EXECUTIVE EDUCATION

VERITAS INSTITUTE®

KNOWLEDGE · LEADERSHIP · INNOVATION

# Executive Education Catalog

CERTIFIED GLOBAL SECURITY PROFESSIONAL®

VERITAS INSTITUTE | 2026

THE PROFESSIONAL DESIGNATION

# Certified Global Security Professional®

BOARD CERTIFIED

A GLOBAL STANDARD
FOR A MORE SECURE WORLD

# A Message from the Founders

The Certified Global Security Professional® (CGSP®) designation was created with a clear purpose: to establish a higher standard for professional excellence in the modern security industry.

Security leadership has changed fundamentally. Today's professionals are expected to do far more than protect people, assets, and facilities. They must anticipate emerging threats, interpret complex risk, lead through crisis, advise senior decision-makers, strengthen organizational resilience, and operate confidently across increasingly interconnected physical, technological, operational, and geopolitical environments.

The profession has evolved. The standard of professional education must evolve with it. When we established Veritas Institute, we believed that those entrusted with protecting organizations, institutions, communities, and critical infrastructure deserved a program equal to the significance of that responsibility. The CGSP® was developed to meet that expectation.

Built through collaboration with senior security executives, accomplished practitioners, global subject matter experts, academic contributors, and university partners, the program combines rigorous professional education with the realities of contemporary security leadership. Its curriculum addresses the disciplines that increasingly define high-performing security organizations: enterprise risk, protective operations, intelligence, resilience, crisis leadership, governance, technology, organizational influence, and strategic decision-making.

The CGSP® is intentionally comprehensive and intentionally demanding. It is not designed simply to validate existing experience. It is designed to elevate it. The program challenges professionals to strengthen their judgment, broaden their strategic perspective, deepen their operational understanding, and develop the leadership capability required to influence organizations at the highest levels. It prepares security leaders to move beyond the traditional boundaries of the function and understand security as an enterprise capability directly connected to organizational continuity, reputation, governance, resilience, and long-term success. This distinction matters.

The modern security leader must be equally credible in the operational environment and the executive boardroom. Technical competence remains essential, but it must be accompanied by sound judgment, business acumen, strategic thinking, communication, ethical leadership, and the ability to make consequential decisions under pressure.

The CGSP® represents our commitment to developing professionals capable of meeting that standard. Our ambition is for the Certified Global Security Professional® designation to represent the gold standard of professional achievement in modern security leadership — a designation recognized for the depth of its curriculum, the quality of its instruction, the relevance of its application, and the caliber of professionals who earn it.

Earning the CGSP® should carry meaning. It should distinguish professionals who have made a serious investment in their development and who are prepared to accept the responsibilities that accompany leadership in this profession. It should signal advanced knowledge, disciplined judgment, professional maturity, and a commitment to continuous excellence.

Above all, the designation reflects a belief at the centre of Veritas Institute: security is no longer simply an operational function. It is a strategic responsibility fundamental to the resilience, stability, and success of organizations worldwide. Those who lead it should be prepared accordingly. That is the standard upon which the CGSP® was built.

**THE FOUNDERS | VERITAS INSTITUTE®**

THE PROFESSIONAL DESIGNATION

# About the CGSP® Program

A structured executive education pathway for security professionals operating at organizational and enterprise level

The Certified Global Security Professional® designation is built to connect academic rigor with the realities of modern security leadership. Its structured executive education pathway is designed around professional capability, applied judgment, ethical leadership and standards-informed practice, creating a consistent benchmark for experienced security professionals seeking advanced leadership recognition. Across approximately 200 hours and 15 integrated courses, the CGSP® establishes a rigorous global standard for modern security leadership and executive capability.

## EDUCATIONAL PHILOSOPHY

At Veritas Institute®, executive education is more than the transfer of knowledge—it is the development of professional capability. Programs integrate research-informed learning, real-world application and internationally recognized management principles so that learning translates into organizational value.

## PROGRAM ARCHITECTURE

- Executive Leadership — strategic leadership, judgment, organizational influence and high-performing teams.
- Executive Business — financial literacy, business strategy, resource stewardship and value creation.
- Executive Communication — executive presence, stakeholder engagement, negotiation and boardroom communication.
- Enterprise Governance — governance, enterprise risk, resilience and integrated security.
- Executive Integration — advanced learning and professional certification across the portfolio.

THE PROFESSIONAL DESIGNATION

# Globally Informed, Standards-Aligned Curriculum

Built on ISO-Aligned Quality Assurance and Curriculum Design Practices

The **Certified Global Security Professional® (CGSP®)** curriculum is developed by Veritas Institute through collaboration among experienced faculty, security practitioners, subject-matter experts, advisory professionals and academic contributors representing diverse industries and operating environments.

The program is designed around a simple principle: professional security education should connect recognized standards and established frameworks with the realities of contemporary security leadership.

## STANDARDS-INFORMED BY DESIGN

Across the CGSP® curriculum, relevant courses draw upon internationally recognized standards, frameworks and authoritative guidance applicable to security management, enterprise risk, organizational resilience, business continuity, emergency management, physical protection, cybersecurity and governance.

Depending on the subject matter of each course, these may include applicable principles and guidance from the **International Organization for Standardization (ISO)**, including **ISO 31000 Risk Management** and **ISO 22301 Security and Resilience – Business Continuity Management Systems**, together with relevant guidance and frameworks published by organizations such as **NIST, CISA, Public Safety Canada, FEMA, NFPA and other recognized national and international authorities**.

Professional practices and competency expectations established by organizations such as **the Business Continuity Institute (BCI), and the International Association of Emergency Managers (IAEM)** may also inform relevant areas of study.

### From Standards to Professional Practice

CGSP® courses are designed to move beyond awareness of standards. Learners are challenged to understand how recognized principles can be interpreted and applied within complex organizational environments.

The curriculum emphasizes the ability to:

- apply structured, risk-based thinking to security decisions;
- identify, assess, prioritize and communicate security risk;
- develop proportionate policies, controls and mitigation strategies;
- strengthen preparedness, response, continuity and organizational resilience;
- integrate physical, operational, personnel and cyber-related security considerations;
- communicate security priorities effectively to senior leadership and stakeholders; and
- exercise professional judgment within established governance, ethical and accountability frameworks.

## Globally Relevant. Operationally Grounded.

Course content is informed by publicly available research, professional standards, government guidance, established industry practices, academic research and the practical experience of security professionals operating across multiple sectors.

This multidisciplinary approach allows CGSP® learners to examine security challenges through both **strategic and operational perspectives**, connecting recognized principles with practical decision-making, leadership and organizational performance.

The result is a professional education framework designed to develop security practitioners who can **interpret risk, exercise sound judgment, lead effectively and translate recognized security principles into responsible organizational action.**

## CGSP® | Professional Knowledge. Applied Judgment. Global Perspective.

*References to external standards, frameworks, agencies, professional bodies or organizations identify sources of publicly available guidance, research or professional practice that may inform relevant curriculum content. Unless expressly stated, such references do not represent sponsorship, accreditation, certification, endorsement or formal affiliation with Veritas Institute or the CGSP® program.*

PORTFOLIO OVERVIEW

# The CGSP® Learning Journey

| 15 | 5 | 200+ |
|---|---|---|
| EXECUTIVE PROGRAMS | LEARNING SERIES | EXECUTIVE EDUCATION HOURS |
| **FLEXIBLE** | **COMPETENCY** | **GLOBAL** |
| DELIVERY | BASED | PERSPECTIVE |

## COURSE DIRECTORY

**1V01** Strategic Security Leadership and Organizational Influence

**1V02** Agile Leadership in Security Organizations

**1V03** Strategic Thinking and Decision-Making in Security Environments

**1V04** Security Business Foundations & Enterprise Operations

**1V05** Finance and Budgeting for Security Leaders (Non-Finance Executives)

**1V06** Security Program Profitability and Value Creation

**1V07** Security Client Experience and Retention Strategy

**1V08** Executive Negotiation and Influence for Security Leaders

**1V09** Public Speaking for Security Leaders

**1V10** Executive Presentation and Boardroom Communication Mastery

**1V11** Building Elite Security Teams and Performance Cultures

**1V12** Leading Multi-Site and Multi-Client Security Programs

**1V13** Enterprise Security Program Design and Governance

**1V14** Integrated Physical and Cyber Security Strategy

**1V15** Global Executive Certification in Physical Security and Risk Leadership

COURSE 01 | 1V01

# Strategic Security Leadership and Organizational Influence

| PROGRAM CODE | DURATION | RECOGNITION |
|---|---|---|
| **1V01** | **10 Modules – Approximately 8 hours** | **Board Certified** |

## COURSE OVERVIEW

The world has entered an era where security leadership demands far more than operational expertise. Today's leaders must navigate geopolitical volatility, hybrid threats, technological disruption, and organizational complexity with clarity, foresight, and ethical strength. This course is a transformational, research-driven leadership program built on the intellectual foundations of Harvard, MIT, LSE, NATO, the UN, and the world's leading security institutions. Developed in close collaboration with senior security practitioners, global risk professionals, and academic experts, it immerses participants in the real tensions, pressures, and decision points that define modern security leadership. Across ten integrated modules, learners are challenged to think beyond incidents and operations. They develop the strategic mindset, executive presence, and systems-level understanding required to lead in environments where the stakes are high, the information is incomplete, and the consequences are global. This is not a course about managing security. It is a course about leading security at the highest level.

COURSE 01 | OUTCOMES & STANDARDS

# Strategic Security Leadership and Organizational Influence

## WHO THIS COURSE IS FOR

- This program is designed for current and emerging leaders across the global security ecosystem who are ready to elevate their thinking and operate at a strategic level.
- Corporate security managers and directors
- Law-enforcement supervisors and senior officers
- Intelligence, risk, and threat-analysis professionals
- Emergency management and crisis leadership personnel
- • Military leaders transitioning to strategic civilian roles

## GOVERNANCE & PROFESSIONAL STANDARDS

**Board Certified and University Approved**

**ISO 31000**

Risk management principles and governance alignment.

**ISO/IEC 27001**

Information security governance and control alignment.

**ISO 22301**

Business continuity and organizational resilience principles.

## EXPECTED LEARNER OUTCOMES

- Graduates of this program emerge with a new cognitive operating system — one that allows them to interpret complexity, influence institutions, and lead with confidence in high-stakes environments.
- Think strategically, using systems thinking, foresight, and advanced decision frameworks
- Lead with influence, shaping organizational direction through credibility, clarity, and executive presence
- Navigate crisis and uncertainty with emotional discipline and stabilizing communication
- Build and sustain high-performance teams grounded in psychological safety and shared mental models
- Integrate intelligence and global risk signals into proactive, anticipatory leadership

### Professional impact

*Strengthens the ability to convert complex risk into strategic direction, influence senior stakeholders, and lead with disciplined judgment when information is incomplete. Graduates are better prepared to position security as an enterprise leadership function that protects resilience, reputation, and long-term organizational value.*

COURSE 02 | 1V02

# Agile Leadership in Security Organizations

| PROGRAM CODE | DURATION | RECOGNITION |
|---|---|---|
| **1V02** | **10 Modules – Approximately 12 hours** | **Board Certified** |

## COURSE OVERVIEW

Modern organizations operate in environments where ambiguity is constant, pressure is cyclical, and decisions ripple across multiple domains. Traditional leadership models — built on linear thinking and technical expertise — no longer match the realities leaders face today. This masterclass delivers a new standard of executive capability. Grounded in adaptive leadership, complex systems theory, organizational psychology, and real-world executive scenarios, the program teaches leaders how to stabilize systems, interpret complexity, and communicate with precision when the stakes are high. Across ten deeply structured modules, learners explore how leadership functions as a system, not a role — and how presence, framing, trust, and resilience become operational tools in high-pressure environments. This is not a theoretical course. It is a transformation in how leaders think, act, and influence. Every module is engineered to elevate leaders into stabilizing forces — individuals who can organize complexity, regulate systems, and lead with clarity when others are overwhelmed.

COURSE 02 | OUTCOMES & STANDARDS

# Agile Leadership in Security Organizations

## WHO THIS COURSE IS FOR

- This program is built for professionals who operate in high-stakes, high-ambiguity environments where leadership must be disciplined, adaptive, and systemic.
- Senior Leaders and Executives
- Directors, Chiefs, VPs, and decision-makers responsible for organizational stability, cross-domain coordination, and strategic communication.
- Security, Risk, and Intelligence Professionals
- Individuals navigating hybrid security environments, threat intelligence, operational risk, and emergency response.
- • Emerging Leaders Preparing for Executive Roles

## GOVERNANCE & PROFESSIONAL STANDARDS

**Board Certified and University Approved**

**ISO 31000**

Risk management principles and governance alignment.

**ISO/IEC 27001**

Information security governance and control alignment.

**ISO 22301**

Business continuity and organizational resilience principles.

## EXPECTED LEARNER OUTCOMES

- Graduates of this masterclass don't just gain knowledge — they gain executive capability.
- They leave with a leadership identity built for modern complexity.
- Unshakeable Executive Presence
- A calm disciplined internal posture that steadies teams and sets organizational tempo.
- Mastery of Communication Under Ambiguity
- The ability to frame uncertainty, deliver clarity, and prevent escalation when pressure spikes.

### Professional impact

*Develops adaptive leaders who can stabilize teams, frame ambiguity, and sustain performance through rapid change, disruption, and competing priorities. The practical impact is stronger executive presence, faster organizational alignment, and more confident leadership across high-pressure security environments.*

COURSE 03 | 1V03

# Strategic Thinking and Decision-Making in Security Environments

| PROGRAM CODE | DURATION | RECOGNITION |
|---|---|---|
| **1V03** | **8 Module – Approximately 24 hours** | **Board Certified** |

## COURSE OVERVIEW

In an era defined by geopolitical volatility, digital interdependence, and rapidly evolving adversarial behavior, organizations need leaders who can see beyond incidents and shape security as a strategic advantage. This master-level program delivers a comprehensive, academically rigorous journey through the full spectrum of modern security leadership — from intelligence-driven decision-making to crisis command, adversary analysis, protective intelligence, and organizational resilience. Developed with the depth and sophistication expected of global executive education, the course synthesizes insights from global security experts, executive board members, and international security research, intelligence studies, behavioral science, and real-world case analysis. Every module is designed to elevate the learner's strategic thinking, sharpen operational judgment, and strengthen their ability to lead in complex, high-pressure environments. This is not a technical training. It is a leadership transformation — equipping security professionals, executives, and organizational leaders with the frameworks, mindset, and strategic clarity required to navigate today's threat landscape and protect the long-term value of their institutions.

COURSE 03 | OUTCOMES & STANDARDS

# Strategic Thinking and Decision-Making in Security Environments

## WHO THIS COURSE IS FOR

- This program is designed for professionals who operate at the intersection of security, leadership, and organizational strategy.
- Senior security leaders responsible for enterprise-wide risk, intelligence, or crisis management
- Executives overseeing global operations, resilience, or governance functions
- Law enforcement, military, and intelligence professionals transitioning into corporate leadership roles
- Directors and managers seeking to elevate their strategic influence within their organizations
- • Emerging leaders preparing for high-stakes decision-making in complex environments

## GOVERNANCE & PROFESSIONAL STANDARDS

**Board Certified and University Approved**

**ISO 31000**

Risk management principles and governance alignment.

**ISO/IEC 27001**

Information security governance and control alignment.

**ISO 22301**

Business continuity and organizational resilience principles.

## EXPECTED LEARNER OUTCOMES

- Graduates of this program emerge with a refined, executive-grade understanding of modern security leadership.
- Interpret global threat environments through an intelligence-driven, strategic lens
- Lead organizations through crises with clarity, composure, and operational precision
- Analyze adversarial behavior — from nation-states to insider threats — and anticipate their evolution
- Build and manage high-performance security operations that integrate physical, cyber, and intelligence domains
- Apply protective intelligence methodologies to detect weak signals and forecast emerging risks

### Professional impact

*Advances the learner from reactive problem solving to anticipatory, intelligence-informed decision-making. Graduates strengthen their ability to interpret weak signals, test assumptions, evaluate second-order consequences, and provide senior leadership with clear, defensible recommendations in complex risk environments.*

- *Interpret global threat environments through an intelligence-driven, strategic lens*
- *Lead organizations through crises with clarity, composure, and operational precision*
- *Analyze adversarial behavior — from nation-states to insider threats — and anticipate their evolution*
- *Build and manage high-performance security operations that integrate physical, cyber, and intelligence domains*
- *Apply protective intelligence methodologies to detect weak signals and forecast emerging risks*
- *Strengthen organizational resilience through cross-functional alignment, culture shaping, and strategic communication*
- *Influence executive decision-making with credibility, insight, and strategic foresight*

COURSE 04 | 1V04

# Security Business Foundations & Enterprise Operations

| PROGRAM CODE | DURATION | RECOGNITION |
|---|---|---|
| **1V04** | **10 Modules – Approximately 10 hours** | **CGSP Professional Designation Curriculum** |

## COURSE OVERVIEW

Security has evolved far beyond its traditional boundaries. Modern organizations operate across distributed geographies, complex regulatory environments, converged cyber-physical ecosystems, and increasingly volatile risk landscapes. Senior security leaders are expected to protect enterprise value, strengthen organizational legitimacy, and govern risk with the same strategic discipline as any other executive function. Security Business Foundations & Enterprise Operations is a comprehensive, research-driven, practitioner-focused program designed to elevate experienced security leaders into enterprise thinkers. It teaches security not as a set of tasks, but as a business discipline. It explores how governance shapes behaviour, how culture influences risk, how data reveals truth, and how leadership determines whether a security program thrives or fragments. Every module is written as a long-form, instructor-level narrative that guides the learner through real scenarios, complex decisions, and the structural realities of modern security ecosystems. This is not a technical course. It is a leadership transformation program. It challenges assumptions, strengthens judgment, and prepares the learner to operate security at enterprise scale with clarity, maturity, and strategic intent.

COURSE 04 | OUTCOMES & STANDARDS

# Security Business Foundations & Enterprise Operations

## WHO THIS COURSE IS FOR

- This program is designed for senior-level security leaders who already understand operations but must now govern complexity.
- It is built for professionals who oversee multisite environments, manage multiclient obligations, navigate regulatory fragmentation, and influence executive stakeholders.
- It is ideal for leaders responsible for risk governance, enterprise continuity, cyber-physical integration, and organizational resilience.
- It is also suited for emerging executives preparing to step into roles where security is no longer a function but a strategic enabler.

## GOVERNANCE & PROFESSIONAL STANDARDS

**Board Certified and University Approved**

**ISO 31000**

Risk management principles and governance alignment.

**ISO/IEC 27001**

Information security governance and control alignment.

**ISO 22301**

Business continuity and organizational resilience principles.

## EXPECTED LEARNER OUTCOMES

- By the end of the program, learners will be able to operate security as a business discipline rather than an operational function.
- They will understand how governance shapes coherence, how culture influences compliance, and how risk appetite guides decision-making.
- They will be able to design management systems that scale, lead cross-domain incident response, and integrate cyber-physical risk into unified governance.
- They will know how to demonstrate value through performance governance, how to communicate with executive clarity, and how to navigate regulatory, contractual, and ethical obligations with defensible reasoning.
- Most importantly, learners will develop the maturity required to lead transformation.
- They will understand how to evolve a security program intentionally, how to anticipate future risks, how to integrate innovation without destabilizing the system, and how to cultivate organizational resilience.

## Professional impact

*Builds the business and governance maturity required to manage security as an integrated enterprise capability rather than a collection of operational activities. Learners leave better equipped to align security with strategy, risk appetite, performance expectations, regulatory obligations, and organizational resilience.*

*By the end of the program, learners will be able to operate security as a business discipline rather than an operational function. They will understand how governance shapes coherence, how culture influences compliance, and how risk appetite guides decision-making. They will be able to design management systems that scale, lead cross-domain incident response, and integrate cyber-physical risk into unified governance. They will know how to demonstrate value through performance governance, how to communicate with executive clarity, and how to navigate regulatory, contractual, and ethical obligations with defensible reasoning. Most importantly, learners will develop the maturity required to lead transformation.*

COURSE 05 | 1V05

# Finance and Budgeting for Security Leaders (Non-Finance Executives)

| PROGRAM CODE | DURATION | RECOGNITION |
|---|---|---|
| **1V05** | **10 Modules – Approximately 8 hours** | **Board Certified** |

## COURSE OVERVIEW

Modern security leadership demands more than operational excellence. Today's executives must speak the financial language of the boardroom, influence strategic decisions, justify investments, and demonstrate measurable value. Security is no longer viewed as a cost centre — it is evaluated as a business function with financial impact, risk implications, and organizational return. This certification program is designed to transform security managers, supervisors, and directors into financially fluent leaders capable of operating at an executive level. Across ten modules, learners gain a complete, practical understanding of financial strategy, budgeting, cost control, P&L management, and investment evaluation. The curriculum bridges the gap between operational expertise and financial mastery, equipping security professionals with the tools, confidence, and executive presence required to lead in modern organizations. This is not theoretical training. It is a hands-on, business-focused program built to elevate decision-making, strengthen credibility, and position security leaders as strategic contributors to organizational performance.

COURSE 05 | OUTCOMES & STANDARDS

# Finance and Budgeting for Security Leaders (Non-Finance Executives)

## WHO THIS COURSE IS FOR

- This certification is designed for professionals who oversee budgets, manage teams, negotiate contracts, or influence organizational decisions.
- Security Managers and Supervisors
- Security Directors and Senior Leaders
- Corporate Security Professionals
- Contract Security Operations Leaders
- Security Consultants and Risk Advisors

## GOVERNANCE & PROFESSIONAL STANDARDS

**Board Certified and University Approved**

**ISO 31000**

Risk management principles and governance alignment.

**ISO/IEC 27001**

Information security governance and control alignment.

**ISO 22301**

Business continuity and organizational resilience principles.

## EXPECTED LEARNER OUTCOMES

- Graduates of this program emerge with the financial intelligence required to operate as true executives.
- Think like a CFO and communicate in financial language
- Read, interpret, and analyze financial statements
- Build, defend, and optimize security budgets
- Control labour costs, overtime, and operational financial leakage
- Manage P&L performance within security operations

### Professional impact

*Builds financial fluency that enables security leaders to defend budgets, evaluate investments, control costs, and communicate the economic consequences of risk in language senior executives understand. This capability increases credibility in resource decisions and strengthens security's position as a disciplined steward of organizational value.*

- *Think like a CFO and communicate in financial language*
- *Read, interpret, and analyze financial statements*
- *Build, defend, and optimize security budgets*
- *Control labour costs, overtime, and operational financial leakage*
- *Manage P&L performance within security operations*
- *Evaluate technology investments using ROI, NPV, and IRR*
- *Negotiate contracts and manage vendors strategically*
- *Quantify risk in financial terms that resonate with senior leadership*
- *Present business cases that secure executive approval*
- *Build long-term financial strategies that align security with organizational goals*

*Security leaders who master financial strategy gain greater influence, stronger credibility with CFOs and CEOs, improved control over resources, and significantly enhanced career advancement opportunities. This certification provides the financial capability that separates operational managers from true executives.*

COURSE 06 | 1V06

# Security Program Profitability and Value Creation

| PROGRAM CODE | DURATION | RECOGNITION |
|---|---|---|
| **1V06** | **10 Modules – Approximately 6 hours** | **Board Certified** |

## COURSE OVERVIEW

Security has evolved. What once functioned as a protective expense is now a strategic business driver influencing revenue stability, operational resilience, customer trust, and competitive positioning. Modern organizations operate in a world shaped by globalization, digital transformation, regulatory pressure, and rising disruption costs — and security sits at the center of all of it. This course introduces the new economics of security leadership, teaching professionals how to quantify, communicate, and maximize the financial value of security programs. Learners gain a practical, executive-level framework for demonstrating how security protects revenue, accelerates compliance, enables innovation, and strengthens brand integrity. Designed with real-world application in mind, the program blends strategic thinking, financial modeling, and governance best practices to elevate security from an operational necessity to a profit-generating business function.

COURSE 06 | OUTCOMES & STANDARDS

# Security Program Profitability and Value Creation

## WHO THIS COURSE IS FOR

- This course is built for professionals who need to operate at the intersection of security, finance, strategy, and organizational leadership.
- Security Directors, Managers and CSOs Ready to evolve from operational supervisors into strategic business leaders.
- Risk, Compliance and Governance Professionals Who must integrate security into enterprise-wide frameworks and regulatory expectations.
- Operations and Facilities Leaders Seeking to understand how security stabilizes productivity, reduces volatility, and protects revenue.
- High-Potential Emerging Leaders Preparing for senior roles where security influences financial and strategic outcomes.
- • Organizations undergoing digital transformation or market expansion Where security maturity directly impacts customer trust, certification timelines, and market access.

## GOVERNANCE & PROFESSIONAL STANDARDS

**Board Certified and University Approved**

**ISO 31000**

Risk management principles and governance alignment.

**ISO/IEC 27001**

Information security governance and control alignment.

**ISO 22301**

Business continuity and organizational resilience principles.

## EXPECTED LEARNER OUTCOMES

- Graduates of this program gain the capability and executive fluency required to position security as a core driver of enterprise value.
- You will learn how to:
- Quantify the financial impact of security Measure cost avoidance, revenue protection, revenue enablement, operational efficiency, and brand enhancement using a modern ROI framework.
- Calculate and present ROSI with executive clarity Use financial modeling to demonstrate measurable returns on security investment.
- Translate security strategy into CEO/CFO language Communicate value in terms of revenue, cost, risk, growth, and competitive advantage.
- Build security programs that enable innovation and expansion Design architectures that support digital transformation, regulatory approvals, and new market entry.

### Professional impact

*Equips leaders to demonstrate how security contributes to revenue protection, operational continuity, customer confidence, compliance, and strategic growth. Graduates can translate protective outcomes into measurable business value, strengthening executive sponsorship and enabling more informed investment in security capability.*

COURSE 07 | 1V07

# Security Client Experience and Retention Strategy

| PROGRAM CODE | DURATION | RECOGNITION |
|---|---|---|
| **1V07** | **8 Modules - Approximately 6 hours** | **Board Certified** |

## COURSE OVERVIEW

Transform the Way Your Organization Builds Trust, Delivers Value, and Retains Clients The private security industry is changing. Clients expect more than compliance, more than manpower, and more than incident response. They expect partnership. They expect strategic alignment. They expect a security provider who understands their world, anticipates their needs, and delivers a consistent, high-trust experience at every stage of the relationship. This advanced, eight-module executive program is designed for senior leaders who want to elevate their organization beyond traditional service delivery and build a culture, system, and strategy that drives long-term retention, operational excellence, and competitive advantage. Built on research from Harvard, MIT, Wharton, Cornell, Stanford, the Disney Institute, Gallup, McKinsey, Deloitte, and global best practices from corporate and private security operations, this course provides a comprehensive blueprint for transforming the client experience from the inside out.

COURSE 07 | OUTCOMES & STANDARDS

# Security Client Experience and Retention Strategy

## WHO THIS COURSE IS FOR

- This program is designed for senior-level professionals who influence strategy, culture, and client relationships within private security organizations.
- Security company executives and senior leadership
- Directors of Operations and Regional Managers
- Client Relationship Executives and Account Directors
- Corporate Security Leaders seeking to elevate vendor performance
- • Organizational development leaders within the protective services sector

## GOVERNANCE & PROFESSIONAL STANDARDS

**Board Certified and University Approved**

**ISO 31000**

Risk management principles and governance alignment.

**ISO/IEC 27001**

Information security governance and control alignment.

**ISO 22301**

Business continuity and organizational resilience principles.

## EXPECTED LEARNER OUTCOMES

This course provides a complete, end-to-end framework for building a world-class client experience and retention strategy. Participants will learn how to:

- Design a security specific Client Experience (CX) architecture inspired by global service excellence leaders
- Build a culture that supports professionalism, accountability, and high trust relationships
- Map the full client journey and engineer loyalty at every stage
- Operationalize excellence through supervision, training, technology, and performance systems
- Strengthen executive communication, expectation management, and strategic relationship leadership
- Use analytics and predictive indicators to identify risk, prevent churn, and reinforce loyalty
- Build a long term retention engine that becomes a competitive advantage

This is not a theoretical program. It is a practical, operational, and strategic roadmap for transforming how your organization engages with clients.

## Professional impact

*Strengthens the leadership systems required to build trust, improve service consistency, anticipate client needs, and protect long-term relationships. Learners are better prepared to connect operational performance with client experience, use early indicators to address service risk, and turn reliable security delivery into a sustainable competitive advantage.*

COURSE 08 | 1V08

# Executive Negotiation and Influence for Security Leaders

| PROGRAM CODE | DURATION | RECOGNITION |
|---|---|---|
| **1V08** | **10 Modules – Approximately, 8 hours** | **Board Certified** |

## COURSE OVERVIEW

The Program That Redefines Security Leadership Security leadership has entered a new era — one where technical expertise is no longer enough, where influence determines outcomes, and where negotiation shapes the resilience of entire organizations. Today's security leaders must operate at the intersection of psychology, strategy, crisis, and executive decision-making. They must be able to shape perception, align stakeholders, negotiate under pressure, and lead with clarity when uncertainty is at its peak. This course was built to meet that reality. Executive Negotiation and Influence for Security Leaders is a master-level program designed to transform senior security professionals into strategic influencers capable of shaping decisions at the highest levels of leadership. It does not teach techniques; it reshapes identity. It does not offer tips; it builds executive presence. It does not prepare you for meetings; it prepares you for moments that define careers. This is not a traditional security course. It is an executive transformation experience.

This program draws on the lived experience, frameworks, and executive practices of leaders from some of the world's most respected organizations.

COURSE 08 | OUTCOMES & STANDARDS

# Executive Negotiation and Influence for Security Leaders

## WHO THIS COURSE IS FOR

- CSOs, CISOs, Directors of Security, and Chiefs of Protective Services
- Senior leaders responsible for enterprise risk, resilience, crisis management, or protective operations
- Security managers preparing for executive roles
- Leaders who negotiate with boards, regulators, law enforcement, intelligence agencies, and cross-functional executives
- Professionals who want to elevate their presence, sharpen their influence, and operate as strategic advisors rather than technical specialists

## GOVERNANCE & PROFESSIONAL STANDARDS

**Board Certified and University Approved**

**ISO 31000**

Risk management principles and governance alignment.

**ISO/IEC 27001**

Information security governance and control alignment.

**ISO 22301**

Business continuity and organizational resilience principles.

## EXPECTED LEARNER OUTCOMES

- This course was built to meet that reality.
- Executive Negotiation and Influence for Security Leaders is a master-level program designed to transform senior security professionals into strategic influencers capable of shaping decisions at the highest levels of leadership.
- It does not teach techniques; it reshapes identity.
- It does not offer tips; it builds executive presence.
- It does not prepare you for meetings; it prepares you for moments that define careers.
- This is not a traditional security course. It is an executive transformation experience.

### Professional impact

*Develops the judgment, composure, and influence required to negotiate resources, resolve competing priorities, and shape decisions without relying on positional authority. Graduates are better prepared to manage difficult conversations, build alignment across functions, and represent security interests credibly in executive and crisis environments.*

COURSE 09 | 1V09

# Public Speaking for Security Leaders

| PROGRAM CODE | DURATION | RECOGNITION |
|---|---|---|
| **1V09** | **12 Modules – Approximately 10 hours** | **Board Certified** |

## COURSE OVERVIEW

Public Speaking for Security Leaders is a comprehensive, graduate-level program designed to transform how security professionals communicate in high-stakes environments. Built around the realities of modern protective work—crisis response, executive briefings, public-facing communication, organizational change, and strategic influence—this course develops the communication capabilities that define today's most trusted security executives. Across twelve deeply immersive modules, learners explore the psychology of audience perception, the discipline of executive presence, the architecture of narrative, and the emotional intelligence required to speak with clarity, authority, and authenticity. The course moves far beyond traditional public speaking techniques. It teaches security leaders how to stabilize anxious audiences, persuade senior decision-makers, guide organizations through uncertainty, and represent the security function with confidence and credibility. This is not a presentation skills course. It is a leadership transformation—one that elevates the security leader's voice into a strategic instrument capable of shaping decisions, influencing culture, and strengthening organizational resilience.

COURSE 09 | OUTCOMES & STANDARDS

# Public Speaking for Security Leaders

## WHO THIS COURSE IS FOR

- This course is designed for security professionals who operate at, or aspire to, senior levels of responsibility—individuals whose communication directly influences safety, trust, and organizational stability.
- It is ideal for:
- Corporate Security Leaders responsible for executive briefings, board-level communication, and enterprise risk alignment.
- Protective Services Professionals who must speak with calm authority during crises, incidents, and public-facing events.
- Security Managers and Directors navigating organizational change, policy adoption, and cross-departmental collaboration.
- • Emergency Management and Business Continuity Leaders who must communicate under pressure with clarity and composure.

## GOVERNANCE & PROFESSIONAL STANDARDS

**Board Certified and University Approved**

**ISO 31000**

Risk management principles and governance alignment.

**ISO/IEC 27001**

Information security governance and control alignment.

**ISO 22301**

Business continuity and organizational resilience principles.

## EXPECTED LEARNER OUTCOMES

- Graduates of this program emerge with a communication capability that is unmistakably executive level.
- Speak with disciplined executive presence—projecting calm authority in boardrooms, crisis centers, and public environments.
- Construct powerful security narratives that transform complexity into clarity and uncertainty into direction.
- Communicate with precision—delivering information that is accurate, accessible, and strategically aligned.
- Persuade senior decision-makers by framing security initiatives in terms of organizational impact, risk posture, and strategic value.
- Stabilize anxious or emotionally charged audiences through tone, pacing, empathy, and psychological awareness.

### Professional impact

*Transforms communication into a practical leadership capability for executive briefings, crisis messaging, public-facing engagements, and organizational change. Graduates strengthen their ability to simplify complexity, project calm authority, build trust with diverse audiences, and communicate security priorities in ways that support timely action.*

COURSE 10 | 1V10

# Executive Presentation and Boardroom Communication Mastery

| PROGRAM CODE | DURATION | RECOGNITION |
|---|---|---|
| **1V10** | **12 Modules – Approximately 16 hours** | **Board Certified** |

## COURSE OVERVIEW

Executive Communication Mastery is a high-performance, graduate-level program built for leaders who operate in high-stakes environments. Across 12 deeply immersive modules, learners develop mastery in strategic narrative design, executive presence, boardroom dynamics, high-impact briefing delivery, cross-cultural communication, crisis leadership, ethical governance communication, and executive-grade writing. This course moves far beyond theory — every module is engineered to build real, immediately applicable executive capability. Learners walk away with the ability to design and deliver boardroom-ready presentations, navigate adversarial questions, communicate strategy and risk with clarity, and lead organizational change through disciplined, authoritative communication.

COURSE 10 | OUTCOMES & STANDARDS

# Executive Presentation and Boardroom Communication Mastery

## WHO THIS COURSE IS FOR

- Who This Is For
- This course is designed for senior leaders, emerging executives, directors, managers, consultants, entrepreneurs, and professionals who must communicate with influence in high-stakes settings.
- It is ideal for individuals preparing for executive roles, boardroom participation, investor engagement, regulatory communication, or leadership positions where clarity, authority, and strategic presence are non-negotiable.
- • Whether you lead teams, manage complex projects, present to senior stakeholders, or shape organizational direction, this program equips you with the communication discipline required at the highest levels of leadership.

## GOVERNANCE & PROFESSIONAL STANDARDS

**Board Certified and University Approved**

**ISO 31000**

Risk management principles and governance alignment.

**ISO/IEC 27001**

Information security governance and control alignment.

**ISO 22301**

Business continuity and organizational resilience principles.

## EXPECTED LEARNER OUTCOMES

- Graduates of this program demonstrate mastery in executive-level communication.
- They can design strategic narratives that influence decisions, deliver concise and authoritative briefings, manage executive pushback with composure, and communicate risk, strategy, and change with clarity.
- They project executive presence consistently, navigate political dynamics intelligently, and write memos, briefs, and decision papers that support governance and organizational alignment.
- Learners leave with the ability to operate confidently in boardrooms, C-suite environments, crisis situations, and global leadership contexts — fully equipped with communication skills that elevate their leadership impact.

### Professional impact

*Prepares leaders to communicate at the level expected in boardrooms and C-suite environments: concise, evidence-based, strategically framed, and decision oriented. Learners strengthen their ability to present risk, respond to challenge, structure executive narratives, and produce written and verbal briefings that support governance and informed decision-making.*

COURSE 11 | 1V11

# Building Elite Security Teams and Performance Cultures

| PROGRAM CODE | DURATION | RECOGNITION |
|---|---|---|
| **1V11** | **10 Modules – Approximately 6 hours** | **Board Certified** |

## COURSE OVERVIEW

Building Elite Security Teams and Performance Cultures is the world's most comprehensive leadership program for senior security professionals. Designed for global executives responsible for protecting people, assets, reputation, and organizational resilience, this course blends academic rigor with real-world application. Over ten modules, learners explore the psychology of leadership under pressure, the architecture of elite team performance, the systems that sustain operational excellence, and the intelligence capabilities required to navigate global complexity. Developed using university-level instructional design and aligned with ISO learning standards, and collaboration of global security leaders and academic professionals, this course delivers a complete leadership blueprint for transforming security teams into high-reliability, high-performance units capable of thriving in volatile environments. Every module includes applied exercises, scenario-based learning, and strategic frameworks that can be implemented immediately. This is not a theoretical course. It is a masterclass in elite security leadership.

COURSE 11 | OUTCOMES & STANDARDS

# Building Elite Security Teams and Performance Cultures

## WHO THIS COURSE IS FOR

- This course is designed for senior security leaders, including:
- Directors, Senior Directors, and Global Heads of Security
- Chief Security Officers (CSOs) and Deputy CSOs
- Security leaders in multinational corporations
- Government, intelligence, and critical-infrastructure security executives
- • Leaders responsible for GSOCs, crisis management, intelligence, or enterprise resilience

## GOVERNANCE & PROFESSIONAL STANDARDS

**Board Certified and University Approved**

**ISO 31000**

Risk management principles and governance alignment.

**ISO/IEC 27001**

Information security governance and control alignment.

**ISO 22301**

Business continuity and organizational resilience principles.

## EXPECTED LEARNER OUTCOMES

- By the end of this course, learners will be able to:
- Build elite security teams grounded in evidence-based organizational models
- Shape high-performance cultures that sustain excellence under pressure
- Apply leadership psychology to improve decision-making and team cohesion
- Integrate security governance with enterprise strategy and executive priorities
- Develop world-class talent pipelines and leadership depth

### Professional impact

*Enables leaders to build high-reliability teams in which accountability, trust, readiness, and continuous improvement reinforce one another. The professional impact extends beyond team performance: graduates develop stronger leadership pipelines, healthier operating cultures, and greater organizational confidence in the security function.*

COURSE 12 | 1V12

# Leading Multi-Site and Multi-Client Security Programs

| PROGRAM CODE | DURATION | RECOGNITION |
|---|---|---|
| **1V12** | **12 Modules - Approximately 10 hours** | **Board Certified** |

## COURSE OVERVIEW

Multisite and multiclient security environments are defined by complexity, fragmentation, and constant change. Traditional security management is no longer enough. Leaders must govern distributed systems, interpret diverse regulatory obligations, shape culture across multiple environments, and make decisions that withstand executive scrutiny. This program elevates security leaders into enterprise-level thinkers. Built on global security standards, organizational behaviour research, systems theory, leadership psychology, and high-reliability organization principles, the course transforms how leaders design, govern, and scale security programs. Across 12 modules, learners move beyond operational management and develop the strategic clarity, governance discipline, and executive reasoning required to lead security at scale.

COURSE 12 | OUTCOMES & STANDARDS

# Leading Multi-Site and Multi-Client Security Programs

## WHO THIS COURSE IS FOR

- This program is designed for:
- Security Directors, Managers, and Senior Leaders overseeing multiple sites, clients, or regions.
- Corporate Security Executives responsible for enterprise governance, risk appetite translation, and strategic alignment.
- Security Providers and Contracted Leaders managing diverse client obligations, regulatory environments, and operational realities.
- Emerging Leaders preparing for executive-level roles in complex security ecosystems.
- • Professionals in Cyber-Physical Converged Environments who must integrate digital and physical risk governance across distributed operations.

## GOVERNANCE & PROFESSIONAL STANDARDS

**Board Certified and University Approved**

**ISO 31000**

Risk management principles and governance alignment.

**ISO/IEC 27001**

Information security governance and control alignment.

**ISO 22301**

Business continuity and organizational resilience principles.

## EXPECTED LEARNER OUTCOMES

- By the end of the program, learners will be able to:
- Design and govern multisite security systems with executive clarity and structural coherence.
- Interpret regulatory, contractual, and ethical obligations across diverse jurisdictions and clients.
- Lead people and shape culture across distributed environments with maturity and influence.
- Integrate cyber-physical risk governance into a unified, strategic framework.
- Manage cross-site incidents with resilience, foresight, and enterprise-level reasoning.

### Professional impact

*Builds the enterprise discipline required to create consistency without losing local responsiveness across sites, clients, regions, and regulatory environments. Graduates are better prepared to standardize governance, strengthen cross-site assurance, lead distributed teams, and manage complex incidents with a coherent enterprise perspective.*

COURSE 13 | 1V13

# Enterprise Security Program Design and Governance

| PROGRAM CODE | DURATION | RECOGNITION |
|---|---|---|
| **1V13** | **12 Modules – Approximately 20 hours** | **Board Certified** |

## COURSE OVERVIEW

Enterprise Security Program Design & Governance is a comprehensive, director level professional development program built for seasoned security leaders who operate at the strategic intersection of risk, governance, resilience, and executive influence. Modern organizations demand more than operational competence — they expect security leaders to design enterprise wide programs, govern complex environments, integrate cyber physical domains, lead during crises, and communicate with clarity at the executive level.

This course delivers a full transformation from operational management to strategic enterprise leadership. Across twelve deeply immersive modules, learners explore the architecture of governance, risk frameworks, policy design, cyber physical integration, protective intelligence, resilience, audits, compliance, and executive influence. The content is academically rigorous, ISO aligned and structured for self-paced LMS delivery without instructor intervention.

Learners emerge with the capability to design, govern, and optimize enterprise security programs that withstand regulatory scrutiny, satisfy executive expectations, and elevate security to a value generating function within the organization.

COURSE 13 | OUTCOMES & STANDARDS

# Enterprise Security Program Design and Governance

## WHO THIS COURSE IS FOR

- This course delivers a full transformation from operational management to strategic enterprise leadership.
- Across twelve deeply immersive modules, learners explore the architecture of governance, risk frameworks, policy design, cyber-physical integration, protective intelligence, resilience, audits, compliance, and executive influence.
- The content is academically rigorous, ISO-aligned, and structured for self-paced LMS delivery without instructor intervention.
- Learners emerge with the capability to design, govern, and optimize enterprise security programs that withstand regulatory scrutiny, satisfy executive expectations, and elevate security to a value-generating function within the organization.
- Who This Is For
- • This course is designed for experienced security professionals who already operate at a senior level or are preparing to transition into enterprise leadership roles.

## GOVERNANCE & PROFESSIONAL STANDARDS

**Board Certified and University Approved**

**ISO 31000**

Risk management principles and governance alignment.

**ISO/IEC 27001**

Information security governance and control alignment.

**ISO 22301**

Business continuity and organizational resilience principles.

## EXPECTED LEARNER OUTCOMES

- Upon completion of this course, learners will be able to:
- Design enterprise-wide security programs that align with organizational strategy, risk appetite, and ISO standards.
- Build governance structures, committees, and decision-rights that strengthen accountability and executive alignment.
- Conduct structured enterprise risk assessments and translate results into program priorities.
- Integrate cyber-physical security domains into unified operating models and incident response frameworks.
- Build protective intelligence programs that identify emerging threats and support proactive intervention.

### Professional impact

*Develops the capability to design security programs that are governable, auditable, scalable, and aligned with enterprise strategy and risk appetite. Graduates strengthen their ability to establish decision rights, integrate risk information, connect physical and cyber domains, and provide executives with credible assurance over security performance.*

COURSE 14 | 1V14

# Integrated Physical and Cyber Security Strategy

| PROGRAM CODE | DURATION | RECOGNITION |
|---|---|---|
| **1V14** | **10 Modules – Approximately 6 hours** | **Board Certified** |

## COURSE OVERVIEW

Integrated Physical and Cyber Security Strategy: Corporate Security Operations Edition is built for the world you actually work in—where a compromised badge becomes a compromised network, and a "minor" sensor alert hides a deliberate attack. Across 10 modules, you step inside Halcyon Global, a realistic multinational enterprise facing hybrid threats that move seamlessly between physical spaces and digital systems. You don't just read about integrated security—you live it through narrative scenarios, crisis decisions, governance redesign, and the build-out of an Integrated Security Operations Center (ISOC). This is not a theoretical course. It is an operational playbook for leaders who need to unify physical and cyber security into a single, coherent strategy that can withstand modern, hybrid risk.

COURSE 14 | OUTCOMES & STANDARDS

# Integrated Physical and Cyber Security Strategy

## WHO THIS COURSE IS FOR

- This course is designed for professionals who carry real responsibility for corporate security and risk, including:
- Corporate Security Leaders and Managers who oversee physical security, cyber security, or both, and need a unified model.
- Security Operations and SOC Leaders who want to fuse physical and cyber monitoring into a single operational picture.
- IT, Risk, and Facilities Executives who must align governance, identity, and access across domains.
- Consultants and Advisors working on security transformation, integrated risk, or resilience programs.
- • If you operate in an environment where physical badges, digital identities, cloud platforms, and global facilities all intersect—this course is built for you.

## GOVERNANCE & PROFESSIONAL STANDARDS

**Board Certified and University Approved**

**ISO 31000**

Risk management principles and governance alignment.

**ISO/IEC 27001**

Information security governance and control alignment.

**ISO 22301**

Business continuity and organizational resilience principles.

## EXPECTED LEARNER OUTCOMES

- By the end of this course, you will be able to:
- Design an integrated security architecture that treats the enterprise as a single organism, not fragmented silos.
- Build and govern a unified security program, including a Global Security Office, CSO role, and cross-functional Security Governance Council.
- Implement hybrid incident response, where every event—physical or digital—is analyzed across domains.
- Create and operate an Integrated Security Operations Center (ISOC) that fuses badge logs, CCTV, authentication data, endpoint telemetry, and environmental sensors into one risk picture.
- Recognize and counter hybrid threats, from phishing-enabled physical intrusions to sensor-driven cyber breaches.

### Professional impact

*Equips leaders to break down physical and digital security silos and manage hybrid risk through shared governance, intelligence, and response. The professional impact is a more unified operating picture, stronger cross-functional accountability, faster recognition of converged threats, and more resilient enterprise security architecture.*

COURSE 15 | 1V15

# Global Executive Certification in Physical Security and Risk Leadership

| PROGRAM CODE | DURATION | RECOGNITION |
|---|---|---|
| **1V15** | **13 Modules – Approximately 50 hours** | **Board Certified** |

## COURSE OVERVIEW

This certification was developed by Veritas Institute's security subject matter experts, faculty and advisory council through rigorous collaboration with senior security leaders across Fortune 500 enterprises, government agencies, critical infrastructure sectors, and international security organizations. The curriculum integrates standards and methodologies from the FBI, DHS, Secret Service, RCMP, Interpol, CISA, NIST, ISO, and leading global corporations — ensuring every module reflects real-world executive practice, validated frameworks, and globally recognized security leadership principles. This certification reflects the realities of modern threat environments — cyber-physical convergence, insider risk, geopolitical instability, violent intrusion, operational disruption, and emerging technologies such as autonomous systems and AI-driven surveillance. Every module is informed by real-world case studies from 2014–2025, including incidents in North America, Europe, Asia-Pacific, and the Middle East. These cases were selected because they represent the most consequential failures and breakthroughs in contemporary security leadership.

COURSE 15 | OUTCOMES & STANDARDS

# Global Executive Certification in Physical Security and Risk Leadership

### WHO THIS COURSE IS FOR

- This program is designed for professionals who operate — or aspire to operate — at the director, senior manager, or executive level within security, risk, resilience, or protective services.
- Ideal Candidates Include:
- Security Leadership
- Directors of Security
- Chiefs of Security / CSO-Track Professionals
- • Global Security Operations Leaders

### GOVERNANCE & PROFESSIONAL STANDARDS

**Board Certified and University Approved**

**ISO 31000**

Risk management principles and governance alignment.

**ISO/IEC 27001**

Information security governance and control alignment.

**ISO 22301**

Business continuity and organizational resilience principles.

## EXPECTED LEARNER OUTCOMES

- Graduates of the Global Executive Certification in Physical Security and Risk Leadership emerge with executive-level capability, able to lead security as a strategic business function rather than an operational department.
- Learners outcome:
- Lead Security at the Executive Level
- Govern enterprise risk with clarity, structure, and authority
- Influence C-suite decision-making through business-aligned communication
- Translate complex threats into actionable executive insights

### Professional impact

*Represents the integrative application of executive leadership, risk governance, physical protection, resilience, intelligence, and strategic communication across the CGSP® professional designation pathway. Graduates are prepared to operate with broader enterprise perspective, translate complex threats into executive decisions, and lead security as a trusted, accountable contributor to organizational resilience and long-term value.*

NEXT STEP

# Advance Your Executive Security Leadership

***The CGSP® portfolio is designed for professionals who want to move beyond operational competence and develop the judgment, influence, governance discipline and enterprise perspective expected of modern security leaders.***

**VERITAS INSTITUTE®**

**KNOWLEDGE • LEADERSHIP • INNOVATION**

VERITAS
INSTITUTE®
KNOWLEDGE · LEADERSHIP · INNOVATION

# Contact Us


info@veritasinstituteltd.com

https://veritasinstituteltd.com