KRITSOL.

Practical Resources: Technical Scoping & Framework Integration Matrix

A strategic reference outline covering operational mapping methods, documentation parameters, and control-testing criteria for seamless advisory practice extension.

Author: Practice Extension Support Team
Date: September 2026
Classification: Public Reference

1. ISO 27001 Audit Preparation

This resource maps the operational steps and evidence-gathering targets required to prepare a client's Information Security Management System (ISMS) for formal certification evaluation. KRITSOL functions as an organic extension of your team by organizing control registers, tracking pre-audit validation mapping, and compiling evidence files directly within your sovereign environment to ensure full readiness prior to Stage 1 and Stage 2 audits.

Control Domain	Documentation & Evidence Targets	Extension Testing Approach
A.5.15 Access Control	User provisioning logs, multi-factor authentication (MFA) enforcement policies, and quarterly privilege access review sign-offs.	Verify active directory configurations, test separation of duties (SoD), and sample joiner/mover/leaver tickets.
A.8.20 Network Security	Firewall rule-base reviews, network architecture diagrams, intrusion detection/prevention logs, and penetration test remediations.	Review configuration parameters against hardening checklists; organize documentation evidence into the client repository.
A.8.24 Use of Crypto	Encryption keys management policy, cryptographic algorithm standards, and data-at-rest/in-transit validation records.	Inspect cryptographic parameters across sample database endpoints and cloud storage buckets.

2. NIST 800-53 Control Mapping

Designed for advisory practices supporting organizations navigating federal or enterprise cybersecurity baselines, this technical scoping matrix outlines standard operational criteria across key NIST Special Publication 800-53 security control families. Our delivery team plugs into your testing cadences to perform control assessments, document operating-effectiveness indicators, and update Plan of Action and Milestones (POA&M;) logs.

Control Family	Technical Scoping / Tracking Metrics	Extension Testing Approach
AC-2 Account Mgmt	Account creation, activation, modification, and termination tracking matrices. Emergency/Group account restriction logs.	Document walkthrough steps, examine automated account lockouts, and confirm periodic account re-certifications.
AU-2 Event Logging	Audit record generation parameters, system-wide log coverage maps, and central SIEM retention policies.	Validate log ingestion states for critical assets and cross-check configuration scripts against standard baseline baselines.

CM-2 Baselines	Configuration management plans, master gold-image inventories, and unauthorized software monitoring records.	Examine system integrity check reports and sample change-management tickets for adherence to approval hierarchies.

3. EU AI Act Gap Assessment

As regulated industries confront cross-border digital compliance mandates, this framework tracking tool summarizes the core documentation criteria for emerging Artificial Intelligence governance models. We support your practice's transformation assurance workflows by building inventory tracking templates, reviewing risk classification matrices, and evaluating model transparency documentation to establish baseline operational compliance readiness.

Compliance Area	Core Documentation Criteria	Extension Testing Approach
Art. 6 System Classification	High-risk AI use-case inventories, safety component assessments, and systemic biometrics impact records.	Review internal AI system registers, track deployment flags, and verify conformity documentation files.
Art. 9 Risk Mgmt System	Structured testing logs, data asset bias evaluations, and continuous post-market monitoring plan frameworks.	Perform analysis of data governance documentation and track known risk remediation vectors in readiness logs.
Art. 13 Transparency	User instruction manuals, algorithmic output explanation papers, and model deployment metadata registers.	Verify presence and operational clarity of user guidelines against baseline disclosure frameworks.