LDR539: **Enterprise Risk Management for CISOs™**

3 Day Course	18 CPEs	Laptop Required

This Course Will Prepare You to:

- Identify why misaligned cyber risk programs fail to influence leadership
- Read ERM maturity from observed behavior across ad hoc, fragmented, and institutionalized environments
- Interpret risk appetite and tolerance signals and translate them into decision boundaries
- Turn existing cyber risk data into decision-relevant information
- Define KRIs as action triggers with predefined responses
- Adapt your risk management practice to function in an environment where machine-speed threats are compressing decision timelines
- Translate risk information into action that supports leadership decisions, no matter how fast the risk is moving

Business Takeaways

- Connect your cyber risk program to how the business makes decisions
- Read the ERM environment you are in and adapt your approach accordingly
- Interpret risk appetite and tolerance signals, even when nothing is formally documented
- Turn existing data into information leadership can compare and act on
- Define KRIs with predefined responses so decisions are consistent, not reactive
- Treat accepted and emerging risk as active inputs, not paperwork
- Build a risk program to respond to an environment where AI is accelerating the pace of attacks and decisions

LDR539 teaches cybersecurity leaders how to apply cyber risk management by connecting it to the enterprise risk management (ERM) program, enabling consistent, risk-informed decision-making. The focus is not on tools or frameworks. It is on how cyber risk leaders bring context, clarity, and discipline to decisions — at a pace that machine-speed threats are starting to demand.

The course follows the natural progression of a leader's journey through risk management. Students start by examining the consequences of misalignment and learning how ERM operates across a range of organizations. From there, they build core risk leadership capabilities: interpreting risk appetite and tolerance, contextualizing existing risk signals, defining Key Risk Indicators (KRIs), and establishing predefined actions with leadership. The final section addresses how AI-driven threats are compressing decision timelines and what that means for how risk leaders define thresholds, structure responses, and act without waiting on a meeting.

Throughout the course, students are positioned as decision enablers, not metric owners or domain experts. They learn to work with existing expertise, operate across different ERM maturity environments, and maintain discipline when organizational structures are imperfect. The course concludes by bringing these elements together into a transferable operating model built to evolve as AI and other emerging risks reshape how enterprises manage exposure.

Author Statement

"Cybersecurity has evolved, and our cyber risk programs have to evolve with it. I wrote this course because I have not seen cyber risk practices evolve the way other areas within cyber have. Time and time again, I have seen risk management hedge around quarterly reviews of risk registers and heat maps, rather than continuous risk monitoring anchored to business objectives through risk appetite and measured against tolerances developed from that appetite. Our job as risk leaders is to enable effective decisions, but too often we're piling up data without ever influencing them. Evolving past that was always necessary. AI has made it mandatory. We no longer have the luxury of time. Facing machine-speed threats requires risk management that can keep pace. This course is how we answer both problems: how to align your cyber risk program to business priorities, and how to build and sustain a cyber risk program that ensures it is prepared for the AI age."

—Ian Frist

Section Descriptions

SECTION 1:
Building Alignment: Don't be the Sushi at the Italian Restaurant

This section establishes the foundation by reframing cyber risk leadership as decision enablement. Students examine how misalignment with enterprise risk management undermines decisions, learn how ERM operates across maturity levels, interpret risk appetite and tolerance, and begin translating cyber risk into enterprise context.

TOPICS:

- Misalignment consequences between cyber risk and enterprise strategy
- How ERM operates across ad hoc, implied, and institutionalized environments
- Risk appetite as leadership intent; risk tolerance as decision boundaries
- Interpreting appetite and tolerance signals, documented or not
- Translating cyber risk into decision-relevant enterprise context

SECTION 2:
Metrics Matter: Operationalizing Risk Management

This section moves from understanding to action. Students learn how frameworks support rather than define risk leadership, clarify the cyber risk leader's role as a decision enabler, define KRIs as action triggers, and select metrics that drive leadership decisions rather than just reporting status.

TOPICS:

- Risk frameworks as tools, not destinations
- The cyber risk leader as decision enabler, not domain owner
- KRIs as action triggers with predefined responses
- Selecting metrics that drive leadership decisions
- How predefined actions enable consistent, risk-informed decisions

SECTION 3:
Sustainment: Getting There Was Tough, Staying There Is Tougher

This section focuses on operating and sustaining cyber risk management over time. Students manage compliance risk, govern accepted risk as a portfolio, assess third-party and AI risk, handle emerging risk without rotting registers, and synthesize the full course approach into an operating model built to hold up as the threat landscape accelerates.

TOPICS:

- Measuring and monitoring compliance risk
- Accepted risk as a portfolio of exposure, not isolated exceptions
- Third-party risk in the AI era: assessing and weighting vendor exposure
- Operating at machine speed: risk management in the AI era
- Emerging risk lifecycle management without the rotting register

Who Should Attend

- Cybersecurity leaders who are responsible for, or moving into, cyber risk management at the enterprise level, including CISOs, deputy CISOs, and senior security leaders who need to connect their risk programs to how the business makes decisions
- Aspiring cyber risk leaders who want to move beyond framework compliance and metric reporting into a role that directly enables leadership decisions
- No formal prerequisites are required. Students should come with some experience in cybersecurity and an interest in how risk management operates at the organizational level.

What is Enterprise Risk Management And Why Is It Important?

Enterprise risk management (ERM) is the discipline through which organizations identify, assess, and manage risk in a way that supports business strategy and leadership decision-making. For cybersecurity leaders, ERM is the operating environment where cyber risk either gets heard or gets ignored. When cyber risk is not aligned to ERM, programs can generate extensive data and still fail to influence a single leadership decision. When it is aligned, cyber risk becomes a direct input into how the business sets priorities, allocates resources, and takes action.