Advanced Forensics & Governance

Level 3: Lucas Cycle

AI Accountability Through Forensic Methods

5-6 Hours

Overview 5 Modules Outcomes

From Detection to Enforcement

Lucas Cycle Focus: Level 3 shifts from identifying governance gaps to operationalizing forensic accountability. These five modules teach the institutional practices, audit frameworks, and technical controls needed to move ESG reporting from theater to evidence.

By the end of Level 3, participants can design and audit **"Sociable Systems"**—workflows where AI and humans have explicit, tested authority boundaries. You'll learn to:

- • Detect institutional harm encoded in algorithms
- • Audit third-party models even when documentation is "black box"
- • Design operational controls that transform trust into evidence
- • Map decision rights and liability so humans never become scapegoats

This is advanced material for ESG Directors, Internal Assurance Leads, and governance professionals. Completion requires demonstrated mastery of forensic methods and systems thinking.

What You Will Build

Fairness Forensics Report

Prove algorithmic bias using statistical methods (bias detection, equity analysis)

Assurance Protocol (SOP)

Define sampling, versioning, and human sign-off procedures for operational AI systems

Third-Party Risk Register

Map vendor models, failure modes, and contractual liability constraints

RACI Governance Blueprint

Assign decision rights and accountability so the "Liability Sponge" is eliminated

Level 3 Modules

- **M5:** Institutional Harm & Fairness Forensics
- **M6:** Cybersecurity as Governance Credibility
- **M7:** The AI Assurance Role & Competency Map
- **M8:** Operational Assurance Controls
- **M9:** Model Risk & Third-Party Governance

Prerequisites

- Completion of Level 1 & 2
- Understanding of Liability Sponge, Evidence Ladder
- Basic familiarity with audit concepts

Five Forensic Modules

Each module builds institutional capability for detecting and preventing algorithmic harm.

L3-M5

Institutional Harm & Fairness Forensics

Forensics

WHY IT EXISTS

Bias in ESG isn't just about people; it's about supplier exclusion. Algorithms that penalize "missing data" systematically harm developing regions.

CORE CONCEPTS

- Institutional Harm Pathways
- Zero-Shot Bias (Data Availability)
- The Appeals Process as Governance

DELIVERABLE

Fairness & Bias Stress-Test Format: Report / Simulation
ACCEPTANCE CRITERIA

✓ Tests for "Missing Data" penalty
✓ Compares False Positive rates across regions

✓ Documents the "Path to Appeal" for rejected vendors

AUTHORITY BOUNDARY

Stop-the-Line: Disparate impact > 20% variance → Pause Vendor Selection Model.

ASSURANCE CONTROL OF THE WEEK

The "Empty Field" Test

Submit a perfect supplier profile with *one* missing non-critical field. If rejected, the model is fragile/biased.

L3-M6

Cybersecurity as Governance Credibility

Governance

WHY IT EXISTS

A breached supply chain dataset is a credibility breach, not only an IT incident. If you can't protect the data, you can't attest to the report's integrity.

CORE CONCEPTS

- Data Integrity vs. Availability
- The "Stop Work Authority" for Data
- Incident Disclosure Protocols

DELIVERABLE

Data Integrity Response Protocol Format: Flowchart

ACCEPTANCE CRITERIA

✓ Defines who declares a "Data Breach"

✓ Mandates notification of assurance providers

✓ Includes "correction/withdrawal procedure" for published reports

AUTHORITY BOUNDARY

Stop-the-Line: Unverified data source injection → Immediate Report Freeze.

ASSURANCE CONTROL OF THE WEEK

Provenance Check

Verify the cryptographic hash or chain-of-custody log for the final dataset.

L3-M7

The AI Assurance Role & Competency Map

Strategy

WHY IT EXISTS

Preparing for the shift from "checking boxes" to "auditing code." The near-term regulatory horizon requires forensic capability.

CORE CONCEPTS

- The AI Assurance Competency Map
- "Training the Trainers" (Recursive Authority)
- Sandboxes & Testing Infrastructures

DELIVERABLE

Career Roadmap / Skill Gap Analysis Format: Personal Assessment
ACCEPTANCE CRITERIA

✓ Assesses Python/SQL literacy
✓ Evaluates "Skepticism" & Forensic Mindset
✓ Maps current role to "AI Assurance" requirements

AUTHORITY BOUNDARY

Stop-the-Line: Assurance Lead cannot sign off if "Black Box" opacity prevents testing.

ASSURANCE CONTROL OF THE WEEK

The "Explanation" Challenge

Can the assurance lead explain the model's decision in plain language? If not, audit fails.

L3-M8

Operational Assurance Controls

Assurance

WHY IT EXISTS

To operationalize the "Calvin Convention" into daily audit practice. Turning "trust" into "evidence."

CORE CONCEPTS

- Sampling Methodologies for AI Outputs
- Reconciliation Trails
- Change Control & Versioning

DELIVERABLE

The Assurance Protocol Format: SOP Document

ACCEPTANCE CRITERIA

- ✓ Defines sampling frequency (e.g., 1 in 10)
- ✓ Requires "Human-in-the-Loop" log signatures
- ✓ Mandates version control for all prompts/models

AUTHORITY BOUNDARY

Stop-the-Line: Missing version history for prompt or model → Audit Failure.

ASSURANCE CONTROL OF THE WEEK

Reconciliation Logic

Total Input Records == Total Output Records + Total Exceptions.

L3-M9

Model Risk & Third-Party Governance

Governance

WHY IT EXISTS

To manage the risk of "outsourced reasoning." When the vendor holds the IP, you still hold the liability.

CORE CONCEPTS

- Vendor Due Diligence
- IP vs. Accountability (The Clarke Constraint)
- Escalation Paths for Black Box Failures

DELIVERABLE

Third-Party Risk Register Format: Risk Log
ACCEPTANCE CRITERIA

- ✓ Lists all AI vendors & model versions
- ✓ Identifies "Black Box" risks (unexplainable outputs)
- ✓ Maps contractual liability limits

AUTHORITY BOUNDARY

Stop-the-Line: Vendor refuses to provide "Known Failure Modes" → Contract Hold.

ASSURANCE CONTROL OF THE WEEK

The "Constraint" Check

Does the contract allow us to audit the training data? If no, risk is HIGH.

Learning Outcomes

Technical Competency

- Design fairness stress-tests for algorithmic bias
- Build audit protocols with sampling & versioning
- Evaluate third-party models for black-box risks
- Create data integrity protocols & incident response

Governance Competency

- Map decision rights (RACI) to eliminate liability scapegoats
- Define "Stop-the-Line" triggers with operational teeth
- Negotiate vendor contracts with accountability constraints
- Build appeals & remediation processes for affected parties

By the End of Level 3, You Can:

Audit a complete ESG-AI system—from the data pipeline to the governance layer—and identify where humans have been turned into "Liability Sponges." You'll be able to design workflows where AI has hard boundaries, humans have real authority, and decisions are defensible.

More importantly, you'll understand **why** this matters: because without accountability, AI in ESG becomes a tool for laundering outcomes, not improving them.

Level 3: Advanced Forensics & Governance | AI-ESG Integrated Strategist (AEIS)

Part of the Sociable Systems research curriculum

Completion certificate only. This program is not an accredited qualification, is not endorsed by any regulator or standards body, and does not confer any professional license or statutory authority.