INNOVATE | SUSTAIN | CREATE VALUE

The DCRO Risk Governance Institute

CERTIFICATE IN CYBER RISK GOVERNANCE®

IMPACT BOARDS EMERGING MARKETS

The Certificate in

CYBER RISK GOVERNANCE®

A GLOBAL CREDENTIAL FOR BOARD MEMBERS

Cyber as a Strategic Issue and Systemic Risk
Unmasking the Enemy
Cyber Incident Preparation and Response
Technology Risk Governance
The Use of Third Parties
The Use of Cloud Technologies
How to Safely Deploy Emerging Technologies
Data Security
Cyber Defense Best Practices
Boards and the Governance of Cyber Risk

Ten critical lessons for current and aspiring board members who seek to effectively oversee cyber risk and the use of technologies as part of their fiduciary duties. Lectures and case study interviews featuring leading directors, c-level executives, law enforcement, intelligence, and technology experts, give you essential practical knowledge to be more effective in boardroom strategic planning and oversight.

THE CERTIFICATE IN CYBER RISK GOVERNANCE®

The need for this credential

Rapidly emerging technologies demand integration into strategic planning but also create new vulnerabilities that require more competent board oversight. Boards tasked with value creation and governance need to be familiar with multiple dimensions of the cyber spectrum. This program delivers practical guidance you can put to use immediately, and that sends a signal to regulators and investors that you take cyber risk governance seriously.

What is required to earn the Certificate in Cyber Risk Governance®?

Candidates must view all lecture and case study videos and study the lecture notes provided with each lesson. At the end of each lesson is a quiz on which candidates must answer 80% of the questions correctly to receive a passing grade.

How long will it take to complete the course?

There are approximately seven hours of lecture and case study videos to watch. In combination with the lecture notes, total study time should be between nine and ten hours. Candidates may move through the program at their own pace, with up to one year to complete all sessions. Most will finish in a matter of days or weeks.

Why this credential and not others?

The DCRO Risk Governance Institute is the world's leading source of risk governance training and credentialing. We are a nonprofit collaboration of current and former board members and c-suite executives delivering peer-led, practical education that aligns with board duties and the pursuit of strategic goals. Our Qualified Risk Directors® are serving on boards in more than 25 countries.

"Technology plays a role in nearly every customer interaction and every strategic initiative our organizations undertake. Understanding how to govern the use of technology and its associated cyber risks is now a fundamental board duty that this program addresses well."

-David R. Koenig, President and CEO, and Qualified Risk Director®

THE CERTIFICATE IN CYBER RISK GOVERNANCE®

THE DCRO RISK GOVERNANCE INSTITUTE

MODULE 1

Cyber as a Strategic Issue and a Systemic Risk

Cyber is not merely a technical matter. It's an increasingly strategic issue and a systemic risk. Become more predictive and less reactive.

JANEY YOUNG

Head of Global Investigations, Chainalysis

The rapid development of technology has had a positive effect across business, enhancing many digitalization opportunities. It has also enabled new and emerging threats and the need for greater prioritization of cyber security. When cyber risks materially threaten the solvency or viability of as many as 1 in 6 businesses, the long-term gains of a board's investment in cyber security strategy cannot be overstated. Striking the right balance so the strategy maintains appropriate defenses while enabling added value to productivity is the key to long-term value creation.

Janey Young is a commended senior investigation specialist who has coordinated some of the most high-profile cyber investigations impacting globally. She has over two decades of experience in international law enforcement, leading the investigations response in the UK National Cyber Crime Unit and at Europol's European Cybercrime Centre in The Hague. As the former Head of Global Investigations at Chainalysis, she is an internationally recognized expert in blockchain technology and cryptocurrency.

MODULE 2

Unmasking the Enemy

New threats and adversaries are exploting global connectivity every day. Learn their tactics, capabilities, motivations, and potential impact.

SELIM AISSI

Board Member and Chief Information Security Officer

Cybercrime is a multibillion-dollar business, led by international criminal organizations with large capabilities, using high-end technology and highly-skilled staff, even outsourcing. The cybercrime market has increased significantly because of the development of cryptocurrencies and deep web marketplaces. We discuss the different faces of the enemy in the cyber domain, their tactics, and the impact of their actions, giving board members the necessary knowledge tools to succeed in their governance role.

Recognized as CISO of the Year in 2019, One of the Top 100 CISO's Globally in 2017, and One of the Most Influential CISOs in 2016, Selim Aissi has a demonstrated track record of aligning security with business strategies. He is focused on driving the information security agenda through balanced strategies and strong partnerships. He's built some of the most advanced cybersecurity capabilities and developed some of the world's most innovative security technologies working in the Defense, Technology, and Financial industries. He serves on the boards of Applied Dynamics International and the National Technology Security Coalition.

Note: Faculty and case study affiliations are for information purposes only. No suggestion is made that these organizations have any affiliation with this course or the DCRO Institute. They are not responsible for its content in any way.

THE CERTIFICATE IN CYBER RISK GOVERNANCE®

THE DCRO RISK GOVERNANCE INSTITUTE

MODULE 3

Cyber Incident Preparation and Response

Do you have an incident plan? Do you have critical external parties on retainer? Do you have your internal team identified and ready to act? Learn how to be ready to respond.

DAVID HAHN

Board Member and Chief Information Security Officer

It's almost certain that your organization will experience some form of a cyber incident. While responding to the attack is critical, the effectiveness of that response is highly dependent upon how well you have prepared. David discusses the various parties involved in pre-planning and response, lessons learned, and best practices for board members and executives to ensure are already in place before you need to respond.

David has a long history in Information Security and is a trusted business partner addressing the ever-growing and complex Cybersecurity landscape. He is the CISO at CDK Global, a leader in software and technology for the automotive industry. His career includes Financial Services with Wells Fargo Bank, Software Product and Services with Intuit (makers of TurboTax and Quickbooks), and large diversified Media/Data company with Hearst Corporation with large stakes in TV, Newspapers, Magazines, Healthcare, Transportation and Financial (Fitch Ratings).

MODULE 4

Technology Risk Governance

It is critical that board members understand the key dimensions of technology risk, and know the areas on which they must focus to adequately oversee and utilize technology to best effect.

RAMY HOUSSAINI

Chief Cyber, Technology Risk, and Privacy Officer

Technology surrounds us and permeates our personal and work environments. Organizations face risks created by their use of technology. When it comes to using technology, cybersecurity is high on the list, but it is also essential to plan for other operational, legal, financial, reputation, and society-driven liabilities and exposures. Increased digitalization underscores the need for today's board to take a step back and verify whether they have the portfolio of skills and completeness to serve as a strategic resource and guide for management on this important topic.

Ramy Houssaini is the Chief Cyber and Technology Risk Officer and Group Data Protection Officer for BNP Paribas. He is an internationally recognized executive with a unique background in Cyber Security, Data Privacy, Operational Risk Management, and Technology. He served as the Vice President of British Telecom in Europe, the Regional Head of the Cyber Practice for Accenture, and as the Vice President for Information Security at Visa.

Note: Faculty and case study affiliations are for information purposes only. No suggestion is made that these organizations have any affiliation with this course or the DCRO Institute. They are not responsible for its content in any way.

THE CERTIFICATE IN CYBER RISK GOVERNANCE®

MODULE 5

The Use of Third Party Service Providers

Do you know the extent to which your organization is an extended ecosystem of third party service providers? What are best practices in governing these diverse and dynamic relationships?

IAN AMIT

Chief Security Officer, Board Member, and Hacker

Business ecosystems are evolving into an extended enterprise of partnerships and collaborations with third parties such as start-ups, contractors, or outsourcers. Fully understanding third-party cyber risk will enable you to build confidence and embed resilience into cooperation. Cyber risks associated with third parties depend on the scope and nature of the contract. In your governance role, you must ensure the organization has adopted controls to mitigate unique risks specific to each third-party category.

Ian is the CSO of Cimpress, a leader in Mass Customization, with over 15 businesses worldwide and remote teams. Before Cimpress, Ian held senior leadership positions with Amazon, ZeroFOX, IOActive and has over 25 years of experience in the security industry as a practitioner. Ian is also the co-founder of DC9723 - the Tel Aviv DEFCON group-and serves as a BSides Las Vegas board member. He is also the creator and co-CEO of The CISO Track - a series of CISO centric curated events. Ian is an IANS Faculty member, a board member and advisor to several startups in the security field, and an angel investor.

MODULE 6

The Use of Cloud Technologies

The shift to the cloud has transformed business, with flexibility, scalability and cost-savings, creating new opportunities, but also new risks. How do you best mitigate exposures and leverage gain?

DAVID HAHN

Board Member and Chief Information Security Officer

The shift to the cloud has accelerated transformation and flexibility in product delivery and collaboration while providing scalability and cost savings. This shift creates creating new opportunities for organizations. Explore the cloud, understand different forms of the cloud, unique new risks that come from using cloud technologies, and how to mitigate these risks to better leverage the value of cloud computing.

David has a long history in Information Security and is a trusted business partner addressing the ever-growing and complex Cybersecurity landscape. He is the CISO at CDK Global, a leader in software and technology for the automotive industry. His career includes Financial Services with Wells Fargo Bank, Software Product and Services with Intuit (makers of TurboTax and Quickbooks), and large diversified Media/Data company with Hearst Corporation with large stakes in TV, Newspapers, Magazines, Healthcare, Transportation and Financial (Fitch Ratings).

Note: Faculty and case study affiliations are for information purposes only. No suggestion is made that these organizations have any affiliation with this course or the DCRO Institute. They are not responsible for its content in any way.

THE CERTIFICATE IN CYBER RISK GOVERNANCE®

THE DCRO RISK GOVERNANCE INSTITUTE

MODULE 7

How to Safely Deploy Emerging Technologies

AI, Blockchain, IoT and 5G – emerging technologies offer unprecedented opportunities and dramatically transform how businesses operate. Learn how industry leaders safely deploy and build on these technologies.

HOMAIRA AKBARI

Chief Executive Officer and Board Member

What cyber risks do we introduce to our enterprises when we adopt new and emerging technologies, and what you should know about these? We focus on three pervasive technologies: Artificial Intelligence, Blockchain, and Internet of Things-5G networks. While still in the process of fully understanding them, firms are already deploying mass applications across many sectors using them. Board members have a duty to accelerate their understanding of how these technologies work, what applications to use them for, and how technology leaders are integrating them into company infrastructure and IT systems.

Dr. Homaira Akbari is CEO of AKnowledge Partners, LLC. She serves on the Board of Directors of Banco Santander (NYSE: SAN) Temenos AG (SWX: TEMN), and Landstar System (NASDAQ: LSTR). She has held senior management roles in Fortune 1000 companies including Microsoft, Thales, and Liberty Media subsidiary, Trueposition, and served as the President and CEO of SkyBitz, a leading IoT provider of asset tracking and security solutions. She holds a Ph.D. in particle physics from Tufts University and an MBA from Carnegie Mellon Tepper School of Business. She is the author of more than 50 scientific articles in international journals and has two patents.

MODULE 8

Data Security

"Data is the new gold," is the repeated mantra. But gold mines invite criminals. Learn best data governance practices to protect your organization. With great data comes great responsibility.

RAMY HOUSSAINI

Chief Cyber, Technology Risk, and Privacy Officer

Data is a critical business asset of growing importance. It must be governed by rigorous protocols, including the existence of a data inventory and classification methodologies that help us to identify the most critical digital assets, such as confidential or secret information. The protection must be end-to-end during the whole data lifecycle and whether is at rest, in motion, or in use. “With great data comes great responsibility”: during the session, you will understand how to evaluate if your staff is using the best data governance practices to protect your organization.

Ramy Houssaini is the Chief Cyber and Technology Risk Officer and Group Data Protection Officer for BNP Paribas. He is an internationally recognized executive with a unique background in Cyber Security, Data Privacy, Operational Risk Management, and Technology. He served as the Vice President of British Telecom in Europe, the Regional Head of the Cyber Practice for Accenture, and as the Vice President for Information Security at Visa.

Note: Faculty and case study affiliations are for information purposes only. No suggestion is made that these organizations have any affiliation with this course or the DCRO Institute. They are not responsible for its content in any way.

THE CERTIFICATE IN CYBER RISK GOVERNANCE®

THE DCRO RISK GOVERNANCE INSTITUTE

MODULE 9

Cyber Defense Best Practices

Defending an organization from cyber-attacks requires board oversight to ensure that a comprehensive approach is in place, including technical and organizational security controls, all at a global standard level.

ED SLEIMAN

Chief Information Security Officer

Organizational and technical cybersecurity controls are essential for securing data and infrastructure. These controls range from access control mechanisms, such as strong passwords and authentication processes, to encryption techniques that protect sensitive information from unauthorized access. Understanding the most relevant technical and organizational security controls at the board level is crucial in your oversight role. In this session, you'll learn about the techniques and protocols used to detect and respond to cyber-attacks and gain an understanding of the purpose and scope of the leading international standards for cyber defense.

Ayed (Ed) Sleiman is the former Head of Information Security for King Abdullah University of Science and Technology (KAUST) in Saudi Arabia. He is an active speaker at security and risk management conferences in the Gulf Region, including the Gartner Security and Risk Management Summit, the RSA Conference, The Gulf Information Security Exhibition (GISEC), and the CISO Summit.

MODULE 10

Boards and the Governance of Cyber Risk

The resilience of your organization fundamentally depends on the ability to accurately and comprehensively understand, manage. and govern cyber risk.

DAVID X MARTIN

Special Counselor, Author, Former Chief Risk Officer

The specific needs of any effective cyber program include careful planning, smart delegation, and a system for monitoring compliance — all of which directors should oversee. It's no longer a question of whether a company will be attacked but more a question of when this will happen — and how the organization will prevent it. Cybersecurity cannot be guaranteed, but a timely and appropriate reaction can. The board should consider cybersecurity as a managerial issue, not just as a technical one

David X Martin co-chaired the DCRO Cyber Risk Governance Council. He is a Special Counselor to the Center for Financial Stability, the author of CyRM: Mastering the Management of Cybersecurity, and the former Chief Risk Officer of Alliance Bernstein. David co-chaired a public/private initiative with the FBI and major corporations on intelligence sharing and best practices, consulted for a leading central bank on cyber security audits of financial institutions, chaired an information security committee for a public corporation, and was Citigroup's first enterprise risk manager.

Note: Faculty and case study affiliations are for information purposes only. No suggestion is made that these organizations have any affiliation with this course or the DCRO Institute. They are not responsible for its content in any way.

CASE STUDY INTERVIEWS

- **Selim Aissi**, Board Member and Global Chief Information Security Officer
- **Lauren Anderson**, Board Member, Former FBI Executive
- **Kevin Brock**, Board Member, Former Head of the FBI National Counter-terrorism Center
- **Peter Cousins**, Chief Technology Officer
- **Dr. Nida Davis**, Qualified Risk Director,® Director of Security Architecture
- **Ursuline Foley**, Qualified Risk Director,® Board Member, and Former Chief Information Officer
- **Dr. Mark Frigo**, Board Member and Head of the Center for Strategic Risk Management
- **Ray Ghanbari**, Chief Technology Officer
- **Susan Holliday**, Qualified Risk Director,® Board Member, and Former Senior Executive
- **Cameron Mitchell**, Global Head of Geopolitical Risk
- **Dr. Philip Moulton**, Qualified Risk Director® and Director of Risk Management
- **Henrik Niels Olsen**, Head of Business Continuity
- **David Schwartz**, Chief Technology Officer

The Certificate in Cyber Risk Governance®

Candidates who successfully complete the course requirements, including passing quizzes at the end of each chapter, are awarded The Certificate in Cyber Risk Governance®, a global credential issued by the DCRO Risk Governance Institute. Graduates receive a digital certificate which can be displayed on their social media and board documents, providing evidence of distinction and success in their studies of cyber risk governance.

Note: Faculty and case study affiliations are for information purposes only. No suggestion is made that these organizations have any affiliation with this course or the DCRO Institute. They are not responsible for its content in any way.

Who is this course for?

This course is for current and aspiring directors and executives who seek a better understanding of technologies for strategic growth and oversight. Along with these technologies come challenging risks, of which you must be aware. We take an agnostic approach to teaching, meaning the content is relevant for all industries and geographies. No technical knowledge or previous cyber experience is required.

What is the format?

Lectures, case study interviews, and additional resources are all available on-demand through the DCRO Institute learning platform - a leading edge interactive learning tool. You can access courses anytime from anywhere with an internet connection. At the end of each lesson is a quiz on which you must get 80% or higher to pass. Abundant additional reading materials and references are provided and you have up to one year to complete the program.

What is the cost?

Exclusive to Impact Boards Emerging Markets members serving in emerging markets, tuition for one year of access to the modules and assessments is US$800 (Regular price: US$2,195).

Register Now

World Class Credentials

The DCRO Institute is the world's leading source of risk governance training and credentialing. We are a 501(c)3 nonprofit peer collaboration among board members and C-suite executives from around the world. Graduates from our programs are leaders in boardrooms and C-suites on six continents. Our emphasis is on the positive use of risk and risk knowledge in the strategic planning and execution of plans at organizations of all sizes worldwide and in developing people to do that work as Qualified Risk Directors®and Qualified Risk Experts™.
