MODERN AI

smart. secure. transformative

AI GOVERNANCE & RISK ASSESSMENT

ALIGNING TO ISO/IEC 42001 FRAMEWORK

ASSESS. MANAGE. ASSURE.

A comprehensive assessment to evaluate AI maturity, identify risks and gaps, and build a roadmap for responsible, secure, and compliant AI adoption.

CLIENT NAME
[Client Name]

REPORT TYPE
AI Risk & ISO/IEC 42001 Alignment Assessment

DATE
[Month Day, Year]

PREPARED BY
Modern AI

TRUSTWORTHY AI
Build trust and ensure accountability

RISK AWARE
Identify, assess and mitigate risks

COMPLIANT
Align with ISO/IEC 42001 and global standards

RESPONSIBLE
Ethical, fair and human-centered AI

FUTURE READY
Drive innovation with confidence

Prepared By: Modern AI Managing Systems Inc.

Smart • Secure • Transformative

AI Strategy | AI Governance | AI Security | AI Operations | AI Risk | AI Data Intelligence | AI Managed Services

Prepared by: Neil Mistry President & CEO

Date: July 13th, 2026

Confidential

Version 1.0

Confidentiality Statement

CONFIDENTIAL

This report has been prepared exclusively for the client identified within this document. The information contained herein is proprietary to Modern AI Managing Systems Inc. and is intended solely for executive leadership, authorized stakeholders, and designated project teams.

The methodologies, recommendations, assessment models, governance frameworks, scoring mechanisms, maturity models, diagrams, graphics, templates, and intellectual property contained within this report remain the exclusive property of Modern AI Managing Systems Inc.

No portion of this document may be copied, distributed, disclosed, reproduced, or transmitted without prior written authorization from Modern AI.

Letter from the CEO

A Message from Neil Mistry

Artificial Intelligence is fundamentally changing how organizations operate, make decisions, serve customers, and manage risk. While AI presents extraordinary opportunities for innovation and competitive advantage, it also introduces new governance, cybersecurity, regulatory, privacy, and operational risks that must be proactively managed.

At Modern AI, we believe successful AI adoption extends far beyond selecting technology. Sustainable AI transformation requires robust governance, disciplined operational processes, executive accountability, secure architectures, trustworthy data, and a culture of responsible innovation.

Our Enterprise AI Governance Assessment is designed to help organizations understand their current AI maturity, identify strategic gaps, prioritize investments, and establish a practical roadmap toward responsible, secure, and scalable AI adoption. Leveraging ISO/IEC 42001 alongside complementary frameworks such as NIST AI RMF, ISO/IEC 23894, MITRE ATLAS, and applicable regulatory guidance, we provide a comprehensive view of organizational readiness.

This report is intended to support executive decision-making by translating technical findings into clear business outcomes, enabling leadership teams to align AI initiatives with organizational objectives, regulatory expectations, and enterprise risk management practices.

We appreciate the opportunity to partner with your organization and look forward to supporting your AI journey.

Sincerely,

Neil Mistry
President & CEO
Modern AI Managing Systems Inc.

Table of Contents

About Modern AI

Company Overview

Modern AI Managing Systems Inc. is a Canadian AI advisory and consulting firm specializing in enterprise AI strategy, governance, cybersecurity, data intelligence, automation, and managed AI services. We help organizations transform AI from isolated experiments into secure, governed, and measurable business capabilities.

Our multidisciplinary approach combines executive strategy, technical implementation, risk management, and operational excellence to enable organizations to deploy AI responsibly while maximizing business value.

Our Seven Service Pillars

1. AI Strategy, Advisory & Transformation
2. AI Governance, Compliance & Responsible AI
3. AI Security, Risk & Resilience
4. AI Data Intelligence & Integration
5. AI Applications, Agents & Workflow Automation
6. AI Infrastructure, Operations & Runtime
7. AI Enablement, Training & Managed Services

Why Organizations Choose Modern AI

- Vendor-neutral AI advisory services
- Executive AI governance expertise
- Deep experience with enterprise cybersecurity
- Practical implementation roadmaps
- Alignment with international standards
- Focus on measurable business outcomes

Executive Summary

Purpose of the Assessment

The objective of this assessment is to evaluate the organization's readiness to establish, operate, and continuously improve an AI Management System aligned with ISO/IEC 42001. The assessment

examines governance structures, leadership commitment, risk management, operational controls, data practices, security, compliance, and organizational capabilities.

By leveraging the accompanying ISO/IEC 42001 assessment workbook, the report translates detailed assessment responses into executive-level insights, enabling leadership to prioritize remediation efforts and guide strategic investment decisions.

Key Objectives

- Establish a baseline AI governance maturity
- Identify strengths and capability gaps
- Evaluate alignment with ISO/IEC 42001 requirements
- Assess AI-related risks and control effectiveness
- Provide a prioritized improvement roadmap
- Support executive decision-making
- Prepare the organization for certification readiness where appropriate

Expected Business Outcomes

Organizations that strengthen AI governance can expect improved executive visibility, reduced operational and regulatory risk, more consistent AI adoption practices, enhanced stakeholder confidence, and greater scalability of AI initiatives.

Overall Executive Dashboard (Template)

Category	Status	Executive Commentary
AI Governance	To be populated from workbook	Leadership, governance structure, and oversight maturity
Leadership	To be populated	Executive sponsorship and accountability
Risk Management	To be populated	AI risk identification, treatment, and monitoring
Security	To be populated	Technical controls protecting AI systems and data
Data Governance	To be populated	Data quality, lineage, privacy, and stewardship

Category	Status	Executive Commentary
Operations	To be populated	AI lifecycle, monitoring, and continuous improvement.
Compliance	To be populated	Alignment with ISO/IEC 42001 and regulatory obligations
Organizational Readiness	To be populated	Skills, culture, and change management

2. Current State Assessment

Executive Overview

The current state assessment provides an enterprise-wide evaluation of the organization's readiness to establish and operate an Artificial Intelligence Management System (AIMS) aligned with ISO/IEC 42001:2023. The assessment draws on the completed workbook, interviews, governance documentation, and available evidence to determine current maturity across governance, leadership, risk management, security, data, operations, and organizational readiness.

Rather than measuring technology alone, this assessment evaluates the organization's ability to govern AI responsibly, consistently, and at enterprise scale.

The results indicate that while foundational AI initiatives may exist, formal governance structures, documented policies, standardized operating procedures, and continuous monitoring capabilities are generally in the early stages of maturity. As AI adoption accelerates, the organization should prioritize governance capabilities to reduce operational risk, improve executive oversight, and support sustainable AI innovation.

2.1 Overall Assessment Summary

Executive Assessment

The assessment indicates that the organization is transitioning from exploratory AI adoption toward enterprise operationalization. Multiple AI initiatives, pilots, or business use cases may already be in progress; however, governance mechanisms have not yet matured at the same pace as technology deployment.

This creates a growing gap between AI innovation and organizational control. Without structured governance, organizations are exposed to inconsistent decision-making, regulatory uncertainty, fragmented ownership, unmanaged AI inventories, and increased cybersecurity risk.

From an executive perspective, the organization demonstrates strong potential for AI transformation but requires a coordinated governance framework to ensure AI investments deliver measurable business value while maintaining trust, compliance, and resilience.

Executive Current State

Capability	Executive Assessment	Risk
Executive Governance	Emerging	High
AI Strategy	Developing	Medium
AI Policy	Limited	High
AI Inventory	Limited	High
AI Risk Management	Developing	High
AI Security	Developing	Medium
Data Governance	Developing	Medium
AI Operations	Emerging	Medium
Monitoring	Limited	High
Compliance	Developing	High

Executive Observations

The assessment highlights several recurring themes that are common among organizations beginning their enterprise AI journey:

Strengths

- Strong executive interest in AI transformation.

- Business units actively exploring AI opportunities.
- Existing cybersecurity and risk management functions provide a strong foundation.
- Leadership recognizes AI as a strategic business priority.
- Technical capabilities exist to support AI deployment.

Areas Requiring Improvement

- Lack of enterprise AI governance structure.
- No formal AI steering committee.
- Limited AI policies and standards.
- Incomplete AI inventory.
- Limited AI-specific risk management.
- Inconsistent AI lifecycle processes.
- Minimal AI monitoring and reporting.
- Undefined accountability across business functions.
- Limited executive dashboards.
- No centralized AI management framework.

2.2 Enterprise AI Governance Assessment

Executive Summary

AI governance forms the foundation of every successful AI program. It ensures that AI systems operate consistently with business objectives, regulatory obligations, ethical principles, and organizational risk appetite.

The assessment indicates governance processes remain largely decentralized. Business units may independently evaluate, procure, or develop AI capabilities without standardized oversight.

As AI adoption expands, centralized governance becomes essential to prevent inconsistent practices, unmanaged risks, and duplication of effort.

Key Findings

Finding 1:

Executive Governance Committee Not Established

Without executive governance, AI decisions become decentralized, reducing visibility into enterprise risk.

Business Impact - High

Recommendation - Create an Executive AI Steering Committee.

Priority - Critical

Finding 2:

AI Policies Are Incomplete

Most organizations possess cybersecurity policies but lack AI-specific governance policies covering:

- Responsible AI
- AI procurement
- AI model approval
- AI ethics
- AI monitoring
- AI lifecycle management
- AI vendor governance

Business Impact - High

Recommendation - Develop an enterprise AI policy framework aligned to ISO/IEC 42001.

Finding 3:

AI Inventory Is Incomplete

Organizations frequently underestimate the number of AI systems already deployed.

Examples include:

- Microsoft Copilot
- ChatGPT
- Claude
- GitHub Copilot
- Internal machine learning models
- AI agents
- Intelligent automation platforms

Without a centralized inventory, executive leadership cannot accurately assess organizational exposure.

Recommendation - Establish an enterprise AI Asset Inventory.

Priority - Critical

2.3 Leadership Assessment

Leadership commitment is one of the strongest indicators of successful AI governance implementation.

The assessment indicates executive sponsorship exists; however, governance responsibilities have not yet been formalized across the organization.

Executive Recommendations

Establish:

- Executive AI Steering Committee
- AI Governance Office
- AI Risk Committee
- Responsible AI Council
- AI Architecture Review Board

These governance bodies should define strategic priorities, oversee AI investments, monitor risk, and provide executive reporting.

2.4 AI Risk Management Assessment

The organization currently manages enterprise technology risk through established cybersecurity and operational risk practices. However, AI introduces new categories of risk that require dedicated governance.

These include:

- Hallucinations
- Prompt injection
- Model drift
- Bias
- Privacy violations
- Unauthorized AI usage
- Shadow AI
- Third-party AI risk
- AI supply chain vulnerabilities
- Autonomous agent misuse

Executive Recommendation

Develop an enterprise AI Risk Register integrated into the organization's existing enterprise risk management program.

Each AI initiative should undergo formal risk assessment prior to deployment and be monitored throughout its lifecycle.

2.5 Organizational Readiness

Successful AI adoption depends on people, culture, governance, and change management.

The assessment indicates the organization has technical capability but requires stronger organizational readiness.

Recommended Focus Areas

- Executive education
- AI literacy programs
- Role-based training
- Change management

- Communication strategy
- AI champions network
- Governance awareness

2.6 Executive Heat Map

Domain	Maturity	Priority
Governance	Low	Critical
Leadership	Medium	High
Risk Management	Low	Critical
AI Security	Medium	High
Data Governance	Medium	High
AI Operations	Medium	Medium
Monitoring	Low	Critical
Compliance	Low	Critical
Training	Medium	Medium
Vendor Governance	Low	High

2.7 Executive Priorities (Next 90 Days)

The first phase of the AI governance program should focus on foundational capabilities that enable safe and scalable AI adoption.

Critical Priorities

1. Establish Executive AI Steering Committee
2. Approve Enterprise AI Policy
3. Build AI System Inventory
4. Launch AI Risk Register
5. Define AI Governance Operating Model

6. Identify Regulatory Obligations
7. Develop AI Lifecycle Standards
8. Implement AI Security Controls
9. Create Executive Reporting Dashboard
10. Begin Continuous Monitoring

Executive Conclusion

The organization is well positioned to realize significant value from AI; however, achieving sustainable success requires strengthening governance capabilities before AI adoption accelerates further. By prioritizing governance, risk management, and executive oversight, the organization can reduce operational and regulatory exposure while enabling innovation at scale.

This section establishes the "Current State & Executive Findings" chapter. The next part will move into a **clause-by-clause ISO/IEC 42001 assessment (Clauses 4–10)**, interpreting the workbook responses, explaining each requirement in business terms, and providing maturity ratings, gap analyses, and actionable recommendations. That section will become the core of the executive assessment report.

ISO/IEC 42001 AI Management System Assessment

Executive Overview

ISO/IEC 42001 provides organizations with a structured management system for governing Artificial Intelligence throughout its lifecycle. Similar to ISO 27001 for information security or ISO 9001 for quality management, ISO 42001 establishes governance processes that ensure AI systems are secure, ethical, transparent, and continuously improved.

This assessment evaluates the organization's readiness against each clause of the standard, identifying capability gaps, implementation priorities, and executive actions required to establish a mature AI Management System (AIMS).

Clause 4 – Context of the Organization

Executive Summary

Organizations must clearly understand how AI supports business objectives, which stakeholders influence AI governance, and which regulatory obligations apply.

Current State

The assessment indicates that AI initiatives are often driven by individual business units rather than an enterprise-wide strategy. AI governance boundaries, stakeholder responsibilities, and organizational objectives require formal definition.

Key Findings

- AI governance scope has not been formally documented.
- Internal and external stakeholders have not been comprehensively identified.
- Regulatory obligations are dispersed across multiple business functions.
- Business objectives are not consistently linked to AI initiatives.

Business Impact

Without a defined governance context, AI investments become inconsistent, priorities compete across departments, and compliance obligations may be overlooked.

Executive Recommendations

- Define the enterprise AI governance scope.
- Create an AI stakeholder register.
- Establish an AI obligations register covering regulatory, contractual, and internal requirements.
- Align AI initiatives with corporate strategy and enterprise risk appetite.

Priority

Critical (0–90 Days)

Clause 5 – Leadership

Executive Summary

Executive leadership is the single most important success factor for AI governance. Leadership must establish policy, assign accountability, provide resources, and demonstrate ongoing commitment to responsible AI.

Current State

Leadership recognizes AI as a strategic priority; however, governance responsibilities are not yet consistently defined.

Key Findings

- No formal Executive AI Steering Committee.
- Limited executive reporting on AI performance and risk.
- AI policies require approval and communication.
- Accountability is distributed without a centralized governance model.

Recommendations

- Establish an Executive AI Steering Committee.
- Appoint an Executive Sponsor for AI Governance.
- Approve an Enterprise AI Policy.
- Define governance roles using a RACI matrix.
- Implement quarterly AI governance reporting.

Expected Business Benefits

- Improved executive oversight
- Faster decision-making
- Reduced regulatory exposure
- Increased accountability

Clause 6 – Planning

Executive Summary

Planning ensures AI risks, opportunities, and objectives are proactively managed rather than reactively addressed.

Current State

AI planning is generally project-focused and lacks enterprise prioritization.

Findings

- AI objectives are not consistently measurable.
- Risk treatment plans vary between departments.
- AI success metrics are not standardized.

- Dependencies between business initiatives are not formally managed.

Recommendations

- Define enterprise AI objectives and KPIs.
- Establish an AI investment roadmap.
- Integrate AI planning into enterprise strategic planning.
- Align AI objectives with business outcomes.

Clause 7 – Support

Executive Summary

Effective AI governance depends on organizational capability, including people, skills, awareness, documentation, and technology.

Findings

- Limited AI-specific training.
- Inconsistent documentation practices.
- AI knowledge concentrated among a small number of specialists.
- Skills inventory not established.

Recommendations

- Launch enterprise AI literacy programs.
- Develop role-based AI training.
- Create AI documentation standards.
- Establish a centralized AI knowledge repository.

Clause 8 – Operation

Executive Summary

Operational controls govern the lifecycle of AI systems from design through retirement.

Findings

- AI lifecycle processes are inconsistent.
- Limited change management for AI models.
- AI testing and validation processes require standardization.

- AI inventories are incomplete.

Recommendations

- Implement an enterprise AI lifecycle framework.
- Introduce model approval workflows.
- Standardize testing and validation procedures.
- Maintain a centralized AI inventory.

Clause 9 – Performance Evaluation

Executive Summary

Organizations must continuously evaluate AI performance using measurable metrics.

Findings

- Executive dashboards are limited.
- AI KPIs are inconsistent.
- Monitoring is largely reactive.
- Formal AI audits have not been established.

Recommendations

- Develop executive AI dashboards.
- Define AI governance KPIs.
- Perform periodic AI governance reviews.
- Conduct annual AI internal audits.

Clause 10 – Improvement

Executive Summary

Continuous improvement enables organizations to mature their AI governance capabilities over time.

Findings

- Lessons learned are not consistently documented.

- Improvement initiatives are decentralized.
- Corrective action tracking requires standardization.

Recommendations

- Implement continuous improvement processes.
- Track corrective actions centrally.
- Review governance effectiveness annually.
- Benchmark against industry best practices.

Executive Clause Summary

Clause	Maturity	Priority	Business Impact
Context	Developing	High	Strategic Alignment
Leadership	Developing	Critical	Governance
Planning	Initial	High	Business Outcomes
Support	Initial	Medium	Organizational Capability
Operation	Developing	High	AI Lifecycle
Performance Evaluation	Initial	Critical	Executive Visibility
Improvement	Initial	Medium	Continuous Maturity

AI Governance Domains

This section expands beyond ISO clauses into operational governance capabilities.

AI Governance Operating Model

Describe the governance structure including:

- Board of Directors
- Executive AI Steering Committee
- Chief AI Officer / AI Governance Lead
- AI Risk Committee
- AI Ethics Committee
- Enterprise Architecture
- Information Security
- Privacy
- Legal
- Business Units

Explain reporting relationships and decision-making authority.

AI Policy Framework

Assess and recommend policies covering:

- Responsible AI Policy
- Acceptable Use of AI
- AI Procurement Policy
- AI Model Lifecycle Standard
- AI Data Governance Standard
- AI Third-Party Risk Standard
- AI Incident Response Procedure
- AI Monitoring and Logging Standard

For each policy include:

- Purpose
- Current maturity
- Gap
- Recommendation
- Owner
- Implementation timeline

AI Risk Management

Provide a detailed AI risk register organized into categories:

- Governance Risks
- Data Risks
- Model Risks
- Security Risks

- Privacy Risks
- Operational Risks
- Third-Party Risks
- Regulatory Risks
- Ethical Risks
- Reputational Risks

Include likelihood, impact, inherent risk, residual risk, mitigation, owner, and target completion.

AI Security Assessment

Evaluate:

- Identity and Access Management
- Model Security
- Prompt Injection Protection
- Retrieval-Augmented Generation (RAG) Security
- Agent Security
- MCP Security
- API Security
- Secrets Management
- Encryption
- Runtime Protection
- Logging and Monitoring
- Incident Response

Provide executive commentary, findings, and recommendations for each area.

Data Governance

Assess:

- Data Quality
- Metadata Management
- Lineage
- Classification
- Retention
- Privacy
- Sovereignty
- Access Controls

Describe business impact and recommended improvements.

AI Operations (AIOps / LLMOps)

Evaluate:

- Model lifecycle management
- Deployment processes
- Monitoring
- Performance management
- Version control
- Rollback procedures
- Automation
- Observability

Recommend a target operating model.

Strategic Roadmap & Executive Recommendations

Executive Priorities

Organize recommendations into four phases:

Phase 1 (0–30 Days)

- Establish Executive AI Steering Committee
- Approve AI Policy
- Define governance scope
- Launch AI inventory

Phase 2 (31–60 Days)

- Complete AI risk assessments
- Build AI risk register
- Develop AI lifecycle procedures
- Begin executive reporting

Phase 3 (61–90 Days)

- Implement AI monitoring
- Deliver training
- Conduct internal AI audits
- Integrate governance with enterprise risk management

Phase 4 (91–120 Days)

- Optimize governance processes
- Benchmark maturity
- Prepare for ISO/IEC 42001 certification
- Establish continuous improvement program

Executive Investment Roadmap

For each initiative include:

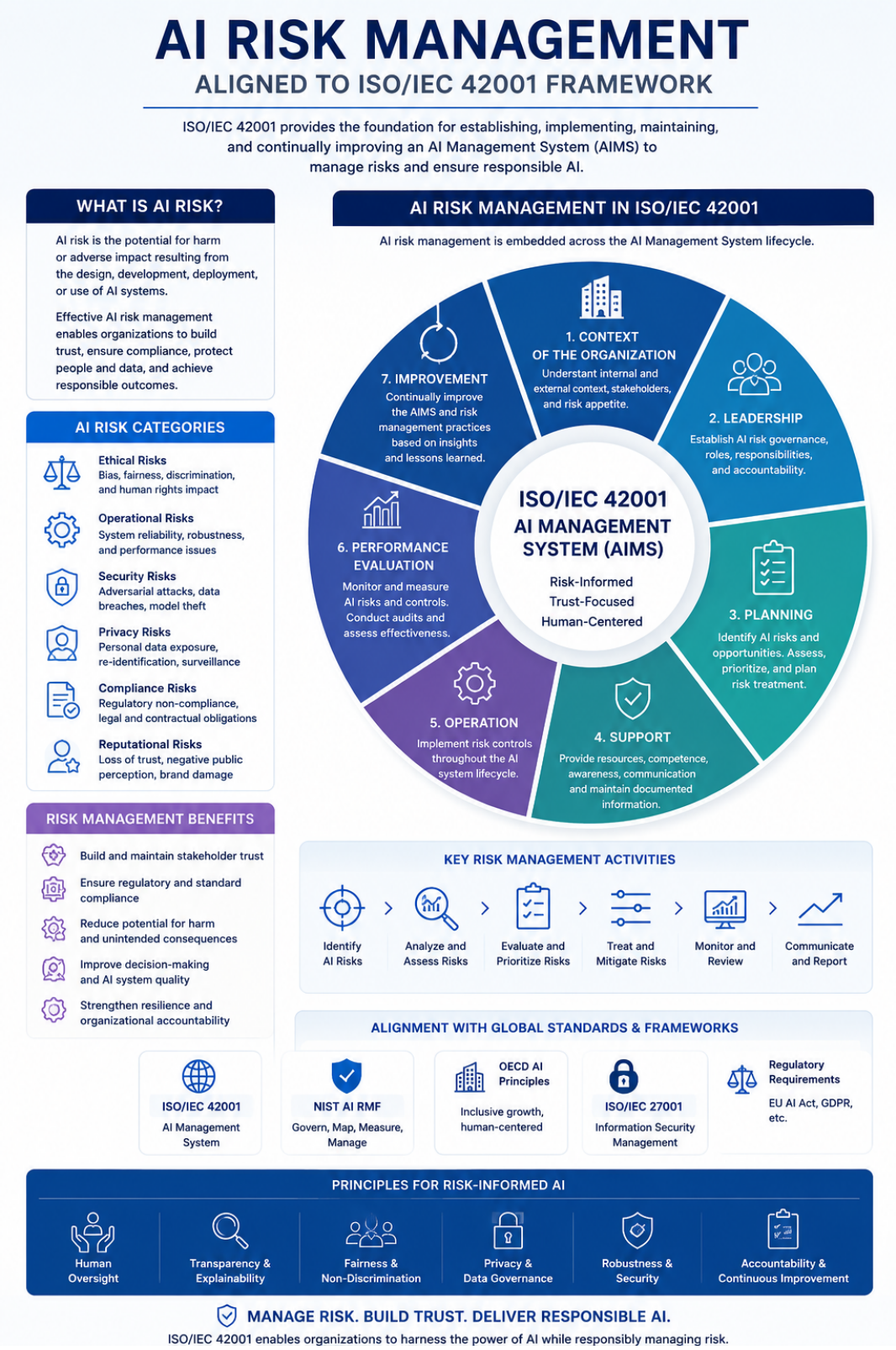
- Business objective
- Estimated effort
- Business value
- Risk reduction
- Dependencies
- Executive owner
- Target completion date

Final Executive Recommendations

Conclude the report with a prioritized list of the top recommendations, emphasizing governance, leadership, risk management, policy development, security controls, continuous monitoring, and organizational capability building. Reinforce that AI governance is an ongoing management discipline that requires executive sponsorship, measurable objectives, and continuous improvement to maximize business value while maintaining trust and compliance.

This completes the core narrative of the report. The remaining appendices should include the detailed workbook outputs, assessment scoring methodology, evidence tracker, glossary, framework mappings (ISO/IEC 42001, NIST AI RMF, ISO/IEC 23894, MITRE ATLAS), and supporting references, allowing the report to function as a reusable Modern AI executive assessment methodology for enterprise clients.

Appendix


AI RISK MANAGEMENT
ALIGNED TO ISO/IEC 42001 FRAMEWORK
ISO/IEC 42001 provides the foundation for establishing, implementing, maintaining, and continually improving an AI Management System (AIMS) to manage risks and ensure responsible AI.
WHAT IS AI RISK?
AI risk is the potential for harm or adverse impact resulting from the design, development, deployment, or use of AI systems.
Effective AI risk management enables organizations to build trust, ensure compliance, protect people and data, and achieve responsible outcomes.
AI RISK CATEGORIES
Ethical Risks
Bias, fairness, discrimination, and human rights impact
Operational Risks
System reliability, robustness, and performance issues
Security Risks
Adversarial attacks, data breaches, model theft
Privacy Risks
Personal data exposure, re-identification, surveillance
Compliance Risks
Regulatory non-compliance, legal and contractual obligations
Reputational Risks
Loss of trust, negative public perception, brand damage
RISK MANAGEMENT BENEFITS
Build and maintain stakeholder trust
Ensure regulatory and standard compliance
Reduce potential for harm and unintended consequences
Improve decision-making and AI system quality
Strengthen resilience and organizational accountability
AI RISK MANAGEMENT IN ISO/IEC 42001
AI risk management is embedded across the AI Management System lifecycle.
1. CONTEXT OF THE ORGANIZATION
Understant internal and external context, stakeholders, and risk appetite.
2. LEADERSHIP
Establish AI risk governance, roles, responsibilities, and accountability.
3. PLANNING
Identify AI risks and opportunities. Assess, prioritize, and plan risk treatment.
4. SUPPORT
Provide resources, competence, awareness, communication and maintain documented information.
5. OPERATION
Implement risk controls throughout the AI system lifecycle.
6. PERFORMANCE EVALUATION
Monitor and measure AI risks and controls. Conduct audits and assess effectiveness.
7. IMPROVEMENT
Continually improve the AIMS and risk management practices based on insights and lessons learned.
ISO/IEC 42001
AI MANAGEMENT SYSTEM (AIMS)
Risk-Informed
Trust-Focused
Human-Centered
KEY RISK MANAGEMENT ACTIVITIES
Identify AI Risks
Analyze and Assess Risks
Evaluate and Prioritize Risks
Treat and Mitigate Risks
Monitor and Review
Communicate and Report
ALIGNMENT WITH GLOBAL STANDARDS & FRAMEWORKS
ISO/IEC 42001
AI Management System
NIST AI RMF
Govern, Map, Measure, Manage
OECD AI Principles
Inclusive growth, human-centered
ISO/IEC 27001
Information Security Management
Regulatory Requirements
EU AI Act, GDPR, etc.
PRINCIPLES FOR RISK-INFORMED AI
Human Oversight
Transparency & Explainability
Fairness & Non-Discrimination
Privacy & Data Governance
Robustness & Security
Accountability & Continuous Improvement
MANAGE RISK. BUILD TRUST. DELIVER RESPONSIBLE AI.
ISO/IEC 42001 enables organizations to harness the power of AI while responsibly managing risk.

MODERN AI
smart. secure. transformative.

OpenAI Microsoft aws Google Cloud
Azure ANTHROPIC cohere NVIDIA

MITRE ATLAS
AI SECURITY ASSESSMENT
EXECUTIVE SUMMARY

Modern AI conducted a comprehensive assessment of your AI ecosystem leveraging the **MITRE ATLAS** framework to identify adversarial threats, evaluate security controls, and provide actionable recommendations to strengthen your AI security posture.

KEY FINDINGS

AI ADOPTION IS ACCELERATING
Your organization is leveraging a diverse set of AI technologies across multiple functions and business units.

THREAT LANDSCAPE IS EVOLVING
Adversaries are increasingly targeting AI systems through prompt injection, data poisoning, model theft, and agent abuse.

CONTROLS ARE IN PLACE BUT INCONSISTENT
Several critical areas have partial or no controls, creating exposure to AI-specific risks.

GOVERNANCE MATURITY IS EMERGING
Governance, policies, and processes are in early stages and need further operationalization.

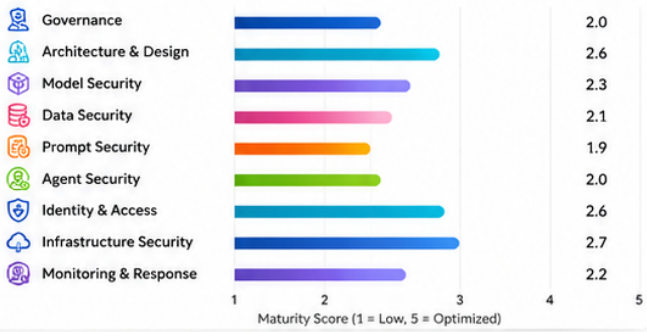
OVERALL AI SECURITY POSTURE

MATURITY SCORE **2.4 / 5**

MATURITY LEVEL **Developing**

1 2 3 4 5

DOMAIN MATURITY OVERVIEW



TOP AI SECURITY RISKS

1	Prompt Injection & Jailbreak Attacks	HIGH
2	Data Leakage via AI Interactions	HIGH
3	Excessive Agent Permissions	HIGH
4	Model Theft & Intellectual Property Exposure	MEDIUM
5	Insufficient Monitoring & Detection	MEDIUM

STRATEGIC RECOMMENDATIONS

STRENGTHEN GUARDRAILS
Implement robust prompt controls, content filtering, and policy enforcement.

SECURE DATA & MODELS
Enhance data governance, model provenance, and supply chain security.

HARDEN AGENTS & TOOLS
Apply least privilege, approval workflows, and tool trust controls.

IMPROVE VISIBILITY & DETECTION
Implement AI-aware monitoring, logging, and anomaly detection.

MITRE ATLAS provides the most comprehensive knowledge base of adversarial attack techniques against AI systems. Use it to proactively assess, detect, and defend.

LET'S BUILD SECURE, TRUSTED AND RESPONSIBLE AI TOGETHER.

www.modernai.ca info@modernai.ca 647-525-7916