Certified Cybersecurity Leadership Strategist (CCLS) Course Description

3-Day Workshop Syllabus

Day 1 – The Role of the Security Leader: From Tactical to Strategic

Instructional Day Length: 9:00 AM – 4:30 PM
Instructional Methods: Lecture, facilitated discussion, case analysis, applied lab, executive roleplay, guided reflection

Day 1 Overview

Day 1 establishes the strategic foundation for modern security leadership. Participants transition from a primarily technical mindset to a business-aligned leadership perspective. Through structured discussion, case study analysis, and applied exercises, participants examine why security programs fail, how executive leaders evaluate risk, and how security must operate as a core business function. By the end of Day 1, participants will understand how to position security as a strategic enabler of mission, revenue, and organizational resilience.

Detailed Schedule and Session Descriptions

9:00 – 9:30 Welcome & Workshop Framing

Instructional Format: Instructor briefing, facilitated discussion

Session Description:
The workshop opens with an overview of program objectives, expectations, and participant outcomes. The instructor introduces the central theme of the program: the transition from technical security practitioner to strategic security leader. The session includes a structured discussion on common causes of security program failure, including lack of executive alignment, unclear value communication, reactive risk posture, and insufficient governance integration.

Participant Value:
Participants establish a clear understanding of the leadership gap the program is designed to address. They begin reframing security as a business-critical function rather than a technical support role, setting the foundation for executive-level

thinking throughout the workshop.

9:30 – 10:30 What Kind of CISO Will You Be?

Internal CISO, vCISO, fCISO – Different Paths to the Same Table

Instructional Format: Guided reflection and peer discussion

Session Description:
This session explores contemporary security leadership models, including internal CISO, virtual CISO (vCISO), fractional CISO (fCISO), and advisory roles. Participants evaluate differences in authority, accountability, organizational influence, and business integration across these models. Through guided reflection, participants assess their current leadership posture and long-term career direction.

Participant Value:
Participants gain clarity regarding the various executive security pathways available to them. They develop greater self-awareness of their leadership style and professional positioning, enabling more intentional career planning and executive presence development.

10:30 – 10:45 Break

10:45 – 12:00 Security as a Business Function

Aligning Security with Revenue, Mission, and Risk Tolerance

Instructional Format: Lecture and applied case study

Session Description:
This session reframes security as a core business function integrated with revenue protection, operational continuity, regulatory compliance, and organizational mission. Participants examine how executive leaders evaluate risk tolerance and strategic priorities. A structured case study illustrates how misalignment between security and business objectives can undermine organizational effectiveness.

Participant Value:
Participants learn to articulate security initiatives in terms of measurable business impact. They gain the ability to align security programs with executive priorities, enabling stronger support, improved funding outcomes, and increased strategic influence.

12:00 – 1:00 Lunch

Networking encouraged

1:00 – 2:30 Critical Business Function Mapping + Data Flows Lab

Instructional Format: Hands-on applied lab and diagramming workshop

Session Description:
Participants engage in a structured exercise to identify and map critical business functions (CBFs), supporting systems, and key data flows within an organization. The session emphasizes identification of high-value assets, operational dependencies, and systemic vulnerabilities. Participants produce visual diagrams that connect business processes to security risk exposure.

Participant Value:
Participants leave with a practical and repeatable methodology for prioritizing security investments based on business impact. They gain a visual communication tool that enhances executive-level discussions regarding risk, resilience, and resource allocation.

2:30 – 2:45 Break

2:45 – 4:00 From Technical Details to Business Decisions

Roleplay: Translating Risk to the CFO

Instructional Format: Structured executive communication roleplay

Session Description:
Participants practice converting technical findings, such as vulnerability data, control gaps, and assessment results, into executive-ready business narratives. Through facilitated roleplay, participants present risk scenarios to a simulated Chief Financial Officer, focusing on financial impact, operational consequences, and decision-making clarity.

Participant Value:
Participants strengthen their ability to communicate risk in language that resonates with executive stakeholders. This session builds practical skills necessary for securing budget approval, influencing leadership decisions, and demonstrating measurable security value.

4:00 – 4:30 Debrief & Personal Reflection

Instructional Format: Guided reflection and leadership journaling

Session Description:

The day concludes with structured reflection on key insights, communication challenges, and leadership growth areas identified during exercises. Participants document actionable leadership commitments and identify areas for continued development throughout the program.

Participant Value:
Participants consolidate learning, reinforce executive mindset development, and establish intentional leadership growth objectives. This reflective process strengthens retention and supports measurable professional advancement.

Day 1 Learning Outcomes
By the conclusion of Day 1, participants will be able to:

- Identify systemic causes of security program failure
- Distinguish between internal, virtual, and fractional CISO models
- Align security initiatives with revenue, mission, and risk tolerance
- Map critical business functions and supporting data flows
- Translate technical findings into executive-level decision narratives
- Demonstrate foundational executive communication skills

Day 2 – Building & Leading a Modern Security Program

Instructional Day Length: 9:00 AM – 4:30 PM

Instructional Methods: Applied framework mapping, lecture, live drafting lab, simulation, tabletop exercise, guided analysis, facilitated discussion

Day 2 Overview

Day 2 transitions participants from leadership mindset development to operational execution. Building upon the strategic foundation established on Day 1, participants examine how to design, govern, defend, and mature a modern security program. Emphasis is placed on defensible program architecture, governance integration, crisis leadership, and translating operational data into strategic direction. Through applied exercises and simulation-based learning, participants develop practical skills necessary to lead security programs that are measurable, sustainable, and aligned with executive priorities.

Detailed Schedule and Session Descriptions

9:00 – 10:30 Using Industry Frameworks to Build Defensible Security Programs

Risk Assessment as a Leadership Tool

Instructional Format: Applied framework mapping and guided analysis

Session Description:
Participants examine widely adopted security and risk frameworks (NIST CSF, ISO 27001, CIS Controls) and evaluate their role in building defensible, scalable security programs. The session emphasizes the leader's responsibility to select, adapt, and operationalize frameworks rather than implement them mechanically. Participants engage in applied mapping exercises to align framework components with organizational priorities and risk tolerance. Risk assessment is reframed as a leadership instrument for decision-making rather than a compliance exercise. Participants analyze how structured risk evaluation supports prioritization, resource allocation, and executive reporting.

Participant Value:
Participants gain the ability to design security programs grounded in recognized standards while maintaining business flexibility. They learn how to use risk assessment as a strategic lever to influence funding, prioritization, and executive confidence.

10:30 – 10:45 Break

10:45 – 12:00 Governance, Policy & Organizational Buy-In

Drafting Enforceable, Business-Aligned Policies

Instructional Format: Lecture and live drafting lab

Session Description:
This session explores governance structures that sustain effective security programs. Participants examine policy hierarchy, accountability models, cross-functional ownership, and executive sponsorship. Emphasis is placed on developing policies that are enforceable, measurable, and aligned with business

operations rather than purely technical mandates. During the live drafting lab, participants revise or construct policy language to ensure clarity, authority alignment, and practical implementation feasibility.

Participant Value:
Participants develop the ability to draft and refine policies that gain organizational buy-in and executive endorsement. They learn to position governance as a leadership mechanism that reinforces accountability, clarity, and operational consistency.

12:00 – 1:00 Lunch + Roundtable Discussion: "How Stakeholders Perceive Risk"

Session Description:
Facilitated peer discussion examining how different stakeholders (executives, operations, legal, finance, customers) interpret and prioritize risk differently.

Participant Value:
Participants deepen their understanding of cross-functional risk perception, strengthening their ability to tailor communication and strategy to diverse audiences.

1:00 – 2:30 Incident Response & Crisis Leadership Simulation

Live Tabletop Exercise: You Are the CISO During a Breach
Instructional Format: Structured simulation and rapid debrief
Session Description:
Participants engage in a facilitated tabletop simulation in which they assume the role of CISO during an unfolding security incident. The exercise emphasizes decision-making under pressure, stakeholder coordination, executive communication, legal considerations, and public messaging. Following the simulation, a structured debrief evaluates leadership posture, communication clarity, and strategic prioritization during crisis conditions.
Participant Value:
Participants gain experiential insight into the demands of executive crisis leadership. They strengthen their ability to make timely, business-informed decisions while maintaining stakeholder confidence and operational stability.

2:30 – 2:45 Break

2:45 – 4:00 Vulnerability Management as a Business Narrative

Using Risk & Scanning Data to Influence Strategic Priorities

Instructional Format: Hands-on analysis and executive reporting exercise

Session Description:
This session reframes vulnerability management from a technical remediation process to a strategic narrative tool. Participants analyze vulnerability scan outputs, risk assessment data, and remediation metrics to determine prioritization strategies aligned with business impact. Participants practice constructing executive-ready summaries that connect technical findings to operational resilience, financial exposure, and strategic objectives.

Participant Value:
Participants develop the ability to translate operational security data into executive decision-making language. They learn how to use measurable metrics to influence prioritization, justify resource allocation, and demonstrate program maturity.

4:00 – 4:30 Debrief & Action Planning

Instructional Format: Facilitated discussion and structured reflection
Session Description:
The day concludes with a guided review of leadership competencies demonstrated throughout applied exercises and simulations. Participants identify strengths, improvement areas, and practical steps for strengthening governance, crisis readiness, and program defensibility within their organizations. **Participant Value:** Participants consolidate applied learning into actionable leadership behaviors. They leave Day 2 with greater confidence in their ability to architect, defend, and mature a security program aligned with executive expectations.

Day 2 Learning Outcomes
By the conclusion of Day 2, participants will be able to:

- Apply recognized security frameworks to design defensible programs
- Use risk assessment as a strategic decision-making tool
- Develop governance structures that promote accountability and buy-in
- Draft business-aligned, enforceable policy language
- Lead incident response activities with executive-level composure
- Translate vulnerability and risk data into strategic narratives
- Align operational metrics with business impact

Day 3 – Executive Influence: Communication, Compliance & Career

Instructional Day Length: 9:00 AM – 4:30 PM

Instructional Methods: Expert briefing, applied budgeting lab, executive presentation practicum, facilitated discussion, career planning workshop, guided reflection

Day 3 Overview

Day 3 focuses on executive influence, financial stewardship, regulatory awareness, and long-term leadership trajectory. Participants refine their ability to communicate

with boards and executive stakeholders, justify security investments, and position themselves for advanced leadership roles. Through applied presentation exercises and strategic career planning, participants integrate the strategic and operational concepts from Days 1 and 2 into a cohesive executive leadership model. The day culminates in executive briefing practice and structured professional development planning.

Detailed Schedule and Session Descriptions

9:00 – 10:15 Data Stewardship, AI Governance & Emerging Risk Leadership

Instructional Format: Expert briefing and facilitated discussion

Session Description:
This session examines evolving leadership responsibilities related to data governance, privacy obligations, artificial intelligence risk, and emerging regulatory expectations. Participants explore ethical considerations, accountability structures, and cross-functional governance models required to manage advanced technologies and sensitive data responsibly. The discussion emphasizes the executive leader's role in balancing innovation, compliance, and risk tolerance within rapidly changing technological environments.

Participant Value:
Participants develop awareness of emerging governance challenges and learn how to position security leadership at the center of responsible technology adoption. They strengthen their ability to advise executives on AI risk, privacy strategy, and long-term data stewardship responsibilities.

10:15 – 10:30 Break

10:30 – 12:00 Security Budgets, Metrics & Executive Reporting

Turning Risk Posture into Approved Funding

Instructional Format: Applied budgeting lab and reporting workshop

Session Description:
Participants examine the financial dimensions of security leadership, including budget construction, cost justification, performance metrics, and return-on-investment considerations. The session introduces methods for aligning budget requests with business objectives, risk tolerance, and strategic initiatives. During the applied lab, participants practice transforming risk assessments and critical business function analyses into structured budget narratives and measurable

performance indicators suitable for executive review.

Participant Value:
Participants gain practical tools for securing and defending security budgets. They strengthen their ability to link metrics, maturity models, and business risk exposure to financial planning discussions with executive stakeholders.

12:00 – 1:00 Lunch + Optional Mentorship Circles

Session Description:
Informal facilitated discussions focused on leadership development, executive presence, and career trajectory considerations.

Participant Value:

Participants gain peer insight, mentorship perspective, and expanded professional networks that support long-term leadership advancement.

1:00 – 2:30 Executive Briefing Practice

Final Roleplay: Presenting to the Board

Instructional Format: Live executive presentation practicum with feedback panel

Session Description:
Participants deliver structured executive briefings based on scenarios developed throughout the workshop. Presentations simulate board-level reporting environments and require integration of business alignment, governance considerations, risk translation, and budget justification. Feedback is provided on clarity, executive presence, narrative strength, and strategic alignment.

Participant Value:
Participants demonstrate executive communication competence and refine their ability to present complex security issues in concise, business-oriented language. This practicum strengthens confidence and professional credibility in high-stakes environments.

2:30 – 2:45 Break

2:45 – 3:45 Designing Your Security Leadership Career

Career Roadmapping Session

Instructional Format: Structured planning workshop and guided reflection

Session Description:
Participants develop a personalized leadership development roadmap aligned with their professional aspirations. The session examines pathways including internal CISO roles, virtual/fractional CISO engagements, advisory positions, and executive leadership tracks. Participants assess experience gaps, credentialing pathways, mentorship strategies, and professional development milestones necessary for progression.

Participant Value:
Participants leave with a structured, actionable plan for advancing toward senior security leadership roles. The session reinforces intentional career development and long-term strategic positioning.

3:45 – 4:30 Final Workshop Wrap-Up

Action Plans, Leadership Commitments & Certificate Preparation

Instructional Format: Facilitated group reflection and program synthesis

Session Description:
The workshop concludes with a synthesis of strategic, operational, and executive leadership competencies developed across all three days. Participants articulate key insights, document leadership commitments, and review next steps related to certification pathways and continued professional development.

Participant Value:
Participants consolidate their learning into measurable action commitments. They leave with greater executive confidence, strategic clarity, and readiness to apply leadership frameworks within their organizations.

Day 3 Learning Outcomes

By the conclusion of Day 3, participants will be able to:

- Advise executives on emerging data governance and AI-related risks
- Develop and defend security budgets aligned with business objectives
- Construct executive-ready metrics and performance reports
- Deliver board-level security briefings with clarity and authority
- Design a structured career roadmap toward senior security leadership roles
- Integrate strategic, operational, and communication competencies into a cohesive leadership model