VENZO_

a valantic company

Security Screening

FiktivBank A/S

Period: 01-01-2026 – 20-01-2026

Company info

Company:
FiktivBank A/S

Address:
FiktivBank Street 123

CVR:
Number

Contact Person:
Name

Prepared by

Security Consultant:
Peter Jensen

Company:
VENZO A/S

Address:
Hejrevej 34B, 2400 Copenhagen NV

Phone: 33110085

E-mail: pxj@venzo.com

About the screening

The report describes the current threat landscape, the relevant regulatory environment, your setup and risk profile. It covers applicable regulatory requirements, key internal change drivers, and external trends in threats and technology that influence the risk landscape.

The screening scope is defined through a set of selected scenarios and focus areas designed to address the most relevant risk drivers, regulatory expectations, and governance considerations for the organization.

The report provides an assessment of maturity across defined security domains and regulatory focus areas, highlighting key observations, identified gaps, and associated risks, supported by targeted recommendations.

The report concludes with agreed decisions, follow-up actions, and potential next steps intended to support prioritization, clarify ownership, and inform further assessment or improvement activities.

Dimensions

The screening and assessment are structured around three core dimensions that together provide a comprehensive view of regulatory compliance, security risk, and emerging technology governance. The dimensions define the lenses through which controls, governance, and evidence are assessed throughout the screening.

REG

Regulatory

We anchor the screening to the frameworks you are required to meet and calibrate criteria and evidence accordingly. In practice, that most often means DORA, NIS2, ISO/IEC 27001, GDPR, SOC 2, and PCI DSS.

Examples:

- Bank subject to DORA: we align the screening to the selected pillars to check readiness and evidence gaps for supervisory review.

- NIS2 essential entity: we align to the directive’s security objectives to confirm governance, incident readiness, and supplier oversight are documented and defensible.

CYB

Cyber Security

We base the screening on the cyber risks that matter most to your organization. Those risks shape what we examine – identity and privileged access, endpoint and email protections, segmentation, data safeguards, monitoring quality, and whether recovery can be proved in practice. Everything is calibrated to your tech stack and real exposure.

Examples:

- Microsoft-centric, focused on ransomware + identity: we align the screening to Conditional Access, enforced PAM/JIT, Defender EDR coverage, and documented restore for critical services.

- Cloud-native, focused on data-exfiltration + key compromise: we align to CSPM guardrails, least-privilege IAM/MFA, KMS hygiene, egress controls, and tuned detections.

AI

Artificial Intelligence

We base the screening on the AI and automation use cases you are actually introducing - whether that is productivity tools, internal decision support, customer-facing flows, or early agent-based automation. Those use cases determine what we look at: policy and acceptable use, data and prompt-leakage safeguards, model/vendor risk, human oversight, and whether the setup is controlled and safe to operate.

Examples:

- An organisation rolling out productivity AI: we check that acceptable-use rules, data boundaries, and logging are in place so everyday use stays safe and predictable.

- A team introducing internal agents: we focus on permissions, oversight points, monitoring, and rollback options to ensure the automation behaves within agreed limits.

Context and risk landscape

This section sets the conditions for the screening: where the company operates, what peers are doing, how strategy and organisation shape exposure, which regulatory baselines apply, and which threats and technologies matter. It explains why the chosen REG/CYB/AI focus is relevant here and helps leadership read the findings in context.

Industry
Positions the organisation within its sector's resilience and assurance expectations - what customers, partners, and supervisors typically require (governance, incident readiness, supplier oversight, and evidence). This anchors why evidence over intent is emphasised.

Example: In highly regulated services, continuity and third-party control carry extra weight, and boards expect clear proof of capability.

Market
Captures peer trends that set the bar for "good": a higher tempo of attacks, more cloud/service-provider dependency, and growing demand for evidence-based security. This explains the focus on containment, recovery proof, and clean reporting to management/board.

Example: Many peers are tightening privileged access, proving restores, formalising incident workflows, and adding light AI guardrails.

Strategy
Links planned changes (platform migrations, new digital channels, vendor shifts) to where risk grows next and why certain actions must start now. Strategy and roadmap choices drive the scope and timing of recommendations.

Example: A core-system upgrade or ERP move often pushes identity, data controls, and restore assurance to the front of the queue.

Organisation
Describes current roles, processes, and maturity - what works today and where structure/evidence are still forming - so targets are ambitious but realistic and ownership is clear.

Typical signals: recent leadership changes, a maturing governance cadence, a major system rollout, or a pending supplier transition.

Relevant Regulatory Framework

Outlines the applicable frameworks/assurance baselines (e.g., NIS2, ISO/IEC 27001, GDPR, SOC 2 - and DORA where relevant) and what they imply for governance, incidents, third-party oversight, data handling, and evidence. This is the reference point for interpreting readiness vs. requirement in the results.

Example: For an essential-entity profile, NIS2 expectations elevate governance, incident handling, and supplier control; ISO 27001 underpins the policy/ISMS layer and metrics.

Threat landscape (cyber)

Highlights the few scenarios most likely to cause material impact - typically identity compromise, ransomware, business email compromise, supplier-originated disruption, and cloud misconfiguration/data exfiltration. This justifies the CYB lens on blast-radius control, signal quality, and proved recoverability.

Example: Screening emphasis on Conditional Access/PAM, segmentation, tuned detections, and documented restore tests reflects these risks.

AI and emerging technology risk

AI/automation by the use cases actually planned (productivity, internal decision support, customer-facing flows, early agents). Focus is on data/prompt leakage, vendor/model risk, oversight of automated actions, and a clear audit trail - so adoption is safe, defensible, and does not create rework later.

Examples: Organisations rolling out productivity AI typically prioritise acceptable-use rules, data boundaries, and logging; teams exploring internal agents emphasise scoped permissions, approval gates and rate-limits, monitoring, and rollback; customer-facing decision flows call for a pre-deployment risk check, transparency notices, human checkpoints, and vendor guardrails.

Scope

VENZO's screening framework includes 10 possible screening areas, but we select the subset that best supports your regulatory obligations, key cyber risks, and AI implementation. This makes the screening more targeted, faster to execute, and far more relevant than a broad, generic assessment.

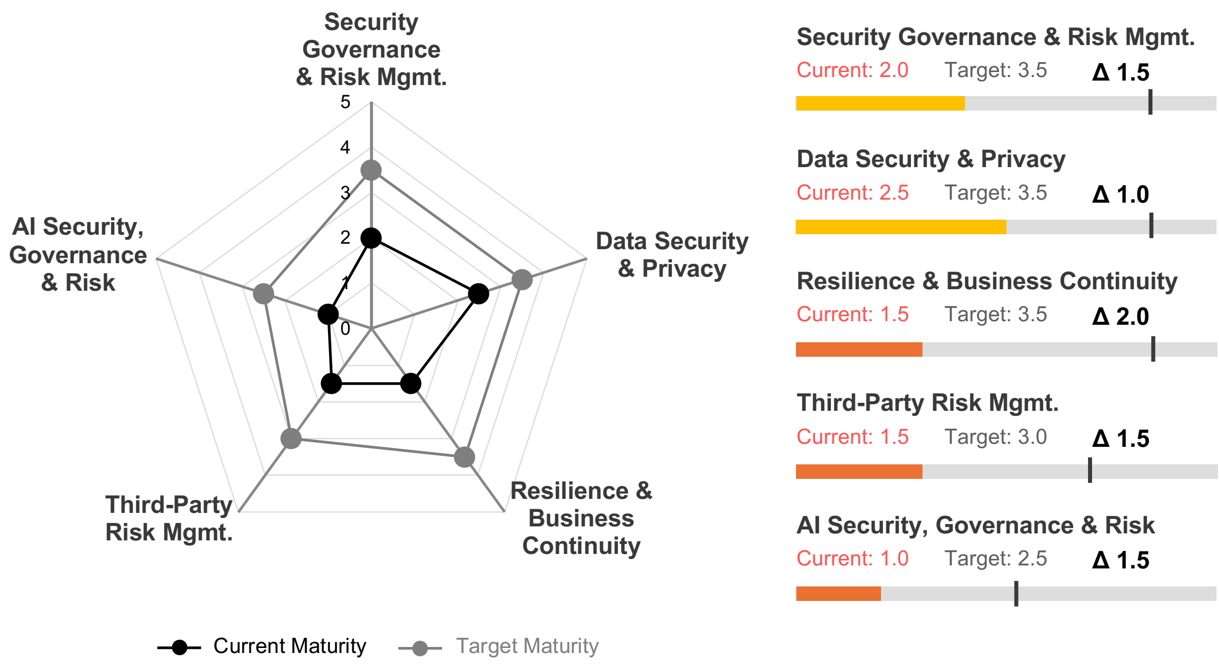
For this example, 5 areas are in scope because they directly map to the agreed Regulatory, Cyber, and AI focus points. The result is a screening that concentrates on the domains that actually influence your risk, compliance exposure, and operational resilience - while still allowing all 10 areas to be assessed if needed.

Example of screening framework areas in scope

1 Security Governance & Risk Management (CYB / REG)	✓
2 Asset Management	✗
3 Identity & Access Management (IAM)	✗
4 Endpoint Protection & Malware Defences	✗
5 Network Security & Segmentation	✗
6 Data Security & Privacy (CYB / AI)	✓
7 Resilience & Business Continuity (CYB / REG)	✓
8 Personnel Security & Training	✗
9 Third-Party Risk Management (REG)	✓
10 AI Security, Governance & Risk (REG / AI)	✓

Example: Regulatory focus pulls in governance, incident readiness, and supplier oversight; Cyber focus highlights identity, detection/response, and recovery assurance; AI focus points toward data handling and oversight. The selected areas reflect these priorities clearly and efficiently.

Summary of findings (Example)



Note: Maturity ratings follow a 1–5 CMMI-aligned scale; Current and target maturity are derived from the domain assessments; full ratings, criteria, and evidence are in the Appendix

This section gives leadership a quick, decision-ready view of your posture. The radar compares current vs. target maturity across the selected domains; targets reflect what a company like yours is expected to demonstrate given obligations, industry norms, peer benchmarks, and your operating model and tech stack.

The overview highlights what is working (capabilities to scale) and where you are exposed (gaps with operational or supervisory impact), so it is clear what to fix first and why. In the example shown, the distances to target make the priority order obvious - we use that to guide the next recommendations and roadmap.

What is working well (strengths)

This highlights the areas where the organisation already has a reliable foundation and practices that can be scaled. For a profile like this, strengths often include solid day-to-day security hygiene, good identity and endpoint practices, and a technically capable team already driving improvements. In the example above, Data Security sits closest to its target - showing that core controls are in place and can support further maturity.

Primary exposure areas (weaknesses)

This focuses on the domains where gaps create real operational or regulatory risk. For similar organisations, exposure is typically concentrated in resilience, incident structure, and third-party/AI governance, where documentation, oversight, and evidence are still developing. In the example above, Resilience & Business Continuity and Third-Party/AI show the widest gaps - making them the clearest priorities for improvement.

VENZO_
a valantic company

Prioritized recommendations and roadmap

This section turns the screening results into a focused, actionable roadmap. Recommendations are grouped into four horizons based on their risk-reduction impact, relevance to your regulatory and business context, and how quickly they can be implemented. Each recommendation is linked to the screening area it strengthens, so it is clear why it matters and where it improves your posture.
The result is a prioritised, realistic plan that shows what to fix first, what to build next, and how to close the most important gaps without unnecessary effort or cost.

P1 **Immediate (Quick Wins)**
Focus on the highest-risk, lowest-effort actions that address the most critical exposure identified in the screening.

P2 **Short-Term**
Actions that require additional planning but deliver substantial risk reduction.

P3 **Medium-Term**
These recommendations address strategic maturity gaps and governance enablement.

P4 **Monitor**
Items placed on the horizon for evaluation once foundational controls are in place.

Security implementation roadmap (Example)

#	Recommendation	Screening area	Horizon	Dimension
P1	Run documented restore tests for top-3 critical services	Resilience & Business Continuity	Immediate	**CYB / REG** Proves recoverability; reduces outage impact and scrutiny *(NIS2, DORA, ISO 22301)*
P1	Create a minimum “critical vendor” register	Third-Party Risk Management	Immediate	**REG** Visibility of critical providers and concentration risk; enables oversight *(DORA, NIS2, ISO 27001, GDPR)*
P2	Activate DLP and sensitivity labels for key data	Data Security & Privacy	Short-term	**CYB / AI / REG** Lowers data exfiltration and AI prompt leakage; supports privacy controls *(GDPR, ISO 27001)*
P2	Publish AI usage policy + pre-deployment risk check; start AI/tool inventory	AI Security, Governance & Risk	Short-term	**AI / REG** Safe, accountable AI adoption; fewer misuse and data-handling incidents *(EU AI Act, ISO/IEC 42001)*
P3	Establish security governance cadence with 5–6 KRIs	Security Governance & Risk Management	Medium-term	**REG** Decision-grade reporting; makes gaps actionable for management/board *(DORA, NIS2, SOC 2)*
P3	Run a business impact analysis (BIA) and set RTO/RPO per critical service	Resilience & Business Continuity	Medium-term	**CYB / REG** Aligns recovery targets to business need; underpins continuity evidence *(ISO 22301, NIS2)*
P4	Tabletop a high-impact scenario (e.g., ransomware or key supplier outage)	Resilience & Business Continuity	Monitor	**CYB / REG** Validates incident and continuity capability end-to-end; actions tracked *(ISO 22301, ISO/IEC 27035)*

Decisions and next steps

Grounded in the screening results, these decisions and next steps confirm who owns what, what starts now, and how progress will be tracked.

Agreed decisions

This locks priorities and accountability so work starts immediately. It confirms who owns the roadmap, what begins now, and how progress is reported - turning findings into action with a clear line of sight for leadership.

Examples: CISO owns the plan; two P1 items start within 30–60 days; monthly management updates and a quarterly board summary are agreed.

Follow-up actions

This sets momentum. You get a short implementation note (effort, dependencies, evidence), a checkpoint date, and a targeted document list to move fast without noise. It removes ambiguity and shortens time-to-value.

Examples: Implementation note delivered in two weeks; checkpoint booked; client shares backup test reports, vendor contracts, and the current policy pack.

Recommended deeper engagements

Based on the screening, this box highlights targeted deep-dives that would benefit from more detail to move from baseline findings to actionable implementation. It explains why an area is worth a closer look now and what you would get to make progress with evidence

Examples: Resilience uplift (BIA, RTO/RPO, restore proof); Third-party risk (critical-vendor register, contract clause fixes, light monitoring cadence); AI governance (usage policy, pre-deployment risk check, AI/tool inventory).

Appendix

The Assessment section provides a comprehensive overview of the organization's security posture, focusing on key domains and evaluating their maturity. It is structured to present findings across several critical areas, detailing current capabilities, identifying priority gaps, and offering actionable recommendations. The section aims to give stakeholders clear insights into strengths and areas for improvement, supporting informed decision-making and strategic planning.

How to read this report

Maturity ratings in this report use a 1-5 scale adapted from the CMMI framework, contextualized for security and GRC screening. The scale describes the overall maturity of each domain, from ad-hoc practices (Level 1) to continuously improved, evidence-based capabilities (Level 5). Full scale definitions are provided in the table below.

Each screening domain is assessed against a target maturity level agreed during the scoping phase. Targets reflect the level at which the organization can demonstrate governed, evidenced capability to supervisors and stakeholders. The gap score (Δ) shows the difference between current and target maturity.

Domain assessments follow a consistent structure:

- Observations - what was identified
- Assessment - what it means for risk and regulatory posture
- Recommendations - prioritized actions and sequencing

Findings are cross-referenced to the prioritized roadmap where relevant.

Maturity scale and level definitions

Level	Rating	Description
Initial	1	Ad-hoc and reactive. Security activities occur but depend on individual initiative rather than defined processes. Controls may exist in isolation but are not consistently applied, documented, or monitored
Documented	2	Recognized and partially documented. Policies and procedures exist for key areas but are not consistently followed or enforced. The organization acknowledges requirements and has begun formalizing its approach, though gaps remain between intent and practice.
Standardized	3	Defined and consistently applied. Documented policies, controls, and procedures are in place, aligned to a recognized standard or framework, and followed across the organization. Roles and responsibilities are clear, and evidence of compliance is available.
Managed	4	Measured and controlled. Security and compliance processes are monitored through defined metrics and key indicators. The organization proactively identifies deviations, tracks effectiveness, and uses data to inform decisions. Processes are predictable and demonstrably effective.
Optimized	5	Continuously improving. The organization systematically reviews and improves its security and compliance posture based on lessons learned, emerging threats, and performance data. Innovation and proactive risk management are embedded in operations.

Ratings reflect the predominant maturity level observed across the controls and practices within each domain. A domain rated at Level 2 may contain individual controls operating at Level 3 alongside others at Level 1 - the rating represents the overall posture, not the strongest or weakest individual control.

Screening methods

The security screening followed a three-phase process designed to produce actionable findings within a compressed timeframe.

Phase 1 – Initiation
A 60-90 minute pre-screening session with the CISO and relevant stakeholders to set context, agree the screening configuration and scope, and identify the threat and regulatory scenarios that will guide the assessment focus. This phase produces the configuration scope and shapes the evidence request issued ahead of the screening day.

Phase 2 – Screening

A structured one-day engagement combining facilitated workshops, targeted interviews, and evidence review with stakeholders for the in-scope domains. Activities include structured questioning against control expectations, review of provided documentation (policies, procedures, configurations, vendor contracts), selective validation of technical configurations (demonstration or screenshots), and calibration of maturity ratings on a 1–5 scale based on the combined evidence.

Phase 3 – Analysis and Reporting

Findings are consolidated, maturity ratings are calibrated across domains for consistency, and gap analysis is performed against the agreed target maturity levels. Recommendations are prioritised by risk-reduction impact, regulatory/business relevance, and implementation feasibility, and organised into a clear roadmap. The report is then produced as the primary deliverable.

Relevant screening framework areas in scope

1 Security Governance & Risk Management (CYB / REG)	✓
2 Asset Management	✗
3 Identity & Access Management (IAM)	✗
4 Endpoint Protection & Malware Defences	✗
5 Network Security & Segmentation	✗
6 Data Security & Privacy (CYB / AI)	✓
7 Resilience & Business Continuity (CYB / REG)	✓
8 Personnel Security & Training	✗
9 Third-Party Risk Management (REG)	✓
10 AI Security, Governance & Risk (REG / AI)	✓

1. Security Governance & Risk Management

Current level: 2.0 (Target level: 3.5 | Difference: 1.5)

Observations

Through the sessions it became clear that governance is running, but without a formal rhythm. Leadership receives narrative updates, yet there is no small, stable set of decision-grade metrics to track posture or progress. Roles and decision rights are understood in practice but not written down, and the risk register exists in parts without consistent owners, treatment status, or review dates. Threat and operational insights are gathered by the technical teams, though they do not consistently feed into a management or board-level view.

Assessment

Without a defined cadence and a handful of well-chosen KRIs, leadership lacks a clear line-of-sight to risk, remediation progress, and whether controls are performing. This makes prioritisation harder, slows decisions, and weakens the organisation's ability to demonstrate governed practice against common expectations (e.g., sector obligations, ISO/IEC 27001, NIS2, SOC 2). Moving to a predictable governance rhythm with concise metrics will turn status updates into decisions and make gaps visible - and fixable - on a predictable schedule.

Recommendations

- **Establish a security governance cadence with 5-6 KRIs** *(Medium-term)*
  Set a monthly management session (with a brief quarterly board update) anchored in a compact KRI pack tied to top risks and obligations. Define owners, thresholds, and the action taken when a threshold is breached; link the pack directly to the risk register so treatments, due dates, and evidence are tracked in one place.

6. Data Security & Privacy

Current level: 2.5 (Target level: 3.5 | Difference: 1.0)

Observations

Data classification is understood in principle but not enforced in tooling. Sensitivity labels are not deployed for key data types, and DLP is disabled across Exchange, SharePoint, and Teams. External sharing and guest access are broad in parts of collaboration, with limited expiry or periodic review. Encryption is provided by platform defaults, but there is no consistent record of data owners, label usage, or policy exceptions. Teams/SharePoint growth has created pockets of over-permissioning that are hard to evidence or reverse quickly.

Assessment

Without labels and DLP, the organisation relies on user behaviour rather than enforceable controls - raising the likelihood of data exfiltration and AI prompt leakage as usage expands. Evidence for privacy and security audits is thin (e.g., GDPR/ISO 27001 control operation), and leadership lacks a clear line of sight to where sensitive information lives, how it is shared, and whether safeguards trigger when they should. The quickest improvement path is to operationalise classification and introduce DLP in controlled steps, paired with tighter external sharing.

Recommendations

– **Activate sensitivity labels and DLP for priority data** *(Short-term)* (e.g., customer/financial/HR), starting in audit mode (2-4 weeks) and moving to enforce with a small, named exceptions process; ensure label-aware sharing rules apply across Exchange/SharePoint/Teams.

7. Resilience & Business Continuity

Current level: 1.5 (Target level: 3.5 | Difference: 2.0)

Observations

Backups exist for key systems, but recoverability has not been proven through documented restore tests. There is no business impact analysis (BIA) to identify critical services, dependencies, and tolerances, so RTO/RPO are not agreed with the business. Incident handling is largely informal: roles, escalation paths, and communications are understood by individuals but not captured in a short, repeatable playbook or exercised.

Assessment

Recoverability is currently assumed, not evidenced, increasing the risk of extended outages and scrutiny when disruptions occur. Without a BIA and service-level RTO/RPO, recovery effort may be mis-directed and business expectations unmet. The absence of a simple, rehearsed playbook slows decisions under pressure and reduces confidence with management, customers, and auditors.

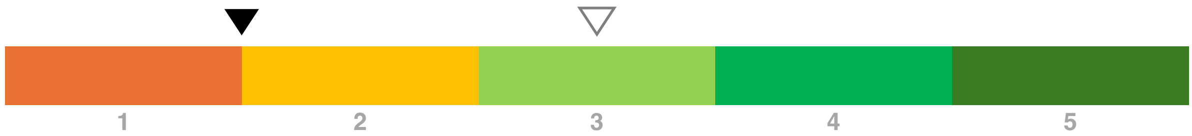
Recommendations

– **Run documented restore tests for the top-3 critical services** *(Immediate).*

– **Conduct a focused BIA and set RTO/RPO per critical service** *(Medium-term).*

– **Tabletop one high-impact scenario** *(Monitor)*
(e.g., ransomware or key supplier outage) to exercise roles, decisions, and comms.

9. Third-Party Risk Management



Current level: 1.5 (Target level: 3.0 | Difference: 1.5)

Observations

A general vendor list exists, but there is no register that singles out critical/important ICT providers or captures the facts leadership needs (service provided, function supported, data categories, processing locations, sub-outsourcing, SLA/OLA, security contacts). Contract language on security/audit rights is inconsistent, and periodic review dates/owners are not recorded. As a result, concentration risk and dependency chains are hard to see at a glance.

Assessment

Without a critical-vendor register, the organisation lacks decision-grade visibility of the suppliers that can materially impact operations or compliance. It is harder to prioritise due diligence, negotiate the right clauses, or respond quickly during an incident when data locations, contacts, and exit considerations are unclear. Expectations from common frameworks (e.g., NIS2, ISO/IEC 27001, GDPR processors) assume this level of oversight and evidence.

Recommendations

– **Create a minimum "critical vendor" register** *(Immediate)*
Triage the vendor list into critical / important / other and capture, at minimum: service & function, business owner, criticality, data categories, processing locations/sub-processors, privileged-access footprint, SLA/OLA, security contact, next review date, and a pointer to exit/transition notes. Assign register ownership (Procurement + Security) and a quarterly review cadence.

10. AI Security, Governance & Risk

Current level: 1.0 (Target level: 2.5 | Difference: 1.5)

Observations

AI use is emerging across teams, but there is no published usage policy, no pre-deployment risk check, and no inventory of AI tools or pilots. Some staff experiment with browser-based services (“shadow AI”) and there is no clear boundary on what data may be placed in prompts. Logging for AI-assisted activities is inconsistent, and accountability (owner, approval, retention, rollback) is not formally defined for higher-risk use cases.

Assessment

Without basic guardrails, the organisation is exposed to data and prompt leakage, unvetted vendor/model risk, and unclear accountability for AI-assisted outputs. As adoption scales, the absence of a lightweight risk check and inventory creates blind spots for security and compliance, making it harder to demonstrate control against common expectations (e.g., EU AI Act principles, ISO/IEC 42001 governance, or equivalent). A short, practical foundation will enable safe productivity gains without rework later.

Recommendations

– **Publish an AI usage policy and implement a pre-deployment risk check; start an AI/tool inventory** *(Short-term)*
  Keep it lean: define acceptable/prohibited uses, data boundaries, logging & retention expectations, and human-in-the-loop for higher-risk decisions. Require a one-page risk checklist before any new AI tool/pilot and record each approved use case in a simple inventory (owner, purpose, data categories, vendor/model, risk tier, review date).

About VENZO

VENZO is a management and technology consultancy within the valantic group, serving organizations across Northern Europe. Our GRC practice operates at the intersection of governance, risk, compliance, and technology – helping organizations make better security decisions consistently, with data, and at business speed.

We specialize in Microsoft-centric enterprises, leveraging the security ecosystem (Defender, Entra, Purview, Intune, Sentinel) not just as security tools but as the data foundation for governed, evidence-based GRC operations. Our approach is built on the Objective-First GRC philosophy: security capabilities derived from business objectives, risk managed quantitatively, and compliance treated as evidence of good security rather than its driver.

Our services span the full GRC lifecycle: from lightweight screenings and capability assessments through strategy development and program design to co-sourced operating models where VENZO embeds with the client to run GRC as a continuous capability. We work with CISOs, Heads of GRC, and IT Directors who want to move beyond checkbox compliance toward decision-grade security governance.