1. Scope & AI System Inventory

• AI systems identified across the organization

• Data flows mapped to ISMS assets

• Ownership and accountability assigned

Score (1–5): _____

2. AI Risk Assessment Integration

• AI-specific risks added to ISMS register

• Bias, adversarial attacks, and model poisoning covered

• Shadow AI monitored and reported

Score (1–5): _____

3. Policy & Procedure Enhancements

• AI Governance Policy created

• Acceptable use, data classification, and change management updated

• AI vendor evaluations included

Score (1–5): _____

4. Governance Structure & Roles

• AI Product Owner, Model Risk Manager roles defined

• Cross-functional AI committee established

• Ethical review process implemented

Score (1–5): _____

5. AI Asset & Lifecycle Management

• AI models registered as assets

• Versioning, lineage, and purpose documented

• Retraining and retirement managed through ISMS change controls

Score (1–5): _____

6. ISO 42001-to-ISO 27001 Control Mapping

• Annex A controls cross-mapped

• Evidence repositories linked

• Duplicate controls minimized

Score (1–5): _____

7. AI Security Awareness & Training

• Responsible AI modules added

• Bias, fairness, and prompt safety included

• Practical real-world scenarios taught

Score (1–5): _____

8. Internal AI Audit Program

• AI-specific audits scheduled

• Bias testing, dataset security reviewed

• Shadow AI scans conducted

Score (1–5): _____

9. Regulatory Alignment & Compliance

• AI regulatory requirements mapped

• Documentation traceability established

• Compliance evidence updated regularly

Score (1–5): _____

10. AI Ethics, Transparency & Trust

• Model transparency practices defined

• Ethical guidelines implemented

• Customer and stakeholder trust considerations documented

Score (1–5): _____