

CIS 2269: Managing AI Risk in Higher Education Environments: A Comprehensive Approach

Colorado Robertson

Associate Vice Chancellor for Risk Management

Elliot Young

Director of Compliance & Equal Opportunity

Objectives

What you'll take away from today's session

1

Understanding AI Risks & Opportunities

- Key AI concepts and terminology
- Cybersecurity issues involving AI
- Navigating the regulatory landscape
- How AI can drive operational efficiency and decision-making

2

Strategies to Mitigate Risks & Capture Opportunities

- Develop responsible AI policies and governance
- Foster cross-functional collaboration for AI risk management
- Apply risk statements you can plug into your institution's ERM program

The Big Questions About AI

Where AI is reshaping the modern campus

OP

Operations & Administration

How will AI reshape operational structures and administrative efficiency across the institution?

TL

Teaching & Learning

In what ways will AI transform pedagogy, curriculum design, and the student experience?

RD

Research & Discovery

What implications does AI carry for research methodologies, integrity, and outcomes?

Your Experience with AI

A quick pulse before we dive in



We're using polling to tailor today's session to your familiarity and interests.



No right or wrong answers — this is a starting point, not a quiz.



Be ready to share examples as we move through each topic.

Generative AI Pervades Higher Education: Here's How Three Institutions Responded

LOOKING FOR MORE?

al State University's \$17 million A.I. funded, attacked

t for higher education

4 higher education lead
t biggest benefits and risks

WILL A.I. MAKE COLLEGE OBSOLETE?

Education Part 1

DEEP DIVE

AI is changing higher education. Here's what faculty members have to say about it

will the rise of AI in the
impact liberal arts
education

AI Causes Worries About Job Market, Value of Higher Education

Survey: When Should College Students Use AI? They're Not Sure

Block 1: Understanding AI Risks & Opportunities

1:35 – 2:15 pm

AI

Concepts & Terminology

Build a shared vocabulary so the rest of the session lands.

CS

Cybersecurity & Regulation

Where AI meets data privacy, FERPA, GDPR, and ISO standards.

OP

Operational Lift

Where AI creates real efficiency gains for higher ed.

?

Element of Engagement

Facilitated discussion: where are AI risks showing up in your workplace today?

Key AI Concepts & Terminology

A shared vocabulary for the rest of the session

AI Artificial Intelligence

Systems that interpret complex data and make informed decisions.

ML Machine Learning

Algorithms that improve automatically through experience and data.

GEN Generative AI

Systems that produce new content (text, image, audio, code).

LLM Large Language Models

Models that interpret and generate human language at scale.

⚠️ Hallucination

AI output that looks plausible but is factually wrong or invented.

⚠️ Deepfake

Realistic but fabricated media; a significant misinformation risk.

Reference:Axios — 'All the AI terms you need to know'

Cybersecurity & AI

AI is changing both sides of the threat surface



Elevated risk of sophisticated, AI-assisted data breaches and social engineering.



Greater vulnerability from AI-driven threats: phishing at scale, voice cloning, prompt injection.



Imperative for robust cybersecurity frameworks and incident response plans built for AI-era attacks.

Regulatory Landscape

Standards and laws shaping AI in higher ed



Integrate emerging international standards — ISO/IEC 42001 and ISO/IEC 23894:2023.



Comply with core data privacy regimes: FERPA, GDPR, state privacy laws.



Address legal, ethical, and reputational risk stemming from non-compliance.

Operational Efficiencies

Where AI creates real impact for higher ed



Streamline administrative processes and enable data-driven decision-making.



Optimize resource allocation and scale operations without scaling headcount linearly.



Plan for and manage disruption associated with AI adoption.

Factors to Consider: Operations

Tensions to manage as you deploy AI in operations

P Privacy & Security

Strengthen data privacy posture and reduce attack surface as AI consumes more data.

W Workforce Transition

Manage role shifts and potential displacement with reskilling and clear communication.

H Human Oversight

Balance AI integration with human review — especially for high-stakes decisions.

E Ethical Decisions

Address ethical dilemmas in automated decision-making before they become incidents.

Factors to Consider: Academics

Where teaching and learning meet AI

AI Academic Integrity

Preserve integrity and respond to new forms of academic dishonesty.

Q Quality Standards

Maintain quality education standards amid growing AI reliance.

F Faculty Support

Provide resources and training so faculty can adopt AI responsibly.

E Ethics & Privacy

Navigate ethics and student privacy in increasingly AI-mediated classrooms.

Factors to Consider: Research

Protecting integrity and IP in AI-enabled research



Secure sensitive research data and protect institutional IP.



Identify and mitigate bias in AI-driven research outcomes.



Uphold ethical standards across research design and publication.



Manage the risk that over-reliance on AI compromises research quality.



Allocate resources to support responsible AI integration in research.

Facilitated Discussion

Your turn — what does this look like at your institution?



Discussion Prompts

- Which AI risks are already impacting your institution today?
- Where have you seen AI integration go well — and where has it gone sideways?
- What risk management practices are you using right now? What's missing?

Block 2: Mitigating Risks & Capturing Opportunities

2:15 – 3:00 pm

P

Responsible AI Policies

Build governance that's both clear and operational.

C

Cross-Functional Collaboration

Pull legal, IT, academic, and admin into the same room.

R

ERM Risk Statements

Concrete language you can plug into your enterprise risk program.



Element of Engagement

Small group breakout: build strategies for risk mitigation and opportunity at your institution.

AI Risk Assessment

Polling questions



How do you view the impact of AI on higher education overall?



Where are the most significant risk areas for your institution?



Where are the biggest opportunities for AI to drive value?

Responsible AI Policies & Governance

Three pillars of an institutional AI policy

1

Clear Guidelines

Formulate actionable, plain-language rules for how AI may and may not be used.

2

Transparency

Disclose where and how AI is shaping decisions, especially those affecting students.

3

Accountability

Stand up oversight mechanisms with named owners and a real escalation path.

Collaboration for AI Risk Management

AI risk doesn't sit in any one office

T

Multidisciplinary Teams

Bring legal, IT, academic, and administrative stakeholders to the same table.

C

Regular Engagement

Schedule recurring sessions to surface and discuss evolving AI risks.

E

Training & Education

Run AI risk management training and workshops across the institution.

AI Impact on Academics

Risk statements and management actions for teaching and learning

Confabulation (AI-Generated Misinformation)

! Risk Statement

AI chatbots and automated systems may give students incorrect information about coursework, degree requirements, or university policies, leading to poor academic decisions.

✓ Management Actions

- Require human oversight and validation of any critical AI-generated information.
- Test AI-generated content in academic and advising contexts before deployment.
- Build feedback channels for students and staff to report misinformation.

Plug this into your ERM register and assign an owner.

Harmful Bias & Discrimination

! Risk Statement

AI used in admissions, grading, or advising can perpetuate racial, gender, or socioeconomic bias, producing unequal academic opportunities.

✓ Management Actions

- Conduct regular bias audits on AI systems involved in academic decisions.
- Use diverse training data and inclusive design practices.
- Periodically review AI performance across demographic groups.

Plug this into your ERM register and assign an owner.

Information Integrity

! Risk Statement

AI used in research or content generation can introduce fabricated or misleading academic material, compromising integrity.

✓ Management Actions

- Track the provenance of AI-generated academic content.
- Educate students and faculty on responsible AI use in research and writing.
- Run plagiarism and integrity checks on AI-generated work.

Plug this into your ERM register and assign an owner.

Obscene, Degrading, or Abusive Content

! Risk Statement

AI used for content creation in academic or creative coursework can generate inappropriate or harmful material.

✓ Management Actions

- Implement content filtering and moderation tools at the platform level.
- Set clear guidelines for AI use in student projects, especially in art and media.
- Define and publish consequences for misuse.

Plug this into your ERM register and assign an owner.

AI Impact on Operations

Risk statements and management actions for the administrative core

Data Privacy

! Risk Statement

Universities use AI for admissions, financial aid, and student tracking. Sensitive student data may be exposed through these systems.

✓ Management Actions

- Establish policies on data collection, anonymization, and use.
- Be transparent about how AI uses institutional data.
- Audit AI systems regularly for compliance with FERPA and other privacy standards.

Plug this into your ERM register and assign an owner.

Security Vulnerabilities

! Risk Statement

AI systems integrated into university operations — student management, research, finance — expand the cyberattack surface.

✓ Management Actions

- Strengthen cybersecurity controls and encrypt data at rest and in transit.
- Run routine security assessments on AI models in critical operations.
- Treat AI vendors with the same scrutiny as any other critical system.

Plug this into your ERM register and assign an owner.

Over-Reliance on AI (Human-AI Configuration)

! Risk Statement

Faculty and staff may lean too heavily on AI for grading, scheduling, or advising, diminishing human judgment and oversight.

✓ Management Actions

- Set policies on appropriate use of AI in decision-making.
- Train faculty and staff on when human judgment should override AI.
- Build audit trails so AI-influenced decisions remain reviewable.

Plug this into your ERM register and assign an owner.

Over-Reliance on AI: Policies & Procedures

! Risk Statement

Institutions can use AI to draft policies, procedures, and training materials faster than they can maintain or follow them. Written policies that go unfollowed become liability, the gap between stated policy and actual practice becomes an exhibit in litigation, audits, and accreditation reviews.

✓ Management Actions

- Pair every AI-drafted policy with a named owner and review cadence.
- Pilot before rollout verify it can actually be operationalized.
- Run periodic gap analyses comparing stated policy to actual practice. (AI Can Help)
- Sunset or revise procedures that aren't yet operationalized.

Faster drafting doesn't mean faster compliance. Adopt only what you can maintain.

Environmental Impact

! Risk Statement

Training and running AI models consumes significant computational resources, driving up energy use and emissions.

✓ Management Actions

- Adopt energy-efficient AI technologies and right-sized models.
- Prioritize sustainable energy practices in cloud and on-prem services.
- Monitor and report the environmental footprint of institutional AI use.

Plug this into your ERM register and assign an owner.

AI Impact on Research

Risk statements and management actions for the research enterprise

Intellectual Property Violations

! Risk Statement

AI models can generate content that infringes on existing IP (including copyrighted academic works) or misuse student-created material.

✓ Management Actions

- Establish clear IP policies for AI-generated content.
- Ensure AI systems comply with copyright and fair-use rules.
- Provide training on IP rights, licensing, and fair use.

Plug this into your ERM register and assign an owner.

Confabulation in Research

! Risk Statement

AI systems can introduce incorrect or fabricated information, leading to integrity failures in research outputs.

✓ Management Actions

- Require human validation of AI-provided information in research and publication.
- Use content provenance tools and structured review processes.
- Build AI use disclosure into the research workflow.

Plug this into your ERM register and assign an owner.

Information Integrity in Research

! Risk Statement

AI-generated content used in research may introduce errors or fabrications, undermining credibility of academic research.

✓ Management Actions

- Track AI-generated contributions and validate them independently.
- Educate researchers on responsible AI use across the research lifecycle.
- Strengthen pre-publication review for AI-assisted manuscripts.

Plug this into your ERM register and assign an owner.

AI & Privacy

Data is the foundation protect it accordingly



Recognize the critical importance of data in contemporary higher ed contexts.



Implement rigorous protocols to safeguard personal and institutional data privacy.



Apply the same privacy diligence to AI systems that you apply to any other system of record.



AI & Insurance

Coverage, liability, and contract language



Evaluate coverage and liability concerns specific to AI-related incidents.



Integrate AI considerations directly into institutional insurance policies.



Insert AI-specific language and indemnification into vendor contracts.



AI & Cybersecurity

Preparing for an evolving threat landscape



Understand and prepare for AI-enhanced cyber threats phishing, deepfakes, prompt injection.



Develop proactive strategies and layered defenses to mitigate emerging risks.



Update incident response and tabletop exercises to include AI-specific scenarios.



Small Group Discussions

Take the framework back to your institution



Targeted Strategies

Develop strategies you'd actually use to manage the AI risks we've discussed.



Opportunities

Identify concrete opportunities for institutional advancement through AI.



Day-to-Day Integration

Where can AI plug into your daily work — budgeting, forecasting, procurement, advising, communications?

Conclusion & Closing Reflections

What you're leaving with

- 1 Summarize key insights, strategies, and best practices from today's session.
- 2 Address remaining participant questions.
- 3 Outline clear next steps for strategic AI implementation and risk management at your institution.

Contacts

Reach out! We'd love to keep the conversation going



Colorado Robertson

Assistant Vice Chancellor for Risk Management

Louisiana State University

colorado.robertson@lsu.edu



Elliot Young

Director of Institutional Compliance & Equal
Opportunity

Kansas City University

elyoung@kansascity.edu

Thank you for spending the afternoon with us.