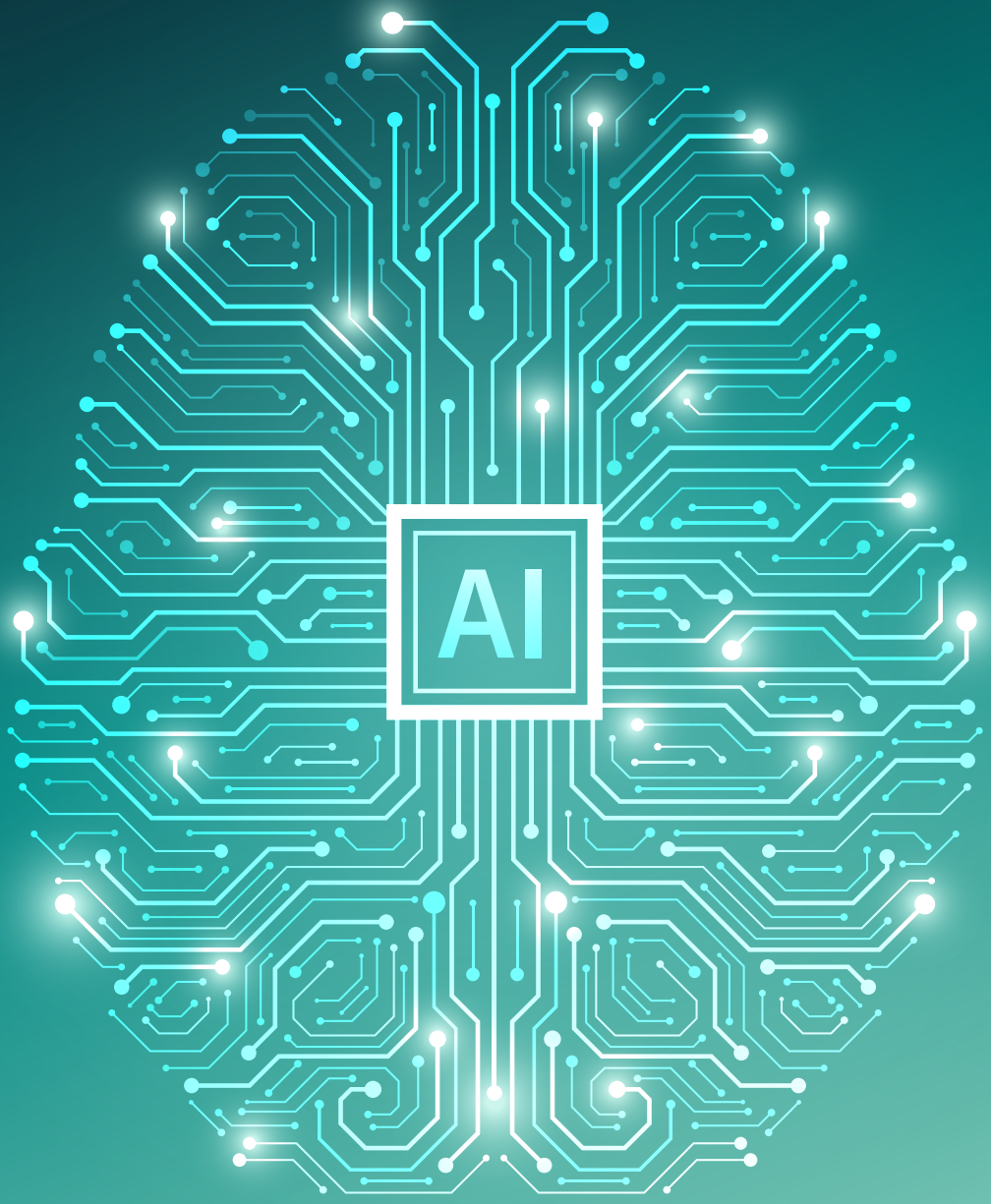
Venzip

THE **AI** *SECURITY READINESS* **GUIDE**

Is Your AI Actually Secure?



Venzip

TABLE OF CONTENTS

Venzip

CHAPTER 1

WHY AI SECURITY READINESS MATTERS RIGHT NOW

AI is embedded in your product, your workflows, and your vendor stack. But most organizations have no structured way to assess whether their AI is actually secure.

The regulatory landscape is shifting fast. The EU AI Act is enforcing risk-based classification. ISO 42001 provides the first international standard for AI management systems. Canada's proposed AIDA will introduce mandatory requirements for high-impact AI. Enterprise buyers are starting to ask: how do you govern your AI?

Meanwhile, shadow AI is spreading through organizations unchecked. Employees are using ChatGPT, Copilot, and dozens of AI tools with sensitive company data, often without any policy or oversight. This is not a future risk. It is happening today.

This guide gives you a structured, practical way to evaluate your AI security posture cross 12 critical domains with 85+ questions. It includes two domains Vanta and other assessments miss entirely: third-party AI model governance and AI regulatory readiness.

What makes this guide different:

- 85+ questions across 12 domains (vs. industry-standard 71 / 10)
- Priority action items after each domain to turn gaps into a roadmap
- Board-ready summary page you can present directly to leadership

Venzip

HOW TO USE THIS ASSESSMENT

This assessment covers 12 domains spanning the full AI governance lifecycle. Each question is tagged with a maturity tier so you can focus on what matters at your stage.

Three Maturity Tiers

Tier 1 — Foundational

The baseline for every organization using AI in any capacity, including third-party tools. If you only complete one tier, complete this one.

Tier 2 — Operational

For organizations deploying AI in customer-facing products or processing sensitive data. Covers testing, monitoring, data quality, and human oversight.

Tier 3 — Advanced

For organizations building, training, or fine-tuning AI models. Includes model governance, ethics reviews, adversarial testing, and formal documentation.

How to Score

1. Work through each domain. Mark Yes or No for each question.
2. Count Yes answers per domain. Review the priority actions for any domain below 50%.
3. Calculate your total score and use the scoring guide on page 12.
4. Use the board-ready summary on page 13 to present findings to leadership.
5. Contact Venzip to turn your assessment into an actionable compliance plan.

Venzip

1. GOVERNANCE & ORGANIZATIONAL MANAGEMENT

Leadership accountability, policies, and structures for responsible AI use across the organization.

TIER ID	QUESTION	YES	NO
T1 GOV-01	Do you classify AI systems by risk level to determine appropriate controls?	☐ YES	☐ NO
T1 GOV-02	Do you have procurement policies specific to AI-enabled tools and vendors?	☐ YES	☐ NO
T1 GOV-03	Do you maintain an inventory of all AI tools and systems in use?	☐ YES	☐ NO
T2 GOV-04	Is there a documented AI development lifecycle with security checkpoints?	☐ YES	☐ NO
T2 GOV-05	Do legal, privacy, and ethics teams review AI deployments cross-functionally?	☐ YES	☐ NO
T2 GOV-06	Is there a formal risk assessment process specific to AI applications?	☐ YES	☐ NO
T3 GOV-07	Is a dedicated governance committee overseeing AI development and deployment?	☐ YES	☐ NO
T3 GOV-08	Does an AI ethics board review high-risk or controversial AI use cases?	☐ YES	☐ NO
T3 GOV-09	Do you score AI models for risk based on use case sensitivity and impact?	☐ YES	☐ NO

PRIORITY ACTIONS IF YOU SCORED LOW:

- Appoint an AI governance owner (CISO, CTO, or dedicated lead)
- Create an AI tool inventory — start with a simple spreadsheet of every AI tool in use
- Draft a basic AI acceptable use policy covering employee use of generative AI

DOMAIN SCORE: ___ / 9 Yes **TIER 1:** ___ / 3 **TIER 2:** ___ / 3 **TIER 3:** ___ / 3

Venzip

2. RISK MANAGEMENT & COMPLIANCE

Identifying prohibited uses, assessing vendor AI risks, and ensuring regulatory alignment.

TIER ID	QUESTION	YES	NO
T1 RMC-10	Have you identified and prohibited unacceptable AI use cases?	☐ YES	☐ NO
T1 RMC-11	Do you evaluate AI vendors for security, privacy, and ethical risk?	☐ YES	☐ NO
T1 RMC-12	Do vendor contracts include specific AI security and compliance terms?	☐ YES	☐ NO
T2 RMC-13	Do you assess security throughout the AI supply chain?	☐ YES	☐ NO
T2 RMC-14	Are post-implementation reviews conducted after deploying AI systems?	☐ YES	☐ NO
T2 RMC-15	Do you assess third-party pre-trained models for security and bias?	☐ YES	☐ NO
T3 RMC-16	Are human rights impact assessments conducted for high-risk AI?	☐ YES	☐ NO
T3 RMC-17	Do you conduct algorithmic impact assessments for high-impact AI decisions?	☐ YES	☐ NO

PRIORITY ACTIONS IF YOU SCORED LOW:

- Define a list of prohibited AI use cases and communicate it company-wide
- Add AI-specific clauses to your vendor contract template

Venzip

3. DATA MANAGEMENT & PRIVACY

Protecting data used to train, fine-tune, and operate AI systems.

TIER ID	QUESTION	YES	NO
T1 DMP-20	Are data protection impact assessments conducted for AI processing personal data?	☐ YES	☐ NO
T2 DMP-21	Do you have a framework to ensure the quality of data used in AI systems?	☐ YES	☐ NO
T2 DMP-22	Are controls in place to validate AI inputs against adversarial manipulation?	☐ YES	☐ NO
T2 DMP-23	Can customers opt out of having their data used for AI training?	☐ YES	☐ NO
T3 DMP-24	Is there governance for managing training data sourcing and labeling?	☐ YES	☐ NO
T3 DMP-25	Do you maintain detailed data provenance records for AI training data?	☐ YES	☐ NO
T3 DMP-26	Are privacy-enhancing techniques used in model design?	☐ YES	☐ NO

PRIORITY ACTIONS IF YOU SCORED LOW:

- Conduct a data protection impact assessment for your highest-risk AI system
- Document whether your AI vendors train on customer data and enable opt-out

Venzip

4. SECURITY CONTROLS & OPERATIONS

Integrating AI systems into your cybersecurity program with access controls, logging, and testing.

TIER ID	QUESTION	YES	NO
T1 SEC-29	Are role-based access controls implemented for AI systems?	☐ YES	☐ NO
T1 SEC-30	Is AI security integrated with your overall cybersecurity framework?	☐ YES	☐ NO
T2 SEC-31	Are there security controls for integration points between AI and other systems?	☐ YES	☐ NO
T2 SEC-32	Does your AI operate within the same security boundaries as your application?	☐ YES	☐ NO
T2 SEC-33	Are AI systems designed with logging to enable auditability of decisions?	☐ YES	☐ NO
T3 SEC-34	Do you conduct adversarial testing to identify AI-specific vulnerabilities?	☐ YES	☐ NO
T3 SEC-35	Are publicly available AI systems subject to continuous security testing?	☐ YES	☐ NO

PRIORITY ACTIONS IF YOU SCORED LOW:

- Apply role-based access to all AI systems and APIs
- Enable decision logging on customer-facing AI features

Venzip

5. TESTING, MONITORING & PERFORMANCE

Ensuring AI outputs remain accurate, reliable, and free from drift over time.

TIER ID		QUESTION	YES	NO
T1	TMPM-36	Are AI tools monitored for performance degradation and anomalies?	☐ YES	☐ NO
T1	TMPM-37	Are third-party audits conducted on AI systems?	☐ YES	☐ NO
T2	TMPM-38	Is there a structured AI testing framework covering pre and post-deployment?	☐ YES	☐ NO
T2	TMPM-39	Do you monitor AI models for data drift and concept drift?	☐ YES	☐ NO
T2	TMPM-40	Do you have processes to identify and mitigate AI hallucinations?	☐ YES	☐ NO
T3	TMPM-41	Are automated monitoring systems in place for continuous AI oversight?	☐ YES	☐ NO
T3	TMPM-42	Do AI systems undergo technical robustness certification?	☐ YES	☐ NO

PRIORITY ACTIONS IF YOU SCORED LOW:

- Set up basic performance monitoring and alerting for production AI systems
- Implement hallucination detection for any customer-facing generative AI

Venzip

6. TRANSPARENCY, EXPLAINABILITY, BIAS & FAIRNESS

Ensuring AI decisions are understandable, fair, documented, and free from harmful bias.

TIER ID	QUESTION	YES	NO
T1 TEBF-46	Are AI transparency requirements defined and communicated to users?	☐ YES	☐ NO
T1 TEBF-47	Are bias and fairness assessments conducted on AI systems?	☐ YES	☐ NO
T2 TEBF-48	Are explainability methods applied to AI decision-making processes?	☐ YES	☐ NO
T2 TEBF-49	Are model documentation requirements defined and enforced?	☐ YES	☐ NO
T3 TEBF-50	Are model interpretability requirements established for high-risk systems?	☐ YES	☐ NO
T3 TEBF-51	Do your AI models have published model cards documenting behavior and limits?	☐ YES	☐ NO

PRIORITY ACTIONS IF YOU SCORED LOW:

- Disclose to users when they are interacting with AI-generated content
- Run a bias assessment on your highest-risk AI system

Venzip

7. HUMAN OVERSIGHT & OPERATIONAL MANAGEMENT

Keeping humans in the loop for AI decisions, changes, versioning, and lifecycle management.

TIER ID	QUESTION	YES	NO
T1 HUM-53	Are AI use cases documented with defined scope and intended purpose?	☐ YES	☐ NO
T1 HUM-54	Are user feedback mechanisms in place to report AI issues?	☐ YES	☐ NO
T2 HUM-55	Are human oversight mechanisms implemented for AI decisions?	☐ YES	☐ NO
T2 HUM-56	Is there a formal change management process for AI systems?	☐ YES	☐ NO
T3 HUM-57	Do you maintain a model versioning and registry system?	☐ YES	☐ NO
T3 HUM-58	Is there a model decommissioning process for retiring AI systems?	☐ YES	☐ NO

PRIORITY ACTIONS IF YOU SCORED LOW:

- Implement a feedback mechanism for users to flag AI errors or concerns
- Define human override procedures for high-stakes AI decisions

Venzip

8. INCIDENT MANAGEMENT & BUSINESS CONTINUITY

Preparing for AI-specific incidents with defined response and recovery procedures.

TIER ID	QUESTION	YES	NO
T1 IRBC-61	Do AI vendor contracts include incident response requirements?	☐ YES	☐ NO
T2 IRBC-62	Is there an incident response plan specific to AI system failures?	☐ YES	☐ NO
T3 IRBC-63	Do AI developers have incident response procedures for model issues?	☐ YES	☐ NO
T3 IRBC-64	Are AI-specific business continuity plans documented and tested?	☐ YES	☐ NO

PRIORITY ACTIONS IF YOU SCORED LOW:

- Add AI failure scenarios to your existing incident response plan

Venzip

9. SKILLS & TRAINING

T1	ST-65	Are employees trained on how to use AI tools securely and responsibly?	☐ YES ☐ NO
T2	ST-66	Is there a skill development program for AI-related competencies?	☐ YES ☐ NO
T3	ST-67	Are advanced AI skills maintained through ongoing education programs?	☐ YES ☐ NO

PRIORITY ACTIONS IF YOU SCORED LOW:

- Roll out a basic AI acceptable use training for all employees

10. REPORTING & COMMUNICATION

T1	COM-68	Do AI vendors provide transparency reports about their systems?	☐ YES ☐ NO
T2	COM-69	Is AI data use communicated clearly to customers and stakeholders?	☐ YES ☐ NO
T3	COM-70	Are AI system reports generated for leadership and governance reviews?	☐ YES ☐ NO
T3	COM-71	Are model development standards documented and communicated?	☐ YES ☐ NO

PRIORITY ACTIONS IF YOU SCORED LOW:

- Request transparency reports from your top 3 AI vendors

11. THIRD-PARTY AI MODEL GOVERNANCE

Managing shadow AI, employee use of generative AI tools, and ungoverned third-party models. This domain addresses the #1 blind spot in most AI security programs today.

TIER	ID	QUESTION	YES	NO
T1	TPAI-72	Do you have a policy governing employee use of generative AI tools (ChatGPT, Copilot, etc.)?	☐	☐
T1	TPAI-73	Is there an approved list of AI tools employees are permitted to use?	☐	☐
T1	TPAI-74	Are employees prohibited from entering sensitive data into unapproved AI tools?	☐	☐
T2	TPAI-75	Do you monitor for unauthorized AI tool usage across the organization?	☐	☐
T2	TPAI-76	Are third-party AI APIs assessed for data retention and training practices?	☐	☐
T2	TPAI-77	Do you evaluate AI model providers for concentration risk and vendor lock-in?	☐	☐
T3	TPAI-78	Are there controls for AI-generated code used in your software development?	☐	☐
T3	TPAI-79	Do you assess the provenance and licensing of third-party AI models before use?	☐	☐

PRIORITY ACTIONS IF YOU SCORED LOW:

- Publish an AI acceptable use policy covering generative AI tools within 30 days
- Create an approved AI tool list and communicate it to all employees
- Block sensitive data categories from being entered into external AI tools
- Audit AI-assisted code in your codebase for security and licensing issues

DOMAIN SCORE: ___ / 8 Yes

Why this domain matters

Shadow AI is the fastest-growing security risk in most organizations. Employees are pasting customer data, source code, and internal documents into AI tools daily. Without governance, every AI tool is a potential data leak waiting to happen.

Venzip

12. AI REGULATORY READINESS

Preparing for current and emerging AI regulations including the EU AI Act, Canada's AIDA, and US state-level AI laws.

TIER ID	QUESTION	YES
T1 REG-80	Have you mapped which AI regulations apply to your organization based on geography and use case?	☐ YES ☐ NO
T1 REG-81	Are your AI systems classified according to the EU AI Act risk categories?	☐ YES ☐ NO
T2 REG-82	Do you track regulatory developments in AI across your operating jurisdictions?	☐ YES ☐ NO
T2 REG-83	Is there a process to assess the impact of new AI regulations on existing systems?	☐ YES ☐ NO
T2 REG-84	Are you prepared for Canada's AIDA requirements on high-impact AI systems?	☐ YES ☐ NO
T3 REG-85	Do you monitor US state-level AI legislation (Colorado AI Act, NYC Local Law 144, etc.)?	☐ YES ☐ NO
T3 REG-86	Is there a regulatory liaison or function responsible for AI compliance across jurisdictions?	☐ YES ☐ NO

PRIORITY ACTIONS IF YOU SCORED LOW:

- Map your AI systems to EU AI Act risk categories (unacceptable, high, limited, minimal)
- Monitor Canada's AIDA progress and assess impact on your operations
- Subscribe to regulatory alerts for AI legislation in your operating regions

DOMAIN SCORE: ___ / 7 Yes

Key AI Frameworks at a Glance

ISO 42001:	First international AI management system standard (2023). Certification-based.
EU AI Act:	World's first comprehensive AI law. Risk-based classification. Enforcement from 2025.
NIST AI RMF:	US voluntary framework: Govern, Map, Measure, Manage. Flexible, non-prescriptive.
Canada AIDA:	Proposed AI and Data Act. Mandatory for high-impact AI systems in Canada.

Venzip

SCORE YOUR GDPR READINESS

Total your Yes answers across all 12 domains. Use the guide below to understand your readiness level.

70-86 Yes — Strong Posture

Mature AI governance. Focus on continuous improvement, formal certification (ISO 42001), and staying ahead of regulatory changes.

45-69 Yes — Developing

Solid foundation with meaningful gaps. Prioritize the domains where you scored lowest and build a 90-day remediation roadmap.

20-44 Yes — Early Stage

Early stages of AI governance. Complete all Tier 1 controls first to establish a baseline before advancing.

0-19 Yes — Critical Gaps

Significant risk exposure. Immediate action needed. Consider engaging a compliance partner to accelerate.

YOUR TOTAL SCORE: _____ / 86

Tier 1 (Foundational): ___ / 26 Tier 2 (Operational): ___ / 32 Tier 3 (Advanced): ___ / 28

Venzip

BOARD-READY AI SECURITY SUMMARY

Use this page to present your AI security posture to the board, executive team, or audit ommittee. Fill in your scores and status.

Organization: _____

Date: _____

Assessed By: _____

AI Security Readiness by Domain

DOMAIN	SCORE	MAX	STATUS (circle)
1. Governance & Organizational Management	___	/ 9	Good / Fair / Gap
2. Risk Management & Compliance	___	/ 8	Good / Fair / Gap
3. Data Management & Privacy	___	/ 7	Good / Fair / Gap
4. Security Controls & Operations	___	/ 7	Good / Fair / Gap
5. Testing, Monitoring & Performance	___	/ 7	Good / Fair / Gap
6. Transparency, Bias & Fairness	___	/ 6	Good / Fair / Gap
7. Human Oversight & Operational Management	___	/ 6	Good / Fair / Gap
8. Incident Management & Business Continuity	___	/ 4	Good / Fair / Gap
9. Skills & Training	___	/ 3	Good / Fair / Gap
10. Reporting & Communication	___	/ 4	Good / Fair / Gap
11. Third-Party AI Model Governance	___	/ 8	Good / Fair / Gap
12. AI Regulatory Readiness	___	/ 7	Good / Fair / Gap
TOTAL	___	/ 86	OVERALL: _____

Venzip

Key Findings & Recommended Actions

1. _____
2. _____
3. _____

Next Steps

1. _____
2. _____
3. _____

Venzip

READY TO GOVERN YOUR AI WITH CONFIDENCE?

Venzip helps organizations build AI governance programs that satisfy regulators, win enterprise trust, and scale with your business.

What we do:

- AI security readiness assessments mapped to ISO 42001, EU AI Act, NIST AI RMF
- Shadow AI governance and acceptable use policy development
- AI governance program design and implementation
- Cross-framework compliance (ISO 27001 + SOC 2 + AI governance)
- Board-ready reporting and executive advisory
- Continuous monitoring and audit preparation

BOOK A FREE AI GOVERNANCE REVIEW

info@venzip.com
(604) 363-7138