

Compliance Assessment Matrix for Risk Evaluation

Project/Area: [Insert Name Here]

Requirement	Control/Criteria	Compliant (Yes/No/Partial)	Risk Level (Low/Medium/High)	Gaps/Issues Identified	Recommended Action	Owner	Due Date
Data Protection	GDPR Article 5 – Data processing principles	Partial	High	Data retention policy incomplete	Update retention policy; staff training	John Doe	2024-07-15
IT Security	ISO 27001 – Access Control	No	High	No MFA on admin accounts	Implement MFA on all admin accounts	Jane Smith	2024-07-10
Operations	SOC2 – Incident Response	Yes	Low	None	Maintain current procedures	Amir Bilal	N/A
Finance	SOX – Segregation of Duties	Partial	Medium	Overlap in invoicing & approval process	Review and revise process flow	Sandra Lee	2024-08-01

Important Notes

- This matrix should be periodically updated to reflect ongoing compliance activities and risk changes.
- Each gap or issue should have clear owners and realistic timelines for remediation.
- Documentation and evidence supporting compliance should be referenced or appended.
- Risk levels should be consistently evaluated based on organizational criteria.
- This matrix supports audit readiness and proactive risk management.