GRCForce

The Audit Readiness Stack Checklist

A 10-point checklist for ISO 27001, TISAX and sustainable audit readiness

Use this canvas to test whether scope, evidence, ownership, cadence and culture are strong enough before audit pressure arrives.

Layer	What this means	ISO 27001 check	TISAX check	Evidence owner	Status
Scope	Boundaries are clear and match reality.	Scope statement is current and reflects services, locations and systems.	Assessment scope matches customer data protection needs.	ISMS / GRC owner	Green / Amber / Red
Evidence	Proof is created by normal operations, not panic.	Access reviews, risk decisions and approvals are timestamped and stored.	Evidence for each control objective is current and verifiable.	Control owners	Green / Amber / Red
Ownership	Every control has a named accountable person.	Control owner list exists and is current.	Each TISAX control has an accountable individual.	GRC / Risk owner	Green / Amber / Red
Cadence	Reviews happen predictably, not randomly.	Risk reviews, management reviews and internal audits are scheduled and occurring.	TISAX readiness is reviewed at defined intervals.	Programme manager	Green / Amber / Red
Culture	The organisation escalates issues, not hides them.	Findings are reported and remediated transparently.	Surprises are reduced through open reporting.	Leadership team	Green / Amber / Red

Page 2 - 10 Critical Health Checks

1. Risk assessment is current	Risk assessment completed within the last 12 months or after significant change. Treatment decisions have owners and dates.	Ready / Needs work / Not ready
2. Statement of Applicability reflects reality	SoA is reviewed, justified, approved and backed by implementation evidence.	Ready / Needs work / Not ready
3. Internal audit programme is running	Annual internal audit schedule exists, is followed, and previous findings are closed with evidence.	Ready / Needs work / Not ready
4. Management review has happened	Formal management review minutes, decisions and actions are documented and stored.	Ready / Needs work / Not ready
5. Policies are connected to practice	Core policies are reviewed on cycle and match how work is actually done today.	Ready / Needs work / Not ready
6. Access reviews are evidenced	Formal access reviews are completed for critical systems and evidence is stored at source.	Ready / Needs work / Not ready
7. Supplier controls are maintained	Critical suppliers are assessed within cycle and sub-processor exposure is documented.	Ready / Needs work / Not ready
8. Incident records are accurate and complete	Incident log is current, reviewed, and escalation paths have been tested.	Ready / Needs work / Not ready
9. Objectives are tracked and meaningful	Security objectives have measurable targets and are reviewed by management.	Ready / Needs work / Not ready
10. Corrective actions are closed	Open items have named owners, root cause, target dates and evidence gates.	Ready / Needs work / Not ready

Page 3 - How to Use This Checklist

Score your current position	Work through the canvas and 10-point checklist honestly with the team responsible for the ISMS or TISAX scope.
Prioritise the weak items	Focus first on gaps likely to create a major nonconformity, customer concern or weak evidence trail.
Assign owners and deadlines	Every open item needs one named owner, one realistic closure date and one evidence expectation.
Run a 30-day pre-audit review	Re-score 30 days before the audit. Items still not ready need an escalation decision.
Keep it alive quarterly	Use the checklist between audits so readiness stays part of the operating model.

Common Failure Points

Policy drift	Policies no longer match how work is done.	Assign policy owners and review quarterly.
Audit-only evidence	Screenshots and folders are created during audit prep.	Build evidence into normal workflows.
Open corrective actions	Findings are acknowledged but not closed.	Assign owners, dates and evidence gates.
Scope mismatch	The certificate scope no longer matches operations.	Review scope annually and after major change.

GRCForce CTA	If you want to test your current programme against this checklist, request a 30-minute Audit Readiness Review at grcforce.com/en/#contact.