SHARED ASSESSMENTS

CTPRP

CERTIFIED THIRD-PARTY RISK PROFESSIONAL (CTPRP) HANDBOOK

Table of Contents

About the CTPRP Certification Program

The CTPRP designation is a professional credential designed to validate knowledge, experience, and proficiency in the design, structure, and implementation of a comprehensive Third-Party Risk Management (TPRM) Program.

The program includes the processes for third-party risk identification and structuring a risk-based vendor classification and risk assessment process. The program incorporates best practices for TPRM program metrics, management reporting, and evaluating the operational performance of the program.

12 CPEs can be earned for completing the course.

CTPRP Certification Requirements

Knowledge Level: Intermediate

- Candidates have a minimum of five years professional experience in a TPRM-related job role.
- Candidates have either direct or indirect responsibilities for third-party risk management functions.
- Candidates may have detailed knowledge or experience in certain technical topics but not broad experience in all topics related to TPRM.
- Candidates tend to use the certification to broaden their skills and knowledge to facilitate job advancement in third-party risk roles or responsibilities.
- Candidates tend to be in mid-level roles within the organization based on years of experience.
- Candidates may have operational or supervisory responsibilities, or both.

The CTPRP is designed for Third-Party Risk, Audit, Procurement and Governance, Risk, and Compliance (GRC) professionals that are involved in the development, implementation, and management of TPRM programs, including:

- Business Vendor Relationship Managers
- Governance, Risk, and Compliance Analysts
- Governance, Risk, and Compliance Managers
- Third Party Risk Analysts
- Enterprise Risk Management Managers
- IT Risk Analysts
- Internal Auditors
- IT Procurement or Sourcing Risk Managers
- Vendor Risk Management Managers

CTPRP Course Curriculum Learning Objectives

- Demonstrate the ability to identify and quantify the impact of regulatory drivers, data governance factors, and types of risk involved in risk mitigation and oversight of third-party relationships.
- Recognize and interpret the set of program components required to structure and operate an effective TPRM program based upon organizational requirements and contractual obligations.
- Interpret knowledge of the control objectives for evaluating distinct types of risk by identified control domains to define TPRM program requirements or conduct third party assessments.
- Implement the TPRM processes and infrastructure required to operate and maintain an effective TPRM program that enables risk-based management decision-making.

CTPRP Course Level Curriculum Learning Objectives

Section I: Third-Party Risk Management Foundation

Understanding TPRM Disciplines

- Explaining the terminology used in outsourcing including the drivers and factors that trigger third-party risk and mitigation strategies based on the nature of the outsourced services.

Data Governance in TPRM

- Identifying unique data protection or safeguarding requirements based on data classification, industry, or regulatory authority.

TPRM and Enterprise Risk Management

- Differentiating important terms used in risk management and the organizational practices required for effective governance and oversight of TPRM programs.

Section II: TPRM Program Design and Structure

Establishing Program Governance

- Establishing the requirements that define TPRM Program accountability and risk rating requirements that set the foundation required to structure an effective TPRM program.

Developing TPRM Program Requirements

- Defining and implementing program requirements that address contractual obligations and required levels of due diligence based on risk tier.

Defining Third-Party Risk Assessment Process

- Organizing and preparing business processes and tools that deploy a third-party assessment process based on the type and category of assessment.

Section III: Controls Evaluation in TPRM

Governance, Risk, and Compliance (GRC)

- Assessing the organization’s approach to corporate governance, compliance, and information assurance for alignment with company policy, ethical business practices, and regulatory obligations.

Information Protection

- Identifying the primary administrative, technological, and physical data protection safeguards, controls, and tactics included in third-party assessments based on the nature of the outsourced product, service, or activity.

IT Operations and Business Resilience

- Demonstrating understanding of the key operating procedures and controls required to ensure the effective management, operation, integrity, and recovery of operations to mitigate the risk of a service disruption.

Cybersecurity and Technology Governance

- Recognizing the risk management and governance requirements that address cybersecurity and threat/vulnerability management based on the type of technology utilized in the delivery of the services.

Section IV: TPRM Program Operations and Implementation

Post-Assessment Reporting and Risk Mitigation

- Executing processes that implement and manage corrective action plans into governance structures for risk acceptance and treatment including risk reporting and ongoing monitoring.

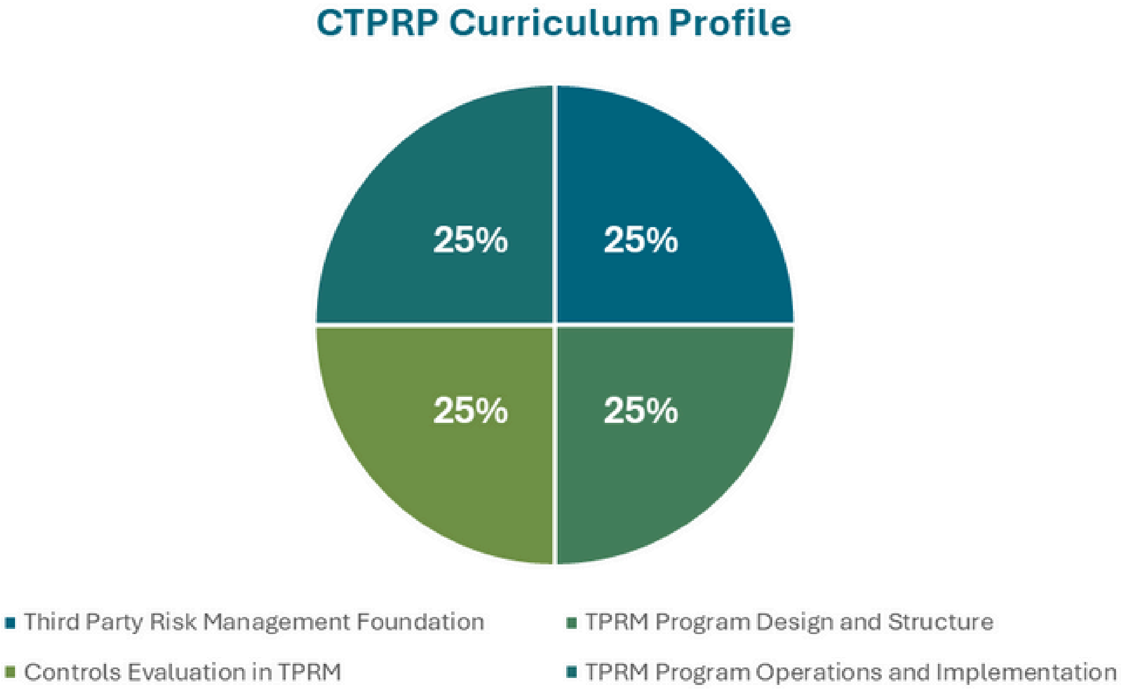
Managing TPRM Program Information and Activities

- Defining the processes, workstreams, and data management functions utilized in operating the TPRM program.

Optimizing TPRM Program Operational Performance

- Identifying the best practices in evaluating and measuring the effectiveness of the TPRM programs in assessing and mitigating third-party risk.

CTPRP Exam Profile



The CTPRP examination contains 120 questions worth up to 125 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 CTPRP 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 CTPRP 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 CTPRP and CTPRP Certifications

The CTPRP 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 CTPRP designation. The Associate CTPRP can be changed to a full CTPRP 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 CTPRP 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 CTPRP 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.