AI Governance, Risk and Compliance (GRC) Assessment

Complete Question Matrix

Domain 1: AI Governance and Risk Management

No.	Question	Control Reference	Remediation
1.1	Does the organization have a documented AI governance policy that aligns with ISO 42001?	ISO 42001 Section 5.2 (AI Policy)	Develop and implement an AI governance policy that establishes principles, roles, and responsibilities for AI systems management, aligned with ISO 42001 requirements
1.2	Has the organization established a formal AI risk assessment methodology?	NIST AI RMF (MAP function), ISO 42001 Section 6.1	Implement a structured AI risk assessment methodology based on NIST AI RMF MAP function, including context analysis, risk identification, and impact assessment
1.3	Are AI governance roles and responsibilities clearly defined, including CAISO and AIGC roles?	ISO 42001 Section 5.3, NIST CSF 2.0 (GOVERN function)	Define and document AI governance roles and responsibilities, establish CAISO and AIGC positions with appropriate authority and resources
1.4	Does the organization maintain an inventory of all AI systems and their risk classifications?	CIS Control 1, NIST AI RMF (MAP function)	Create and maintain a comprehensive inventory of all AI systems with appropriate risk classifications based on potential impact
1.5	Is there a process for regular review and approval of AI systems before deployment?	ISO 42001 Section 8.1, NIST AI RMF (MEASURE function)	Establish a formal AI system review and approval process that includes security, ethics, and compliance assessments before deployment
1.6	Does the organization have metrics to measure the effectiveness of AI governance controls?	ISO 42001 Section 9.1, NIST CSF 2.0 (GOVERN function)	Develop and implement metrics to measure AI governance effectiveness, with regular reporting to leadership

Domain 2: AI Data Governance and Privacy

No.	Question	Control Reference	Remediation
2.1	Does the organization have a documented data governance framework specific to AI training and operational data?	ISO 42001 Section 7.5, NIST AI RMF (MAP function)	Develop and implement an AI-specific data governance framework that addresses data quality, privacy, and security throughout the AI lifecycle
2.2	Are there processes to assess and mitigate bias in AI training data?	NIST AI RMF (MEASURE function), ISO 42001 Section 8.2	Implement formal processes for bias assessment in training data, including diverse data sampling, statistical analysis, and regular bias audits
2.3	Does the organization maintain data lineage and provenance tracking for AI systems?	CIS Control 3, NIST AI RMF (MAP function)	Establish data lineage and provenance tracking systems that document the origin, transformations, and usage of all AI-related data
2.4	Are there data protection controls specific to AI training datasets and model outputs?	CIS Control 3, ISO 42001 Section 8.3	Implement enhanced data protection controls for AI datasets, including encryption, access controls, and data minimization techniques
2.5	Does the organization have a data retention and disposal policy for AI training data?	CIS Control 3, NIST CSF 2.0 (PROTECT function)	Develop and implement a data retention and disposal policy specific to AI training data that complies with relevant regulations and minimizes risk
2.6	Is there a process for regular data quality assessment for AI systems?	ISO 42001 Section 9.1, NIST AI RMF (MEASURE function)	Establish formal data quality assessment processes for AI systems, including completeness, accuracy, and relevance checks

Domain 3: AI Model Development and Security

No.	Question	Control Reference	Remediation
3.1	Does the organization follow a secure AI model development lifecycle?	ISO 42001 Section 8.1, NIST AI RMF (MANAGE function)	Implement a secure AI model development lifecycle that includes security requirements, threat modeling, and security testing at each phase
3.2	Is there comprehensive documentation for all AI models, including version control?	ISO 42001 Section 7.5, CIS Control 2	Establish standardized documentation practices for AI models, including architecture, parameters, training methods, and version control
3.3	Are AI models tested for security vulnerabilities before deployment?	CIS Control 16, NIST CSF 2.0 (PROTECT function)	Implement comprehensive security testing for AI models, including adversarial testing, input validation, and output filtering
3.4	Does the organization assess and manage supply chain risks for AI components?	CIS Control 15, NIST CSF 2.0 (IDENTIFY function)	Develop and implement a supply chain risk management program for AI components, including vendor assessment and component verification
3.5	Are there processes for secure model updates and versioning?	CIS Control 7, ISO 42001 Section 8.1	Establish formal processes for secure model updates, including testing, approval, and rollback capabilities
3.6	Does the organization perform regular security assessments of third-party AI models?	CIS Control 15, NIST AI RMF (MEASURE function)	Implement a program for regular security assessments of third-party AI models, including documentation review, testing, and compliance verification

Domain 4: AI Operations and Deployment

No.	Question	Control Reference	Remediation
4.1	Does the organization implement secure deployment practices for AI systems?	CIS Control 4, NIST CSF 2.0 (PROTECT function)	Develop and implement secure deployment procedures for AI systems, including configuration management, environment separation, and deployment verification
4.2	Is there continuous monitoring of AI systems in production for security anomalies?	CIS Control 13, NIST AI RMF (MEASURE function)	Implement continuous monitoring solutions for AI systems that detect security anomalies, unexpected behaviors, and performance issues
4.3	Are there robust access controls and authentication mechanisms for AI systems?	CIS Control 6, ISO 42001 Section 8.3	Establish strong access controls for AI systems, including multi-factor authentication, role-based access, and privilege management
4.4	Does the organization maintain comprehensive logs of AI system operations and access?	CIS Control 8, NIST CSF 2.0 (DETECT function)	Implement comprehensive logging for AI systems, including system operations, access attempts, and administrative actions
4.5	Are there processes to detect and address model drift or performance degradation?	ISO 42001 Section 9.1, NIST AI RMF (MEASURE function)	Establish processes to detect and address model drift, including performance monitoring, statistical analysis, and remediation procedures
4.6	Does the organization have secure configuration standards for AI infrastructure?	CIS Control 4, NIST CSF 2.0 (PROTECT function)	Develop and implement secure configuration standards for AI infrastructure, including servers, networks, and cloud environments

Domain 5: AI Incident Response and Recovery

No.	Question	Control Reference	Remediation
5.1	Does the organization have AI-specific incident response procedures?	CIS Control 17, NIST CSF 2.0 (RESPOND function)	Develop and implement AI-specific incident response procedures that address unique AI failure modes, security incidents, and ethical breaches
5.2	Are there capabilities to roll back AI systems to previous versions in case of incidents?	CIS Control 11, NIST CSF 2.0 (RECOVER function)	Implement and test AI system rollback capabilities, including version control, configuration backups, and deployment automation
5.3	Does the organization maintain backups of AI models, training data, and configurations?	CIS Control 11, ISO 42001 Section 7.5	Establish comprehensive backup procedures for AI assets, including models, training data, and configurations, with regular testing of restoration processes
5.4	Is there a business continuity plan that addresses AI system failures?	NIST CSF 2.0 (RECOVER function), ISO 42001 Section 6.1	Develop and test a business continuity plan that addresses AI system failures, including alternative processes and recovery time objectives
5.5	Does the organization conduct post-incident analysis for AI-related incidents?	CIS Control 17, NIST AI RMF (MANAGE function)	Implement post-incident analysis processes for AI-related incidents, including root cause analysis, impact assessment, and improvement recommendations
5.6	Are AI incident response team members trained on AI-specific incident scenarios?	CIS Control 17, NIST CSF 2.0 (RESPOND function)	Provide specialized training for incident response team members on AI-specific incident scenarios, including technical, ethical, and reputational aspects

Domain 6: AI Transparency and Explainability

No.	Question	Control Reference	Remediation
6.1	Does the organization implement explainable AI methodologies for high-risk AI applications?	NIST AI RMF (MAP function), ISO 42001 Section 8.4	Implement appropriate explainable AI methodologies based on use case requirements, including local and global explanation techniques
6.2	Is there documentation of AI decision processes for critical systems?	ISO 42001 Section 7.5, NIST AI RMF (MEASURE function)	Develop and maintain detailed documentation of AI decision processes, including model logic, key features, and decision boundaries
6.3	Are there mechanisms to ensure transparency in AI-human interactions?	NIST AI RMF (MANAGE function), ISO 42001 Section 8.4	Implement transparency mechanisms for AI-human interactions, including disclosure of AI use, confidence levels, and limitations
6.4	Does the organization have methods to interpret and validate model outputs?	NIST AI RMF (MEASURE function), ISO 42001 Section 9.1	Establish methods for interpreting and validating model outputs, including statistical analysis, human review, and comparison with expected outcomes
6.5	Is there clear communication to stakeholders about AI system limitations?	ISO 42001 Section 7.4, NIST AI RMF (GOVERN function)	Develop clear communication materials about AI system limitations, including accuracy boundaries, known biases, and appropriate use cases
6.6	Are there processes to address algorithmic transparency requirements from regulations?	ISO 42001 Section 6.1, NIST CSF 2.0 (GOVERN function)	Establish processes to identify and address algorithmic transparency requirements from applicable regulations, including documentation and reporting mechanisms

Domain 7: AI Literacy and Training

No.	Question	Control Reference	Remediation
7.1	Does the organization have an AI awareness program for all employees?	CIS Control 14, NIST CSF 2.0 (GOVERN function)	Develop and implement an AI awareness program for all employees, covering AI capabilities, limitations, and responsible use
7.2	Is there specialized technical AI security training for relevant personnel?	CIS Control 14, ISO 42001 Section 7.2	Establish specialized technical AI security training for IT, security, and development personnel, including threat modeling, secure development, and vulnerability management
7.3	Does the organization provide AI ethics training for staff involved in AI development and deployment?	ISO 42001 Section 7.3, NIST AI RMF (GOVERN function)	Implement AI ethics training that covers fairness, accountability, transparency, and privacy considerations in AI systems
7.4	Is there training on AI risk management for leadership and risk management personnel?	ISO 42001 Section 7.2, NIST AI RMF (MAP function)	Develop and deliver AI risk management training for leadership and risk personnel, covering AI-specific risks, assessment methodologies, and mitigation strategies
7.5	Does the organization have a continuous learning program for AI security and governance?	CIS Control 14, ISO 42001 Section 7.2	Establish a continuous learning program for AI security and governance, including regular updates on emerging threats, regulatory changes, and best practices
7.6	Are there mechanisms to assess AI literacy and competency across the organization?	ISO 42001 Section 7.2, NIST CSF 2.0 (GOVERN function)	Implement mechanisms to assess AI literacy and competency, including knowledge assessments, skills evaluations, and certification programs

AI Governance, Risk and Compliance (GRC) Assessment

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