IronRoot
Risk Consultants

AI Risk Radar

The 6 risks every business should know -- and how to manage them.

AI tools are moving faster than most governance programs. This guide maps the most common AI risks to practical mitigation steps so your team can adopt AI confidently -- without flying blind.

01

Hallucination & Inaccuracy

WHAT IT IS

AI models generate plausible-sounding but incorrect information -- dates, citations, calculations, legal text.

BUSINESS IMPACT

Decisions based on bad data; reputational or legal exposure.

HOW TO MANAGE IT

-- Treat AI output as a first draft -- always require human review for consequential decisions.

-- Define which use cases require citation or source verification.

-- Log AI-assisted decisions so errors can be traced and corrected.

02

Data Leakage & Privacy

WHAT IT IS

Employees paste sensitive data (customer PII, financial records, trade secrets) into AI tools that may use it for model training.

BUSINESS IMPACT

Regulatory violations (GLBA, HIPAA, GDPR), breach of client trust.

HOW TO MANAGE IT

-- Publish a clear AI Use Policy defining what data may never be entered into AI tools.

-- Evaluate vendor data retention and training opt-out settings.

-- Use enterprise-tier AI products with contractual data protections where possible.

03

Shadow AI & Ungoverned Adoption

WHAT IT IS

Employees use unapproved AI tools without IT or security awareness.

BUSINESS IMPACT

Unknown data flows, unvetted vendors, no audit trail.

HOW TO MANAGE IT

-- Create an approved AI tools list and communicate it org-wide.
-- Include AI tools in your vendor/third-party risk management program.
-- Conduct periodic discovery to identify unapproved tool usage.

04

Bias & Discriminatory Output

WHAT IT IS

AI outputs reflect biases in training data -- affecting hiring, lending, customer service, or content moderation.

BUSINESS IMPACT

Regulatory scrutiny, discrimination claims, brand damage.

HOW TO MANAGE IT

-- Test AI outputs for disparate impact before deploying in high-stakes decisions.
-- Require explainability for AI-assisted decisions affecting individuals.
-- Document how AI is used in regulated decision-making contexts.

05

Vendor Lock-in & Model Dependency

WHAT IT IS

Critical workflows built around a single AI vendor with no fallback.

BUSINESS IMPACT

Operational disruption if the vendor changes pricing, policy, or goes dark.

HOW TO MANAGE IT

-- Document all AI-dependent processes and their business impact.
-- Evaluate alternatives before committing to a single platform.
-- Include AI tools in your business continuity and resilience planning.

06

Compliance & Regulatory Uncertainty

WHAT IT IS

Regulatory expectations around AI use (in lending, healthcare, HR) are evolving quickly.

BUSINESS IMPACT

Non-compliance before your organization realizes a rule applies.

HOW TO MANAGE IT

-- Monitor your regulatory environment for AI-specific guidance.
-- Flag AI use cases in regulated domains (lending, benefits, hiring) for legal review.
-- Build AI governance documentation now so you're not starting from scratch.

Want to Build a Governance Framework Around AI?

IronRoot Risk Consultants offers AI Risk & Governance Advisory services designed for regulated and growing businesses.

chris@ironrootrisk.com | ironrootrisk.com