SFG | SHARED ASSESSMENTS

CERTIFIED THIRD PARTY RISK ASSESSOR (CTPRA) CERTIFICATION

CTPRA Certification Job Practice Guide

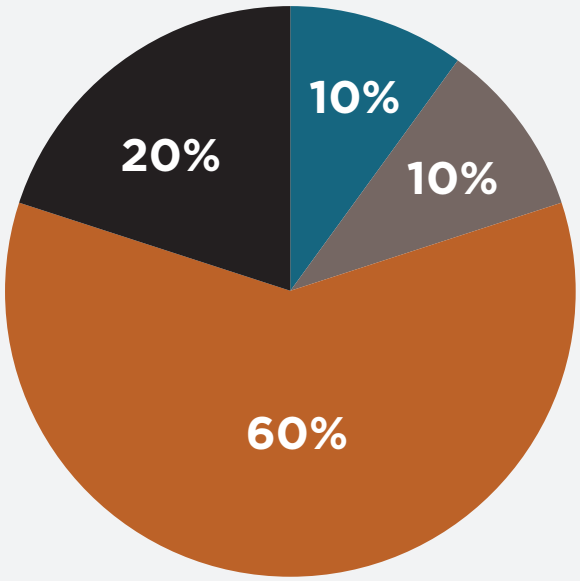
Role description

The CTPRA designation is designed to validate knowledge and experience within specific third party risk management competencies that an individual will need to be able to conduct a thorough risk evaluation of a third party during an assessment including risk analysis and reporting. The job practice guide identifies the domains, topics, skills, competencies and job role accountabilities that represent the type of work performed in the role of a third party risk assessor who plans, performs and oversees third party assessments across multiple risk domains. The structure of the job practice guide is based on the inputs of Shared Assessments Program members, recognized best practices, education and tools that drive third party risk assurance.

Certification Blueprint

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

CTPRA 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. Third Party Risk Management Program Components

II. Risk Assessment Fundamentals

A. Assessment Frameworks and Standards

B. Types of Third Party Risk Assessments

C. Risk Assessment Techniques

D. Vendor Classification and Due Diligence Requirements

E. Risk Assessor Skills and Competencies

III. Risk Control Domains

A. Governance and Risk Management

- Risk assessment and treatment
- Information security policy and 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

D. Security Incident and Threat Management

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

IV. Assessment Planning and Preparation

A. Pre-Assessment and Preparation Activities

B. Scoping

C. Information Gathering

D. Logistics Planning

V. Management Reporting and Remediation

A. Logistics Execution

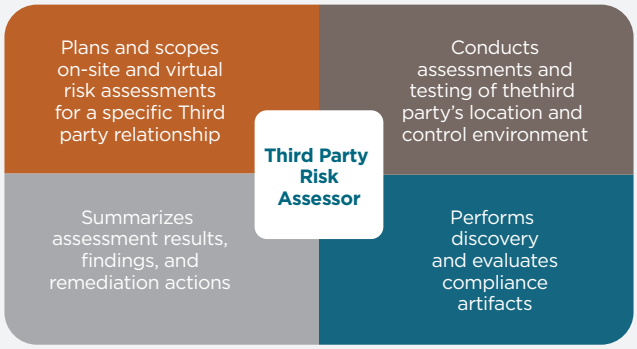
B. Conducting Discovery

C. Compliance Artifacts Review

D. Controls Testing

E. Risk Reporting and Remediation Management

Role Accountabilities



Role Accountabilities

- Actively drives coordination and execution of conducting third party risk assessment reviews either on-site or through virtual assessments.
- Participates in the creation, development and deployment of security and risk plans and mitigation controls
- Manages and deploys third party risk intake, assessment, remediation, risk acceptance and communication processes
- Conducts security, vulnerability and control assessments using standard methodologies
- Plans and coordinates testing and verification of controls
- Reviews compliance artifacts and technical materials to identify and evaluate controls
- Monitors existing and proposed security, risk and control frameworks
- Monitors changes in regulation that impact third party risk
- Builds and manages remediation plans for third party due diligence risk assessments
- Manages and maintains information in governance, risk, compliance systems and tools
- Prepares reports on risk ratings, findings and assessment results
- Identifies and evaluates compensating controls based on risk mitigation techniques
- Analyzes complex situations where an in-depth evaluation of risk is required
- Accountable to synthesize information to technical and non-technical audiences
- Ability to use judgement within established policies and procedures to evaluate control effectiveness and control attributes
- Creates management reporting on third party risk activities across multiple engagements
- Conducts audits or assessments in alignment with standards and risk based strategies
- Conducts interviews with subject matter experts to gain thorough understanding of the control environment
- Identifies synergies and dependencies in planning third party assessments
- Manages project management timelines, status reports, findings, results and recommendations to stakeholders
- Interacts directly with key personnel within both IT and lines of business to understand the roles and responsibilities