SFG | SHARED ASSESSMENTS

CERTIFIED THIRD PARTY RISK PROFESSIONAL (CTPRP)

CTPRP Certification Job Practice Guide

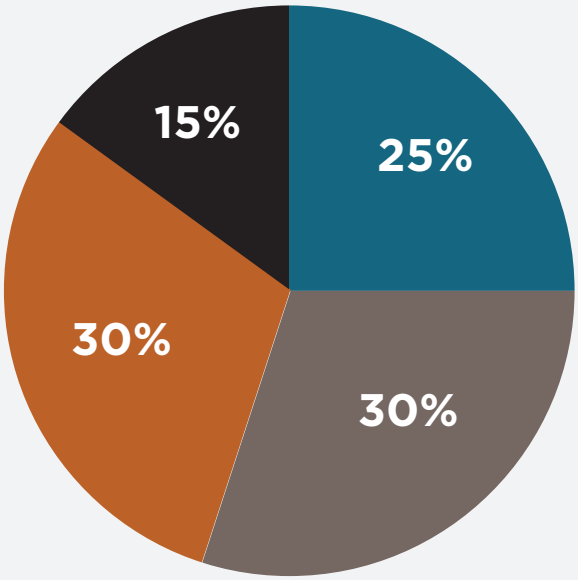
Role description

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

The CTPRP examination is organized by grouping the required body of knowledge topics into specific job practice focus areas. The CTPRP examination will contain 150 questions testing the job practice based on the overall area of knowledge percentages indicated as follows:

CTPRP Examination Profile



Body of Knowledge

I. Third Party Risk Management Foundation

A. Regulatory Drivers for Third Party Risk

B. Information Classification and Data Governance

C. Assessment Frameworks and Standards

II. Third Party Risk Program Management

A. Program governance

B. Policies, standards and procedures

C. Contract development, adherence and contract management

D. Vendor risk assessment process

E. Skills, Expertise

F. Tools, Measurements and Analysis

G. Monitoring and review

III. Third Party Risk Control Domains

A. Governance and Risk Management

- Risk assessment and treatment
- Information security policy
- Organizational security
- Human resources security
- Compliance

B. Information Protection

- Access control
- Application security
- Cloud security
- End user device security
- Network security
- Physical and environmental security
- Privacy
- Server security

C. IT Operations and Business Resiliency

- Asset management
- Operations management
- Business resiliency
- Disaster Recovery

D. Security Incident and Threat Management

- Incident event and communications
- Threat management
- Vulnerability program
- Security awareness

IV. Third Party Risk Assessment Processes and Procedures

A. Pre-assessment

B. Assessment activities

C. Post-Assessment activities

D. Evaluating the assessment process

V. Management Reporting and Remediation

A. Defining and Negotiating Remediation Strategies

B. Remediation Process Management

C. Management reporting

D. Escalation and Managing Exceptions

Role Accountabilities

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