SHARED ASSESSMENTS

CTPRA

CERTIFIED THIRD-PARTY RISK ASSESSOR (CTPRA) HANDBOOK

Table of Contents

About the CTPRA Certification Program

The Certified Third-Party Risk Assessor (CTPRA) designation is a professional credential that validates expertise, decision-making, and proficiency in third-party risk and controls evaluation. The program includes the processes for identifying, quantifying, and mitigating third-party risk within an organization's TPRM program.

The program structure emphasizes control evaluation within specific risk domains to conduct comprehensive governance, operational risk, IT, and cyber-risk third-party evaluations using distinct assessment techniques.

12 CPEs can be earned for completing the course.

CTPRA Certification Requirements
Knowledge Level: Advanced

- Candidates have a minimum of five years professional experience in a TPRM-related role.
- Candidates are seasoned risk or audit professionals, or have deep technical expertise in information security, resilience, and information technology management.
- Candidates have strong security and technological acumen and the ability to apply that knowledge into evaluating a third party's control environment.
- Candidates have in-depth experience on risk identification and quantification to properly scope and conduct third-party risk assessments.
- Candidates tend to have experienced IT backgrounds based on years of experience.
- Candidates may have operational or supervisory responsibilities, or both.
- Candidates tend to use the certification to broaden their skills and knowledge in techniques for conducting assessments to facilitate job advancement in assessment or audit roles.

The CTPRA is designed for Third-Party Risk, Information Security, Cyber risk, Audit, Information Technology, and Governance, Risk, and Compliance (GRC) professionals that are involved in the planning, scoping, and conducting the evaluation of a third-party's control environment, including:

- Cybersecurity Risk Auditors/Assessors
- Governance, Risk, and Compliance Analysts/Managers
- Operational Risk Analysts
- Third Party Risk Analysts
- Security Engineering Analysts
- Enterprise Risk Managers
- Security and Risk Analysts
- Information Security Auditors
- Internal Audit Managers
- IT Procurement Specialists
- Third Party Relationship Managers

CTPRA Curriculum Learning Objectives

- Demonstrate a thorough understanding of outsourcing business models, regulatory drivers, data governance factors, and the types of risks in third-party relationships to understand the core components of a TPRM program.
- Incorporate industry and technology assessment frameworks for control evaluation to conduct risk-based due diligence based on vendor classification, risk rating, scoping factors, and criticality.
- Evaluate the potential risks in a third party's control environment for governance, information protection, operational risk, technology management, and evolving technologies.
- Define, scope, and manage the risk assessment process by conducting discovery, reviewing artifacts, and validating controls in order to identify risk rate findings in corrective action plans based on organizational requirements.

CTPRA Course-Level Curriculum Learning Objectives

Section I: Third-Party Risk Program Management

Understanding TPRM Disciplines

- Demonstrate understanding of third-party risk management concepts and the regulatory environment for third-party risk to identify and quantify third-party obligations risks based on analysis of the outsourcing business model and applicable industry and regulatory requirements.

Information Classification and Data Governance

- Differentiate the various classifications of personal information based upon industry sector or regulatory jurisdiction that trigger specific data protection safeguarding requirements for third-party relationships.

TPRM Program Components

- Understand the structural components of an organization's third-party risk management program in order to utilize and implement a defined vendor risk management process throughout the complete vendor relationship and contract lifecycle.

Section II: Performing Risk-Based Due Diligence

TPRM Program Assessment Requirements

- Conduct assessments based on risk rating, vendor classification, and defined due diligence standards using standardized risk or compliance control frameworks.

Third-Party Risk Assessment Process

- Devise and deploy multiple due diligence techniques for conducting discovery and controls evaluation through the use of repositories, questionnaires, interviews with subject matter experts, compliance artifact reviews, testing, and use of external assurance reports.

Post-Assessment Reporting and Remediation

- Analyze and quantify assessment results by identifying risk rating findings for inclusion in corrective action plans, remediation status tracking, and closure of identified risks.

Risk Control Domains

Section III: Controls Evaluation: Governance and Information Protection

Governance, Risk, and Compliance (GRC)

- Evaluate the organization's corporate governance and compliance functions to ensure adequate policies and controls are in place to address both risk assurance and legal, regulatory, and standards compliance.

Information Protection

- Analyze the administrative, technological, and physical data protection safeguards and controls in place in order to identify risks, gaps, or differences in policy requirements.

IT Operations and Business Resilience

- Evaluate a third party's IT operations functions and resilience strategies to validate the effective management, operation, integrity, and recovery of systems designed to mitigate the risk of service disruption in response to internal or external events.

Section IV: Controls Evaluation: Technology Management and Operational Risk

Architecture and Technology Governance

- Analyze a third party's approach to IT governance, architecture, and technology acquisition to identify potential risks of the use of specific technologies used in the services.

Cloud Services

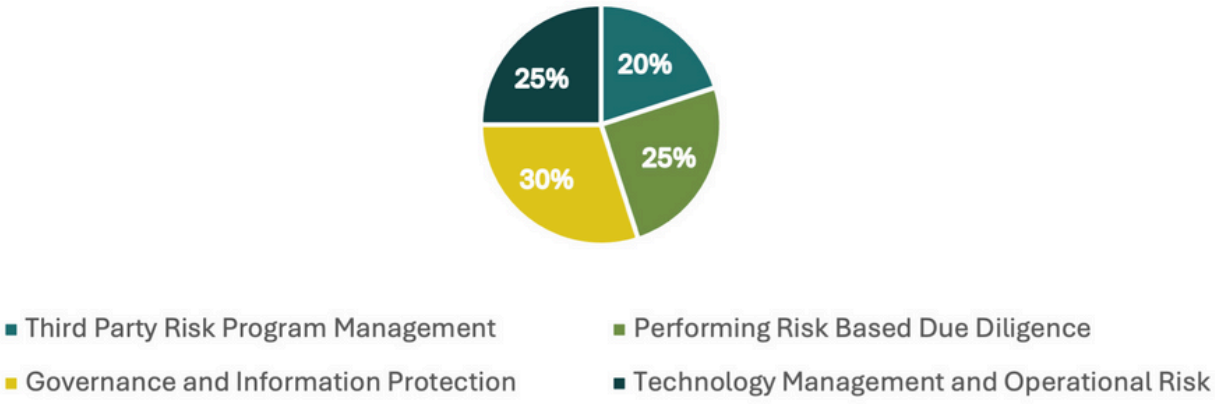
- Identify and evaluate the use of cloud services by the third party, including control evaluation of shared responsibilities between parties based upon the service and deployment model.

Emerging Technologies

- Analyze a third party's use of new technologies within outsourced services leveraging industry practices to address evolving risks posed by an increasingly complex technology ecosystem.

CTPRA Exam Profile

CTPRA Curriculum Profile



The CTPRA examination contains 125 questions worth up to 140 points. Examination questions include testing the domain knowledge and application of knowledge using third-party risk situations.

Multiple choice questions are presented using third-party risk management scenarios from the outsourcer or the service provider's point of view. A score of 70% or higher must be achieved to pass the exam.

The CTPRA examination is a closed-book exam with a three-hour time limit.

Upon completion of the exam, a survey may be presented to provide feedback on the method of instruction, curriculum, materials, or examination content.

Scheduling Exam and Process

After completing the class, test-takers can schedule their exam through our exam platform called Proctor 360.

Scheduling Exam

To schedule the CTPRA exam, click on the exam scheduling link provided by the Shared Assessments Education team. If you already have an account with Proctor 360, please log in and start scheduling. If you do not have an account with Proctor 360, you will be required to create one and verify your email address. If you don't receive a verification email, click "resend" or check your spam folder.

Once logged in, select an available date and time to schedule the exam.

System Check

Once you have scheduled your exam, you will receive an email with instructions to complete a System Check to verify that your computer works properly for the testing process. This email contains important information about your exam.

When you click on the system check link, you will be taken to a new tab with Proctor360's privacy policy and requirements. Accept the policy and click "Start System Inspection" to verify that your computer meets the necessary capabilities for the exam. If you don't already have it, you may need to install Proctor360's Chrome Extension.

Taking the Exam

After finishing the System Check requirements, you will receive another email with a Check-In link. During Check-In, proctor support will walk you through the authentication process. You will be asked to:

- Verify your identity by presenting your photo ID in front of the webcam. The proctor needs to clearly see your name and photo.
- Show your desk and workspace. The proctor will ask you to complete a 360˚ room pan and desk sweep with your webcam. This is to ensure your workspace is clear of any materials unauthorized by your instructor.

You are strongly encouraged to sign up at least 48 hours before the selected exam time to avoid a $15 USD “on-demand” testing fee. Additionally, any cancellation or modification within 48 hours of an existing exam appointment will result in a $15 USD fee.
Candidates are encouraged to complete the testing process within 15 weeks of the course training.

Please Note: We encourage test-takers to arrive 15 minutes before the start of their exam. This will allow ample time to connect with your proctor and troubleshoot any technical issues that may arise.

Exam Retake

If you do not pass the exam with a minimum score of 70%, you may take it again. There is a $150 USD fee to retake the exam. You may re-take the exam up to three (3) times. After the third attempt, you must re-take the class at your expense. Individuals who wish to retake the class will receive a 50% discount on the program.

Exam Results

You will receive provisional results after completing the exam. Final exam results are released pending review and approval by the exam proctors and Shared Assessments. Final exam results and next steps will be sent to you via email within two weeks of completing the exam with information on the application process or re-testing options.

Application Process

The application form is provided to you upon passing the exam. You are required to fill out your relevant work experience and provide the name and contact information of a person who can verify your employment experience.

Applicants will need to provide relevant work history detailing a minimum of five years experience in a TPRM-related job role.

In lieu of TPRM work experience, an applicant can receive up to a year of work experience credit if they have a bachelor's or master's degree in information security or information technology from an accredited university. An additional year of work experience may be waived if the applicant holds an active industry certification related to TPRM.

Associate CTPRA and CTPRA Certifications

The CTPRA certification is awarded to those who complete the steps indicated above and hold a minimum of five years experience in TPRM.

An individual who passes the exam but does not meet the prerequisite of five years of experience as a risk management professional will be awarded the Associate CTPRA designation. The Associate CTPRA can be changed to a full CTPRA designation at no additional cost if the certification is kept active and the five (5) year professional experience requirement is achieved.

For more information on the application process see our CTPRA Eligibility Requirements and Policy page.

Certification Awarded

The application review process may take up to two weeks from submission. Once your application has been approved, you will receive a congratulatory email explaining how to download your Certification and information on receiving your digital certification badge via Credly.

Maintaining the CTPRA Certification

- Certification holders must pay an annual maintenance fee of $100.00 USD to maintain their certification.
- Earn the required 36 CPE credits per three-year certification term (we recommend earning 12 CPEs per year)
- Successfully abide by the Shared Assessments Code of Ethics

Shared Assessments Code of Ethics

The Shared Assessments Program has established a Code of Professional Ethics to guide the conduct of its certification holders. The goal of the code of ethics is to clarify every certified risk professional's responsibility to support the risk management profession by conducting themselves in a professional and ethical manner.

Action will be taken against anyone who violates the ethics code. These actions may range from a warning to the withdrawal of their risk professional certification. Rather than seek to regulate its certificate holders, Shared Assessments intention is that this code aid in providing guidance in making ethical decisions.

Shared Assessments certification holders shall:

1. Abide by the law of the jurisdiction in which services are provided, perform all duties in an honorable manner, and respect the rights of others in performing professional responsibilities.
2. Perform their duties with objectivity and professional care, and in accordance with professional standards.
3. Encourage compliance with appropriate standards and procedures for the effective management of enterprise information systems and technology including: audit, risk controls, privacy, security and risk management.
4. Maintain the privacy and confidentiality of information obtained in the course of their activities unless disclosure is required by legal authority. Such information shall not be used for personal benefit or released to inappropriate parties.
5. Maintain competency in their respective fields and agree to undertake only those activities they can reasonably expect to complete with the necessary skills, knowledge and competence.
6. Not knowingly provide misleading or inaccurate information, nor encourage or otherwise participate in the release of such information.