

Training Proposal Certified Risk Professional training (ISO 31000:2018, ISO 27001:2022, ISO 22301:2019) tailored for EGRC Archer Team

Technological advantages

Standards-to-solution mapping in Archer: Establish a canonical risk taxonomy (ISO 31000), control library and Annex A mappings (ISO 27001), and BIA/continuity data models (ISO 22301) to drive consistent design patterns across Archer applications. Accelerated solution delivery: Reusable content blueprints for risk assessment, control testing, issues/observations, and plan exercises reduce configuration cycles by 20–30% and lower rework.

Automation and integration uplift: Systematic use of Archer APIs, Data Feeds, job schedulers, and connectors to automate evidence collection, risk scoring updates, and plan-testing workflows—targeting a 15–25% reduction in manual steps.

Data quality and traceability by design: Standardized metadata (risk criteria, control IDs, asset catalogs) improves lineage and report fidelity; consistent change artifacts enhance CAB throughput.

Advanced analytics readiness: Training lays the groundwork for scenario analysis, risk heatmaps, and control effectiveness dashboards; enables integration with quantification tools and data lakes for trend analytics.

Futuristic growth opportunities

Risk quantification and scenario modeling: Enable FAIR-aligned or scenario-based quantification via Archer extensions/integrations to support capital allocation and prioritization decisions.

AI-assisted control and evidence management: Governed use of LLMs to pre-classify evidence, summarize test results, and flag control gaps, with human-in-the-loop review.

DORA and resilience-by-default: Codify incident parent–child relationships, impact thresholds, and severe incident reporting aligned to DORA; scale playbooks and continuity exercises.

Cloud/SaaS migration readiness: Standardized control mappings and portability patterns (control-as-data, risk-as-data) de-risk Archer-to-SaaS transitions and multi-instance governance.

Third-party and cyber fusion: Harmonize ISO 27001 controls with vendor risk and vulnerability inputs to enable continuous control monitoring and adaptive risk scoring.

Organizational benefits

Faster, consistent risk decisions: Common methods and criteria shorten assessment/approval cycles by 25–40% and reduce decision variance across squads and regions.

Resilience and recovery outcomes: ISO 22301-aligned BIAs and exercise programs improve plan coverage and test pass rates (target 90%+), reduce RTO/RPO breaches, and enhance incident readiness.

Cost optimization: Automation and reusable patterns lower configuration and operations effort (10–20% FTE savings over 12 months) and reduce duplicated tooling/processes.

Talent development and engagement: Clear skill paths for engineers and developers increase certification rates and internal mobility; cross-squad ceremonies and blameless RCA strengthen culture.