

SECTUTOR

Single Point of Failure

Technology Dependence Risk Register

The 56 risks in eleven categories from the consolidated register in *Single Point of Failure: Managing Europe's Dependence on US Technology*, with notes on managing them in GRCompliance.

Emmanuel Aigbehi Walstra

Companion to the book • Published by Sectutor

First edition • October 2026

Risk ratings in this register are illustrative expert judgement for the reference organisation described in the book. They are not measured data. Every organisation must re-rate them against its own context, risk appetite and control environment. This document is not legal advice.

1. About this register

This document reproduces the consolidated risk register from Chapter 13 of *Single Point of Failure: Managing Europe's Dependence on US Technology* by Emmanuel Aigbehi Walstra (Sectutor). It contains the book's 56 risks in eleven categories, with the fields the book gives for each: identifier, category, risk description, inherent likelihood and impact, velocity, key risk indicators (KRIs), mitigations, suggested owner, target residual rating and, where relevant, the tabletop scenario in Chapter 14 that exercises the risk.

Purpose. The register gives boards, risk owners and second-line functions a ready-made starting point for recording technology dependence risk in an enterprise risk-management (ERM) tool or a governance, risk and compliance (GRC) platform. It does not replace the book: the chapters explain the evidence behind each risk, and the scenarios show how several risks can be triggered by a single event.

What has changed from the book. Nothing in the risks themselves. The risk texts, ratings, KRIs, mitigations, owners and residual targets are copied from the manuscript (v0.9, 26 October 2026) without edits. Only the layout differs. Section 7 is new: it explains how an organisation can load and manage these risks in GRCompliance.

Contents.

- Section 2 – How to read the ratings (scales, bands, velocity and the book's caveats)
- Section 3 – Register at a glance (rating profile and heat maps)
- Section 4 – Summary register (all 56 risks on one table)
- Section 5 – Detailed risk sheets, by category
- Section 6 – Maintaining the register
- Section 7 – Using this register in GRCompliance
- Next steps

2. How to read the ratings

Each entry has an inherent likelihood and impact rating on the five-point scales defined in Chapter 1 of the book, a velocity indicator, and a target residual rating that assumes the listed mitigations are implemented. Likelihood is assessed over a 24-month horizon.

Score	Likelihood (24 months)	Impact
1	Rare – not expected; would require an unprecedented event	Minor – limited disruption, absorbed in normal operations
2	Unlikely – could occur; precedents exist elsewhere	Moderate – disruption of non-critical services; minor regulatory interest
3	Possible – plausible; precedents in comparable organisations	Significant – disruption of important services for days; regulatory reporting
4	Likely – expected to occur in some form	Major – disruption of critical services; material financial loss; supervisory action
5	Almost certain – occurring now or expected repeatedly	Severe – prolonged loss of critical functions; threat to licence or viability

Risk score = likelihood × impact. **Bands:** Low 1–4, Medium 5–9, High 10–15, Critical 16–25. **Velocity:** F (fast – impact within hours to days), M (medium – weeks to months), S (slow – many months to years). One risk is rated F/M (fast to medium).

Caveats from the book

Three caveats apply. First, the ratings are **illustrative expert judgement** for the reference organisation described in Chapter 1 – a large EU entity in scope of NIS2 or DORA that uses mainstream US cloud, identity and security

services. They are not measured data, and every organisation must re-rate them against its own context, risk appetite and control environment. Second, risks are not independent: several share common causes (for example, a single sanctions event can trigger LEG-03, EP-02, IAM-01, CLD-04 and FIN-01 at the same time), so the register should be read together with the scenarios. Third, residual ratings are targets, not promises; they are only reached when mitigations are implemented and tested.

Owner roles are suggestions. In most organisations a C-level owner is accountable for each risk while operational management sits with a named manager. The Chief Risk Officer (CRO) or equivalent should own the register as a whole and report it to the board at least annually and after material events.

3. Register at a glance

The register contains **56 risks** across eleven categories. Inherent ratings: 1 Critical, 20 High, 33 Medium and 2 Low. After the mitigations listed, the target residual profile is 0 Critical, 0 High, 19 Medium and 37 Low.

Band	Inherent (count)	Target residual (count)
Critical	1	0
High	20	0
Medium	33	19
Low	2	37

Prefix	Category (book chapter)	Risks
LEG	Legal and geopolitical levers (Ch. 2)	7
NET	Internet core (Ch. 3)	7
SPC	Space (Ch. 4)	3
HW	Hardware and semiconductors (Ch. 5)	5
EP	Operating systems and endpoints (Ch. 6)	4
CLD	Cloud and SaaS (Ch. 7)	6
IAM	Identity (Ch. 8)	4
SEC	Security stack (Ch. 9)	6
AI	Artificial intelligence (Ch. 10)	5
FIN	Payments and communications (Ch. 11)	5
GOV	Governance and organisation (Ch. 12, 15)	4
	Total	56

Two observations stand out in the book. The highest inherent ratings are concentrated in **technical failure** risks with fast velocity – hyperscale cloud outage (CLD-01), identity lockout (IAM-01) and faulty security-agent updates (SEC-01) – rather than in the politically prominent legal risks. These are the risks that have actually materialised repeatedly in 2024–2025. The legal-denial risks (LEG-03, EP-02, CLD-04) have lower likelihood for most organisations but very high impact and almost no warning time once triggered, which is why they dominate the scenario chapter. Mitigations reduce impact far more readily than likelihood: an organisation cannot prevent a US sanctions decision or a hyperscaler outage, but it can make sure it survives one.

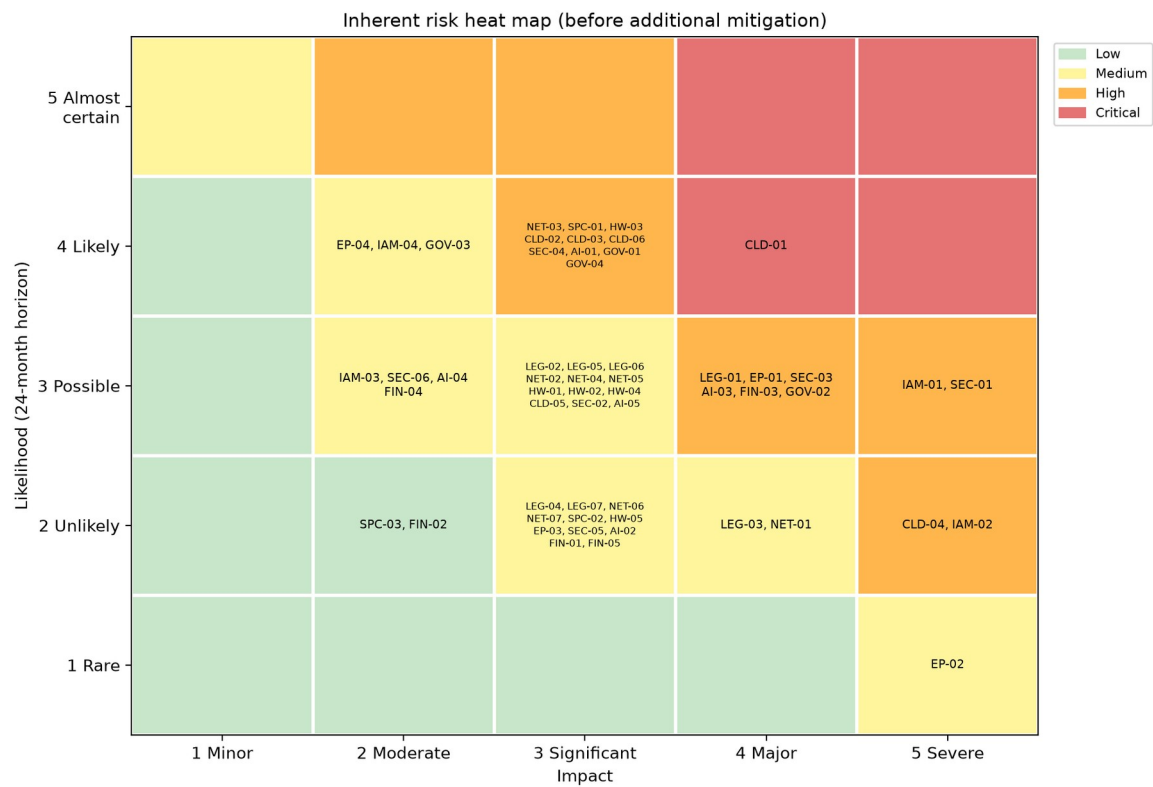


Figure 1 – Inherent risk heat map (illustrative; Figure 13.1 in the book)

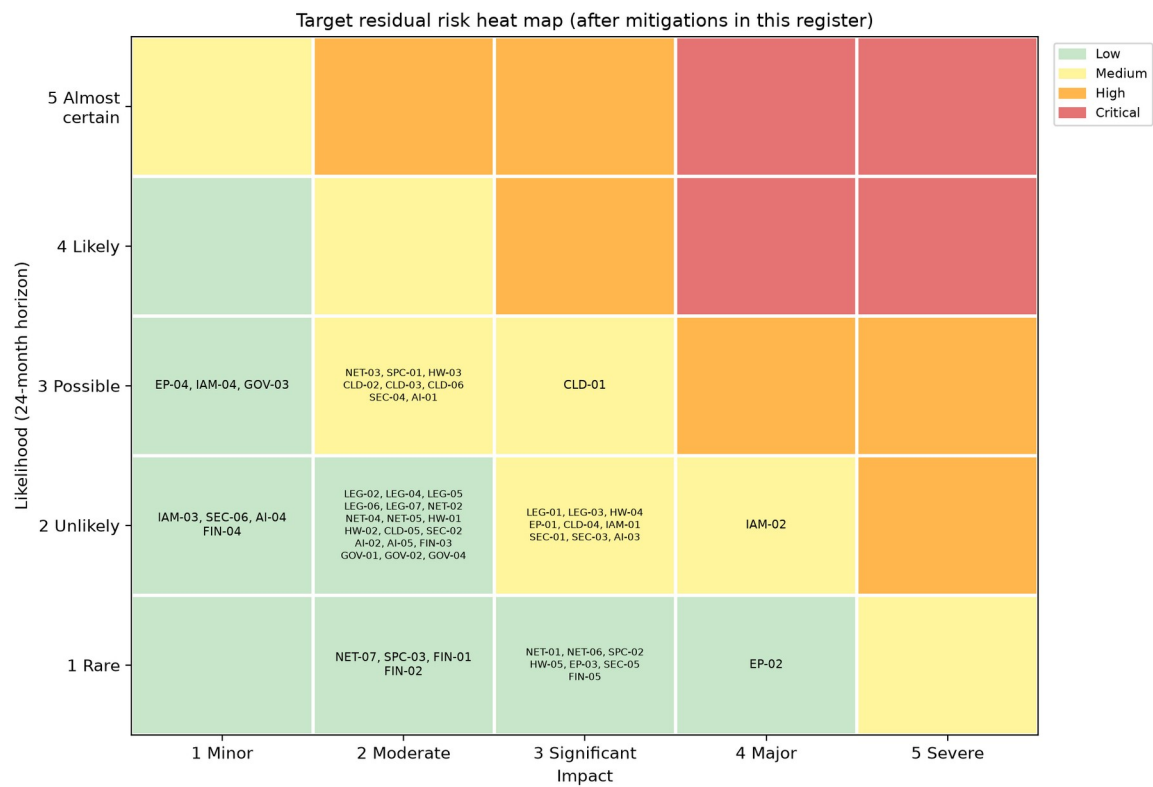


Figure 2 – Target residual risk heat map (illustrative; Figure 13.2 in the book)

Top risks by inherent score

Rank	ID	Risk	Score	Why it ranks high
1	CLD-01	Hyperscale cloud outage	16	Repeated major outages in 2025; most organisations have not designed for provider failure
2	IAM-01	Organisation-wide identity lockout	15	Single point of failure for all federated access; break-glass often untested
3	SEC-01	Faulty update from privileged security agent	15	Kernel-level agents on every host; the 2024 event affected 8.5 million devices
4	LEG-01	Compelled disclosure via US provider	12	Structural; cannot be contracted away while a US entity controls the data
5	EP-01	Faulty or compromised update through vendor channels	12	Updates are pushed at fleet scale
6	SEC-03	Security visibility loss or telemetry exposure	12	Security operations depend on the same concentrated providers
7	AI-03	Confidential data exposure via AI services	12	Widespread unsanctioned use of AI services
8	FIN-03	Loss of collaboration platform without out-of-band channel	12	Crisis communication usually depends on the system that failed
9	GOV-02	Non-compliance with third-party and exit requirements	12	See detail sheet
10	NET-03	CDN/WAF/DDoS provider outage	12	A handful of edge providers front a large share of the web
11	SPC-01	GNSS disruption of positioning/timing	12	Persistent GNSS interference around the Baltic and Eastern Europe
12	HW-03	Network-equipment vendor dependency	12	Edge devices are the most-exploited class of vulnerability

4. Summary register

All 56 risks, in the order the book lists them. L = likelihood, I = impact (1–5). Score = L × I. Vel. = velocity. Residual = target residual score and band after the listed mitigations. All ratings are illustrative expert judgement.

ID	Risk	Category	L	I	Score	Band	Vel.	Owner (suggested)	Residual	Scen.
LEG-01	Compelled disclosure via US provider	Legal and geopolitical levers	3	4	12	High	F	CISO / DPO	6 (Medium)	D
LEG-02	Invalidation of EU-US Data Privacy Framework	Legal and geopolitical levers	3	3	9	Medium	M	DPO / General Counsel	4 (Low)	D
LEG-03	Sanctions-driven loss of US services	Legal and geopolitical levers	2	4	8	Medium	F	General Counsel / CRO	6 (Medium)	A
LEG-04	Export-control restriction on US technology	Legal and geopolitical levers	2	3	6	Medium	M	CTO / Compliance	4 (Low)	E
LEG-05	Trade/regulatory retaliation affecting providers	Legal and geopolitical levers	3	3	9	Medium	S	CFO / Procurement	4 (Low)	–
LEG-06	Over-compliance by EU intermediaries	Legal and geopolitical levers	3	3	9	Medium	F	CFO / General Counsel	4 (Low)	A
LEG-07	Conflict of laws if EU Blocking Statute extended	Legal and geopolitical levers	2	3	6	Medium	M	General Counsel	4 (Low)	A
NET-01	Loss of DNS resolution or domain control	Internet core	2	4	8	Medium	F	CIO / Network	3 (Low)	C
NET-02	Web PKI trust and certificate operations	Internet core	3	3	9	Medium	M	CISO / Infrastructure	4 (Low)	–
NET-03	CDN/WAF/DDoS provider outage	Internet core	4	3	12	High	F	CIO / Digital channels	6 (Medium)	C
NET-04	Transatlantic or US control-plane dependency	Internet core	3	3	9	Medium	F	CTO / Architecture	4 (Low)	C
NET-05	Email outage, suspension or deliverability failure	Internet core	3	3	9	Medium	F	CIO	4 (Low)	A
NET-06	Routing incidents (BGP hijack/leak)	Internet core	2	3	6	Medium	F	Network	3 (Low)	–
NET-07	Time synchronisation failure or manipulation	Internet core	2	3	6	Medium	F	Infrastructure	2 (Low)	B
SPC-01	GNSS disruption of positioning/timing	Space	4	3	12	High	F	COO / Infrastructure	6 (Medium)	B
SPC-02	Loss of satellite connectivity	Space	2	3	6	Medium	F	CIO / Network	3 (Low)	–
SPC-03	Loss of commercial imagery access	Space	2	2	4	Low	F	Business owner	2 (Low)	–
HW-01	Restricted access to advanced AI accelerators	Hardware and semiconductors	3	3	9	Medium	M	CTO	4 (Low)	E
HW-02	Vendor-controlled firmware and trust anchors	Hardware and semiconductors	3	3	9	Medium	M	Infrastructure / CISO	4 (Low)	–
HW-03	Network-equipment vendor dependency	Hardware and semiconductors	4	3	12	High	F	CISO / Network	6 (Medium)	–
HW-04	Semiconductor or hardware supply shock	Hardware and semiconductors	3	3	9	Medium	M	COO / Procurement	6 (Medium)	–
HW-05	Loss of vendor support or spares	Hardware and semiconductors	2	3	6	Medium	S	CIO	3 (Low)	–
EP-01	Faulty or compromised update through vendor channels	Operating systems and endpoints	3	4	12	High	F	CIO / CISO	6 (Medium)	C
EP-02	Withdrawal of vendor cloud services from endpoints	Operating systems and endpoints	1	5	5	Medium	F	CIO	4 (Low)	A
EP-03	App-store removal or platform-policy friction	Operating systems and endpoints	2	3	6	Medium	F	Digital channels	3 (Low)	–

ID	Risk	Category	L	I	Score	Band	Vel.	Owner (suggested)	Residual	Scen.
EP-04	Vendor lifecycle and licensing shocks	Operating systems and endpoints	4	2	8	Medium	S	CIO / CFO	3 (Low)	-
CLD-01	Hyperscale cloud outage	Cloud and SaaS	4	4	16	Critical	F	CIO / CTO	9 (Medium)	C
CLD-02	Lock-in prevents exit	Cloud and SaaS	4	3	12	High	S	CTO	6 (Medium)	F
CLD-03	Commercial shock from dominant vendor	Cloud and SaaS	4	3	12	High	M	CFO / Procurement	6 (Medium)	-
CLD-04	Sustained loss of productivity suite	Cloud and SaaS	2	5	10	High	F	CIO	6 (Medium)	A
CLD-05	Sovereignty washing	Cloud and SaaS	3	3	9	Medium	S	CISO / General Counsel	4 (Low)	-
CLD-06	Hidden n-th-party dependency	Cloud and SaaS	4	3	12	High	F	Procurement / CRO	6 (Medium)	C
IAM-01	Organisation-wide identity lockout	Identity	3	5	15	High	F	CISO / CIO	6 (Medium)	A
IAM-02	Compromise of IdP infrastructure	Identity	2	5	10	High	F	CISO	8 (Medium)	-
IAM-03	Passkey and social-login lock-in	Identity	3	2	6	Medium	S	CISO / Digital channels	2 (Low)	-
IAM-04	Delayed European identity alternatives	Identity	4	2	8	Medium	S	Digital channels	3 (Low)	-
SEC-01	Faulty update from privileged security agent	Security stack	3	5	15	High	F	CISO	6 (Medium)	C
SEC-02	Disruption of CVE/NVD ecosystem	Security stack	3	3	9	Medium	M	CISO	4 (Low)	F
SEC-03	Security visibility loss or telemetry exposure	Security stack	3	4	12	High	F	CISO	6 (Medium)	-
SEC-04	Open-source supply-chain compromise or unavailability	Security stack	4	3	12	High	F	CTO / CISO	6 (Medium)	-
SEC-05	Code-signing and platform trust decisions	Security stack	2	3	6	Medium	M	CTO	3 (Low)	-
SEC-06	Erosion of US public cyber information sharing	Security stack	3	2	6	Medium	S	CISO	2 (Low)	F
AI-01	Disruption of AI-enabled processes	Artificial intelligence	4	3	12	High	F/M	CTO / Business owners	6 (Medium)	E
AI-02	Restricted AI compute access	Artificial intelligence	2	3	6	Medium	M	CTO	4 (Low)	E
AI-03	Confidential data exposure via AI services	Artificial intelligence	3	4	12	High	F	CISO / DPO	6 (Medium)	D
AI-04	Loss of European AI option via acquisition	Artificial intelligence	3	2	6	Medium	M	Procurement	2 (Low)	-
AI-05	AI Act compliance gaps from provider information	Artificial intelligence	3	3	9	Medium	S	Compliance / DPO	4 (Low)	-
FIN-01	Card-payment exclusion	Payments and communications	2	3	6	Medium	F	CFO / Treasury	2 (Low)	A
FIN-02	Mobile wallet dependency	Payments and communications	2	2	4	Low	M	Head of Payments	2 (Low)	-
FIN-03	Loss of collaboration platform without out-of-band channel	Payments and communications	3	4	12	High	F	COO / CISO	4 (Low)	A
FIN-04	Marketing, analytics and public-comms disruption	Payments and communications	3	2	6	Medium	M	CMO / Comms	2 (Low)	D
FIN-05	Over-compliance by EU financial providers	Payments and communications	2	3	6	Medium	F	CFO	3 (Low)	A
GOV-01	Insufficient visibility of dependencies	Governance and organisation	4	3	12	High	S	CRO / CIO	4 (Low)	-
GOV-02	Non-compliance with third-party and exit requirements	Governance and organisation	3	4	12	High	M	CRO / Compliance	4 (Low)	-

ID	Risk	Category	L	I	Score	Band	Vel.	Owner (suggested)	Residual	Scen.
GOV-03	Skills and organisational lock-in	Governance and organisation	4	2	8	Medium	S	CIO / HR	3 (Low)	-
GOV-04	Exit and continuity plans untested	Governance and organisation	4	3	12	High	S	CRO / COO	4 (Low)	All scenarios

Scenario key: A – Sanctions designation; B – GNSS disruption; C – Hyperscaler/IdP outage; D – Transfer-basis collapse; E – AI-compute escalation; F – Vulnerability-intelligence lapse; All – all scenarios.

5. Detailed risk sheets

The following sheets give, for each risk, the information needed to populate an ERM tool. KRIs are written so that they can be monitored by a second-line function; mitigations are listed in approximate order of priority.

Legal and geopolitical levers (Ch. 2)

LEG-01 – Compelled disclosure via US provider

Category	Legal and geopolitical levers (Ch. 2)
Description	Organisational or customer data held by a US provider is disclosed to US authorities under the CLOUD Act, FISA or other powers, possibly with a gag order, without the organisation's knowledge or consent.
Inherent rating	L3 × I4 = 12 (High); velocity Fast
Key risk indicators	• Status of FISA 702 reauthorisation (deadline pressure Nov 2026–Mar 2027) • Provider transparency-report volumes for EU requests • Changes to EO 14086 or DPRC/PCLOB functioning • Supervisory-authority guidance on transfers
Mitigations	• Classify data; keep the most sensitive in EU-controlled environments • Customer-held keys (external KMS/HSM) with architecture preventing provider access to plaintext • Contractual commitments to challenge orders and notify where lawful • Transfer impact assessments kept current • Prefer EU-operated or partner-operated offerings for regulated data
Owner (suggested)	CISO / DPO
Target residual	L2 × I3 = 6 (Medium)
Scenario link	D – Transfer-basis collapse

LEG-02 – Invalidation of EU-US Data Privacy Framework

Category	Legal and geopolitical levers (Ch. 2)
Description	The CJEU annuls the DPF adequacy decision (appeal C-703/25 P), removing the transfer basis relied on for US providers and potentially without a grace period.
Inherent rating	L3 × I3 = 9 (Medium); velocity Medium
Key risk indicators	• Scheduling of hearing / AG opinion in C-703/25 P • Changes to US surveillance law or EO 14086 • EDPB statements • Supervisory enforcement on transfers
Mitigations	• Maintain SCCs as fallback in all US provider contracts • Keep TIAs current; pre-define supplementary measures • Inventory which processing relies solely on DPF • Encryption with EU-held keys for high-risk transfers
Owner (suggested)	DPO / General Counsel
Target residual	L2 × I2 = 4 (Low)
Scenario link	D – Transfer-basis collapse

LEG-03 – Sanctions-driven loss of US services

Category	Legal and geopolitical levers (Ch. 2)
Description	A US sanctions designation of the organisation, a subsidiary, a board member, employee or key counterparty requires US providers to terminate services (email, cloud, identity, payments).
Inherent rating	L2 × I4 = 8 (Medium); velocity Fast
Key risk indicators	• New designations under EO 14203 and similar programmes • Amendment/expiry of OFAC general licences (e.g., ICC GL 13 on 7 Apr 2027) • Public statements targeting EU institutions or officials • Provider notices on sanctions compliance
Mitigations	• Sanctions-exposure screening for staff in sensitive roles and for counterparties • Pre-arranged alternative services for exposed individuals (EU email, EU cards, EU devices) • Data portability and offline copies for critical records • Legal playbook for designation events, including EU Blocking Statute analysis
Owner (suggested)	General Counsel / CRO
Target residual	L2 × I3 = 6 (Medium)
Scenario link	A – Sanctions designation

LEG-04 – Export-control restriction on US technology

Category	Legal and geopolitical levers (Ch. 2)
Description	Changes to US export controls (AI chips, encryption, advanced computing, entity listing) restrict or condition access to technology needed by the organisation or its EU providers.
Inherent rating	L2 × I3 = 6 (Medium); velocity Medium
Key risk indicators	• BIS rules or draft rules on AI chips (post-diffusion framework) • Entity List additions affecting EU firms • Conditions tied to US investment or security guarantees • Allocation delays from vendors
Mitigations	• Diversify compute sources (EU AI Factories/Gigafactories, multiple clouds) • Track export-classification of critical items • Contract clauses on export-control-driven termination • Maintain non-frontier fallback models
Owner (suggested)	CTO / Compliance
Target residual	L2 × I2 = 4 (Low)
Scenario link	E – AI-compute escalation

LEG-05 – Trade/regulatory retaliation affecting providers

Category	Legal and geopolitical levers (Ch. 2)
Description	US–EU disputes over the DMA, DSA, digital taxes or tariffs lead US providers to change EU offerings, prices or terms, or to withhold features from the EU market.
Inherent rating	L3 × I3 = 9 (Medium); velocity Slow
Key risk indicators	• Formal USTR Section 301 initiation • Tariff announcements tied to digital rules • Provider statements on EU feature availability
Mitigations	• Price-protection and change-notice clauses • Avoid single-vendor feature dependencies for core processes • Scenario budgets for licence increases
Owner (suggested)	CFO / Procurement
Target residual	L2 × I2 = 4 (Low)
Scenario link	–

LEG-06 – Over-compliance by EU intermediaries

Category	Legal and geopolitical levers (Ch. 2)
Description	European banks, payment providers or IT providers terminate services to the organisation or its people beyond legal requirements to manage their own US exposure.
Inherent rating	L3 × I3 = 9 (Medium); velocity Fast
Key risk indicators	• Reports of EU banks closing accounts of sanctioned persons • EU guidance on over-compliance • Blocking Statute debate
Mitigations	• Relationship-level agreements with key banks and providers • Multiple banking relationships • Escalation route to supervisors where over-compliance affects lawful activity
Owner (suggested)	CFO / General Counsel
Target residual	L2 × I2 = 4 (Low)
Scenario link	A – Sanctions designation

LEG-07 – Conflict of laws if EU Blocking Statute extended

Category	Legal and geopolitical levers (Ch. 2)
Description	If the EU extends the Blocking Statute to US sanctions (e.g., ICC), compliance with one regime may breach the other, creating legal exposure for the organisation and disruption from its US providers.
Inherent rating	L2 × I3 = 6 (Medium); velocity Medium
Key risk indicators	• Commission decision on Blocking Statute annex • MEP and Member State pressure • US response to EU countermeasures
Mitigations	• Prepare legal analysis and authorisation-request templates • Identify services where US providers would continue to apply US law • Board-approved decision framework
Owner (suggested)	General Counsel
Target residual	L2 × I2 = 4 (Low)
Scenario link	A – Sanctions designation

Internet core (Ch. 3)

NET-01 – Loss of DNS resolution or domain control

Category	Internet core (Ch. 3)
Description	Failure of a single managed-DNS provider, or legal/registry action against a .com/.net domain, makes the organisation's services unreachable or hijackable.
Inherent rating	$L2 \times I4 = 8$ (Medium); velocity Fast
Key risk indicators	- Managed-DNS provider incidents - Registry/registrar policy changes - Domain seizure cases
Mitigations	- Authoritative DNS on two independent providers - Registry lock and DNSSEC on critical domains - European ccTLD alternative for critical services - Zone data held in-house; tested failover
Owner (suggested)	CIO / Network
Target residual	$L1 \times I3 = 3$ (Low)
Scenario link	C – Hyperscaler/IdP outage

NET-02 – Web PKI trust and certificate operations

Category	Internet core (Ch. 3)
Description	A browser root-program decision or CA failure forces an urgent certificate change, or shortening lifetimes (100 days from Mar 2027, 47 from Mar 2029) cause outages where renewal is manual.
Inherent rating	$L3 \times I3 = 9$ (Medium); velocity Medium
Key risk indicators	- Root-program distrust announcements - CA/B Forum ballots - Certificate-related outages internally
Mitigations	- Full ACME automation with second CA (incl. European CA) pre-configured - Certificate inventory and expiry monitoring - Avoid single-CA dependence for critical services
Owner (suggested)	CISO / Infrastructure
Target residual	$L2 \times I2 = 4$ (Low)
Scenario link	–

NET-03 – CDN/WAF/DDoS provider outage

Category	Internet core (Ch. 3)
Description	Failure of the single CDN/WAF/DDoS provider fronting customer-facing services causes an outage of those services.
Inherent rating	$L4 \times I3 = 12$ (High); velocity Fast
Key risk indicators	- Provider incident frequency (e.g., Cloudflare 18 Nov 2025, Azure Front Door 29 Oct 2025) - Share of services behind single edge provider
Mitigations	- Secondary edge path (second CDN or protected origin) switchable via DNS - DDoS mitigation not tied to same provider - Runbooks and periodic failover tests
Owner (suggested)	CIO / Digital channels
Target residual	$L3 \times I2 = 6$ (Medium)
Scenario link	C – Hyperscaler/IdP outage

NET-04 – Transatlantic or US control-plane dependency

Category	Internet core (Ch. 3)
Description	Degradation of transatlantic connectivity or failure of US-hosted control planes/global services affects EU-hosted workloads.
Inherent rating	L3 × I3 = 9 (Medium); velocity Fast
Key risk indicators	• Hidden dependencies on US regions found in architecture reviews • Cable incidents • Provider global-service outages
Mitigations	• Map and remove US-region dependencies for critical services • Prefer providers with EU-contained control planes • Test operation under transatlantic degradation
Owner (suggested)	CTO / Architecture
Target residual	L2 × I2 = 4 (Low)
Scenario link	C – Hyperscaler/IdP outage

NET-05 – Email outage, suspension or deliverability failure

Category	Internet core (Ch. 3)
Description	Email hosted with a US provider becomes unavailable (outage, account action) or customer email fails to deliver due to mailbox-provider policy.
Inherent rating	L3 × I3 = 9 (Medium); velocity Fast
Key risk indicators	• Mailbox-provider policy changes • DMARC failure rates • Provider outage frequency
Mitigations	• SPF/DKIM/DMARC enforcement and monitoring • Alternative channels for critical notifications • Backup mail routing/MX and archive outside primary provider
Owner (suggested)	CIO
Target residual	L2 × I2 = 4 (Low)
Scenario link	A – Sanctions designation

NET-06 – Routing incidents (BGP hijack/leak)

Category	Internet core (Ch. 3)
Description	Route hijacks or leaks divert or black-hole traffic to the organisation's networks or providers.
Inherent rating	L2 × I3 = 6 (Medium); velocity Fast
Key risk indicators	• RPKI coverage of own prefixes • Route-leak incidents affecting providers
Mitigations	• Publish ROAs for all prefixes (RIPE NCC) • Choose transit providers enforcing ROV • BGP monitoring
Owner (suggested)	Network
Target residual	L1 × I3 = 3 (Low)
Scenario link	–

NET-07 – Time synchronisation failure or manipulation

Category	Internet core (Ch. 3)
Description	Undiversified time sources (GPS-disciplined NTP, single public pool) fail or are manipulated, breaking authentication, logging or trading timestamps.
Inherent rating	$L2 \times I3 = 6$ (Medium); velocity Fast
Key risk indicators	• Time-offset alerts • GNSS interference reports near sites
Mitigations	• Multiple independent time sources incl. national metrology/NTS • Multi-constellation timing receivers with holdover • Monitor offsets as security signal
Owner (suggested)	Infrastructure
Target residual	$L1 \times I2 = 2$ (Low)
Scenario link	B – GNSS disruption

Space (Ch. 4)

SPC-01 – GNSS disruption of positioning/timing

Category	Space (Ch. 4)
Description	Jamming, spoofing or regional degradation of GNSS (especially GPS-only equipment) disrupts logistics, field operations or timing-dependent systems.
Inherent rating	$L4 \times I3 = 12$ (High); velocity Fast
Key risk indicators	• EASA interference bulletins • Interference reports in operating regions • Share of GPS-only receivers in inventory
Mitigations	• Inventory GNSS-dependent assets • Multi-constellation (GPS+Galileo) and OSNMA-capable receivers • Holdover and terrestrial time • Degraded-mode procedures
Owner (suggested)	COO / Infrastructure
Target residual	$L3 \times I2 = 6$ (Medium)
Scenario link	B – GNSS disruption

SPC-02 – Loss of satellite connectivity

Category	Space (Ch. 4)
Description	Satellite links used for backup or remote sites (often a single LEO provider) become unavailable due to provider decision, legal restriction or outage.
Inherent rating	$L2 \times I3 = 6$ (Medium); velocity Fast
Key risk indicators	• Provider policy statements • Export or sanctions measures affecting service • Outage history
Mitigations	• Diversify satellite providers/orbits • Contract review for suspension rights • Plan for GOVSATCOM/IRIS² where eligible
Owner (suggested)	CIO / Network
Target residual	$L1 \times I3 = 3$ (Low)
Scenario link	–

SPC-03 – Loss of commercial imagery access

Category	Space (Ch. 4)
Description	Access to very-high-resolution imagery delivered via US channels is suspended or restricted.
Inherent rating	L2 × I2 = 4 (Low); velocity Fast
Key risk indicators	• Government decisions on imagery access • Provider ownership changes
Mitigations	• Diversify across US and European imagery suppliers • Retain Copernicus-based capability
Owner (suggested)	Business owner
Target residual	L1 × I2 = 2 (Low)
Scenario link	–

Hardware and semiconductors (Ch. 5)

HW-01 – Restricted access to advanced AI accelerators

Category	Hardware and semiconductors (Ch. 5)
Description	Supply concentration or US export-control changes delay or condition access to GPUs and AI compute for the organisation or its EU providers.
Inherent rating	L3 × I3 = 9 (Medium); velocity Medium
Key risk indicators	• BIS rules • Lead times and allocation • GPU cloud pricing
Mitigations	• Multi-source compute (EU clouds, hyperscalers, EuroHPC) • Efficiency: smaller/open-weight models • Capacity reservations
Owner (suggested)	CTO
Target residual	L2 × I2 = 4 (Low)
Scenario link	E – AI-compute escalation

HW-02 – Vendor-controlled firmware and trust anchors

Category	Hardware and semiconductors (Ch. 5)
Description	Firmware, management engines or boot trust anchors controlled by vendors cause a fleet-wide security or availability event (e.g., key compromise, certificate expiry, faulty firmware).
Inherent rating	L3 × I3 = 9 (Medium); velocity Medium
Key risk indicators	• Vendor firmware advisories • Trust-anchor expiry notices (e.g., Secure Boot 2011 CAs, 2026)
Mitigations	• Firmware inventory and update governance • Disable unused management features; isolate BMCs • Measured boot/attestation
Owner (suggested)	Infrastructure / CISO
Target residual	L2 × I2 = 4 (Low)
Scenario link	–

HW-03 – Network-equipment vendor dependency

Category	Hardware and semiconductors (Ch. 5)
Description	Concentrated use of US network/security appliances exposes the organisation to mass-exploited vulnerabilities, cloud-management outages and vendor licensing decisions.
Inherent rating	L4 × I3 = 12 (High); velocity Fast
Key risk indicators	• KEV entries for edge devices • Vendor cloud-management incidents • Licensing/EoL announcements
Mitigations	• Rapid patching of edge devices; attack-surface reduction • Diversity at perimeter for critical sites • Local management fallback
Owner (suggested)	CISO / Network
Target residual	L3 × I2 = 6 (Medium)
Scenario link	–

HW-04 – Semiconductor or hardware supply shock

Category	Hardware and semiconductors (Ch. 5)
Description	A supply shock from any jurisdiction (e.g., Nexperia 2025) delays projects or halts production of the organisation or its suppliers.
Inherent rating	L3 × I3 = 9 (Medium); velocity Medium
Key risk indicators	• Export restrictions by any state • Lead-time increases • Single-source components in BOM
Mitigations	• Component-level dependency mapping for critical products • Buffer stocks and second sources • Supplier contingency clauses
Owner (suggested)	COO / Procurement
Target residual	L2 × I3 = 6 (Medium)
Scenario link	–

HW-05 – Loss of vendor support or spares

Category	Hardware and semiconductors (Ch. 5)
Description	Sanctions, acquisition or end-of-life ends vendor support, spares or updates for installed hardware.
Inherent rating	L2 × I3 = 6 (Medium); velocity Slow
Key risk indicators	• M&A announcements • End-of-life notices
Mitigations	• Lifecycle planning • Third-party maintenance options • Spares strategy
Owner (suggested)	CIO
Target residual	L1 × I3 = 3 (Low)
Scenario link	–

Operating systems and endpoints (Ch. 6)

EP-01 – Faulty or compromised update through vendor channels

Category	Operating systems and endpoints (Ch. 6)
Description	An OS or agent update delivered through vendor update channels disrupts or compromises the endpoint fleet.
Inherent rating	L3 × I4 = 12 (High); velocity Fast
Key risk indicators	• Vendor update incidents • Share of fleet on single update ring
Mitigations	• Staged update rings incl. for content updates • Offline recovery tooling and keys • Golden-image rebuild capability
Owner (suggested)	CIO / CISO
Target residual	L2 × I3 = 6 (Medium)
Scenario link	C – Hyperscaler/IdP outage

EP-02 – Withdrawal of vendor cloud services from endpoints

Category	Operating systems and endpoints (Ch. 6)
Description	Vendor cloud services (identity, MDM, activation, signing) are withdrawn for the organisation, rendering endpoints unmanageable.
Inherent rating	L1 × I5 = 5 (Medium); velocity Fast
Key risk indicators	• Sanctions events • Licensing disputes
Mitigations	• Documented degraded-mode device management • Local admin/break-glass procedures • Pilot alternative management stack
Owner (suggested)	CIO
Target residual	L1 × I4 = 4 (Low)
Scenario link	A – Sanctions designation

EP-03 – App-store removal or platform-policy friction

Category	Operating systems and endpoints (Ch. 6)
Description	Customer-facing apps are removed or restricted by app-store operators, or friction from developer verification affects distribution.
Inherent rating	L2 × I3 = 6 (Medium); velocity Fast
Key risk indicators	• Store policy changes • Government removal requests • Android developer verification rollout (2027 EU)
Mitigations	• Maintain alternative distribution capability (DMA) • Web-based fallback for critical functions • Store-policy monitoring
Owner (suggested)	Digital channels
Target residual	L1 × I3 = 3 (Low)
Scenario link	–

EP-04 – Vendor lifecycle and licensing shocks

Category	Operating systems and endpoints (Ch. 6)
Description	End-of-support, hardware requirements or licensing changes impose forced refresh and cost.
Inherent rating	$L4 \times I2 = 8$ (Medium); velocity Slow
Key risk indicators	• EoL roadmaps • Licence-model changes
Mitigations	• Lifecycle roadmap; budget reserves • Negotiate extended support • Evaluate alternatives for suitable user groups
Owner (suggested)	CIO / CFO
Target residual	$L3 \times I1 = 3$ (Low)
Scenario link	–

Cloud and SaaS (Ch. 7)

CLD-01 – Hyperscale cloud outage

Category	Cloud and SaaS (Ch. 7)
Description	A region, control-plane or global-service outage at a hyperscaler disrupts critical services, including EU-hosted workloads with hidden US dependencies.
Inherent rating	$L4 \times I4 = 16$ (Critical); velocity Fast
Key risk indicators	• Provider outage frequency and post-incident reviews • Share of critical services in single region/provider
Mitigations	• Multi-region design; remove hidden global dependencies • Critical services designed for provider failure (warm standby elsewhere) • Tested continuity runbooks
Owner (suggested)	CIO / CTO
Target residual	$L3 \times I3 = 9$ (Medium)
Scenario link	C – Hyperscaler/IdP outage

CLD-02 – Lock-in prevents exit

Category	Cloud and SaaS (Ch. 7)
Description	The organisation cannot exit or switch providers within acceptable time and cost due to proprietary services, data gravity and skills.
Inherent rating	$L4 \times I3 = 12$ (High); velocity Slow
Key risk indicators	• Proportion of workloads using proprietary PaaS • Untested exit plans • Egress cost exposure
Mitigations	• Portability standards (Kubernetes, open databases, S3-compatible) • Exit plans per critical service, tested • Use Data Act switching rights
Owner (suggested)	CTO
Target residual	$L3 \times I2 = 6$ (Medium)
Scenario link	F – Vulnerability-intelligence lapse

CLD-03 – Commercial shock from dominant vendor

Category	Cloud and SaaS (Ch. 7)
Description	A dominant cloud or virtualisation vendor changes prices, licensing or partner programmes (e.g., Broadcom/VMware).
Inherent rating	L4 × I3 = 12 (High); velocity Medium
Key risk indicators	• Vendor M&A • Licence-model announcements • Renewal quotes
Mitigations	• Multi-year price protection • Avoid single-vendor platforms for core infrastructure • Pre-qualified alternatives
Owner (suggested)	CFO / Procurement
Target residual	L3 × I2 = 6 (Medium)
Scenario link	–

CLD-04 – Sustained loss of productivity suite

Category	Cloud and SaaS (Ch. 7)
Description	The productivity and collaboration suite (M365/Workspace) is unavailable for an extended period due to outage, account suspension or legal denial.
Inherent rating	L2 × I5 = 10 (High); velocity Fast
Key risk indicators	• Provider outages • Sanctions events • Account-security incidents
Mitigations	• Offline copies of critical documents and contacts • Out-of-band communications channel • Pilot European/open-source suite for a defined group
Owner (suggested)	CIO
Target residual	L2 × I3 = 6 (Medium)
Scenario link	A – Sanctions designation

CLD-05 – Sovereignty washing

Category	Cloud and SaaS (Ch. 7)
Description	The organisation relies on 'sovereign' offerings whose controls do not mitigate the exposures it believes they mitigate.
Inherent rating	L3 × I3 = 9 (Medium); velocity Slow
Key risk indicators	• Gap between marketing claims and contractual terms • Absence of external key control • Dependence on US parent for updates
Mitigations	• Evaluate offerings against exposure matrix (Ch. 7) • Contractual verification and audit rights • Independent legal opinion for critical use
Owner (suggested)	CISO / General Counsel
Target residual	L2 × I2 = 4 (Low)
Scenario link	–

CLD-06 – Hidden n-th-party dependency

Category	Cloud and SaaS (Ch. 7)
Description	A European SaaS or service provider depends on US hyperscale infrastructure or services, inheriting their risks without the organisation's awareness.
Inherent rating	$L4 \times I3 = 12$ (High); velocity Fast
Key risk indicators	• Sub-processor lists • DORA register of information gaps
Mitigations	• Require sub-processor and hosting disclosure • Map n-th parties for critical services • Contract notification of changes
Owner (suggested)	Procurement / CRO
Target residual	$L3 \times I2 = 6$ (Medium)
Scenario link	C – Hyperscaler/IdP outage

Identity (Ch. 8)

IAM-01 – Organisation-wide identity lockout

Category	Identity (Ch. 8)
Description	Outage, misconfiguration or suspension of the cloud identity provider locks out users from all federated applications.
Inherent rating	$L3 \times I5 = 15$ (High); velocity Fast
Key risk indicators	• IdP incidents • Conditional-access change failures • Sanctions events
Mitigations	• Break-glass accounts and emergency authentication path independent of primary IdP • Critical systems accessible without cloud IdP • Tested IdP-outage runbook
Owner (suggested)	CISO / CIO
Target residual	$L2 \times I3 = 6$ (Medium)
Scenario link	A – Sanctions designation

IAM-02 – Compromise of IdP infrastructure

Category	Identity (Ch. 8)
Description	Compromise of the identity provider's own infrastructure (e.g., signing keys) enables attacker access to organisational data.
Inherent rating	$L2 \times I5 = 10$ (High); velocity Fast
Key risk indicators	• Provider security incidents and CSRB-type findings • Anomalous token activity
Mitigations	• Phishing-resistant MFA; token-binding where available • Independent logging and detection of identity anomalies • Contractual incident-notification duties
Owner (suggested)	CISO
Target residual	$L2 \times I4 = 8$ (Medium)
Scenario link	–

IAM-03 – Passkey and social-login lock-in

Category	Identity (Ch. 8)
Description	Customers or staff depend on platform-synchronised passkeys and social logins controlled by US platforms.
Inherent rating	L3 × I2 = 6 (Medium); velocity Slow
Key risk indicators	• Share of customers using social login only • Passkey portability progress
Mitigations	• Always offer independent sign-in path • Hardware-bound FIDO2 keys for privileged users • Plan EUDI Wallet acceptance
Owner (suggested)	CISO / Digital channels
Target residual	L2 × I1 = 2 (Low)
Scenario link	–

IAM-04 – Delayed European identity alternatives

Category	Identity (Ch. 8)
Description	Delays in EUDI Wallet roll-out prolong dependence on platform identity for customer onboarding and authentication.
Inherent rating	L4 × I2 = 8 (Medium); velocity Slow
Key risk indicators	• Member State wallet certification • Commission implementing acts
Mitigations	• Prepare for wallet acceptance; participate in pilots • Avoid exclusive reliance on platform identity
Owner (suggested)	Digital channels
Target residual	L3 × I1 = 3 (Low)
Scenario link	–

Security stack (Ch. 9)

SEC-01 – Faulty update from privileged security agent

Category	Security stack (Ch. 9)
Description	A defective update from an EDR/XDR agent crashes or disables a large share of the fleet (CrowdStrike 2024 class event).
Inherent rating	L3 × I5 = 15 (High); velocity Fast
Key risk indicators	• Vendor update practices; customer control of content updates • Concentration of single EDR across all tiers
Mitigations	• Staged rings for all update types • Offline-accessible recovery keys and mass-recovery runbooks • Consider diversity on most critical systems
Owner (suggested)	CISO
Target residual	L2 × I3 = 6 (Medium)
Scenario link	C – Hyperscaler/IdP outage

SEC-02 – Disruption of CVE/NVD ecosystem

Category	Security stack (Ch. 9)
Description	Disruption of CVE assignment or NVD enrichment degrades vulnerability prioritisation and tooling.
Inherent rating	L3 × I3 = 9 (Medium); velocity Medium
Key risk indicators	• CVE contract renewal (current award to 27 Aug 2027) • NVD backlog metrics • CISA budget decisions
Mitigations	• Multiple enrichment sources incl. EUVD, vendor advisories, KEV • Tool configuration not dependent on NVD scores • Participate in ENISA/CSIRT CNA ecosystem
Owner (suggested)	CISO
Target residual	L2 × I2 = 4 (Low)
Scenario link	F – Vulnerability-intelligence lapse

SEC-03 – Security visibility loss or telemetry exposure

Category	Security stack (Ch. 9)
Description	Dependence on US-hosted SIEM/MDR/threat-intelligence services causes loss of visibility in an outage or exposes sensitive telemetry to compelled access.
Inherent rating	L3 × I4 = 12 (High); velocity Fast
Key risk indicators	• SIEM/MDR outages • Location of analyst access • Telemetry residency
Mitigations	• EU residency and customer-managed keys for telemetry • Local copy of critical logs • IR capability not dependent on vendor console
Owner (suggested)	CISO
Target residual	L2 × I3 = 6 (Medium)
Scenario link	–

SEC-04 – Open-source supply-chain compromise or unavailability

Category	Security stack (Ch. 9)
Description	Malicious or unavailable packages on US-hosted registries (npm, PyPI, GitHub) compromise builds or block delivery.
Inherent rating	L4 × I3 = 12 (High); velocity Fast
Key risk indicators	• Registry incidents (e.g., Shai-Hulud 2025) • Unpinned dependencies • Build dependence on live registries
Mitigations	• Internal mirrors/artefact repositories • Pinning, verification, SBOM, provenance (SLSA/Sigstore) • Source backups outside primary platform
Owner (suggested)	CTO / CISO
Target residual	L3 × I2 = 6 (Medium)
Scenario link	–

SEC-05 – Code-signing and platform trust decisions

Category	Security stack (Ch. 9)
Description	Platform code-signing, notarisation or reputation decisions block distribution or execution of software.
Inherent rating	L2 × I3 = 6 (Medium); velocity Medium
Key risk indicators	- Platform policy changes - Certificate revocations
Mitigations	- Maintain signing relationships; monitor policies - Contingency distribution for internal software
Owner (suggested)	CTO
Target residual	L1 × I3 = 3 (Low)
Scenario link	–

SEC-06 – Erosion of US public cyber information sharing

Category	Security stack (Ch. 9)
Description	Policy or funding changes reduce US public threat-intelligence and advisories on which European defenders rely.
Inherent rating	L3 × I2 = 6 (Medium); velocity Slow
Key risk indicators	- CISA capacity - CISA 2015 Act status - Advisory volumes
Mitigations	Diversify to ENISA, CERT-EU, national CSIRTs, ISACs, MISP communities
Owner (suggested)	CISO
Target residual	L2 × I1 = 2 (Low)
Scenario link	F – Vulnerability-intelligence lapse

Artificial intelligence (Ch. 10)

AI-01 – Disruption of AI-enabled processes

Category	Artificial intelligence (Ch. 10)
Description	Provider outage, model deprecation, behaviour change or price change disrupts AI-enabled business processes.
Inherent rating	L4 × I3 = 12 (High); velocity Fast–Medium
Key risk indicators	- Model deprecation notices - API incidents - Price changes
Mitigations	- Model abstraction layer; multi-provider - Regression tests for AI behaviour - Open-weight fallback; manual fallback
Owner (suggested)	CTO / Business owners
Target residual	L3 × I2 = 6 (Medium)
Scenario link	E – AI-compute escalation

AI-02 – Restricted AI compute access

Category	Artificial intelligence (Ch. 10)
Description	Export controls, allocation or price restrict access to GPUs or cloud AI capacity.
Inherent rating	L2 × I3 = 6 (Medium); velocity Medium
Key risk indicators	• BIS rules • GPU pricing • EU AI Gigafactory progress
Mitigations	• Diversified compute sources; efficiency • Reserved capacity for critical workloads
Owner (suggested)	CTO
Target residual	L2 × I2 = 4 (Low)
Scenario link	E – AI-compute escalation

AI-03 – Confidential data exposure via AI services

Category	Artificial intelligence (Ch. 10)
Description	Confidential data sent to US AI services is exposed to compelled access or provider misuse.
Inherent rating	L3 × I4 = 12 (High); velocity Fast
Key risk indicators	• Shadow AI usage • Provider terms changes
Mitigations	• Data-classification rules for AI use • EU-operated or self-hosted models for sensitive data • Contractual no-training/retention limits
Owner (suggested)	CISO / DPO
Target residual	L2 × I3 = 6 (Medium)
Scenario link	D – Transfer-basis collapse

AI-04 – Loss of European AI option via acquisition

Category	Artificial intelligence (Ch. 10)
Description	A European AI provider used by the organisation is acquired by a non-EU entity or changes control.
Inherent rating	L3 × I2 = 6 (Medium); velocity Medium
Key risk indicators	• M&A announcements (e.g., Cohere–Aleph Alpha) • Funding rounds led by non-EU investors
Mitigations	• Change-of-control clauses • Portable integrations; alternative providers qualified
Owner (suggested)	Procurement
Target residual	L2 × I1 = 2 (Low)
Scenario link	–

AI-05 – AI Act compliance gaps from provider information

Category	Artificial intelligence (Ch. 10)
Description	Insufficient information or cooperation from non-EU model providers creates AI Act compliance gaps for deployers.
Inherent rating	L3 × I3 = 9 (Medium); velocity Slow
Key risk indicators	• Provider GPAI documentation • Code of Practice participation
Mitigations	• Contractual information and cooperation duties • AI inventory and risk classification
Owner (suggested)	Compliance / DPO
Target residual	L2 × I2 = 4 (Low)
Scenario link	–

Payments and communications (Ch. 11)

FIN-01 – Card-payment exclusion

Category	Payments and communications (Ch. 11)
Description	Persons connected with the organisation, or (very unlikely) the organisation at scale, cannot use card payments due to scheme decisions or sanctions.
Inherent rating	L2 × I3 = 6 (Medium); velocity Fast
Key risk indicators	• Sanctions on individuals • Scheme policy changes
Mitigations	• Alternative payment rails (SEPA Instant, Wero, domestic schemes) • Corporate payment contingency for exposed staff
Owner (suggested)	CFO / Treasury
Target residual	L1 × I2 = 2 (Low)
Scenario link	A – Sanctions designation

FIN-02 – Mobile wallet dependency

Category	Payments and communications (Ch. 11)
Description	Changes by Apple/Google wallet operators affect payment channels.
Inherent rating	L2 × I2 = 4 (Low); velocity Medium
Key risk indicators	• Wallet terms changes • DMA/NFC enforcement
Mitigations	• Support third-party wallets via NFC access • Account-to-account options
Owner (suggested)	Head of Payments
Target residual	L1 × I2 = 2 (Low)
Scenario link	–

FIN-03 – Loss of collaboration platform without out-of-band channel

Category	Payments and communications (Ch. 11)
Description	Primary collaboration/messaging platform is lost during a crisis, and no independent channel exists.
Inherent rating	L3 × I4 = 12 (High); velocity Fast
Key risk indicators	• Absence of tested out-of-band channel • Provider outages
Mitigations	• Independent crisis channel (e.g., self-hosted Matrix, Threema, phone trees) • Regular crisis-comms drills
Owner (suggested)	COO / CISO
Target residual	L2 × I2 = 4 (Low)
Scenario link	A – Sanctions designation

FIN-04 – Marketing, analytics and public-comms disruption

Category	Payments and communications (Ch. 11)
Description	Platform policy, account action or transfer-law changes disrupt marketing, analytics or public communications.
Inherent rating	L3 × I2 = 6 (Medium); velocity Medium
Key risk indicators	• DPA decisions on analytics • Platform account actions
Mitigations	• Owned channels; EU analytics alternatives • Consent and transfer compliance
Owner (suggested)	CMO / Comms
Target residual	L2 × I1 = 2 (Low)
Scenario link	D – Transfer-basis collapse

FIN-05 – Over-compliance by EU financial providers

Category	Payments and communications (Ch. 11)
Description	European banks or PSPs restrict the organisation, staff or customers beyond legal requirements.
Inherent rating	L2 × I3 = 6 (Medium); velocity Fast
Key risk indicators	• Account closures linked to US sanctions
Mitigations	• Multiple banking relationships • Supervisory escalation
Owner (suggested)	CFO
Target residual	L1 × I3 = 3 (Low)
Scenario link	A – Sanctions designation

Governance and organisation (Ch. 12, 15)

GOV-01 – Insufficient visibility of dependencies

Category	Governance and organisation (Ch. 12, 15)
Description	The organisation lacks a complete view of its technology dependencies, including jurisdiction and n-th parties.
Inherent rating	L4 × I3 = 12 (High); velocity Slow
Key risk indicators	- Coverage of dependency map - DORA/NIS2 register completeness
Mitigations	- Build and maintain dependency map with jurisdiction and substitutability - Integrate with procurement and architecture review
Owner (suggested)	CRO / CIO
Target residual	L2 × I2 = 4 (Low)
Scenario link	–

GOV-02 – Non-compliance with third-party and exit requirements

Category	Governance and organisation (Ch. 12, 15)
Description	Failure to meet NIS2/DORA supplier-risk, concentration and exit-strategy requirements leads to supervisory action.
Inherent rating	L3 × I4 = 12 (High); velocity Medium
Key risk indicators	- Supervisory findings - Audit observations
Mitigations	Map obligations to risks; documented exit plans; testing evidence
Owner (suggested)	CRO / Compliance
Target residual	L2 × I2 = 4 (Low)
Scenario link	–

GOV-03 – Skills and organisational lock-in

Category	Governance and organisation (Ch. 12, 15)
Description	Skills, certifications and processes are built around single vendor ecosystems, making change slow and risky.
Inherent rating	L4 × I2 = 8 (Medium); velocity Slow
Key risk indicators	- Vendor-specific skill concentration - Training budgets
Mitigations	- Invest in portable skills (open standards, Linux, Kubernetes) - Rotate staff across platforms
Owner (suggested)	CIO / HR
Target residual	L3 × I1 = 3 (Low)
Scenario link	–

GOV-04 – Exit and continuity plans untested

Category	Governance and organisation (Ch. 12, 15)
Description	Exit strategies and continuity plans exist on paper but have never been exercised, so they fail when needed.
Inherent rating	L4 × I3 = 12 (High); velocity Slow
Key risk indicators	• Date of last exercise • Exercise findings closed
Mitigations	• Annual tabletop (Ch. 14) and technical exit drills for top services • Board reporting on results
Owner (suggested)	CRO / COO
Target residual	L2 × I2 = 4 (Low)
Scenario link	All scenarios

6. Maintaining the register

From the book: a register is only useful if it is maintained. The book recommends the following cadence:

- **Quarterly:** second-line review of KRIs; update likelihood ratings for legal and geopolitical risks in light of developments (FISA 702, DPF litigation, sanctions designations, export-control rules, trade disputes).
- **Semi-annually:** first-line owners attest to the status of mitigations; open findings from tests and exercises are tracked to closure.
- **Annually:** full re-rating, linked to the DORA register of information or NIS2 supply-chain risk assessment; board review together with the results of the scenario exercises in Chapter 14.
- **Event-driven:** re-rating within ten working days after a trigger event (for example a new sanctions designation affecting the sector, a major provider outage, a CJEU ruling, or a change of control at a critical provider).

Integration with existing processes matters more than the register's format. Each new procurement of a critical technology service should be checked against the register (does it add to an existing concentration? which risk IDs does it affect?), and architecture review boards should be asked to state which register entries a design change improves or worsens.

7. Using this register in GRCompliance

GRCompliance is a self-hosted governance, risk and compliance platform from the same author. This section describes how an organisation can load the 56 risks into it and manage them. It describes features in the open-source GRCompliance Core as of 26 October 2026; screens and labels can change between releases.

7.1 Getting started

- **Try it first.** The demo at demo.grcompliance.com is a temporary server that is reset every week. Do not enter confidential data there.
- **Install your own.** GRCompliance Core is a free download on GitHub (repository Sectutor/GRCompliance-Core) and runs with Docker on your own or EU infrastructure, so the register does not need to sit with another third-party provider.
- **Community edition (free).** It includes the risk register, controls, policies and evidence. A Community instance holds one workspace of your own plus the seeded “Latore LTD” demo workspace, which is useful for practice. More workspaces and the premium features need a commercial licence from grcompliance.com. There is no free trial of the paid editions.

More information: grcompliance.com

7.2 Set up the method before loading risks

In **Risk Management** › **Risk Framework**, record the risk-management scope and context, the risk appetite statement and tolerances, and the methodology (ISO 27005 by default, which matches the book's approach). Under **Risk Criteria**, enter the book's likelihood and impact descriptions from Section 2 so that everyone rates against the same scales. The same page shows a risk heat map.

Bands differ. GRCompliance scores risks as likelihood × impact on the same 5 × 5 matrix, so the numeric scores match the book. It applies its own five band labels, however: Low (1–3), Medium (4–8), High (9–14), Very High (15–19) and Critical (20–25). The book uses four bands (Low 1–4, Medium 5–9, High 10–15, Critical 16–25). A book score of 9, for example, is Medium in the book and High in GRCompliance. Compare the numeric scores, and keep the book's band in the risk description if you need it for reporting.

7.3 Load the 56 risks

Option A – Add each risk (all editions). In **Risk Management** › **Risk Register**, choose **Add Risk**. The wizard records a title, a description, likelihood and impact (1–5), a risk owner, a treatment strategy, a priority and the controls that treat the risk. For each register entry:

1. Title: put the book ID in front of the title, for example “LEG-01 – Compelled disclosure via US provider”. GRCompliance gives each risk its own reference number (RA-year-number), so the title is where the book ID is kept.
2. Description: paste the book's description. Add the category, velocity, target residual rating and scenario link at the end, because the risk record has no dedicated fields for them.
3. Likelihood and impact: enter the book's inherent ratings, then re-rate them for your organisation, as the book advises.
4. Owner: GRCompliance assigns the owner from the users in the workspace. Turn the book's suggested owner role (for example CISO / DPO) into a named person.

Option B – Spreadsheet import (paid editions). Paid editions include a Spreadsheet Importer under **Settings** › **Backup & Restore**. It reads a CSV file and lets you map columns to risk title, description, likelihood (1–5), impact (1–5) and status. A row whose title matches an existing risk updates it, and other rows are added. A CSV of this register laid out for this importer is part of the \$49 book bundle on sectutor.com. Its first five columns are named after those fields, and the book ID is part of each title. After an import, check that the entries appear as expected in your instance, then add owners, treatments and controls as in Option A.

7.4 Treat the risks: mitigations, owners and controls

The book's mitigations become **treatments**. Each treatment has a type (mitigate, transfer, accept or avoid), a strategy description, an owner, a due date, a priority, an estimated cost and a status (planned, in progress, implemented, verified). Treatments can be linked to controls with a rating of how effective each control is. **Risk Management** › **Treatment Plan** lists every treatment with its owner, due date, cost and status, which gives the semi-annual owner attestation in Section 6 a single place to work from.

GRCompliance calculates a residual score from the treatment and the linked controls rather than taking a typed-in target. Use the book's target residual rating as the goal, and compare the calculated residual with it once the mitigations are in place and tested.

Mapping to frameworks. The control library includes ISO 27001:2022 and NIS2 Article 21 controls, and evidence is linked to controls. Linking a treatment to a control therefore connects a dependence risk to the framework requirement and the evidence behind it. Relevant controls include ISO 27001 A.5.19 (supplier relationships), A.5.23 (cloud services, including exit), A.5.30 (ICT readiness for business continuity) and A.8.13 (information backup), and NIS2 Article 21(2)(c) (business continuity) and 21(2)(d) (supply chain security). These are examples. Choose the controls that match your own control set.

7.5 Monitor KRIs and report

- **Key risk indicators.** Under **Risk Framework** › **Key Risk Indicators**, create a KRI for each indicator you will track, with green, amber and red thresholds, a current value and status, and an owner. KRIs are kept as their own list rather than attached to a single risk, so start each KRI name with the risk ID it monitors (for example “LEG-01 – Status of FISA 702 reauthorisation”).
- **Dashboard and indicators.** The risk dashboard shows overdue items and upcoming deadlines. The Risk Assessments page shows overdue risk reviews, risks scoring 15 or more that have no treatment, and the share of risks whose residual score is below the inherent score.
- **Board reporting. Risk Reports** lets you draft a risk-management report (executive summary, scope, methodology, key findings, recommendations and conclusions) and export it as a Word document or as Markdown. The export includes the register table, which supports the book’s advice that the CRO reports the register to the board at least annually and after material events.
- **Audit trail.** Changes to risks are written to the activity log.

7.6 Keep the book’s caveats

When the register is loaded into GRCompliance or any other tool, the book’s ratings remain a starting point. Re-rate each risk for your organisation, read the risks together with the scenarios, and treat residual ratings as targets that are only reached once mitigations are implemented and tested.

Next steps

This register is one part of a wider body of work. If it is useful, these are the places to go next.

Read the book

Single Point of Failure: Managing Europe's Dependence on US Technology is coming soon from Sectutor. The book explains the evidence behind each of the 56 risks. It also includes seven tabletop scenarios, ten questions for the board to ask management and a 24-month management playbook. Details will be at sectutor.com.

Work with an editable copy

The book bundle on sectutor.com (\$49) includes the book, the register as an editable Word document, and a CSV of the 56 risks laid out for import into GRCompliance. The editable copy lets you re-rate the risks, assign named owners and add your own entries.

Manage the risks in GRCompliance

To see how the register works in practice, try the demo at demo.grcompliance.com. It is reset every week, so do not enter confidential data. To run GRCompliance on your own infrastructure, GRCompliance Core is a free download on GitHub (repository [Sectutor/GRCompliance-Core](https://github.com/Sectutor/GRCompliance-Core)). The Community edition is free and includes the risk register, controls, policies and evidence.

More information: grcompliance.com

Source: Single Point of Failure: Managing Europe's Dependence on US Technology, Chapter 13 (Consolidated Risk Register), manuscript v0.9, 26 October 2026. © Sectutor. This register is not legal advice.