vCISO AI Compliance Checklist

1. Governance & Accountability

- ☐ Assign AI governance ownership (board, CISO, product owner).
- ☐ Define escalation paths for AI incidents.
- ☐ Align AI initiatives with organizational risk appetite and compliance obligations.

2. Policy Development

- ☐ Establish AI policies on ethics, fairness, transparency, security, and privacy.
- ☐ Define rules for sensitive data usage and regulatory compliance (GDPR, HIPAA, CCPA).
- ☐ Document roles, responsibilities, and AI lifecycle procedures.

3. Data Governance

- ☐ Ensure training and inference data quality, lineage, and access control.
- ☐ Track consent, privacy, and anonymization requirements.
- ☐ Audit datasets periodically for bias or inaccuracies.

4. Model Oversight

- ☐ Validate models before production deployment.
- ☐ Continuously monitor for bias, drift, or unintended outcomes.
- ☐ Maintain a model inventory and lifecycle documentation.

5. Monitoring & Logging

Please reach out to us at info@deurainfosec.com ☎ +1(707) 998 5164

- ☐ Implement logging of AI inputs, outputs, and behaviors.
- ☐ Deploy anomaly detection for unusual or harmful results.
- ☐ Retain logs for audits, investigations, and compliance reporting.

6. Human-in-the-Loop Controls

- ☐ Enable human review for high-risk AI decisions.
- ☐ Provide guidance on interpretation and system limitations.
- ☐ Establish feedback loops to improve models and detect misuse.

7. Transparency & Explainability

- ☐ Generate explainable outputs for high-impact decisions.
- ☐ Document model assumptions, limitations, and risks.
- ☐ Communicate AI capabilities clearly to internal and external stakeholders.

8. Continuous Learning & Adaptation

- ☐ Retrain or retire models as data, risks, or regulations evolve.
- ☐ Update governance frameworks and risk assessments regularly.
- ☐ Monitor emerging AI threats, vulnerabilities, and best practices.

9. Integration with Enterprise Risk Management

- ☐ Align AI governance with ISO 27001, ISO 42001, NIST AI RMF, or similar standards.
- ☐ Include AI risk in enterprise risk management dashboards.
- ☐ Report responsible AI metrics to executives and boards.
