AI Governance, Risk and Compliance (GRC) Assessment

Executive Summary

This document provides a comprehensive assessment framework for evaluating an organization's compliance with AI Governance, Risk and Compliance (GRC) requirements. Based on ISO 42001, CIS Controls, and NIST Cybersecurity Framework (CSF), this assessment helps organizations identify gaps in their AI governance practices and develop remediation plans.

The assessment is organized into seven domains covering the full spectrum of AI security and literacy:

1. AI Governance and Risk Management
2. AI Data Governance and Privacy
3. AI Model Development and Security
4. AI Operations and Deployment
5. AI Incident Response and Recovery
6. AI Transparency and Explainability
7. AI Literacy and Training

Each domain contains assessment questions with corresponding control references, compliance criteria, and remediation recommendations. This matrix-style assessment allows organizations to clearly identify controls that are compliant versus those out of compliance.

How to Use This Assessment

1. **Assessment Preparation:** Gather relevant documentation, including AI policies, procedures, risk assessments, and training materials.
2. **Compliance Evaluation:** For each question, determine the compliance status (Compliant, Partially Compliant, Non-Compliant, or Not Applicable) and document supporting evidence.
3. **Gap Analysis:** For items that are not fully compliant, document the specific gaps and assign a priority level (High, Medium, Low).
4. **Remediation Planning:** Use the provided remediation recommendations to develop an implementation plan with timelines and responsible parties.
5. **Progress Tracking:** Regularly update the assessment to track remediation progress and overall compliance improvement.

AI Governance vs. Cybersecurity GRC

It's important to note that AI Governance differs from traditional Cybersecurity GRC in several key ways:

- AI Governance focuses primarily on input/output data and associated outcomes
- Traditional Cybersecurity GRC operates within a total enterprise risk methodology
- AI security requires specialized roles like the Chief AI Security Officer (CAISO) and AI Governance Certifier (AIGC)
- AI Security Operations Centers (AiSOCs) have unique requirements compared to traditional SOCs

This assessment framework accounts for these differences by incorporating AI-specific controls and considerations throughout all domains.

Key Benefits

- Comprehensive coverage of AI governance, risk, and compliance requirements
- Alignment with leading industry frameworks (ISO 42001, CIS, NIST CSF)
- Practical remediation recommendations for addressing compliance gaps
- Flexible format that can be used for both pre- and post-engagement assessments
- Clear documentation of compliance status for stakeholder reporting

AI Governance, Risk and Compliance (GRC) Assessment

Based on ISO 42001, CIS Controls, and NIST CSF frameworks