Enterprise Risk Register & Residual-Risk Treatme...

ISO 31000 framing ? ISO 27005 ? ISO 42001 Cl. 6.1

Tenant: demo-tenant
Framework: ISO 31000 + ISO 27005 + ISO 42001
Period: 2026-01-01 ? 2026-03-31
Generated: 2026-04-01T09:00:00Z

Metrics

Risks registered: 87
Residual-high (top quartile): 8
Treatments in flight: 14
Risks closed (Q1 2026): 11
Open Risk-Acceptance memos: 3
Median time-to-treatment (days): 47
Treatment-plan signoff cadence: Quarterly

Residual-high risks (top quartile)

Eight risks remain in the top quartile after treatment; CEO + CFO + CISO + DPO co-signed.

Record 1
id: R-014
title: Insider ? privileged ops
likelihood: 2
impact: 4
residual: 8
treatment: Just-in-time access (in roll-out)

Record 2
id: R-021
title: Vendor concentration (IdP)
likelihood: 2
impact: 4
residual: 8
treatment: Second IdP onboarded; dual-write in design

Record 3
id: R-028
title: Endpoint coverage (BYOD)
likelihood: 3
impact: 3
residual: 9
treatment: MDM extension Q2 2026

Record 4
id: R-041
title: Model-drift on AIS-001
likelihood: 3
impact: 4
residual: 12
treatment: Drift-detection rule + retrain trigger live

Record 5
id: R-052
title: Sub-processor outage
likelihood: 2
impact: 3
residual: 6

treatment: Failover playbook tested 2026-03-12

Record 6

id: R-073
title: DSAR backlog
likelihood: 3
impact: 2
residual: 6
treatment: Self-serve DSAR portal ? Q3 2026

Record 7

id: R-088
title: Phishing ? finance team
likelihood: 4
impact: 3
residual: 12
treatment: FIDO2-mandatory + quarterly tabletop

Record 8

id: R-095
title: EU AI Act re-classification
likelihood: 1
impact: 5
residual: 5
treatment: Outside counsel retained; FRIA refresh underway

Treatment-plan progress

14 treatments in flight; per-treatment milestone + owner + due.

Record 1

treatment: Just-in-time access
owner: IAM platform team
due: 2026-06-30
pct complete: 65

Record 2

treatment: Second IdP onboarding
owner: Identity platform team
due: 2026-07-15
pct complete: 45

Record 3

treatment: MDM BYOD extension
owner: Endpoint security
due: 2026-08-31
pct complete: 30

Record 4

treatment: FIDO2 + tabletop
owner: CISO office
due: 2026-06-01
pct complete: 80

Risk-acceptance memos

Three open memos; each signed by C-level owner + retention scheduled.

Record 1

id: RA-2026-003
risk: Vendor concentration (IdP)
owner: CISO
retention until: 2027-01-01

Record 2

id: RA-2026-007
risk: DSAR backlog over 30d
owner: DPO
retention until: 2026-09-30

Record 3

id: RA-2026-009
risk: EU AI Act re-classification
owner: GC + CEO
retention until: 2026-12-31