SIG UNIVERSITY
CERTIFYING SOURCING AND RISK LEADERS

COURSE SYLLABUS

3PRM: Third Party CyberSecurity Risk Management (3PRM-CyberSecurity)

This eLearning training program was created in partnership with Linda Tuck Chapman, a leading expert in third party risk and relationship management and CEO of the Third Party Risk Institute, and will provide you with a strong working knowledge of the basics of cybersecurity. This program includes lessons on globally accepted frameworks including ISO and NIST, terminology in common use, and the sources and mitigants for third party cybersecurity risk.

The following guide will provide you with all the necessary information about this program offered by SIG University.

About SIG University

SIG University was founded on the ideals of elevating sourcing and risk professionals to deliver strategic value to the corporation. It is an inclusive, internationally recognized university with a mission of advancing the sourcing and risk management industries and transforming careers.

SIG University was created at the request of SIG members, who saw an educational training gap for today's workforce. It uses an adult learning model to transfer the knowledge and skills to its students. The learning model is focused on the self-directed learner, who has the basic knowledge and skills of the material, is motivated, has good time management skills, and has the ability to self-evaluate.

The SIG University learning model is supported by a practitioner faculty who currently hold senior leadership positions in sourcing and risk management, allowing them to guide students to a better learning outcome.

Classroom Format

This program is offered online in a self-paced model, allowing for ultimate flexibility for you or your organization's needs.

Our state of the art learning management system can be accessed from any device and saves the student's progress from where they left off. This allows students to balance their busy schedules and pause, replay, or pick back up when is most convenient for them.

In this delivery model, there is no required discussion with faculty nor essay requirements or quiz assessments.

*For this program, students must complete all graduation requirements within 3 months of starting. Graduation requirements include completing all lessons and reviewing all supplemental resources.

What is “third party cybersecurity risk management”?

Third Party Cybersecurity Risk Management refers to the process of identifying, assessing, and mitigating the risks posed by external parties (third parties) that have access to a company’s systems, data, or networks. These external parties can include vendors, suppliers, contractors, or any other entities with whom the organization shares sensitive information or resources.

As businesses increasingly rely on third parties for critical operations, they also inherit potential security vulnerabilities that could expose them to data breaches, regulatory non-compliance, and operational disruptions. Effective risk management involves continuous monitoring, due diligence during vendor selection, contractually enforcing security requirements, and implementing controls to minimize threats. This approach ensures that third-party relationships do not become weak links in an organization’s cybersecurity posture, protecting sensitive information and maintaining compliance with industry regulations.

In this course, you’ll understand the fundamentals and importance of managing third party cybersecurity risks in businesses. You’ll learn best practices for identifying, mitigating, and managing risks effectively, while developing a keen sense of risk awareness and its impact on business decisions.

Who should take this course?

The 3PRM-CyberSecurity program is applicable to so many roles in sourcing, outsourcing, procurement, vendor management, third party risk management, and related fields. Whether you’re responsible for risk management, oversight, compliance, or audit, or contemplating a career in cybersecurity risk management, our Certificate Program delivers practical, actionable knowledge.

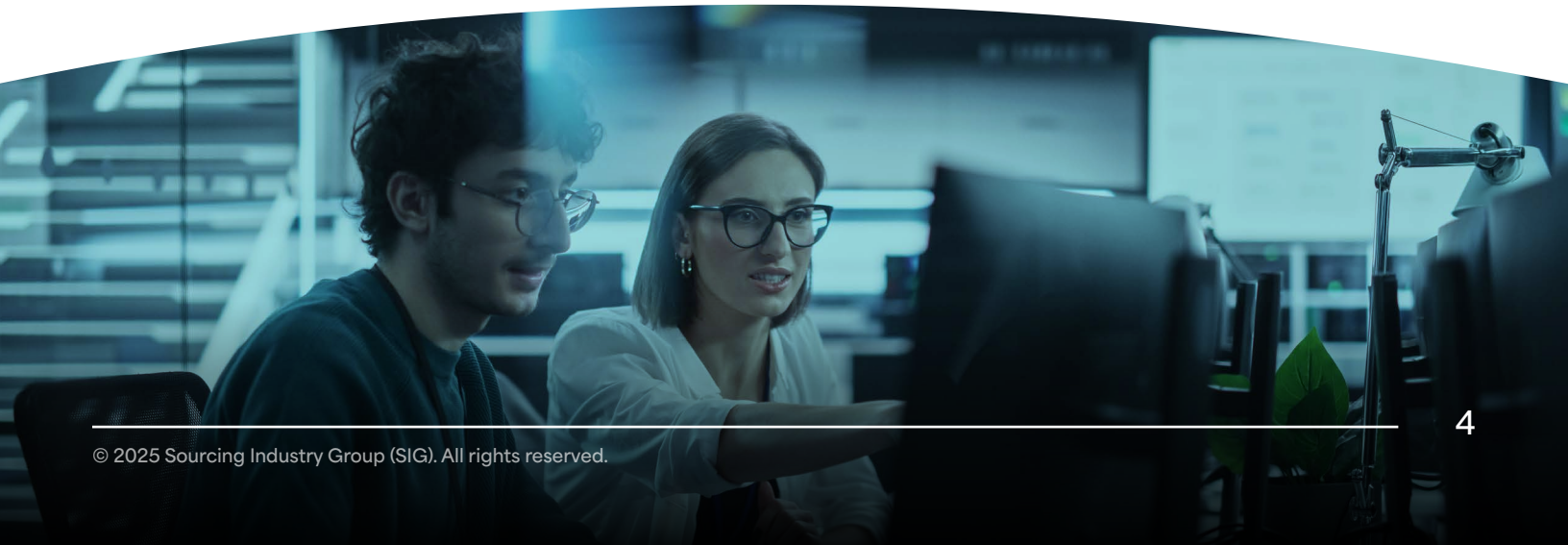
This self-paced program was created by industry experts who share their insights into globally recognized frameworks, threat actors’ motivations and techniques, and how cybersecurity professionals protect their organizations.

What will I learn in this course?

Created in partnership with Third Party Risk Institute, the 3PRM-CyberSecurity program covers the fundamentals of cybersecurity. The online, video-based program was developed by Linda Tuck Chapman, a renowned expert in third party risk and relationship management.

The program covers:

- **Introduction to CyberSecurity Risk Management:**
  Overview of CyberSecurity risk managment, aligning enterprise and Cyber Security risks, identifying threat actors and their tactics, lifecycle activities, key terminology, and role based accountabilities.
- **Mitigating CyberSecurity Risk:**
  Focuses on key CyberSecurity concepts, risk mitigation strategies, security controls, penetration testing, disaster recovery, business continuity, risk transference, and continuous monitoring.
- **Standards and Frameworks:**
  Introduces ISO and NIST frameworks, special publications, and controls for CyberSecurity risk management.
- **CyberSecurity Risk Management Frameworks:**
  Explores the Risk Management Framework (RMF), high-impact controls, control assessments, third party control evaluations, and the role of a Software Bill of Materials.
- **Threats and Attack Vectors:**
  Discusses common CyberSecurity threats, attack methods, and risk exposures, including malware, phishing, deep fakes, and SQL injection.



Why choose this course?

- **Practical Content:**
  Current frameworks and third party controls which ones have the highest impact. How threat actors successfully commit breaches, and what organizations can do to protect themselves from hackers.
- **Real-World Learning:**
  Engaging content delivered by recognized experts. Real-life examples that deliver relevant, hands-on knowledge.
- **Enhance Your Credentials:**
  A Certificate of Completion from a respected institution and CPE credits showcase your professionalism.
- **Flexible, Self-Paced Learning:**
  You set the pace, balancing the learning activities and your daily responsibilities.

What can I expect after completing the course?

In addition to the knowledge, skills, and tools gained, those who have completed the 3PRM-CyberSecurity program have loved the learning experience provided, and they are able to **apply what they learned immediately**. All graduates of the 3PRM-CyberSecurity program are issued a digital badge and a certificate of completion to include on their CVs and LinkedIn profile.

Graduates of the 3PRM-Essentials program are invited to join the SIG University Alumni and Faculty private LinkedIn group to stay connected with peers and faculty.

Who are the Subject Matter Experts?

Linda Tuck Chapman

President, Third Party Management advisor, Author, Speaker

Ontala Performance Solutions Ltd.

Linda Tuck Chapman: Advisor. Educator. Author. Expert. Linda is a recognized subject-matter expert, trusted advisor, published author and popular speaker. As former Chief Procurement Officer in three major banks, her clients benefit from her experience, expertise and pragmatic approach.

Linda is creator/professor of the "Certified Third Party Risk Management Professional" (C3PRMP) program for SIG University, based on her book "Third Party Risk Management: Driving Enterprise Value", available on Amazon. Her expertise is frequently profiled in industry-leading publications such as The RMA Journal, Wall Street Risk Journal and Future of Sourcing, strengthened by her extensive network, professional associations and SIG University.

Keith Bowie

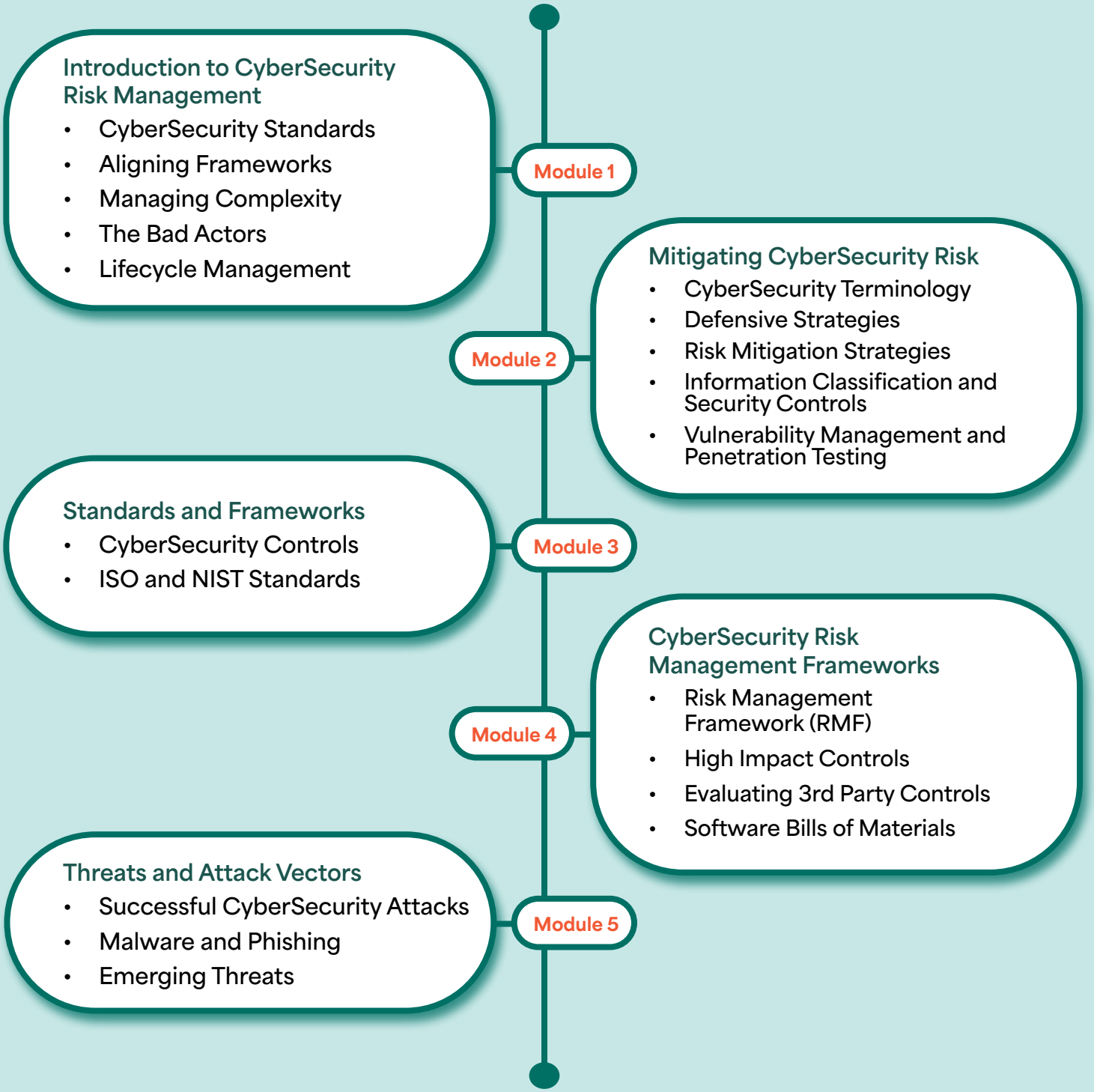
Chief Information Officer

SessionGuardian

Keith Bowie is currently part of the executive leadership team at SessionGuardian, bringing innovative and unique products to market. Keith has over 30 years' experience in leading large global technology teams and successfully delivering complex technology and business transformation initiatives in multi-national financial services and commodoty trading organizations. Keith was Scotiabank's first US CIO.

Keith completed a 2-year assignment at the Digital Financial Services Observatory, within the Columbia Institute for Tele-Information at Columbia University in New York, where he led the creation of a process-based CyberSecurity Risk Management Framework for use in Digital Financial Services in the developing world. This project was funded by the Gates Foundation to promote financial inclusion in a safe environment.

What is the learning journey?



Course Outline

The program is self-paced with e-learning modules. Below is a listing of the modules of the program and what topics they cover.

Each module includes:

- Engaging video lectures
- Compelling slides and visual aides

Module 1 : Introduction to CyberSecurity Risk Management

In this module, students will gain an understanding of key aspects of Third Party Cybersecurity Risk Management, including the role of global cybersecurity standards like ISO and NIST in building a strong security program, aligning risk management with enterprise frameworks, and navigating the complexity of third-party risk. Students will also learn about different cyber threat actors and their motivations, along with best practices for managing risks throughout the entire vendor lifecycle, from onboarding to offboarding.

Module 2: Mitigating CyberSecurity Risk

In this module, students will learn essential cybersecurity terminology to effectively communicate with stakeholders. They will explore defensive strategies for protecting organizational assets and proven risk mitigation techniques for managing third-party cybersecurity risks. Students will also learn the importance of information classification and security controls, along with best practices for vulnerability management and penetration testing to assess and strengthen security measures.

Module 3: Standards and Frameworks

In this module, students will explore key cybersecurity controls that have a high impact on managing third-party risk. They will also examine globally recognized cybersecurity frameworks, focusing on ISO 27000 series and NIST Special Publications, to understand their role in strengthening cybersecurity practices.

Module 4: CyberSecurity Risk Management Frameworks

In this module, students will learn about the Risk Management Framework (RMF) and its application in cybersecurity. They will examine high-impact third-party controls, assess their effectiveness in protecting critical assets, and explore strategies for evaluating third-party cybersecurity measures. Additionally, students will gain an understanding of Software Bills of Materials (SBOMs) and their role in cybersecurity risk management.

Module 5: Threats and Attack Vectors

In this module, students will study real-world examples of successful Cybersecurity attacks and the lessons learned. They will also learn to distinguish between different types of attacks, such as malware and phishing, and how to protect against them. Students will also explore deep fake technologies, SQL injection, DDOS attacks, insider threats, zero-day vulnerabilities, and more.

What are the enrollment fees?

Non-SIG Member Price: **$795**

SIG Member Price: **$695**

What are my next steps?

Enroll today at:

https://go.sig.org/3prm-cybersecurity-request-to-enroll

View our other courses and certifications and learn more about SIG U at:

https://sig.org/sig-university