AI Risk Management Checklist

Use this standardized checklist to keep track of your organization's AI risks arising from vendors, applications, devices and other technology platforms, in compliance with NIST CSF, ISO 27001:2022 & applicable data protection laws.

1. Acquisition of New Technologies that Include AI

- ❑ Vendor Assessment: Conduct thorough assessments of AI technology vendors to ensure they comply with NIST CSF and ISO 27001 standards. Verify their security practices, data privacy measures, and incident response plans.
- ❑ Data Security: Ensure that the AI technology includes robust data security measures such as encryption, access controls, and secure data storage.
- ❑ Compliance and Legal Risks: Review the legal and regulatory requirements for using AI technologies in your industry. Ensure that the technology complies with all relevant laws and regulations.

2. Building Artificial Intelligence into New Technologies

- Data Privacy and Compliance: Ensure that the integration of AI respects data privacy regulations such as GDPR or CCPA. This includes secure handling, storage, and processing of personal data.
- Ethical Considerations: Evaluate the ethical implications of the AI applications being developed. This includes considering the potential social impact and ensuring that the technology aligns with the organization's ethical standards.
- Technical Debt: Be aware of the long-term maintenance and update requirements of AI components. AI systems may require continuous monitoring, updating of models, and retraining to remain effective and secure.

3. Hiring Companies that Offer AI Services or Solutions

- Due Diligence: Perform due diligence on AI service providers. Evaluate their security policies, incident response capabilities, and compliance with NIST CSF and ISO 27001.
- Service Level Agreements (SLAs): Establish clear SLAs that define security requirements, data handling procedures, and response times for security incidents.
- Third-Party Risk Management: Continuously monitor the security practices of AI service providers. Conduct regular audits and reviews to ensure ongoing compliance and security

Other Recommendations for Managing AI Risk

- Continuous Monitoring: Implement ongoing monitoring of AI systems to detect and mitigate any emerging risks or performance issues. This includes setting up alerts for unusual behavior or outcomes.
- User Training: Train users on how to effectively and safely interact with AI systems. This includes understanding the limitations of AI and how to interpret its outputs.
- Robust Testing: Conduct thorough testing of AI systems in various scenarios to identify potential failures or biases before deployment. This includes stress testing and simulating adversarial conditions.
- Compliance Audits: Regularly audit AI systems for compliance with relevant laws, regulations, and industry standards. Ensure that any changes in regulations are promptly addressed in the AI systems.
- Ethical AI Framework: Develop and implement an ethical AI framework that guides the development, deployment, and use of AI technologies within the organization. This framework should align with the organization's values and societal expectations.

This professional checklist will help in managing the risks associated with the acquisition, development, and outsourcing of AI technologies and services.

Talk to us about customizing your AI Risk program:
https://www.AIRisk.ca

DATARISK
CANADA