JUPITER
CAPITAL MANAGEMENT

EXPERT ADVISORY & CONSULTING SERVICES

AI

Risk Identification

AI risk identification is a critical component of AI risk management. It involves systematically recognizing potential risks that could arise from the development, deployment, and use of artificial intelligence systems.

TECHNICAL RISK

- **Understand the AI System:** Analyze the AI model's architecture, algorithms, data sources, and intended applications to grasp potential vulnerabilities.
- **Review Technical Documentation:** Examine of design documents, development processes, and previous testing results for potential weaknesses.
- **Assess Model Performance:** Analyze accuracy, robustness, and generalization capabilities through testing datasets and validation methods.
- **Identify Biases and Fairness Issues:** Check for biases in training data and model outputs that could lead to unintended discrimination or unfair outcomes.
- **Evaluate Security Vulnerabilities:** Look for susceptibility to adversarial attacks, data breaches, or hacking attempts.
- **Perform Simulation and Stress Testing:** Run the AI system under diverse scenarios to uncover failure points or unexpected behaviors.
- **Monitor System Lifecycle:** Continuously track performance and behavior post-deployment to catch emerging technical risks.

OPERATIONAL RISK

- **Mapping Business Processes:** Understand how the AI system integrates into existing operations and workflows to identify potential disruptions or failures.
- **Stakeholder Interviews:** Engage with users, operators, and domain experts to gather insights on possible operational challenges and risks in real-world use.
- **Review Past Incidents:** Analyze historical data and incident reports related to AI or similar systems to recognize recurring operational issues.
- **Process and Change Management Reviews:** Evaluate how changes in AI models, data, or environment may impact operations.
- **Assess Human-AI Interaction:** Identify risks arising from user errors, inadequate training, or inappropriate reliance on AI outputs.
- **Evaluate Resource Availability:** Ensure availability of technical support, maintenance, and monitoring resources necessary for smooth operation.
- **Implement Monitoring Frameworks:** Establish key operational metrics and alerts to detect anomalies, failures, or performance drops during deployment.
- **Simulate Operational Scenarios:** Test the AI system under various operational conditions to reveal potential risks and failure modes.

ETHICAL & SOCIAL RISK

- **Assess Impact on Stakeholders:** Evaluate how AI deployment may affect different groups, including vulnerable populations, communities, and society at large.
- **Review Bias and Fairness:** Analyze training data and model outputs for potential biases that could lead to discrimination or unfair treatment.
- **Examine Privacy and Data Security:** Ensure data collection, storage, and usage comply with privacy standards and do not infringe on individuals' rights.
- **Evaluate Transparency and Explainability:** Determine if the AI system's decisions are interpretable and whether users and stakeholders understand how outcomes are generated.
- **Align with Ethical Guidelines and Regulations:** Check compliance with relevant ethical standards, legal frameworks, and societal norms.
- **Conduct Ethical Impact Assessments:** Engage ethicists and social scientists to evaluate potential moral dilemmas, societal consequences, or misuse risks.
- **Scenario Planning and Stakeholder Feedback:** Use scenarios and gather input from diverse stakeholders to anticipate and mitigate negative social or ethical outcomes.
- **Monitor Societal Trends and Public Perception:** Stay informed about societal values, public concerns, and debates related to AI technologies.

www.jupiter-cap.com Email: rod.boothe@jupiter-cap.com

JUPITER
CAPITAL MANAGEMENT

EXPERT ADVISORY & CONSULTING SERVICES

Risk Identification

AI

AI risk identification is a critical component of AI risk management. It involves systematically recognizing potential risks that could arise from the development, deployment, and use of artificial intelligence systems.

LEGAL & REGULATORY RISK

- **Review Applicable Laws and Regulations:** Understand local, national, and international laws related to data privacy (e.g., GDPR), AI use, safety standards, intellectual property, and industry-specific regulations.
- **Consult Legal Experts:** Engage legal professionals to interpret relevant regulations and identify potential compliance issues related to AI deployment.
- **Conduct Compliance Checklists:** Develop or use existing checklists to verify adherence to data protection, transparency, accountability, and non-discrimination requirements.
- **Analyze Data Usage and Consent:** Ensure data collection, processing, and storage comply with privacy laws and that proper consent mechanisms are in place.
- **Review Intellectual Property Rights:** Confirm that training data, models, and outputs do not infringe on third-party rights.
- **Assess Liability and Accountability:** Define responsibility for AI system errors, failures, or harm, considering legal frameworks for liability.
- **Monitor Regulatory Developments:** Stay updated on evolving laws, standards, and policies impacting AI at regional and global levels.
- **Perform Scenario Analysis:** Evaluate potential legal risks under different use cases or misuse scenarios to anticipate regulatory challenges.
- **Document Risk Assessments:** Keep records of legal and regulatory evaluations to facilitate audits and demonstrate compliance efforts.

DATA RISK

- **Assess Data Quality:** Evaluate the accuracy, completeness, consistency, and reliability of the data used for training and deployment.
- **Examine Data Biases:** Identify potential biases or prejudices inherent in the data that could lead to unfair or discriminatory outcomes.
- **Review Data Provenance and Lineage:** Ensure transparency about data sources, collection methods, and transformation processes to verify data integrity and authenticity.
- **Evaluate Data Privacy and Security:** Check compliance with data privacy laws and standards to prevent unauthorized access, leaks, or misuse of sensitive information.
- **Analyze Data Representativeness:** Ensure the data adequately represents the real-world scenarios and populations the AI system will serve.
- **Assess Data Volume and Variability:** Confirm that the dataset is sufficiently large and diverse to support robust model training and generalization.
- **Identify Data Management Risks:** Review data storage, version control, and access controls to prevent errors, corruption, or manipulation.
- **Perform Data Audits and Validation:** Regularly verify the correctness and appropriateness of data through audits, validation checks, and quality testing.

STAKEHOLDER RISK

- **Map Stakeholders:** Identify all relevant stakeholders, including users, developers, regulators, impacted communities, and business leaders.
- **Engage Stakeholders:** Conduct interviews, surveys, or workshops to gather their concerns, expectations, and perceptions about the AI system.
- **Analyze Expectations and Trust Levels:** Assess whether stakeholders understand, trust, and accept the AI system. Misaligned expectations can lead to resistance or misuse.
- **Evaluate Communication and Transparency:** Determine if stakeholders have sufficient information about AI decision-making processes and limitations.
- **Identify Resistance or Conflict Risks:** Recognize potential conflicts, opposition, or misunderstanding that could hinder deployment or adoption.
- **Assess Impact on Stakeholders:** Analyze how AI outcomes might affect different groups, especially vulnerable or marginalized communities, to identify risks of harm or social discontent.
- **Monitor Stakeholder Feedback:** Establish channels for ongoing feedback to detect emerging concerns or dissatisfaction.
- **Review Legal and Social Constraints:** Consider legal obligations and societal norms that might affect stakeholder acceptance or lead to compliance risks.

www.jupiter-cap.com **Email: rod.boothe@jupiter-cap.com**