES OVERVIEW

SERVICE 01 · INITIAL ASSESSMENT

Assessments & Audits

NIS2, CRA, GDPR, EU AI Act, TISAX, ISO/IEC 27001

01

Description

You answer a highly detailed and structured compliance questionnaire. We review the answers, flag inconsistencies and red flags, and translate the result into an executive report with identified gaps, risks, and a prioritised 90-day action plan with owners and clear next steps.

Best For

Organisations working towards a certification project or compliance initiative.

Format

- Questionnaire
- Evidence review (Tier 2)
- Report

Timeline

- Tier 1: 7 w. days
- Tier 2: 14 w. days

Output

- Report
- 90-day action plan
- Guiding workshops

How it works

01 Questionnaire
You answer a set of compliance questions.

02 Assessment
Review of your answers and gaps.

+ Evidence TIER 2
Deep-dive into submitted evidence.

03 Report
Executive report with risk ratings.

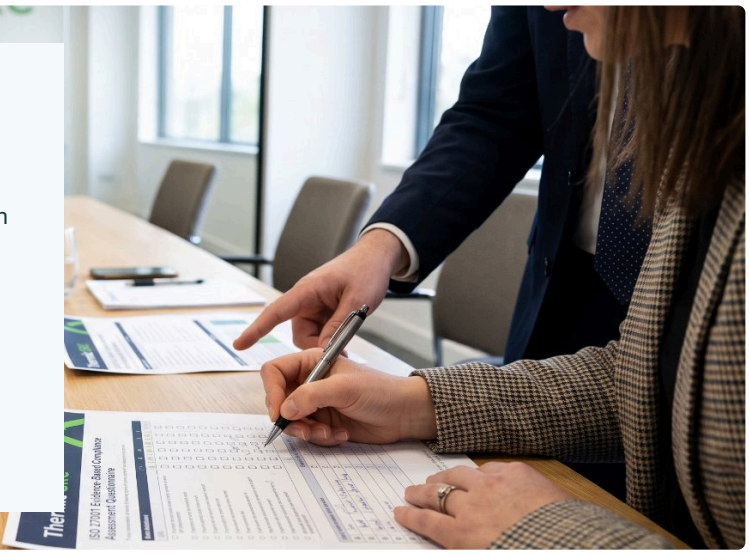
04 90-day plan
Prioritised 90-day action plan.

05 Workshops
Guiding workshops to set you off right.

FORMATS

Tier 1: A diagnostic gap assessment questionnaire with a clear report, a 90-day action plan, and a 90-minute strategy workshop.

Tier 2: Everything in Tier 1, plus an audit-grade review of your policies and configurations. The single session is replaced by four 60-minute workshops to guide your 90-day action plan.



Check out what a report looks like!

An example report in Appendix 1.

See example report

SERVICE 02 · OPERATION

Core GRC Advisory

The security governance engine

02

Description

The service fulfils a dedicated security governance role to develop, maintain, and improve your information security management system, including drafting auditable policies, maintaining procedures and risk registers, preparing management reviews, running internal audits, providing security awareness training, and supporting your unique operational needs.

Best For

Organisations in need of continuous support, oversight, or operation of their ISMS or GRC programme.

Format

- ✓ Foundation (8h+/month)
- ✓ Active (16h+/month)
- ✓ Intensive (24h+/month)

Output

- ✓ Policies
- ✓ Procedures
- ✓ Training
- ✓ Ad-hoc requirements

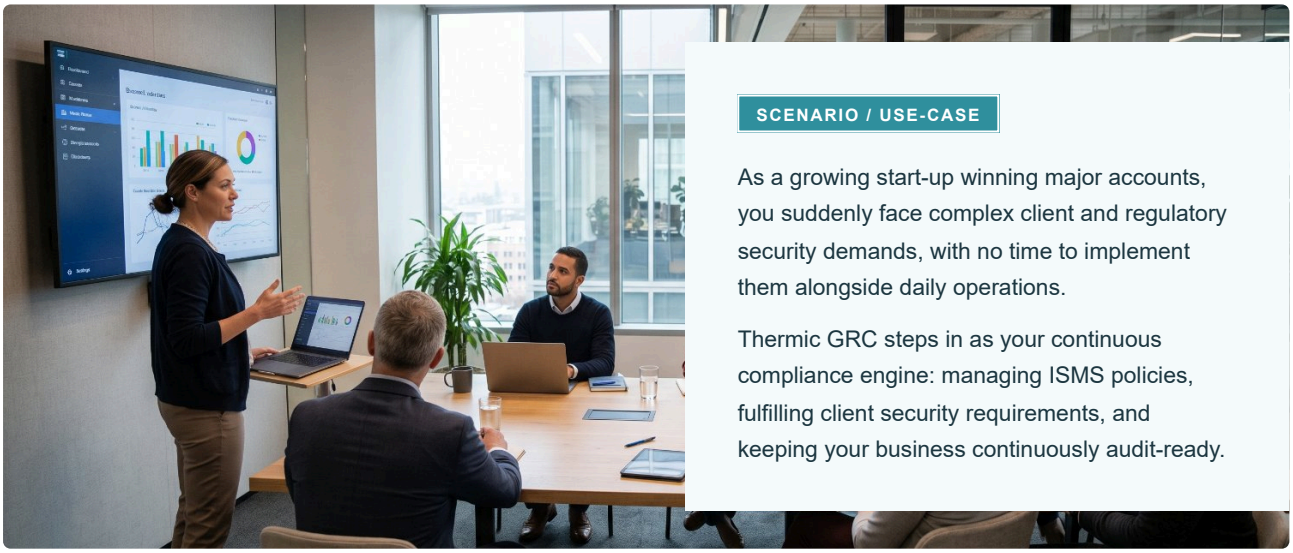
How it works

01 Set up
Scope, policies and ISMS baseline.

02 Operate
Monthly governance, risk management.

03 Assure
Internal audits and compliance reviews.

04 Improve
Continuous improvement, evidence tracking.



SCENARIO / USE-CASE

As a growing start-up winning major accounts, you suddenly face complex client and regulatory security demands, with no time to implement them alongside daily operations.

Thermic GRC steps in as your continuous compliance engine: managing ISMS policies, fulfilling client security requirements, and keeping your business continuously audit-ready.

Facing a security initiative?

Book a virtual coffee, no strings attached.

Speak to an expert

SERVICE 03 · STRATEGY

Enterprise vCISO

Management-level security leadership

03

Description

The service provides a designated information security officer who translates technical risk into business metrics, represents you in external audits and customer reviews, and can take over incident management activities, including regulatory reporting (CRA/NIS2).

Best For

Scale-ups and mid-market companies selling to regulated or enterprise customers, and organisations that need a named security officer.

Format

- ✓ Strategic vCISO 16h+/month
- ✓ Full vCISO 24h+/month

Output

- ✓ Board KPI/KRI reporting
- ✓ Customer assurance
- ✓ Incident management
- ✓ Supply chain security

How it works

01 Kick-off
Goals, stakeholders, risk appetite.

02 Baseline
Current posture and priorities.

03 Run
Monthly leadership cycle.

04 Report
Board, customer, and regulator ready.

SCENARIO / USE-CASE

You are an industrial equipment manufacturer and have identified that your European entities fall within the scope of NIS2, exposing your managing directors to personal liability.

We step in as your vCISO: training top management, delivering GRC KRIs/KPIs, managing incidents, and acting as the official security representative for your organisation.



In need of a vCISO?

Book a virtual coffee, no strings attached.

Speak to a CISO

SERVICE 04 · AT ANY POINT ON THE ROAD

Specialised & On-Demand

Expert help where you need it.

04

Description

Not every need fits a pre-defined service. This on-demand advisory covers such moments with fixed prices and transparent hourly rates. Whatever project, initiative, or urgent challenge you face, this service covers them, with an approach tailored to your needs.

Best For

Any organisation that needs senior GRC expertise for a defined moment or deliverable.

Format

- ✓ Flexible approach based on what best suits your needs

Output

- ✓ Full-day workshops
- ✓ Customer audits
- ✓ Incident management
- ✓ Standalone advisory



SCENARIO / USE-CASE

One of your critical suppliers suffers a breach, leaving your organisation exposed to disruption and regulatory scrutiny. You must verify their controls and conduct an on-site audit before restoring trust.

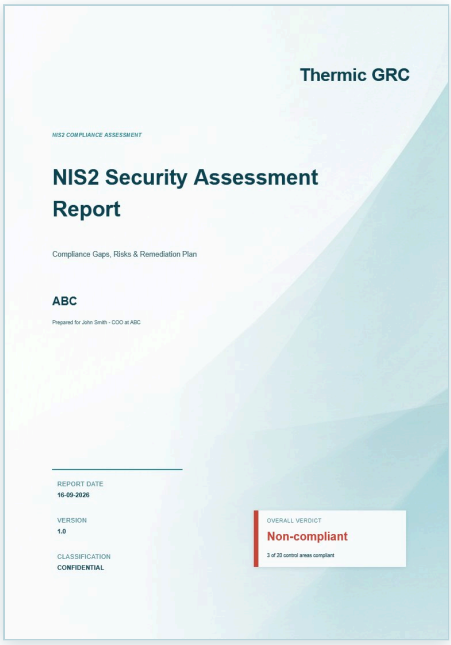
We step in to lead the end-to-end audit on your behalf, examining relevant evidence and delivering an independent assessment.

How can we help?

Book a virtual coffee, no strings attached.

Let's talk

Appendix 1


Thermic GRC

NIS2 COMPLIANCE ASSESSMENT

NIS2 Security Assessment Report

Compliance Gaps, Risks & Remediation Plan

ABC

Prepared for John Smith - COO at ABC

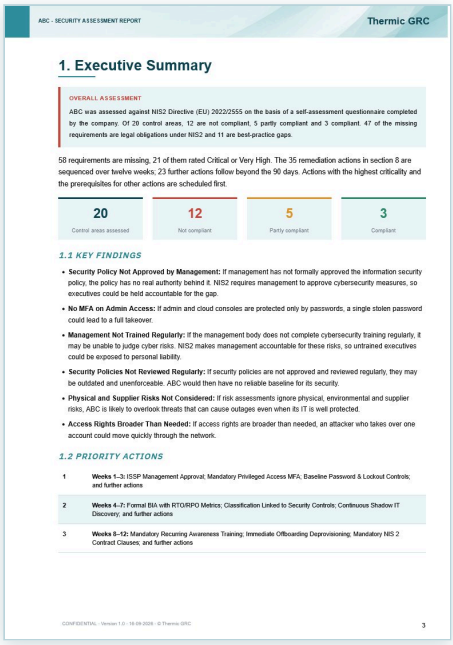
REPORT DATE
16-09-2026

VERSION
1.0

CLASSIFICATION
CONFIDENTIAL

OVERALL VERDICT
Non-compliant
3 of 20 control areas compliant

Cover page: what the report covers


ABC - SECURITY ASSESSMENT REPORT Thermic GRC

1. Executive Summary

OVERALL ASSESSMENT

ABC was assessed against NIS2 Directive (EU) 2022/2555 on the basis of a self-assessment questionnaire completed by the company. Of 20 control areas, 12 are not compliant, 5 partly compliant and 3 compliant. 47 of the missing requirements are legal obligations under NIS2 and 11 are best-practice gaps.

58 requirements are missing, 21 of them rated Critical or Very High. The 35 remediation actions in section 8 are sequenced over twelve weeks; 23 further actions follow beyond the 90 days. Actions with the highest criticality and the prerequisites for other actions are scheduled first.

20	12	5	3
Control areas assessed	Not compliant	Partly compliant	Compliant

1.1 KEY FINDINGS

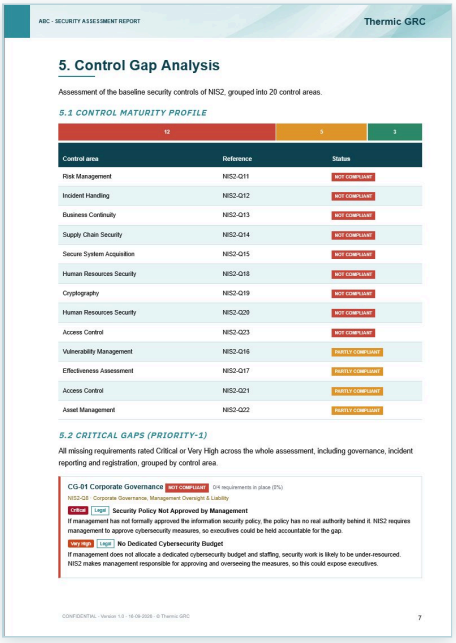
- **Security Policy Not Approved by Management:** If management has not formally approved the information security policy, the policy has no real authority behind it. NIS2 requires management to approve cybersecurity measures, so executives could be held accountable for the gap.
- **No MFA on Admin Access:** If admin and cloud consoles are protected only by passwords, a single stolen password could lead to a full takeover.
- **Management Not Trained Regularly:** If the management body does not complete cybersecurity training regularly, it may be unable to judge cyber risks. NIS2 makes management accountable for these risks, so untrained executives could be exposed to personal liability.
- **Security Policies Not Reviewed Regularly:** If security policies are not approved and reviewed regularly, they may be outdated and unenforceable. ABC would then have no reliable baseline for its security.
- **Physical and Supplier Risks Not Considered:** If risk assessments ignore physical, environmental and supplier risks, ABC is likely to overlook threats that can cause outages even when its IT is well protected.
- **Access Rights Broader Than Needed:** If access rights are broader than needed, an attacker who takes over one account could move quickly through the network.

1.2 PRIORITY ACTIONS

1	**Weeks 1–3:** ISSP Management Approval; Mandatory Privileged Access MFA; Baseline Password & Lockout Controls; and further actions
2	**Weeks 4–7:** Formal BIA with RTO/RPO Metrics; Classification Linked to Security Controls; Continuous Shadow IT Discovery; and further actions
3	**Weeks 8–12:** Mandatory Recurring Awareness Training; Immediate Offboarding Deprovisioning; Mandatory NIS 2 Contract Clauses; and further actions

CONFIDENTIAL - Version 1.0 - 16-09-2026 - © Thermic GRC 3

Executive summary: ratings for every domain


ABC - SECURITY ASSESSMENT REPORT Thermic GRC

5. Control Gap Analysis

Assessment of the baseline security controls of NIS2, grouped into 20 control areas.

5.1 CONTROL MATURITY PROFILE

Control area	Reference	Status
Risk Management	NIS2-Q11	NOT COMPLIANT
Incident Handling	NIS2-Q12	NOT COMPLIANT
Business Continuity	NIS2-Q13	NOT COMPLIANT
Supply Chain Security	NIS2-Q14	NOT COMPLIANT
Secure System Acquisition	NIS2-Q15	NOT COMPLIANT
Human Resources Security	NIS2-Q18	NOT COMPLIANT
Cryptography	NIS2-Q19	NOT COMPLIANT
Human Resources Security	NIS2-Q20	NOT COMPLIANT
Access Control	NIS2-Q23	NOT COMPLIANT
Vulnerability Management	NIS2-Q16	PARTLY COMPLIANT
Effectiveness Assessment	NIS2-Q17	PARTLY COMPLIANT
Access Control	NIS2-Q21	PARTLY COMPLIANT
Asset Management	NIS2-Q22	PARTLY COMPLIANT

5.2 CRITICAL GAPS (PRIORITY-1)

All missing requirements rated Critical or Very High across the whole assessment, including governance, incident reporting and registration, grouped by control area.

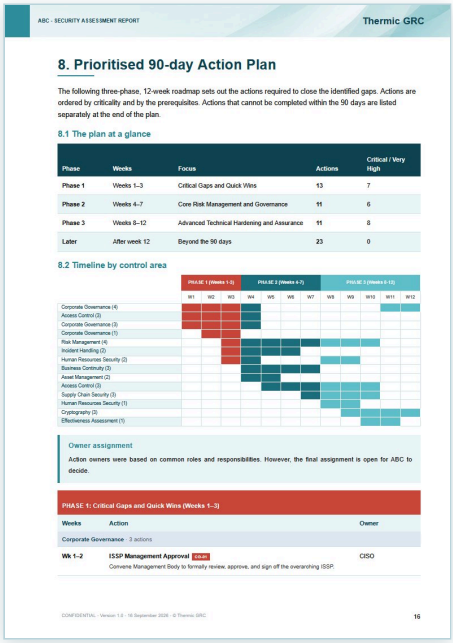
CG-01 Corporate Governance NOT COMPLIANT 0/4 requirements in place (0%)
NIS2-Q8 · Corporate Governance, Management Oversight & Liability

Critical Legal **Security Policy Not Approved by Management**
If management has not formally approved the information security policy, the policy has no real authority behind it. NIS2 requires management to approve cybersecurity measures, so executives could be held accountable for the gap.

Very High Legal **No Dedicated Cybersecurity Budget**
If management does not allocate a dedicated cybersecurity budget and staffing, security work is likely to be under-resourced. NIS2 makes management responsible for approving and overseeing the measures, so this could expose executives.

CONFIDENTIAL - Version 1.0 - 16-09-2026 - © Thermic GRC 7

Findings: critical gaps ranked by risk


ABC - SECURITY ASSESSMENT REPORT Thermic GRC

8. Prioritised 90-day Action Plan

The following three-phase, 12-week roadmap sets out the actions required to close the identified gaps. Actions are ordered by criticality and by the prerequisites. Actions that cannot be completed within the 90 days are listed separately at the end of the plan.

8.1 The plan at a glance

Phase	Weeks	Focus	Actions	Critical / Very High
Phase 1	Weeks 1–3	Critical Gaps and Quick Wins	13	7
Phase 2	Weeks 4–7	Core Risk Management and Governance	11	6
Phase 3	Weeks 8–12	Advanced Technical Hardening and Assurance	11	8
Later	After week 12	Beyond the 90 days	23	0

8.2 Timeline by control area

Owner assignment
Action owners were based on common roles and responsibilities. However, the final assignment is open for ABC to decide.

PHASE 1: Critical Gaps and Quick Wins (Weeks 1–3)

Weeks	Action	Owner
Corporate Governance · 3 actions		
Wk 1–2	**ISSP Management Approval** Critical Convene Management Body to formally review, approve, and sign off the overarching ISSP.	CISO

CONFIDENTIAL - Version 1.0 - 16 September 2026 - © Thermic GRC 16

90-day action plan: owners and next steps

Looks interesting? Let's talk!

Book a virtual coffee, no strings attached.

Schedule a meeting