Wisconsin Counties Association

2025 ANNUAL CONFERENCE GAME DAY

1:00 – 2:00 PM

Cybersecurity, Compliance and AI Policies: Governing in the Digital Era

Governing in the Digital Era: Cybersecurity, Compliance, and AI Policies

Ben Hall

Practice Manager – Governance, Risk, & Compliance - Heartland Business Systems

Seth Johnson

Senior Cyber Risk Professional – Charles Taylor – County Mutual

Barry West

IT Director Waushara County – GIPAW Board Chairperson

T.J. Podmolik

IT Director Price County – GIPAW Board Member

Cybersecurity & Risk Management

Importance of Cybersecurity Maturity

- Cybersecurity maturity refers to the level of sophistication, effectiveness, and resilience of an organization's cybersecurity practices, policies, and controls.
- It indicates how well an organization has implemented and optimized its cybersecurity framework to protect against threats, vulnerabilities, and attacks.

Information Security Risk Management Program

- Aligning security risk with business objectives through risk assessments
- Guides an organization in making rational decisions to improve security posture and aligning risk with acceptable tolerance levels
- Build out your Information Security Policy & Program
- Increase your preparedness and responses to Incidents and Disasters

Steps to Achieve Cybersecurity Maturity

1. Establish a vision & risk appetite

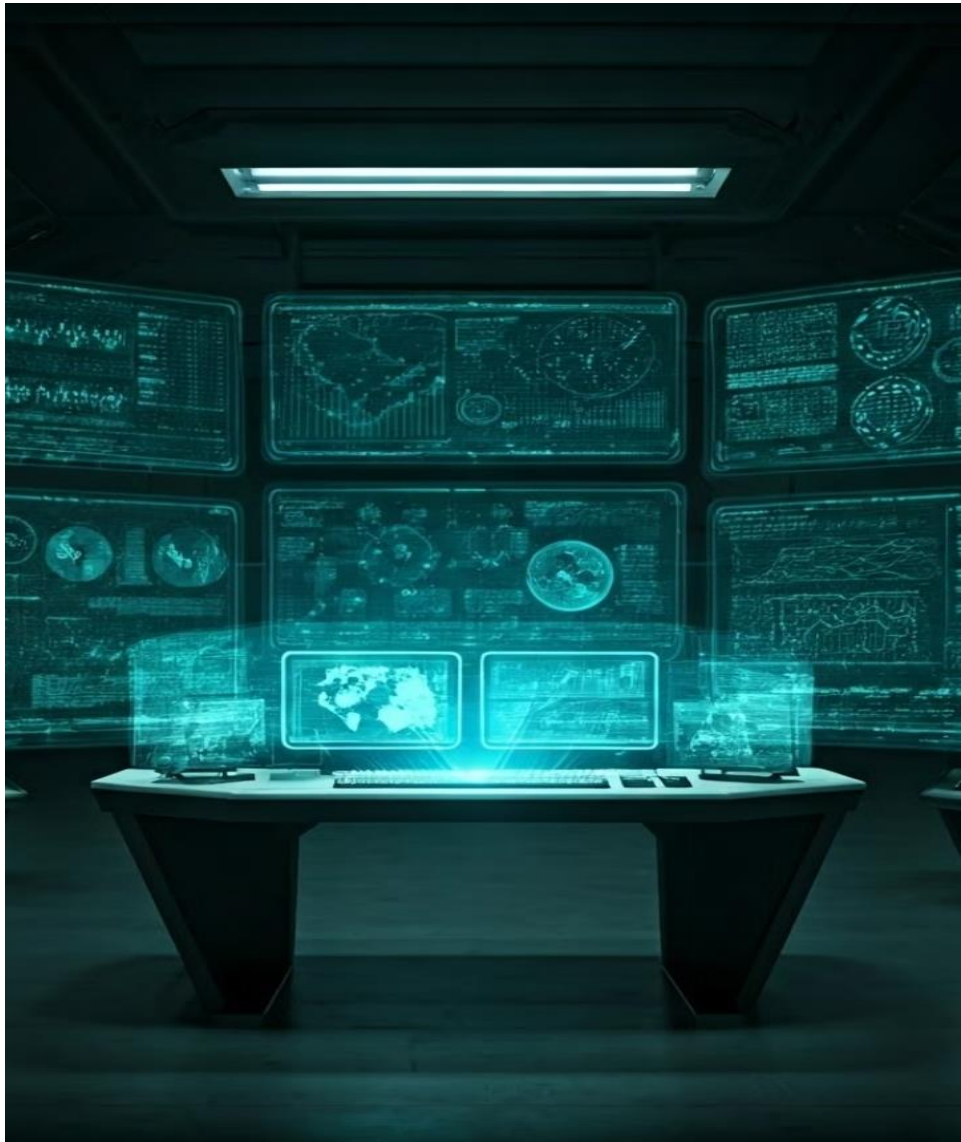
   Develop a comprehensive security strategy aligned with your business objectives and risk tolerance.

2. Prioritize Initiatives

   Provide strategic direction to help the organization achieve your goals. Determine and prioritize security initiatives to reduce risk in an efficient and cost-effective manner.

3. Reduce Risk & Continuous Improvement

   Continuously evaluating and addressing security risk. Ongoing monitoring, testing, and optimization ensure your security infrastructure remains effective against evolving threats.



AI Risk Management Goals

Build safeguards around the use of AI systems for individuals and the organization

- Implement bias detection and mitigation techniques for AI-driven hiring tools to ensure fairness and avoid discrimination.

Enforce AI principles for the development and deployment of AI systems

- Create an AI risk council to assess alignment of AI initiatives to foundational AI principles before evaluating the AI solution.

Ensure accuracy and validity in AI systems

- Implement explainable AI techniques to ensure AI responses and decision-making processes are more transparent and interpretable.

Comply with existing and emerging AI regulations

- Implement an AI risk management program to comply with the future AI regulatory requirements for high-risk AI systems.

Maximize the value from AI systems

- Implement continuous monitoring and evaluation of AI systems to ensure performance is optimized and any gaps are identified.

AI Risk Management Framework

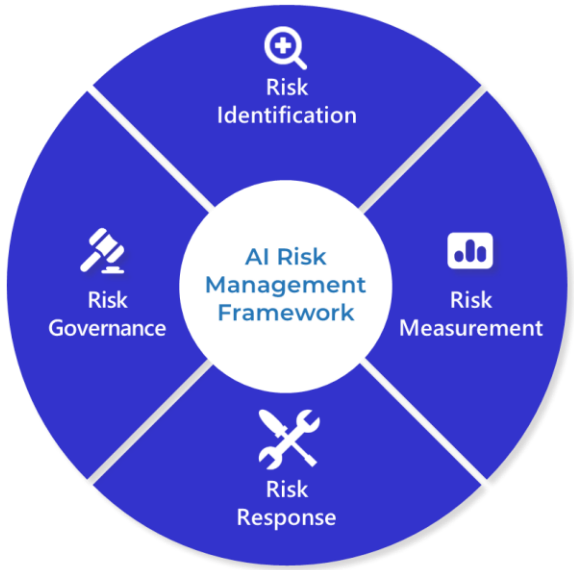
Four Core Functions

Risk Governance

- Risk prioritization, treatment, and response.
- Accountability structures are in place so that the appropriate teams and individuals are empowered, responsible, and trained for mapping, measuring, and managing AI risks.
- Organizational teams are committed to a culture that considers and communicates AI risk.
- Processes are in place for robust engagement with relevant AI actors.

Risk Response

- Risk prioritization, treatment and response
- Decommissioning mechanisms (“Kill switches”)
- Incident response plans
- ML and endpoint security countermeasures
- Regulatory compliance
- Software quality assurance



Risk Identification

- Context is established and understood.
- Categorization of the AI system is performed.
- AI capabilities, targeted usage, goals, and expected benefits and costs compared with appropriate benchmarks are understood.

Risk Measurement

- Appropriate methods and metrics are identified and applied.
- AI systems are evaluated for alignment to foundational AI principles.
- Mechanisms for tracking identified AI risks over time are in place.
- Feedback about efficacy of measurement is gathered and assessed.