2020 CTPRP Certification Job Practice Guide

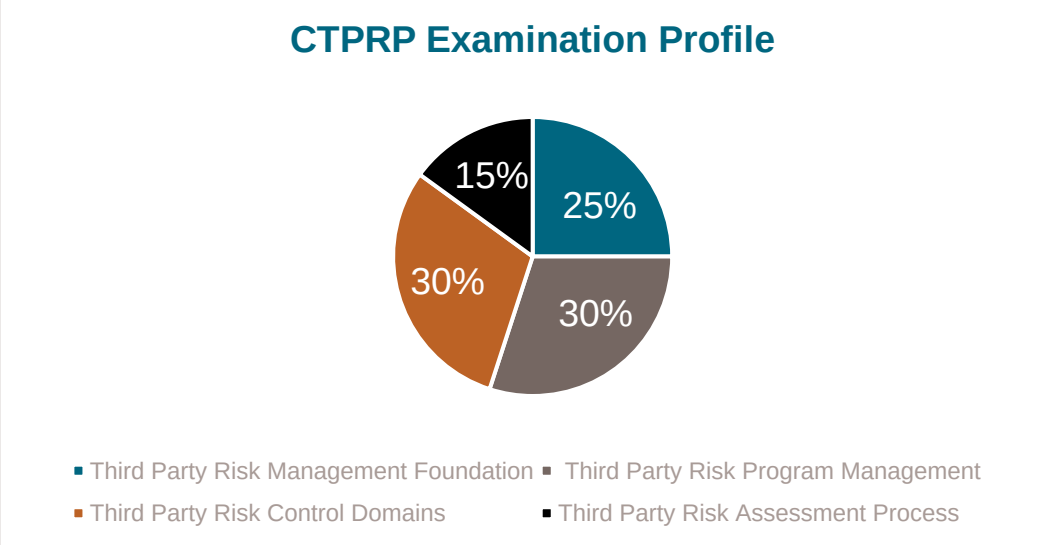
Role description

The CTPRP designation is designed to validate knowledge and experience to demonstrate proficiency in the development of a comprehensive Third Party Risk Management (TPRM) Program; and, the assessment, analysis, management, and remediation of third-party risk issues. The job practice guide identifies the domains, topics, skills, competencies, and job role accountabilities that represent the type of work performed by an individual who supports the development, implementation, maintenance, and training of a third-party risk management program within their organization. The structure of the job practice guide is based on the inputs of Shared Assessments Program members, recognized best practices, and tools that drive third party risk assurance.

Certification Blueprint

To achieve the CTPRP credential, candidates must provide both evidence of their years of experience and successfully passing a rigorous exam. Earning a qualified credential, requires prior knowledge and simply completing a training course does not guarantee you will pass the test. We recommend at least **30** hours of preparation prior to taking the examination. The course materials and examination are career resources designed for those professionals who plan to certify, as well as for those who simply need to deepen their knowledge in third party risk management.

The CTPRP training material and examination is organized by grouping the required body of knowledge topics into specific job practice focus areas. The CTPRP examination will contain questions testing the domain technical knowledge and application of on the job knowledge based on the CTPRP Curriculum Outline:



Examination Protocols & Question Formats

The CTPRP examination will contain 125 questions worth up to 140 points. Examination questions will include testing the domain technical knowledge and application of knowledge using third party risk situations.

The CTPRP examination is a time-based, closed book exam, completed within 2 hours. The exam is taken online and remote proctoring will be required to monitor examination compliance. Upon completion of the exam a survey may be presented to provide feedback on the method of instruction, curriculum, materials, or examination content.

Multiple choice questions will be presented to users using third party risk management scenarios from the outsourcer or the service provider point of view.

Example#1:

Knowledge Based Question

Perimeter controls are part of the first layer of defense to prevent unauthorized physical access, as well as accidental and intentional damage to the organization's physical premises, systems and information. Which of the following is NOT considered a perimeter control:

A. Building monitoring and intrusion alarms
B. Personnel Access Controls
C. Firewall Logs
D. Environmental controls

Example#2:

Controls Evaluation Focus Question

When conducting a perimeter security review, the most effective sequence of testing the physical security controls is:

A. Test restricted entry areas first
B. Test public areas of the building first
C. Test only the exterior areas of the building
D. Start on the outside of the building and work inward

Example#3:

Multiple Choice/Factors Question

Physical access logs should:

A. Be kept for no more than 60 days

B. Record both successful and unsuccessful access attempts

C. Include the investigation of unsuccessful access attempts

D. Apply only to server rooms or data centers

Select which set of choices represents the best selection

- A, B, C
- B, C
- A, D
- A, B, C, D

Example#4:

Scenario-Based Question

A. You are a third party risk analyst, conducting a review of your TPRM program. When quantifying the actual resource requirements to operate your program which metric is least important in assessing whether your current resources can achieve your program goals? The number of people you need to perform control assessments based on your policies
B. The dollar amount of your budget
C. The number of people you need to maintain the program
D. The number of people you need to interpret vendor responses

I. Third Party Risk Management Foundation

A. Regulatory Drivers for Third Party Risk
B. Information Classification & Data Governance

Third Party Risk Management Program Components

II. Third Party Risk Program Management

A. TPRM Program Structure
   - Program governance
   - Policies, standards, and procedures

B. TPRM Operations
   - Contract development, adherence and contract management
   - Vendor risk classification
   - Due Diligence Standards
   - Skills and Expertise
   - Communications and Information Sharing

C. TPRM Measurements
   - Tools, Measurements & Analysis
   - Monitoring and review

III. Third Party Risk Control Domains

A. Governance & Risk Management
   - Risk assessment & treatment
   - Information security policy
   - Organizational security
   - Data Privacy Governance
   - Human resources security
   - Compliance & Audit

B. Information Protection
   - Access control
   - End User Device Security
   - Server Security
   - Network Security
   - Application Security
   - Privacy Data Safeguards
   - Cloud security
   - Physical & environmental security

C. IT Operations & Business Resiliency
   - Asset management
   - Operations management
   - Business Continuity Management
   - Disaster Recovery

D. Security Incident & Threat Management
   - Incident event and communications

- Threat management
- Vulnerability program
- Security awareness

IV. Third Party Risk Assessment Process

A. Phases of an Engagement
B. Assessment Planning & Preparation
C. Assessment Engagement & Communication
D. Post-Assessment Reporting & Remediation

Role Accountabilities

- Participates in the classification and risk tiering of third parties, including defining the frequency of risk assessments
- Coordinates the identification, ranking and tracking of third -party risks for the organization.
- Defines the due diligence standards based on risk rating or classification to be applied in third party assessments
- Manages communication plans and escalation plans regarding third party risk governance activities
- Actively drives coordination and implementation for the overall third-party risk management program function within the organization.
- Monitors changes in the regulatory landscape to identify relevant compliance requirements
- Facilitates the escalation process for management risk acceptance or remediation approvals
- Partners with lines of business to manage third party risk as defined in contracts and third-party policies and procedures
- Collaborates with internal functions to deploy standard contract provisions for security and privacy requirements.
- Monitors remediation actions and mitigation plans for identified third party risks
- Defines and tracks third party risk assessment metrics
- Communicates third party risk requirements to internal stakeholders
- Negotiates with third parties and business partners to address compliance with risk management policies
- Coordinates gathering and analysis of risk assessment data for management
- Maintains third party governance policies, procedures and practices
- Provides dashboard reporting on third party risk management program activities, results, and outcomes
- Identifies and implements monitoring functions for critical vendors
- Supports the vendor due diligence process by ensuring data protection requirements are maintained in contractual relationships