



AI RegRisk™
Think Tank

AI STRATEGY & RISK PROGRAM

Guiding Your Organization Toward
Responsible and Effective AI Adoption





The AI Imperative

- AI is transforming industries and driving innovation.
- Challenge: Many organizations feel unprepared for AI adoption.
- Risks: Regulatory compliance, ethical considerations, operational risks.

AI Strategy and Risk Program Overview

- Adapts to the constantly changing digital environment of AI.
- Combines strategic alignment with proactive risk mitigation.
- Designed to guide responsible AI deployment.
- Tailored to your organization's needs and industry context



Built on Experience, Standards, and Adaptability

- Experience-Driven Insights
- Industry Standard Frameworks
- Dynamic and Adaptive Approach
- Changing regulatory and legislative rules



Why Choose the AI Strategy and Risk Program?




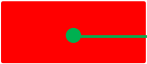


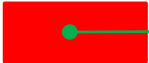







- Establishes a robust governance foundation.
- Promotes responsible and ethical AI adoption.
- Enables proactive risk management.
- Aligns AI initiatives with business objectives.
- Provides flexibility and scalability for future growth.
- Speed of implementation and consistency of implementation.



AI Strategy and Risk Assessment

Use Case: GenAI CRM Module



COMPONENT	BASELINE	EVOLVING	MATURE
 AGILE GOVERNANCE			
 RESPONSIBLE AI APPROACH			
 RISK-INFORMED SYSTEM			
 STRATEGY AND EXECUTION			
 RISK ESCALATION AND REPORTING			

01

Agile Governance

- Adapts to the constantly changing digital environment of AI.
- Combines strategic alignment with proactive risk mitigation.
- Designed to guide responsible AI deployment.
- Tailored to your organization's needs and industry context





02

Responsible AI Approach

- Ethical AI deployment with a focus on explainability and transparency
- Model Risk Management (MRM) to monitor soundness, fairness, robustness and model drift.
- Data governance to protect privacy and ensure compliance
- Prompting Guidelines and Assurance

03

Risk-informed System

- Clear definition of AI-related risk tolerance levels
- Maturity models to evaluate and improve risk management capabilities
- Key Risk Indicators (KRIs) for monitoring risks and triggering necessary actions





04

Strategy and Execution

- Needs Research (Use Cases)
- Understanding Capabilities
- Risk and Mitigation Mapping
- Regulatory and Compliance Obligations

05

Risk Escalation and Reporting

- Escalation protocols for risks exceeding tolerance levels
- Internal reporting to keep executives and boards informed
- External disclosures to maintain compliance and stakeholder trust



AI Strategy and Risk Assessment

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud

COMPONENT	Key Themes
AGILE GOVERNANCE	<p>Strength: The Business has established a robust governance structure, with multiple reporting avenues to executive leadership and the board.</p> <p>Growth Opportunity: While responsibilities for each of the three lines of defense have been formally defined, additional clarification and alignment of responsibilities would enhance The Business’s ability to define and execute a cohesive cybersecurity strategy.</p>
RESPONSIBLE AI APPROACH	<p>Strength: Executive and Board leadership are frequently and regularly presented with information security metrics.</p> <p>Growth Opportunity: The Business has not yet formally defined a risk appetite, tolerance thresholds, or acceptance criteria. Additionally, metrics and key indicators have not been tied to business objectives.</p>

COMPONENT	Key Themes
STRATEGY AND EXECUTION	<p>Strength: Executive and Board leadership are frequently and regularly presented with information security metrics.</p> <p>Growth Opportunity: The Business has not yet formally defined a risk appetite, tolerance thresholds, or acceptance criteria. Additionally, metrics and key indicators have not been tied to business objectives.</p>
RISK ESCALATION AND REPORTING	<p>Strength: Executive and Board leadership are frequently and regularly presented with information security metrics.</p> <p>Growth Opportunity: The Business has not yet formally defined a risk appetite, tolerance thresholds, or acceptance criteria. Additionally, metrics and key indicators have not been tied to business objectives.</p>
RISK-INFORMED SYSTEM	<p>Strength: Executive and Board leadership are frequently and regularly presented with information security metrics.</p> <p>Growth Opportunity: The Business has not yet formally defined a risk appetite, tolerance thresholds, or acceptance criteria. Additionally, metrics and key indicators have not been tied to business objectives.</p>