NSU 4TH ANNUAL CYBERSECURITY GRADUATE RESEARCH SYMPOSIUM

Governance, Ethics, and Institutional Preparedness for Emerging Intelligent Systems

George Antoniou, PhD | Full Professor of Cybersecurity Management

Lynn University • Boca Raton, Florida

October 28, 2026

The institutional preparedness challenge

The pace of adoption and the pace of governance are not always aligned

ADOPTION IS NOT THE SAME AS PREPAREDNESS



AI CAPABILITY

Systems and use cases

≠



INSTITUTIONAL READINESS

Policies and safeguards

The gap is a governance challenge

Research problem and contribution

A conceptual perspective—not a validated maturity score

FROM AN ADOPTION PROBLEM TO A RESEARCH QUESTION



Conceptual perspective • not an empirically validated maturity score

Governance: who is accountable?

Responsible AI requires decision rights—not policy statements alone



THE OPERATING MODEL FOR

AI GOVERNANCE

STRUCTURE. OVERSIGHT. TRUST AT SCALE.





OWNERSHIP & ROLES

BOARD	EXECUTIVE	BUSINESS OWNER	RISK & COMPLIANCE	DATA SCIENCE	IT & SECURITY
Oversight and strategy	Leadership and resources	Implementation and compliance	Monitoring and assurance	Models and data	Technical safeguards

DECISION RIGHTS (APPROVAL GATES)

SUBMIT Proposal → ASSESS Risk & Impact → APPROVE with Conditions → AUTHORIZE Deployment → MONITOR and Review

REVIEW PATHWAYS (CHECKPOINTS)

DESIGN Ethical & Privacy Review → DEVELOP Security & Bias Testing → TEST Performance and Compliance → DEPLOY with Oversight → OPERATE and Reassess

CONTROL POINTS (MONITORING SIGNALS)

MODEL PERFORMANCE | DATA QUALITY and USAGE | RISK INDICATORS | POLICY COMPLIANCE | USER FEEDBACK

LIFECYCLE OVERSIGHT (DASHBOARDS)



WORKFORCE PREPAREDNESS

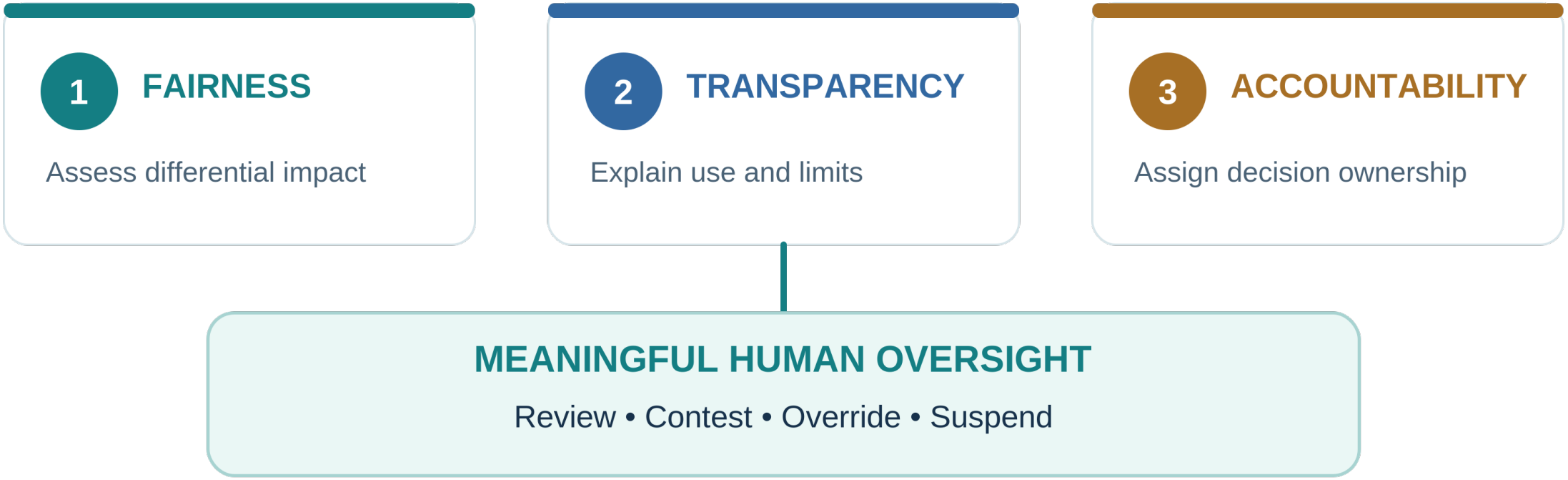
AI LITERACY	TRAINING	SKILLS	CULTURE
for Faculty, Staff and Students	and Professional Development	and Competency Growth	of Responsible AI Use

STRATEGY ALIGNED | RISK MANAGED | VALUE REALIZED | TRUST EARNED

Ethics: principles must become oversight

Human intervention must be meaningful, documented, and actionable

FROM ETHICAL PRINCIPLES TO ACTIONABLE OVERSIGHT



Cybersecurity and institutional resilience

AI expands the attack surface while preserving existing security obligations

AI EXPANDS THE ATTACK SURFACE

1 DATA

Privacy

sensitive records • provenance

2 MODELS

Manipulation

misuse • reliability

3 OPERATIONS

Access

vendors • incident response

INSTITUTIONAL DEFENSE IN DEPTH

Risk ownership • Monitoring • Incident response • Recovery

Workforce preparedness is institutional capacity

AI literacy must reach the people making, using, and supervising decisions

PREPAREDNESS DEPENDS ON PEOPLE AND ROLES



LEADERSHIP

Decision rights and risk appetite



PRACTITIONERS

Secure implementation and monitoring



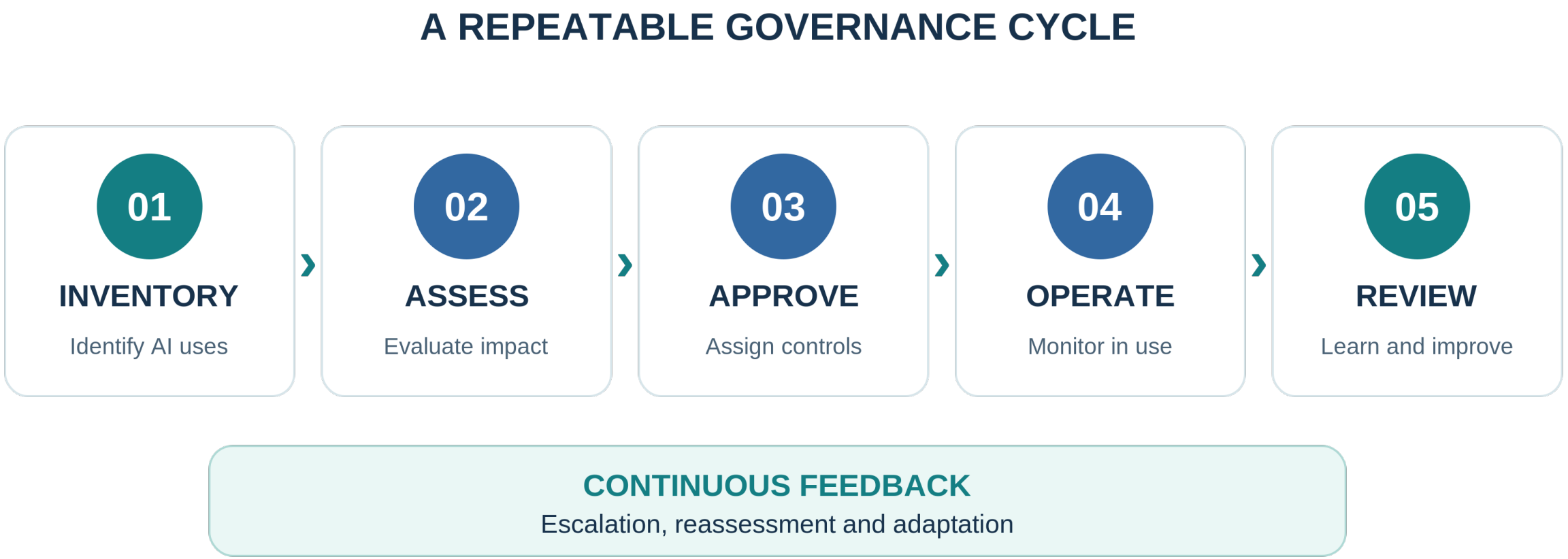
USERS

AI literacy and responsible use

Training must be role-specific, sustained and documented

Operational integration: principles into practice

A repeatable institutional governance cycle



Institutional Readiness: Illustrative Assessment Areas

Five NSU presentation themes — not the five dimensions of the Valencia conceptual framework

READINESS IS EVIDENCED — NOT ASSUMED

GOVERNANCE	Approved policies + accountable owners
ETHICS	Impact reviews + contestability
CYBERSECURITY	Threat assessments + response plans
WORKFORCE	Training records + role-specific competence
OPERATIONS	AI inventory + monitoring records

Illustrative indicators; no validated numerical maturity score

Informed by conceptual AI readiness research, cybersecurity governance, and AI risk-management guidance.

NIST and European guidance inform readiness

Complementary foundations for institutional governance

GLOBAL GUIDANCE → LOCAL INSTITUTIONAL PRACTICE

NIST AI RMF

- GOVERN • MAP • MEASURE • MANAGE
- Lifecycle risk management and governance

EUROPEAN GOVERNANCE

- Trustworthiness, rights and transparency
- Risk-based safeguards and human oversight

INSTITUTIONAL READINESS

Policies • People • Controls • Evidence

International collaboration: a practice-informed lens

Fulbright experience informs the questions—not claims of empirical validation

INTERNATIONAL COLLABORATION AS A PRACTICE-INFORMED LENS



POLICY ALIGNMENT

Who authorizes AI use?



FACULTY CAPACITY

Who is prepared to teach and use it?



ETHICAL OVERSIGHT

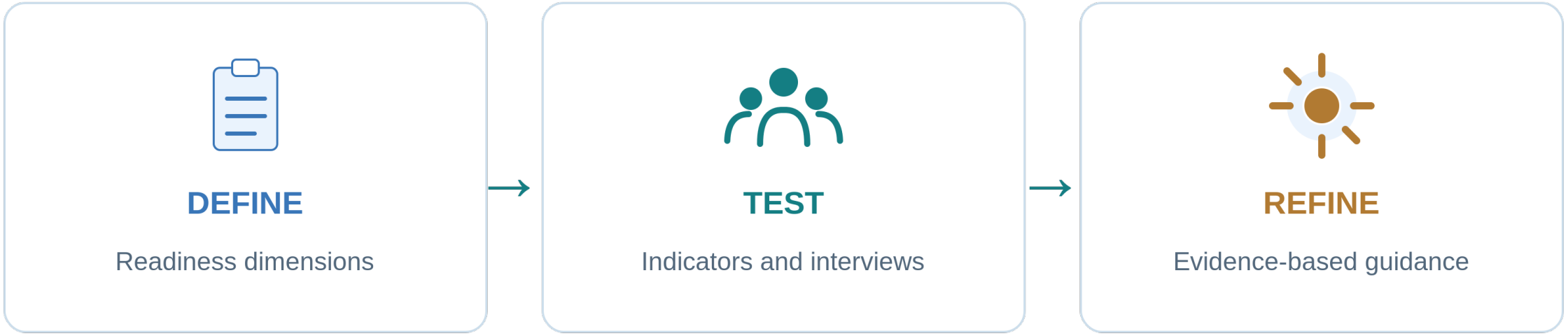
Who reviews consequences?

Illustrative institutional questions — not measured research outcomes

Research contribution and next steps

From a conceptual perspective toward testable institutional evidence

FROM A CONCEPTUAL PERSPECTIVE TO TESTABLE EVIDENCE



Future research: validation, cross-institutional comparison and refinement

Institutional preparedness is a governance capability

Three takeaways for research and practice

THREE MESSAGES FOR INSTITUTIONS



ADOPTION ≠ READINESS

Capability is only the start



ACCOUNTABILITY MATTERS

Human oversight and security



EVIDENCE MATTERS

Governance must be demonstrable

Preparedness is a continuing institutional capability

Thank You

Questions?

George Antoniou, PhD

Full Professor of Cybersecurity Management

Lynn University

gantoniou@lynn.edu

Boca Raton, Florida

Scan to email me

Connect on LinkedIn

linkedin.com/in/cyberninja