AI RISK READINESS CHECKLIST

A Practical Guide for Organizations Using AI Systems

This checklist helps you figure out if your organization is ready to handle AI risks. Go through each section honestly. If you find gaps, that's normal. The goal is to know where you stand and what needs work.

1. Understanding What AI You're Actually Using

Before you can manage AI risks, you need to know what AI systems are running in your organization. This includes everything from chatbots to automation tools to data analysis systems.

- ☐ We have a complete list of all AI systems we're using
- ☐ We know which departments are using which AI tools
- ☐ We track both official AI systems and tools employees use on their own
- ☐ We document what data each AI system has access to
- ☐ We know if our AI systems are cloud based, on premises, or both
- ☐ We regularly update this inventory when new AI tools are added

2. Data Protection and Privacy

AI systems often process sensitive information. You need to know what data is being used, where it's going, and whether it's being protected properly.

- ☐ We know what type of data our AI systems process (customer data, employee data, financial data, etc.)
- ☐ We have policies about what data can and cannot be fed into AI systems
- ☐ Employees know they shouldn't put confidential information into public AI tools
- ☐ We understand where our data is stored when we use third party AI services
- ☐ We have data retention policies for AI generated outputs
- ☐ We know if our AI vendors use our data to train their models
- ☐ We have contracts with AI vendors that specify data protection requirements
- ☐ We regularly audit what data is being sent to AI systems

3. Security and Access Control

AI systems can be entry points for security breaches if not properly protected. Access needs to be controlled and monitored.

- ☐ We control who can access each AI system in our organization
- ☐ We use proper authentication (passwords, two factor authentication) for AI tools

- ☐ We remove access when employees leave or change roles
- ☐ We log who uses AI systems and what they do with them
- ☐ We have security assessments done on our AI systems
- ☐ We keep AI software and platforms updated with security patches
- ☐ We test for vulnerabilities like prompt injection attacks
- ☐ We have an incident response plan if an AI system is compromised

4. Quality and Accuracy of AI Outputs

AI can make mistakes, hallucinate information, or produce biased results. You need processes to catch these problems before they cause damage.

- ☐ We have humans review important AI generated outputs before using them
- ☐ We test our AI systems regularly to check if they're producing accurate results
- ☐ Employees know that AI can be wrong and shouldn't be trusted blindly
- ☐ We have a way to report problems when AI gives bad outputs
- ☐ We test for bias in AI systems that make decisions about people
- ☐ We document known limitations of each AI system we use
- ☐ We track incidents where AI produced wrong or harmful outputs

5. Compliance and Legal Risks

Different regions have different laws about AI. You need to understand what regulations apply to your use of AI and make sure you're following them.

- ☐ We know which AI regulations apply to our industry and location
- ☐ We understand GDPR requirements if we operate in Europe
- ☐ We follow industry specific regulations (healthcare, finance, etc.) when using AI
- ☐ We have legal review of AI contracts and terms of service
- ☐ We understand who owns AI generated content we create
- ☐ We check if AI tools might violate copyright or intellectual property
- ☐ We have transparency about using AI when required by law
- ☐ We maintain records that regulators might request about our AI use

6. Employee Training and Awareness

Your team needs to understand both how to use AI effectively and what risks to watch out for. Training isn't a one time thing.

- ☐ Employees receive training on safe AI usage
- ☐ People know what kinds of information shouldn't go into AI systems
- ☐ We have clear guidelines on when AI output needs human review

- ☐ Employees know how to report AI related security incidents
- ☐ We update training when we adopt new AI tools
- ☐ Leadership understands AI risks, not just benefits
- ☐ We have someone responsible for AI governance and policy

7. Vendor and Third Party Risk

When you use external AI services, you're trusting those vendors with your data and operations. You need to know what you're getting into.

- ☐ We vet AI vendors before using their services
- ☐ We review vendor security practices and certifications
- ☐ We have contracts that specify what vendors can and cannot do with our data
- ☐ We know if vendors subcontract to other companies
- ☐ We understand vendor data retention and deletion policies
- ☐ We have backup plans if a vendor goes down or out of business
- ☐ We regularly review vendor performance and compliance
- ☐ We check if vendors have insurance for data breaches or AI failures

8. Business Continuity and Operational Risk

What happens if your AI systems fail or behave unexpectedly? You need plans for when things go wrong.

- ☐ We can operate if AI systems go down temporarily
- ☐ We have manual processes as backup for critical AI functions
- ☐ We monitor AI system performance and uptime
- ☐ We have alerts for when AI systems behave abnormally
- ☐ We test disaster recovery for AI dependent processes
- ☐ We know which business functions depend most heavily on AI
- ☐ We have documented procedures for AI system failures

9. Ethical Use and Reputation Risk

How you use AI affects your reputation and stakeholder trust. Some uses of AI can damage relationships even if they're technically legal.

- ☐ We have ethical guidelines for AI use in our organization
- ☐ We consider whether AI use might harm or discriminate against people
- ☐ We're transparent with customers when AI is making decisions about them
- ☐ We think about how AI use aligns with our company values
- ☐ We have a process to review ethically sensitive AI applications

- ☐ We consider environmental impact of large scale AI usage
- ☐ We have a way for people to appeal or contest AI decisions

10. Documentation and Accountability

Good documentation helps you understand what went wrong when problems happen and proves due diligence to regulators and stakeholders.

- ☐ We document why we chose specific AI systems
- ☐ We keep records of AI system testing and validation
- ☐ We document known issues and limitations of our AI systems
- ☐ We maintain version history when AI models or systems change
- ☐ We track incidents and how they were resolved
- ☐ We have clear ownership for each AI system (who's responsible)
- ☐ We document compliance efforts for audit purposes
- ☐ We regularly review and update all AI documentation

11. Financial and Cost Management

AI can get expensive fast, especially if usage isn't monitored. Unexpected costs are a real risk that affects your budget and operations.

- ☐ We track spending on all AI services and tools
- ☐ We have budgets set for AI usage
- ☐ We monitor AI usage to prevent runaway costs
- ☐ We understand pricing models for the AI services we use
- ☐ We have alerts for unusual spending spikes
- ☐ We review AI ROI regularly to ensure value for money
- ☐ We plan for AI costs in our long term financial forecasts

12. Code and Development Risks (If Building AI)

If your team builds AI systems or uses AI to write code, there are additional technical risks to manage. This section is especially important if you're a software company.

- ☐ We review AI generated code before deploying to production
- ☐ We test AI generated code thoroughly
- ☐ We scan for security vulnerabilities in AI written code
- ☐ We document which parts of our codebase were AI generated
- ☐ We have version control for AI models we develop
- ☐ We validate training data quality and sources
- ☐ We test AI models for bias and fairness

- ☐ We have processes for updating and retraining models safely

What Your Score Means

Count how many boxes you checked honestly. Here's a rough guide to where you stand:

Score	What It Means
0-25	High Risk: You have significant gaps in AI risk management. Start with the basics like knowing what AI you use and protecting sensitive data.
26-50	Medium Risk: You have some basics in place but major gaps remain. Focus on the sections where you checked the fewest boxes.
51-75	Moderate Risk: You're doing better than most organizations. Keep improving in weak areas and maintain what's working.
76-95	Low Risk: You have strong AI risk management practices. Keep monitoring and updating as AI technology and regulations evolve.

What To Do Next

Don't try to fix everything at once. Pick 3 to 5 items where you're weakest and start there. Here are some practical first steps:

- ☐ Create or update your inventory of AI systems
- ☐ Write clear policies about what data can go into AI tools
- ☐ Train employees on safe AI usage (even a simple one pager helps)
- ☐ Review contracts with AI vendors
- ☐ Assign someone to be responsible for AI governance
- ☐ Set up basic monitoring for AI system performance and costs

Remember: Perfect is the enemy of good. Start somewhere, make progress, and keep improving. The biggest risk is doing nothing because you think you need to do everything.
