SHARED ASSESSMENTS

CTPRA

CERTIFIED THIRD-PARTY RISK ASSESSOR (CTPRA) EXAM PREP GUIDE

Table of Contents

Introduction

About the CTPRA Credential

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 and methodologies for identifying, quantifying, and mitigating third-party risk within an organization's TPRM program. The CTPRA is designed for personnel directly involved in the planning, scoping, and conducting of the evaluation of a third party's control environment in an audit or risk assessor role.

The CTPRA certification reflects the attainment of established criteria for proficiency or competency in a profession or occupation. It is granted upon an assessment of an individual's knowledge, skills, and abilities.

The CTPRA credential is issued for a specific time period and requires ongoing maintenance of TPRM knowledge through the acquisition of Continuing Professional Education (CPE) credits issued by Shared Assessments or recognized organizations for professional development content related to TPRM.

The experience and eligibility requirements to qualify for receiving the credential are outlined in the Shared Assessments CTPRA Handbook. The Handbook also provides the requirements for the Continuing Professional Education (CPE) obligations during each certification period and renewal date.

Examination and Preparation Guide Overview

The purpose of this guide is designed to assist individuals preparing for the Shared Assessments CTPRA certification exam. It is not a substitute for course materials or training and does not guarantee exam success. Candidates come from diverse backgrounds and should prepare based on their own experience, exam-taking skills, and educational and professional history.

This guide is broken into four sections:

1. CTPRA Curriculum Content Review
2. Curriculum Content Validation
3. Examination Preparation and Practice Test
4. Supplemental Study Materials

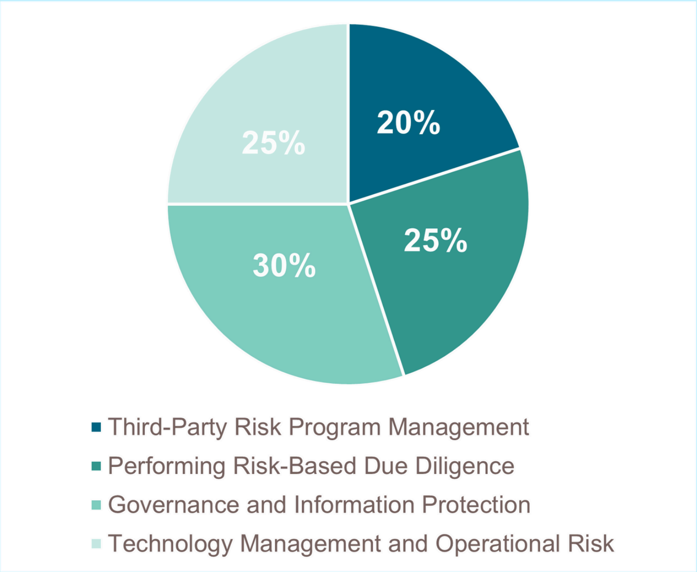
The CTPRA curriculum structure incorporates the methods of performing due diligence within specific risk domains to conduct comprehensive governance, information protection, operational risk, IT, and cyber-risk third party controls evaluation using distinct assessment techniques.

Section A: CTPRA Curriculum Content Review

Understanding the Curriculum Structure

The CTPRA curriculum is comprised of four distinct courses. Content within each course, examination questions, and practice test items are allocated based on the following course distribution:

Figure 1: Curriculum Distribution



Course 1. Third-Party Risk Program Management

Learning Objectives

The purpose of **Course I: Third-Party Risk Program Management** is to enable third-party risk practitioners to demonstrate their understanding of terminology used to define third party relationships. Risk assessors need to be able to apply the risk management principles and methodologies used in TPRM, including identifying the scoping factors that define specific types of risk posed by outsourced services.

The initial course is designed to set a foundation for TPRM disciplines used in the establishment and implementation of mature TPRM programs. The subsequent CTPRA courses focus on the specific skills, knowledge and competencies required to plan, define, and conduct comprehensive third-party risk assessments.

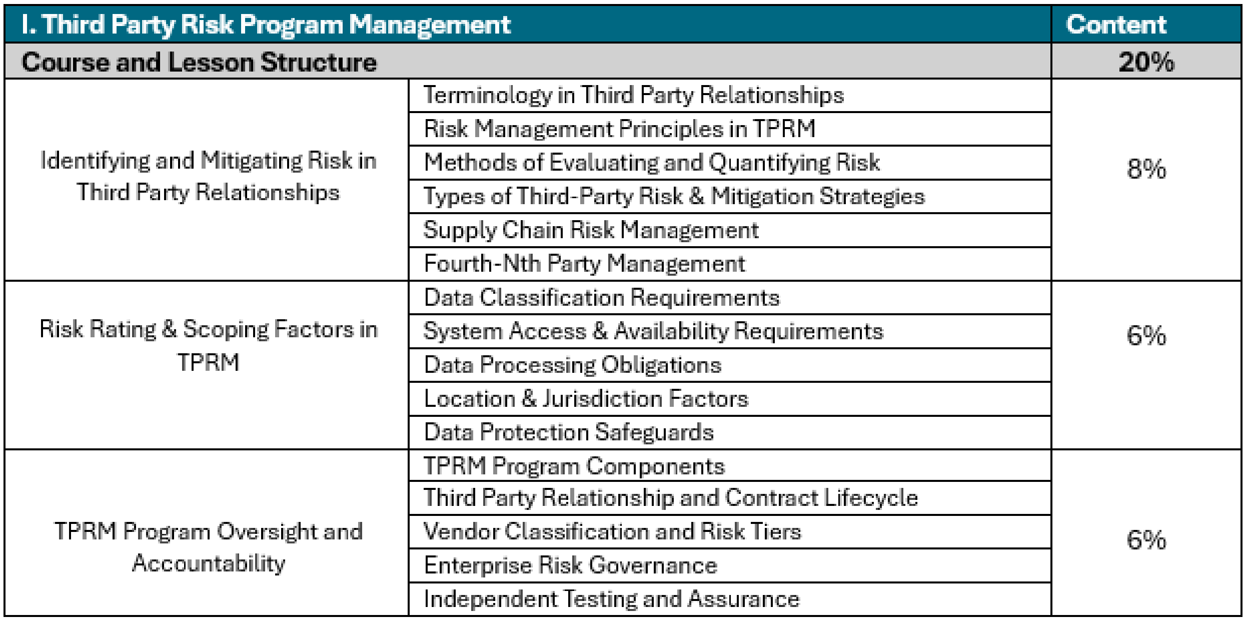
To successfully confirm a thorough understanding of Course I: Third-Party Risk Program Management, you should be able to answer practice and examination questions related to:

- Utilizing various methods of identifying, quantifying, and mitigating third-party risk based on analysis of the nature of the business relationship and type of outsourcing.

- Differentiating the factors that trigger specific risks and data processing obligations to prioritize the controls that require validation.

- Identifying the structural components used by effective TPRM programs that provide oversight and governance of third-party relationships throughout the contract lifecycle.

Content Distribution



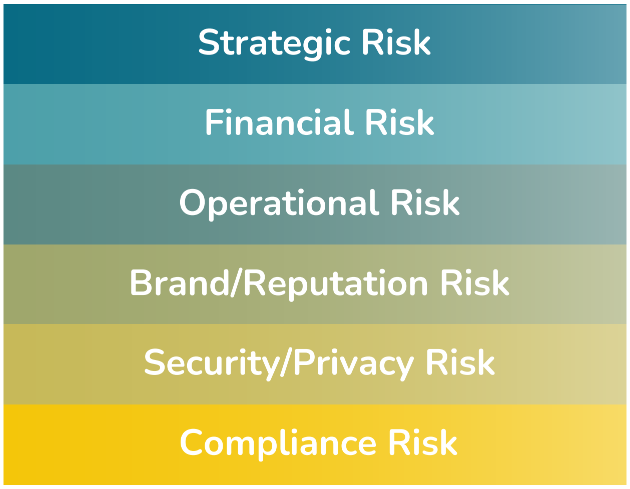
I. Third Party Risk Program Management		Content
Course and Lesson Structure		**20%**
Identifying and Mitigating Risk in Third Party Relationships	Terminology in Third Party Relationships	8%
	Risk Management Principles in TPRM	
	Methods of Evaluating and Quantifying Risk	
	Types of Third-Party Risk & Mitigation Strategies	
	Supply Chain Risk Management	
	Fourth-Nth Party Management	
Risk Rating & Scoping Factors in TPRM	Data Classification Requirements	6%
	System Access & Availability Requirements	
	Data Processing Obligations	
	Location & Jurisdiction Factors	
	Data Protection Safeguards	
TPRM Program Oversight and Accountability	TPRM Program Components	6%
	Third Party Relationship and Contract Lifecycle	
	Vendor Classification and Risk Tiers	
	Enterprise Risk Governance	
	Independent Testing and Assurance	

Content Description

Identifying and Mitigating Risk in Third-Party Relationships

Third-parties can be categorized by the nature of the products and services, and the type of contractual relationship established between parties. Determining the type of outsourcing enables the assessor to understand the scope of requirements that extend to a third party, or the third party's vendors. Risk assessors need to understand the distinction between inherent risk and residual risk to prioritize risk mitigation recommendations. In TPRM, risk can be evaluated qualitatively or quantitatively. Each relationship should be evaluated for distinct types of risk, which may be influenced by regulatory, industry, or contractual factors.

Categorizing Risk in Third Party Relationships



Strategic Risk

Financial Risk

Operational Risk

Brand/Reputation Risk

Security/Privacy Risk

Compliance Risk

Assessors need to be able to use judgment to determine the impact and likelihood of specific risks creating harm to the outsourcer. Taking actions to mitigate each identified risk is defined by risk treatment plans, which are influenced by the organization's risk culture and willingness to accept risk. By measuring risks based on inherent risk factors or service criticality, assessors can focus their control evaluation and resource allocation on the risks of higher importance. Third-party risk is evolving, especially with new focus areas in Environmental, Social, and Governance (ESG) programs. TPRM practitioners need to know what, how, and why to measure specific ESG criteria and categories that may be a part of baseline TPRM program requirements.

TPRM involves not only direct control evaluation but also a review of the extended set of relationships in the supply chain. Risk assessors need to understand how to evaluate risks posed by Fourth-Nth party relationships. Supply chain risks include exposures, threats, and vulnerabilities associated with the products and services traversing the supply chain, as well as the exposures, threats, and vulnerabilities to the supply chain. Service organizations should have a formalized TPRM program that demonstrates their commitment to managing Fourth-Nth party risks by responding to the due diligence requirements of their customers.

Risk Rating and Scoping Factors in TPRM

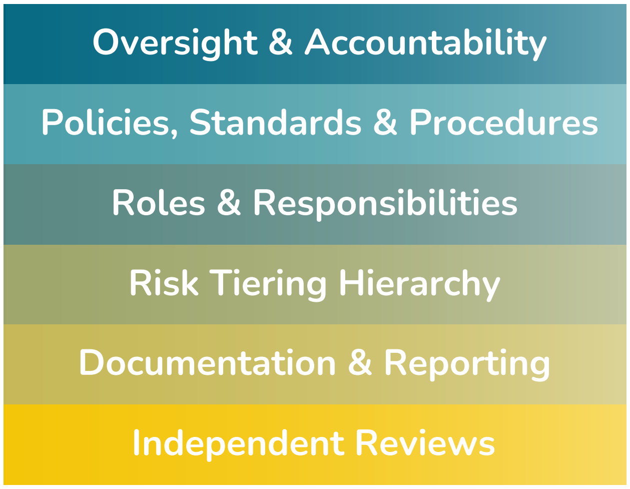
Third-party risk assessments are structured based on a third party's overall risk rating and identified scoping factors that can trigger specific types of risk. A common starting point is understanding the type of data in scope for the service or entity being evaluated. Risk assessors need to be able to classify personal data by the level of sensitivity of data elements. Understanding data flows, data maps and data inventories is critical in TPRM for assessors to understand the environment. TPRM risk assessors need to be able to differentiate classifications of personal information based on industry sector or regulatory jurisdiction that triggers specific data protection safeguarding requirements.

Data protection safeguards include techniques to encrypt, redact, and segment data in any environment. Managing data risk in third-party relationships requires data access controls, processing rules, and retention or storage requirements. The TPRM risk assessment process requires the analysis of location, industry, contract, and type of activity to determine the appropriate controls evaluation requirements. Risk assessors need to be able to interpret the risk factors for both system access and availability by evaluating the structure and deployment of the service, system, or application in scope for the risk assessment.

TPRM Program Oversight and Accountability

TPRM programs are structured with a defined governance model and set of operating policies/procedures that assessors use to guide assessment activities. Company risk culture, appetite, and risk tolerance set the tone for governance. TPRM programs establish the goals, objectives, and processes to structure, operate, and measure program effectiveness.

TPRM Program Components


Oversight & Accountability
Policies, Standards & Procedures
Roles & Responsibilities
Risk Tiering Hierarchy
Documentation & Reporting
Independent Reviews

Risk assessors must understand how program components, including vendor inventories, risk registers, risk rating factors, and inherent risk criteria, shape TPRM program assessment requirements. The vendor risk rating and classification hierarchy triggers a higher level of depth/breadth for due diligence information gathering and testing of controls. The level of testing of controls is based on the outsourcer's risk parameters and priorities/resources. The necessary level of assurance may change over time. Contracts define the relationship between the outsourcer and the third party, establishing requirements for controls evaluation. While risk assessors may not be directly involved in contract negotiation, they need to know how their organization enforces contractual obligations and can interpret when gaps or findings are deemed non-compliant with contractual commitments. Risk assessors should be prepared to assess a relationship at any phase of the contract lifecycle.

TPRM programs include oversight mechanisms for governance, risk management, and internal controls. Risk assessors must know how TPRM assessment results provide input to Board and Management reporting. Work products performed by assessors may be utilized directly by external auditors as part of independent testing or assurance that TPRM program requirements are being enforced.

Course II. Performing Risk-Based Due Diligence

Learning Objectives

The purpose of **Course II: Performing Risk-Based Due Diligence** is to enable third-party risk practitioners to confirm their understanding of the techniques and methods of conducting assessments. Risk assessors need to be knowledgeable about using risk rating and vendor classification and defined due diligence standards to scope, configure, and perform due diligence using standardized methodologies.

To successfully demonstrate an understanding of Course II content, you should be able to answer practice and examination questions related to:

- Interpreting organizational requirements and applying industry frameworks to configure assessment requirements based on risk domain.
- Planning and using multiple risk-based due diligence techniques based on the type of assessment and required level of control validation or testing.
- Analyzing, quantifying, and reporting assessment results to develop corrective action plans and ongoing monitoring that manage remediation through closure of identified risks.

Content Distribution

II. Performing Risk-Based Due Diligence		Content
Course and Lesson Structure		**25%**
Structuring Assessment Requirements	Frameworks, Standards, and Methodologies	8%
	Use of Control Mapping & Crosswalks	
	Using External Audit Reports	
	Scoping and Configuring Assessments	
Third Party Risk Assessment Processes	Assessment Roles and Responsibilities	10%
	Methods and Techniques in Assessments	
	Controls Validation and Testing	
	Categories of Risk Monitoring	
	Using Risk and Threat Intelligence Reports	
Analyzing and Reporting Assessment Results	Identifying and Classifying Findings	7%
	Mapping Results to TPRM Program Requirements	
	Documenting and Reporting Assessment Results	
	Developing Corrective Action Plans and Managing Remediation	
	Risk Reporting and Monitoring	
	Evaluation of the Assessment Process	

Content Description

Structuring Assessment Requirements

TPRM programs establish the set of frameworks, standards, and methodologies to be utilized in the assessment process for both conducting the evaluation and risk-rating the severity of gaps or findings to a set of compliance requirements. Organizations conduct internal or external control evaluations to gain assurance. Risk assessors must understand the relationships between control objectives and controls to translate and interpret assessment results. Regulations, frameworks, or policies of the organization may define control objectives.

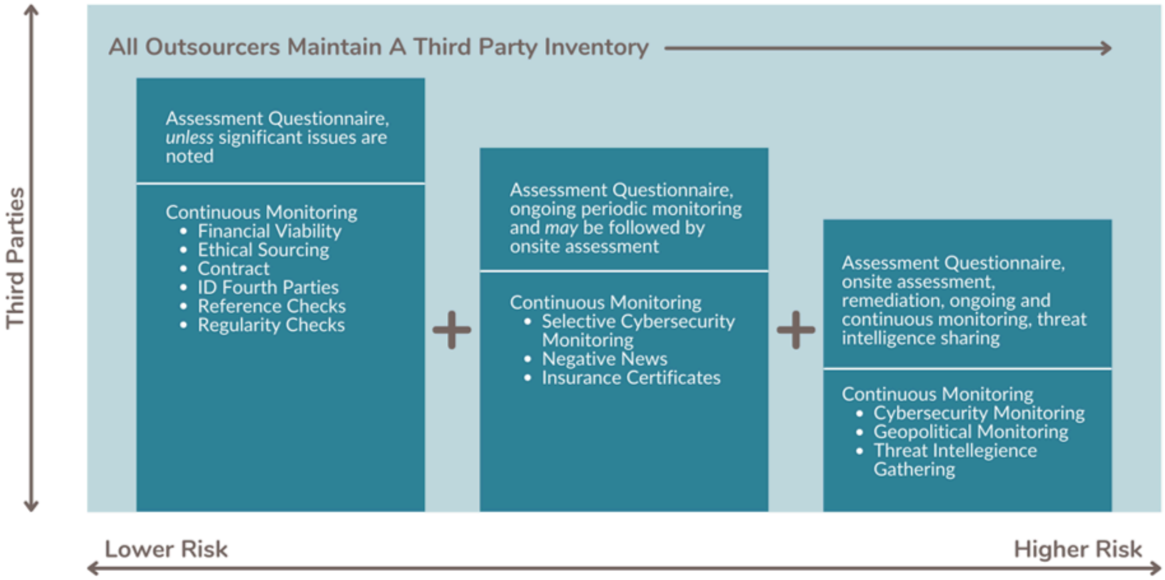
Risk assessors should be familiar with mapping controls to multiple frameworks or standards. Frameworks provide a measurable scale for control evaluation and consistency in evaluation. Control mapping enables the identification of common controls across diverse requirements. Risk assessors may perform control evaluation activities directly or utilize external audit reports as part of the validation process. Technology and audit frameworks are used in external certifications or audits to validate the design and effectiveness of the controls within a scoped technical environment. Assessors require the technological background to scope and configure assessments based on the type of technology, level of integration, complexity, and scale of systems infrastructure.

Third-Party Risk Assessment Processes

The "*Trust, but Verify*" approach addresses third-party risk throughout the relationship lifecycle. The TPRM program defines the type of survey instruments, risk and threat intelligence reports, and types of questionnaires used to gather information about the third party's environment. Based upon the "Trust" phase results, risk assessors perform additional control validation and testing. Risk assessors use analytical skills to interpret assessment results and determine how to test or validate specific controls. Risk assessors must understand how to incorporate external audit report results into their assessment process.

TPRM programs leverage multiple risk techniques to address inherent and residual risk. Risk assessors need to be able to conduct discovery sessions by interviewing subject matter experts, review and analyze compliance documentation, and interpret the results of external reports. Risk assessors must be versed in technical and soft skills to manage the assessment process. Risk assessors manage and deploy third-party risk intake, assessment, remediation, risk acceptance, and communication processes. Based on the organization's size, the risk assessor may be accountable for addressing all risk domains or performing a focused or specialized assessment for a specific risk control domain.

TPRM Program Components


All Outsourcers Maintain A Third Party Inventory
Assessment Questionnaire, *unless* significant issues are noted
Continuous Monitoring
• Financial Viability
• Ethical Sourcing
• Contract
• ID Fourth Parties
• Reference Checks
• Regularity Checks
+
Assessment Questionnaire, ongoing periodic monitoring and *may* be followed by onsite assessment
Continuous Monitoring
• Selective Cybersecurity Monitoring
• Negative News
• Insurance Certificates
+
Assessment Questionnaire, onsite assessment, remediation, ongoing and continuous monitoring, threat intelligence sharing
Continuous Monitoring
• Cybersecurity Monitoring
• Geopolitical Monitoring
• Threat Intellegience Gathering
Third Parties
Lower Risk
Higher Risk

TPRM assessments may utilize various monitoring tools. The cadence or frequency of monitoring functions increases from periodic to real-time based on the level of risk. An organization may adjust or amend its defined risk tiers based on changes in scope, risk, or updated due diligence standards.

Analyzing and Reporting Assessment Results

Assessment results are categorized and organized using defined templates established in the TPRM program. Findings are identified, and risk is rated for severity. The risk assessor is accountable for interpreting the risk impact of the finding and mapping the results back to the TPRM program policies, standards, and procedures. A key element of the assessor's role is communicating the technical assessment results verbally or by providing written reports to the TPRM program leadership and business representatives.

Assessment results are maintained for audit purposes and reported to management. Risk assessors participate in creating, developing, and deploying security and risk plans and mitigation controls. The risk assessor may be involved in developing the technical recommendations to include in corrective action plans or explaining the remediation tasks to the third party. The risk assessor may also be called upon to review updates to corrective action plans to provide insight into whether the findings can be closed and mitigate the risks. TPRM assessors need to stay current on changes in the risk landscape and assurance expectations to adapt their approach to performing due diligence.

It is also essential for risk assessors to understand their role in the TPRM organization and how to engage organization control owners or subject matter experts where specific knowledge or experience is required. The risk assessor may not be the expert in all areas potentially requiring control evaluation but has the skills and abilities to utilize the organization’s assessment criteria and instrument to collect and validate control attributes. The risk assessor synthesizes the information and returns it to the TPRM process.

Course III. Controls Evaluation: Governance and Information Protection

Learning Objectives

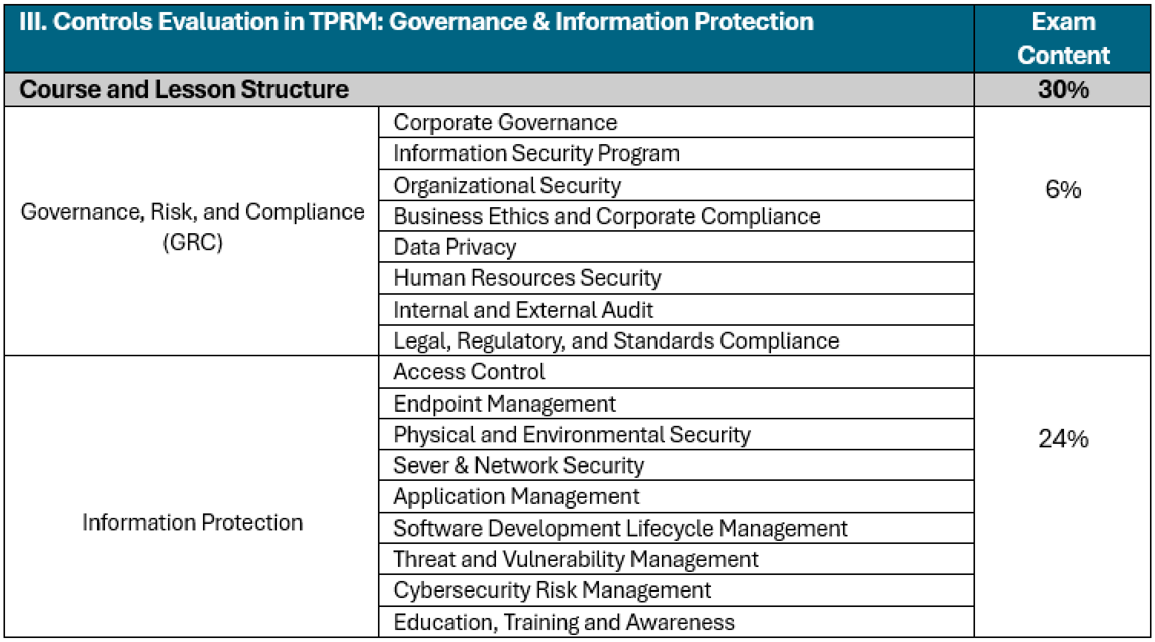
The purpose of **Course III: Controls Evaluation: Governance & Information Protection** aims to summarize governance, risk, information security, and compliance expectations for third-party risk assessments based on service risk ratings. TPRM programs and risk assessors determine which risk control domains to include based on assessment scope. Assessors must possess broad knowledge across risk domains while maintaining in-depth expertise in critical control areas.

To successfully demonstrate an understanding of Course III content, you should be able to answer practice and examination questions related to:

- Evaluating the organizational structure and established governance and compliance functions that provide risk assurance based upon regulatory or contractual obligations.
- Analyzing the third party's administrative, technological, physical, and environmental controls to identify and quantify potential risks to the security, confidentiality, or integrity of data processing.
- Assessing a third-party's threat, vulnerability, and cybersecurity risk management programs to determine the level of risk posed by the systems, applications, and platforms used in the outsourced services.

The curriculum in this course requires risk assessors to gain an understanding of the overall governance, policy, and enforcement framework in place, not just the technological aspects of controls. Gaps identified in information protection, resilience, or operational risk are funneled into Enterprise Risk Management or Compliance functions.

Content Distribution



III. Controls Evaluation in TPRM: Governance & Information Protection		Exam Content
Course and Lesson Structure		**30%**
Governance, Risk, and Compliance (GRC)	Corporate Governance	6%
	Information Security Program	
	Organizational Security	
	Business Ethics and Corporate Compliance	
	Data Privacy	
	Human Resources Security	
	Internal and External Audit	
	Legal, Regulatory, and Standards Compliance	
Information Protection	Access Control	24%
	Endpoint Management	
	Physical and Environmental Security	
	Sever & Network Security	
	Application Management	
	Software Development Lifecycle Management	
	Threat and Vulnerability Management	
	Cybersecurity Risk Management	
	Education, Training and Awareness	

Content Distribution

Governance, Risk, and Compliance (GRC)

The objective of the GRC domain is to evaluate the service organization’s corporate governance and compliance functions to ensure adequate controls are in place that address both risk assurance and legal, regulatory, and standards compliance. Risk assessors need to understand the decision-making framework the third party uses to identify and respond to risks. The absence of an enterprise risk management and risk governance program may result in the service organization’s inability to recognize, classify, and react to internal or external risks. Organizational reporting structures convey the governance model for privacy, security, audit & compliance functions. Information security policies define the set of requirements for data security. Data protection policies outline the measures an organization takes to process and handle personal data.

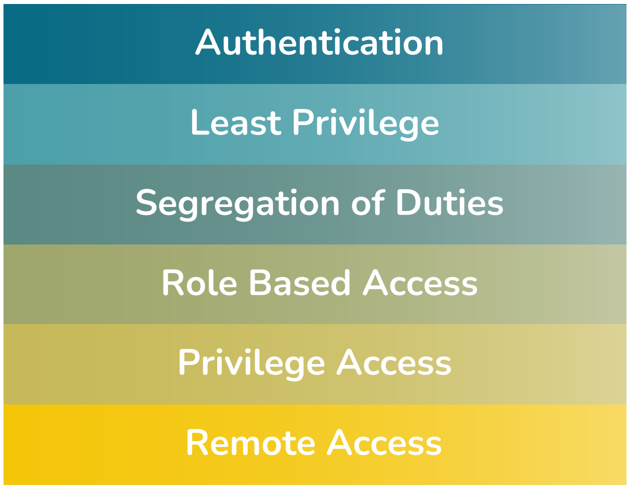
The GRC risk assessment should evaluate governance and oversight structures to confirm the identification of compliance requirements and implementation of compliance management programs that include reporting and escalation to management or boards of directors. The level and type of compliance programs differ between public and private companies based on shareholder expectations. Enterprise Compliance and Ethics Programs are typically based on a defined set of values, core operating models, or principles. Risk assessors review these commitments to align with the company's risk culture but may require a more detailed inspection due to legal, regulatory, and contractual obligations.

Risk assessors need to understand the scope and maturity of the third party’s approach to information assurance and their Information Security Program. The Information Security Program sets the security tone for the whole company and is reviewed at planned intervals to ensure continued suitability, adequacy, and effectiveness. The security policy should incorporate the key security areas (confidentiality, integrity, and availability). The absence of an information security policy may lead to unknowingly accepting inherent Information Security (IS) risks. Human Resource Security discipline is designed to examine key controls applied before, during, and after hiring human resources. Human Resources are critical in addressing personnel risk and enforcing organizational policies. GRC evaluations typically include reviewing independent testing of controls performed by external auditors or achieving external assurance via certifications. Risk assessors need to understand the types of external assurance mechanisms relevant to the outsourced services.

Information Protection

Organizations should develop, implement, and maintain an information assurance program that provides oversight and defines processes for managing all security risks related to confidential information throughout its transmission, storage, and processing. Information protection policies should be established using an accepted framework with clearly defined organizational responsibilities. Information protection starts with effective access control to the environment from any endpoint to ensure control over access to data, information processing systems, and facilities.

Access Control Across Endpoints



Authentication

Least Privilege

Segregation of Duties

Role Based Access

Privilege Access

Remote Access

Information protection includes evaluating a third party's physical and environmental security controls, secure workplace standards, and testing or compliance inspections based on organizational requirements.

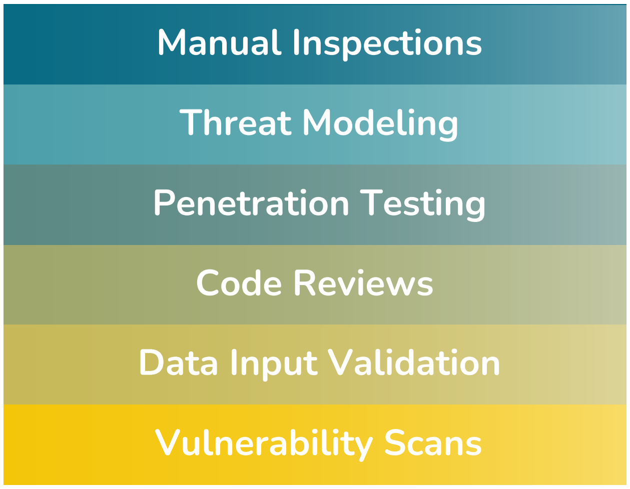
Risk assessors need the skills and knowledge to conduct evaluations across disparate types of technology. Technology and system controls are evaluated from server, network, application, and cloud hosting perspectives. The evaluation of server and network security controls includes all equipment and/or software used to move data inside and outside the corporate environment. The security measures at the application level aim to prevent data or code within the software from being susceptible to theft or hijacking by non-authorized or external personnel. Information Security programs should have sufficient authority to approve changes to the technical environment, including formal approvals embedded in the software development lifecycle.

Risk assessors need to be able to inspect the controls established in the third party's formalized Information Security/Information Technology incident management program. The process of incident identification involves identifying and analyzing indicators of potential compromise. Security and privacy incidents follow an incident lifecycle from detection, containment, response, and notification. Incident Response Management requires well-defined and regularly tested escalation, reporting, notification, and resolution procedures. Risk assessors review the criteria and triggers to report and escalate incidents that may require notification to users, vendors, employees, clients, or customers.

Changes in technology, nation-state attacks, cybercriminal activity, and ransomware have accelerated the threat landscape. Third parties should ensure that security threats are managed using both automated and manual scanning tools. Threat management is about defending the organization, while vulnerability management focuses on defects or vulnerabilities that could be exploited.

A vulnerability assessment is a structured examination of systems and applications to identify, quantify, and prioritize the security deficiencies in the systems. Risk assessments require the ability to discern the various methodologies used in threat and vulnerability management and apply that knowledge to the potential impact on the outsourcer's systems or technical environment.

Threat and Vulnerability Management Techniques



- Manual Inspections
- Threat Modeling
- Penetration Testing
- Code Reviews
- Data Input Validation
- Vulnerability Scans

Regular updates and refreshers are essential to ensure that all personnel remain aware of current threats and best practices. Furthermore, it's important for organizations to foster a culture of security where employees feel empowered and responsible for safeguarding information. This can be achieved through interactive workshops, engaging e-learning modules, and real-world simulations that challenge employees to think critically about security issues.

Additionally, organizations should encourage open communication about potential security concerns, allowing employees to report suspicious activities without fear of reprisal. By continually adapting training materials to address emerging threats and incorporating lessons learned from past incidents, companies can create a robust defense against data breaches and unauthorized access.

Ultimately, the goal is to create an environment where information protection is seen as a shared responsibility, and every team member, from entry-level staff to senior management, understands the critical role they play in maintaining the integrity and confidentiality of sensitive data.

Course IV. Controls Evaluation: Technology Management and Operational Risk

Learning Objectives

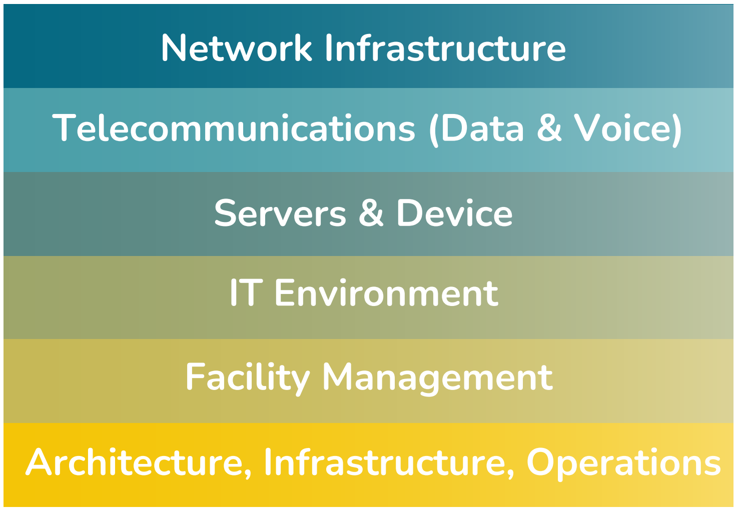
The purpose of **Course IV: Controls Evaluation: Technology Management and Operational Risk** is to enable TPRM practitioners to assess a third party's IT operations functions and resilience strategies to validate the effective management, operation, integrity, and recovery of systems.

To successfully demonstrate an understanding of Course IV content, you should be able to answer practice and examination questions related to:

- Analyzing a third-party's approach to IT governance and technology acquisition to identify potential risks in managing the technology used in the outsourced services.
- Categorizing the use of cloud services to validate accountabilities between parties for managing controls based on the service and deployment model.
- Assessing the risks posed by the use of evolving technologies in the delivery of outsourced activities by evaluating the governance structures maintained by the third party.
- Evaluating a third party's IT operations, service levels, and resilience strategies that maintain and manage the recovery of systems to minimize business disruption in response to internal or external events.

The structure of Course IV is based on the risk assessor's understanding of the third party's environment from an architecture, infrastructure, and IT operations perspective.

Assessing the Technical Environment



Network Infrastructure

Telecommunications (Data & Voice)

Servers & Device

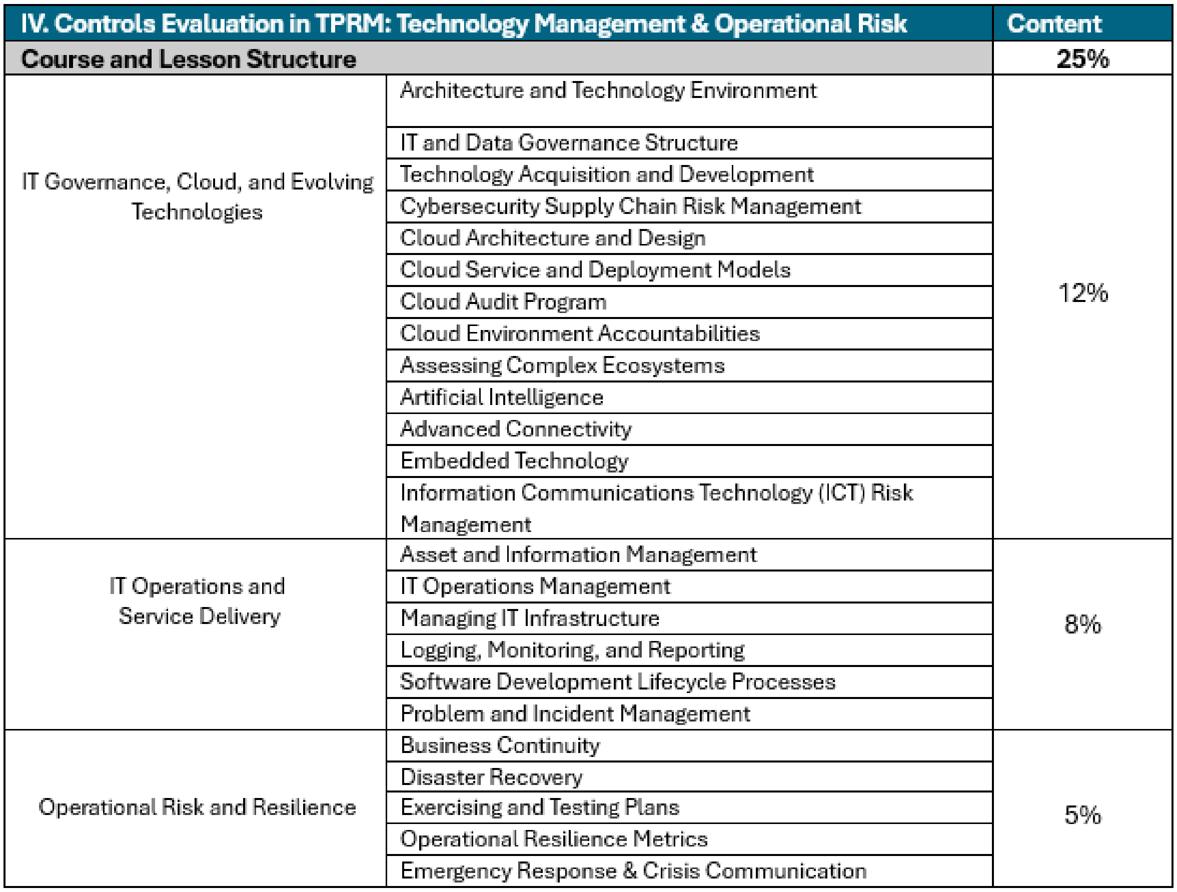
IT Environment

Facility Management

Architecture, Infrastructure, Operations

Risk assessors need the technical acumen to be able to make judgements on controls across complex ecosystems. Control evaluation is not simply a binary viewpoint but nuanced by applying a risk-based approach to due diligence.

Content Distribution



IV. Controls Evaluation in TPRM: Technology Management & Operational Risk		Content
Course and Lesson Structure		**25%**
IT Governance, Cloud, and Evolving Technologies	Architecture and Technology Environment	12%
	IT and Data Governance Structure	
	Technology Acquisition and Development	
	Cybersecurity Supply Chain Risk Management	
	Cloud Architecture and Design	
	Cloud Service and Deployment Models	
	Cloud Audit Program	
	Cloud Environment Accountabilities	
	Assessing Complex Ecosystems	
	Artificial Intelligence	
	Advanced Connectivity	
	Embedded Technology	
	Information Communications Technology (ICT) Risk Management	
IT Operations and Service Delivery	Asset and Information Management	8%
	IT Operations Management	
	Managing IT Infrastructure	
	Logging, Monitoring, and Reporting	
	Software Development Lifecycle Processes	
	Problem and Incident Management	
Operational Risk and Resilience	Business Continuity	5%
	Disaster Recovery	
	Exercising and Testing Plans	
	Operational Resilience Metrics	
	Emergency Response & Crisis Communication	

Content Description

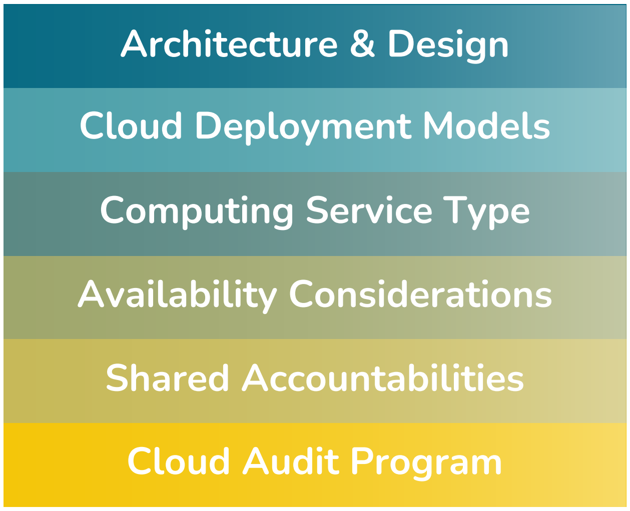
IT Governance, Cloud, and Evolving Technologies

Information Technology functions may be centralized or decentralized based on the company culture. IT governance standards should be established based on information security policy and risk management program requirements. Technology management-focused assessments are initiated by the risk assessor, who gathers information to understand the enterprise architecture, which describes the third party's complete set of information systems. Risk assessors identify how systems are configured, how they interface with the external environment, and the governance mechanisms in place to maintain an overall security posture. The purpose of reviewing a third party's approach to IT governance, architecture, and technology acquisition is to identify potential risks of using specific technologies in the outsourced services.

Assessing the technology environment requires understanding the use of Operational Technology (OT) and Information and Communications Technology (ICT). Risk assessors must be prepared to assess technology acquisition and development from a governance and a cybersecurity supply chain risk perspective. The level of risk posed by the supply chain is based on the type of supply chain and the corresponding potential impact of harm due to internal/external risk factors. Technology-focused risk assessments address the measures to manage exposure to cybersecurity risks throughout the supply chain and develop appropriate response strategies, policies, processes, and procedures.

Assessors need to be well versed in cloud security, which comprises a set of practices that reduce the impact or likelihood of exploitation of flaws in services and protocols relating to the delivery of cloud-based services. Assessors identify and evaluate the use of cloud services, including control evaluation of shared responsibilities between parties based on the service and deployment model.

Assessing the Third Party's Cloud Environment



Architecture & Design

Cloud Deployment Models

Computing Service Type

Availability Considerations

Shared Accountabilities

Cloud Audit Program

Cloud assessments require the assessor to understand the terminology used in cloud hosting, including, but not limited to, containerization, multi-tenancy, hypervisors, microservices, and cloud bursting. Cloud hosting accountabilities are defined by service model and by contract terms. Assessments involving cloud services and evolving technology require risk assessors to stay current on updated industry practices. Assessors need to identify and understand the type of cloud data center and its tier to confirm an understanding of control ownership and the level of redundancy in the related services. Industry requirements assign ratings to the data center based on criteria for power, cooling, maintenance protocols, redundancy, and fault tolerance. These ratings are capabilities-based and agnostic to the specific technologies and vendors providing the facilities.

Today's technical environment often integrates the use of evolving or embedded technology to deliver services. Threats from embedded systems can originate from the use of open web interfaces, hostile users, failures in storage and maintenance, and risk of adjacent vulnerable systems and supply chains. Assessors should be able to identify the risks of connected devices and the use of the Internet of Things (IoT), which is the network of physical objects or "things" embedded with electronics, software, sensors, and network connectivity, which enable the collection, monitoring, or exchange of data. A rapidly evolving area of TPRM is the assessment of how a third party may use AI to support or enable the delivery of services. The potential harms of AI can be viewed as harm to people, organizations, or an ecosystem.

Understanding AI in TPRM

Artificial Intelligence

Machine Learning

Deep Learning

Generative AI

Risks associated with the ungoverned use of AI can include bias, accuracy, transparency, intellectual property, privacy, and supply chain management. AI assessments focus on the governance and deployment of the technology and the models that systems use to perform functions typically associated with human intelligence, reasoning, and learning.

Network connectivity methods include traditional telecom services that focus on voice, data, internet, and cloud. To properly scope the technology aspects of the risk assessment, assessors need to understand how both the connectivity method and the volume of connections are rapidly expanding. Changes in technical standards for wireless, 6G, Edge computing, and Quantum computing will require updates to assessment requirements.

IT Operations and Service Delivery

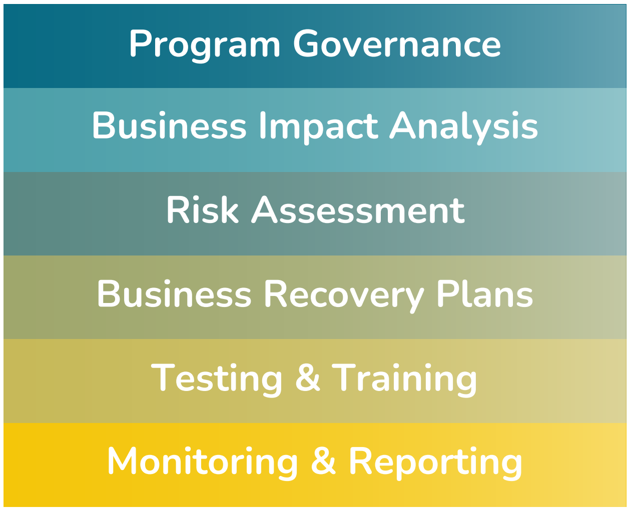
IT Operational risk is the failure or loss resulting from inadequate or failed people, processes, or technology. Using disparate systems and technology makes security controls more challenging to implement and maintain. The purpose of assessing IT operations is to evaluate the capability of the third party to adequately manage technology and the operating environment in a controlled approach to enable day-to-day operations and infrastructure maintenance. IT Asset Management programs establish the requirements, protocols, and algorithms used to protect physical and information assets. Asset management includes managing the inventory of assets and deploying controls for data at rest, in motion, and at disposal. IT Asset Management processes should address tracking, managing, and reporting on information and technology assets.

IT operations involve the ongoing maintenance, monitoring, and support of business systems, products, and services. Risk assessors must identify controls and understand the consequences of gaps in critical processes such as change management, patch management, key management, and the overall software development lifecycle (SDLC). Operations play a crucial role in risk management through system hardening and configuration management. Change management encompasses planning, oversight, project management, testing, and implementation. Risk assessors should be prepared to evaluate evidence of the notification, identification, deployment, installation, and verification of software code changes for operating systems and applications. Assessments may also involve reviewing the management of cryptographic keys and relevant security parameters throughout the key lifecycle, from generation and storage to usage, output, and destruction. Assessors should recognize the importance of maturity in operational processes, focusing on logging, monitoring, capacity management, database management, backup, and application performance monitoring. Failures in these operational processes can hinder performance and lead to disruptions that require resilience planning.

Operational Risk and Resilience

Operational resilience is based on defining and deploying Disaster Recovery and Business Continuity plans to minimize disruption. Risk assessors need to review the third party's resilience strategy to determine the ability of the approach to meet the stated goals for recovery of operations. Pros and cons of alternative methods should be evaluated for their impact on the recovery of the systems that are in scope for the outsourced services. Strategies should address technology, personnel, data business processes, and specific facility requirements. Resilience-focused assessments require evaluation of evidence that addresses redundancy requirements, workforce displacement or reduction, and unavailability of workspace or technology resources.

Business Continuity Program Components



Program Governance

Business Impact Analysis

Risk Assessment

Business Recovery Plans

Testing & Training

Monitoring & Reporting

Business continuity recognizes the requirement to recover and resume technology operations and critical business processes by end-users performing their respective job roles. Continuity and resilience allow an organization to continue to serve its customers within acceptable impact tolerances regardless of the business disruption. Risk assessors need to be able to differentiate the metrics used in measuring resilience, including the Recovery Point Objective (RPO) and Recovery Time Objective (RTO). RPO refers to the specified period of time in the past to which the business will recover its data from a failure or disaster incident. RTO refers to a time in the future when the business will be up and running again to resume normal operations.

Risk assessors need to evaluate the third party's risk assessment process to validate they have adequately addressed potential internal and external events that could impact the delivery of services. The Business Impact Analysis (BIA) identifies the critical processes and systems prioritizing recovery efforts to minimize business disruption based on risk impact and likelihood. The BIA provides input to setting recovery requirements and metrics such as RPO, RTO and Redundancy. The redundancy of each component in a system is labeled as the variable "n," "+1" refers to the backup for a given variable "n." As a technique, n+1 provides redundancy through the availability of a backup for databases, systems, infrastructure, or facilities.

Disaster recovery plans should include an enterprise-wide, process-oriented approach that considers technology, business operations, testing, and communication strategies. Risk assessors need to be able to review evidence that demonstrates the periodic testing of restoration of backup data to ensure availability within agreed-upon timescales. Disaster recovery and emergency response plans should enable the organization to address catastrophic events, such as natural disasters, fire, acts of terror, active shooter, pandemics, or cybercrime events. Based on the scale of the event, the organization may trigger crisis communication plans. Risk assessors need to be able to evaluate an organization's distinct response programs to validate the level of notification and readiness of the outsourced services or alternative providers. Effective crisis management combines incident response from multiple processes, including emergency preparedness, disaster recovery, breach response, and privacy notification procedures.

Section B: Curriculum Content Validation

TPRM Skills and Competencies

TPRM job roles, functions, and career paths are based on a set of common competencies based on job role and experience level.

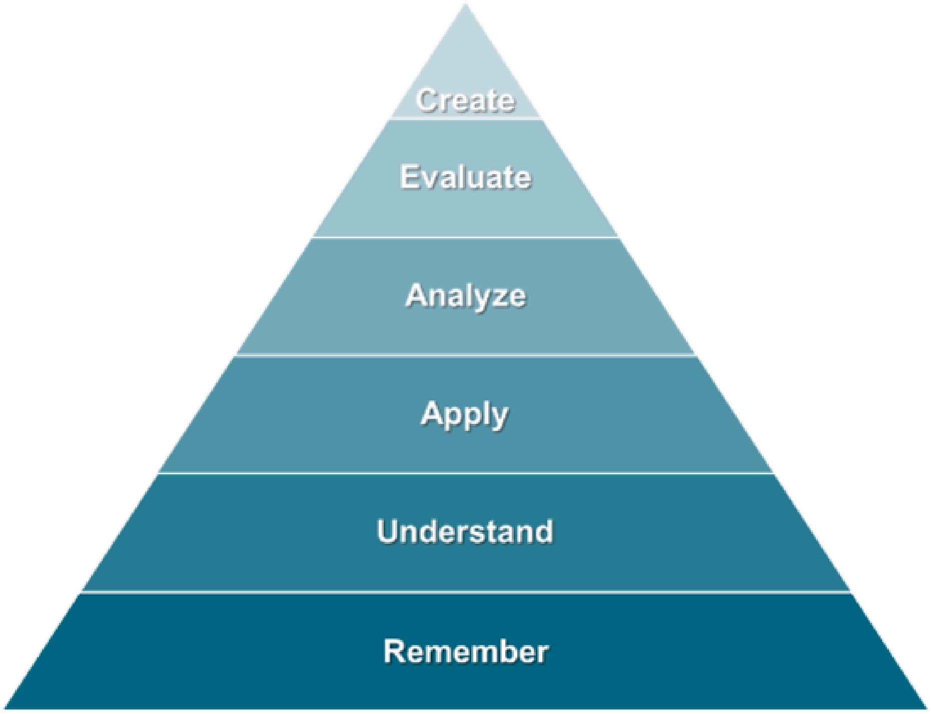
- **JUDGEMENT**: TPRM disciplines require strong analytical and systems thinking to enable risk-based decision-making
- **TECHNICAL APTITUDE**: TPRM involves the analysis of controls across diverse risk domains using broad knowledge of the control environment.
- **COMMUNICATION**: TPRM professionals use effective verbal and written communication skills to gather information, summarize findings, and prepare reports on complex concepts.
- **TIME MANAGEMENT**: TPRM requires strong project management skills to manage tasks and deliverables across concurrent assessment activities.
- **ATTENTION TO DETAIL**: TPRM focuses on accuracy, transparency, and integrity in identifying and managing risk mitigation activities.
- **COLLABORATION**: TPRM is based on a business relationship. Assessments are designed to focus on identifying and mitigating risk with mutually agreed upon solutions.

Skills and competencies may be transferable, knowledge-based, or personal attributes. Skills may be learned and transferred to different career fields and job roles. Knowledge-based skills are developed through education, training, and firsthand experience. Knowledge-based competencies require continuing professional education to maintain current knowledge in a changing landscape.

Knowledge Levels

Course content is constructed and evaluated using Bloom's Taxonomy hierarchy to align the knowledge level and type of knowledge expected from candidates who prepare to take the certification examination. Examination and practice test questions used for content reinforcement are assigned a knowledge level within each item's hierarchy and type of knowledge.

Figure 2: Bloom's Taxonomy Knowledge Level Hierarchy



Type of Knowledge

CTPRA curriculum content is categorized by the type of knowledge the candidate may have for each lesson and topic area. The Types of Knowledge used for content validation in the curriculum include Facts, Concepts, Principles, and Procedures. The following table outlines the differences in the level of knowledge and judgment needed for content reinforcement and validation of comprehension of the identified content topic.

Table 1: Categorizing the Type of Knowledge

Content Categories	Description
Fact	A fact is known by truth or experience. There is consensus about a fact. A test-taker either knows or does not know the fact, it is not open to interpretation or judgment.
Concept	An item with a set of shared characteristics. Concepts may be abstract or concrete. Concepts may require the recall of definitions or the use of examples.
Principle	Principles involve a statement of a relationship, usually between two or more concepts. Principles apply information in situations or scenarios but require increased judgement in applying and analyzing the concept.
Procedure	Procedures involve the understanding or comprehension of the appropriate series of related actions based upon an objective or desired results.

**Source: Thomas M. Haladyna, Developing and Validating Multiple-Choice Test Items, Third Edition, 2015*

Examination Blueprint

Certification content is broken into courses and lessons based on the curriculum structure. Each examination question is assigned to a course, lesson, and learning content topic. Based on the question's difficulty level, the item is assigned both an Item Knowledge Level and the Type of Knowledge. The overall knowledge level requirements distribution is part of the examination and content blueprint.

Chart 1: CTPRA Item Knowledge Level Breakdown

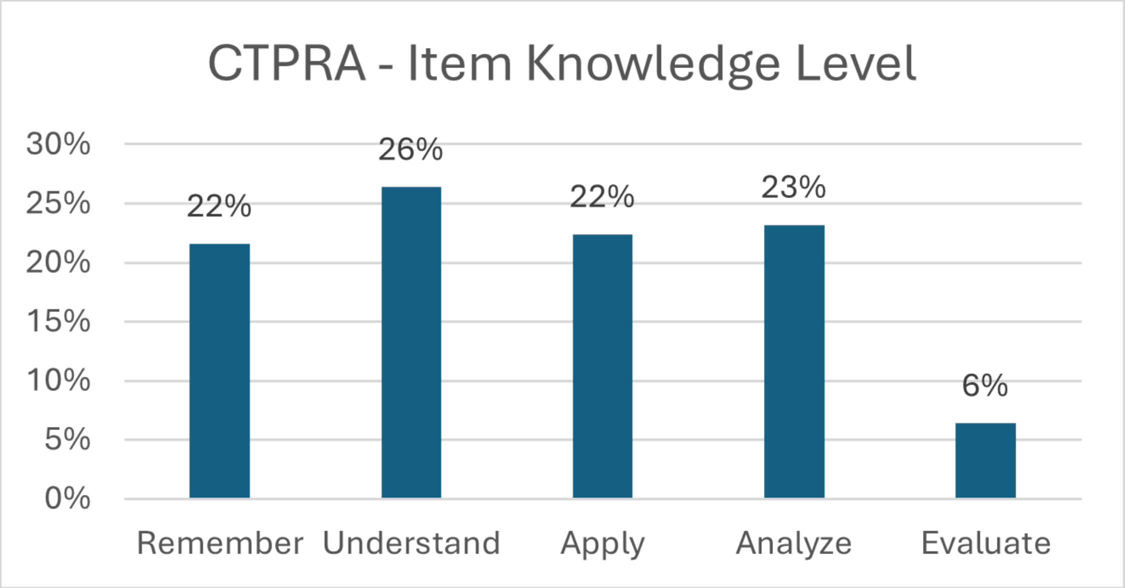
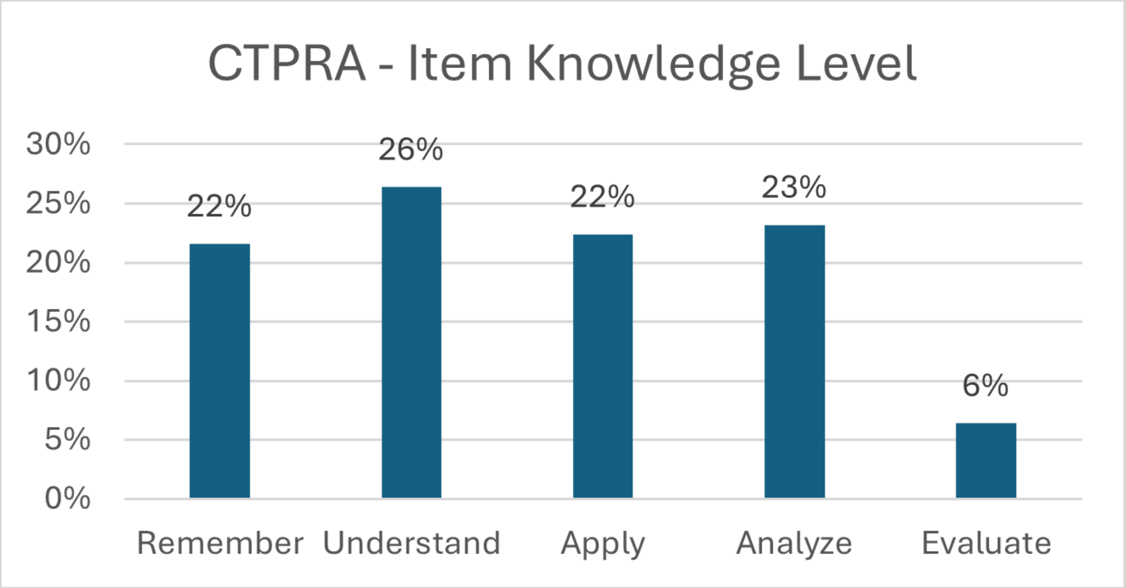


Chart 2: CTPRA Type of Knowledge Breakdown



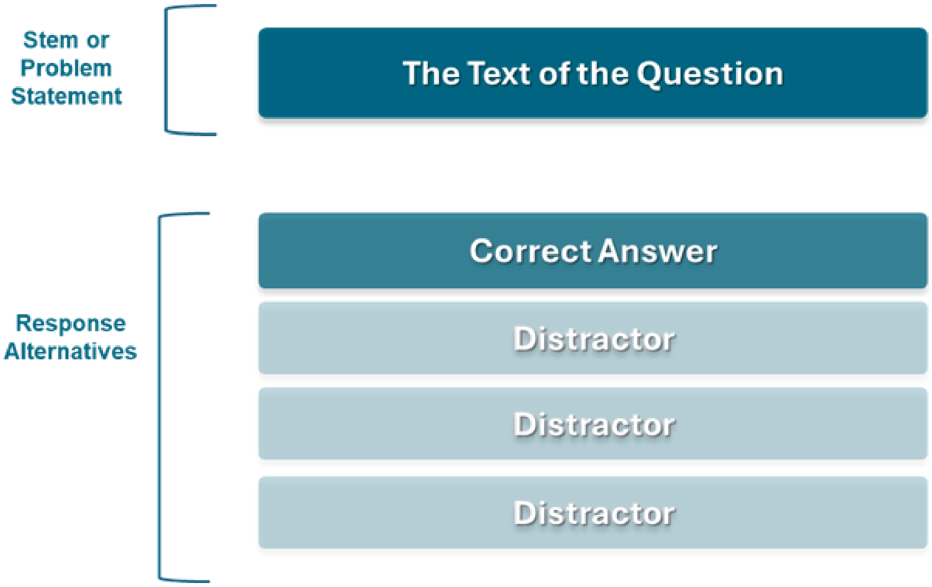
Section C: Practice Test and Examination Preparation

Question and Response Formats

In a certification program, testing assesses knowledge and validates competency in prior knowledge, experience, and abilities. Certification holders demonstrate a mastery of knowledge and application of that knowledge in a specific topic.

The examination utilizes multiple-choice question formats that follow a standard educational hierarchy. It assesses a test taker's knowledge of a specific topic but will require judgment and experience to differentiate between the proposed solutions. Examination questions in a credentialing program follow a standard question hierarchy, which includes concepts of STEM, the Key, Alternatives, and Distractors.

Figure 3: Structure of an Exam Question



Shared Assessments maintains documented item rationales for both correct and incorrect answer responses. Rationales are reviewed as part of the item update process to provide a quality assurance technique to ensure that questions submitted are clear, and the correct answer has reasonable justification for why the correct answer is the best choice.

Question formats may include statements to identify a True or False statement, or the best definition of a TPRM term or concept. Questions may also present a role or introduction that is important to understanding the context of the question. In this scenario, a brief 2-3 sentence scenario or visual is presented, followed by a single multiple-choice question to confirm understanding of functionality or technical information provided directly in the training course.

Preparation Tips

Learning objectives presented in the course are a starting point for understanding the framework of each lesson area in the curriculum. Test takers should prepare by reviewing the course slides and supplemental reading materials, with additional study for topics least familiar based on knowledge or experience.

It is recommended that students spend an average of 30 hours of study or preparation. Completing the training course alone does not guarantee a passing score.

The following "**Do's and Don'ts**" help analyze and improve your ability to respond to the questions accurately:

Review the curriculum outline and question distribution to prioritize your study and preparation efforts to those topics that require more content reinforcement or new learning.

- Use the self-assessment checklist to help you prioritize
- Develop a study timeline for the identified topic area

Read the questions carefully.

- Read the scenario or roles presented
- All questions will have only one correct response based on the rationale
- You can skip questions and return to change your responses. However, testing trends suggest that first instincts are often more aligned with correct answers.

Review the available responses.

- Pick the BEST response from the choices provided
- Don't think about exceptions or options that are not listed in the multiple-choice selection
- Don't overthink the questions; they are not designed to be trick questions!
- Don't rush and pick a response that has "words" in it that relate to the topic identified in the question.

Review the Grammar and tone of voice of the question.

- Certain questions may be worded to identify an outlier, an exception, which evaluates the ability of the learner to discern between different terms.
- Look for words or phrases like ALL OF THE FOLLOWING, NOT, EXCEPT that convey identification of the existing gaps in the relationship between the responses.
- Look for qualifying words like LEAST, STRONGEST, or MOST to identify the response with the more significant potential to address the risk management question.

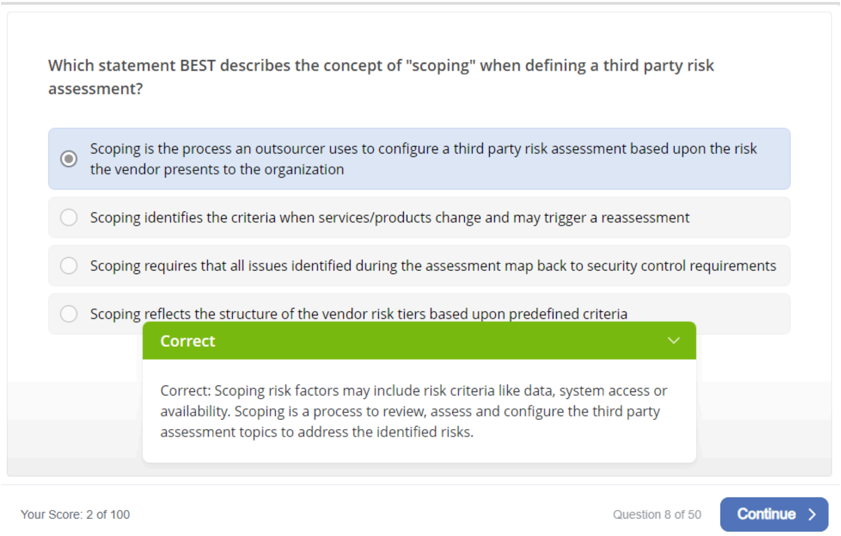
Using the Practice Exam

The practice exam includes 50 multiple-choice questions designed to reflect the types of questions you may encounter during the actual exam. It is part of the online CTPRA study guide. The questions are distributed according to the CTPRA exam profile as follows:

- Third-Party Program: 20%
- Performing Risk-Based Due Diligence: 25%
- Controls Evaluation in TPRM: Governance and Information Protection: 25%
- Controls Evaluation in TPRM: Technology Management and Operational Risk: 30%

In the practice exam, you will have one (1) opportunity to answer each question. After receiving your score, you can review the questions, answers, and explanations. You can retake the practice exam as many times as you desire.

Both correct and incorrect answers will provide a rationale for your selected option to assist in your understanding.



Which statement BEST describes the concept of "scoping" when defining a third party risk assessment?

● Scoping is the process an outsourcer uses to configure a third party risk assessment based upon the risk the vendor presents to the organization

○ Scoping identifies the criteria when services/products change and may trigger a reassessment

○ Scoping requires that all issues identified during the assessment map back to security control requirements

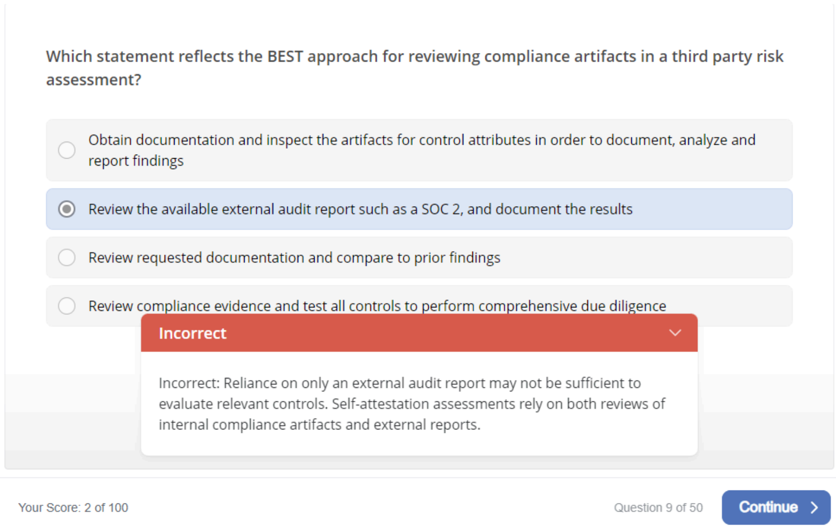
○ Scoping reflects the structure of the vendor risk tiers based upon predefined criteria

Correct

Correct: Scoping risk factors may include risk criteria like data, system access or availability. Scoping is a process to review, assess and configure the third party assessment topics to address the identified risks.

Your Score: 2 of 100

Question 8 of 50



Which statement reflects the BEST approach for reviewing compliance artifacts in a third party risk assessment?

○ Obtain documentation and inspect the artifacts for control attributes in order to document, analyze and report findings

● Review the available external audit report such as a SOC 2, and document the results

○ Review requested documentation and compare to prior findings

○ Review compliance evidence and test all controls to perform comprehensive due diligence

Incorrect

Incorrect: Reliance on only an external audit report may not be sufficient to evaluate relevant controls. Self-attestation assessments rely on both reviews of internal compliance artifacts and external reports.

Your Score: 2 of 100

Question 9 of 50

Examination Logistics

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.

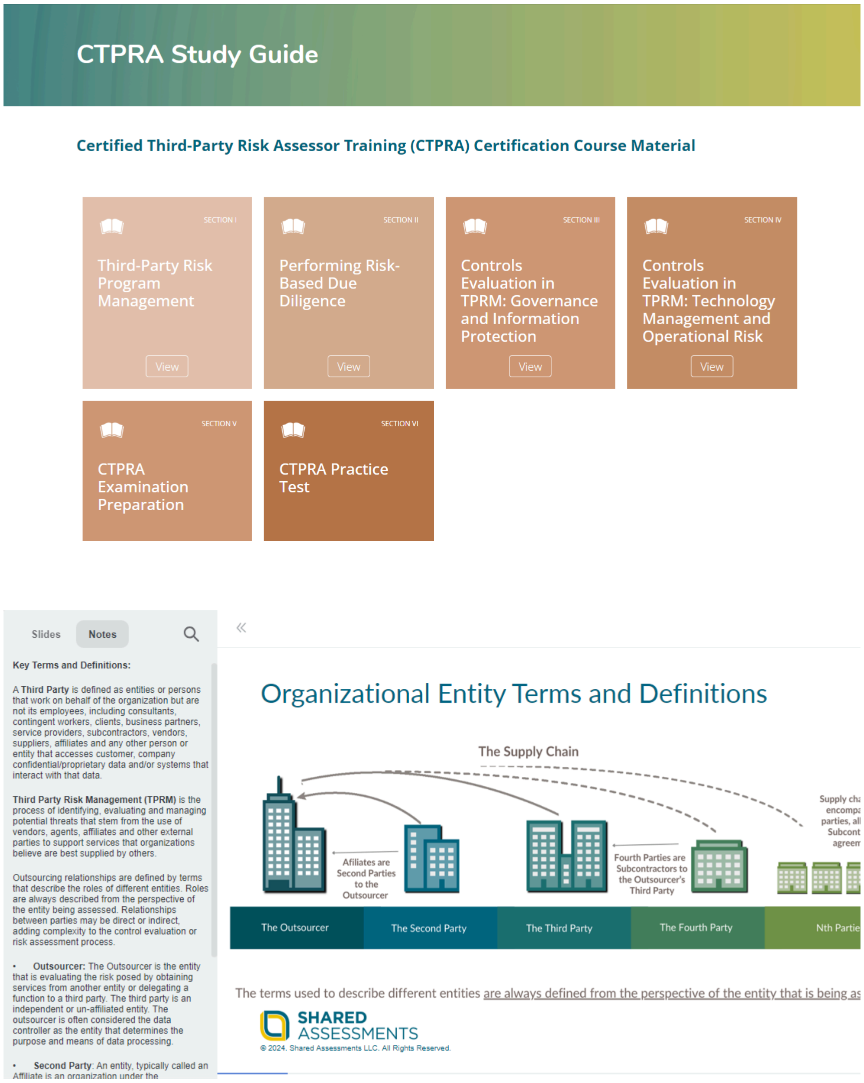
Please Note: We encourage test-takers to arrive 15 minutes before the start of their exam. This will allow ample time to connect with your proctor and troubleshoot any technical issues that may arise.

Section D: Supplemental Study Material

Study Guide

Learners can access each course and lesson multiple times to review specific lessons based on the results of practice exams or knowledge check questions. The format of the Study Guide provides both a view of the content for each slide and additional content for slides with additional notes to provide further clarification, terms, explanations, or narrative.

Figure 4: Example of Study Guide & Notes View



CTPRA Study Guide

Certified Third-Party Risk Assessor Training (CTPRA) Certification Course Material

SECTION I
Third-Party Risk Program Management
View

SECTION II
Performing Risk-Based Due Diligence
View

SECTION III
Controls Evaluation in TPRM: Governance and Information Protection
View

SECTION IV
Controls Evaluation in TPRM: Technology Management and Operational Risk
View

SECTION V
CTPRA Examination Preparation

SECTION VI
CTPRA Practice Test

Key Terms and Definitions:

A **Third Party** is defined as entities or persons that work on behalf of the organization but are not its employees, including consultants, contingent workers, clients, business partners, service providers, subcontractors, vendors, suppliers, affiliates and any other person or entity that accesses customer, company confidential/proprietary data and/or systems that interact with that data.

Third Party Risk Management (TPRM) is the process of identifying, evaluating and managing potential threats that stem from the use of vendors, agents, affiliates and other external parties to support services that organizations believe are best supplied by others.

Outsourcing relationships are defined by terms that describe the roles of different entities. Roles are always described from the perspective of the entity being assessed. Relationships between parties may be direct or indirect, adding complexity to the control evaluation or risk assessment process.

- **Outsourcer:** The Outsourcer is the entity that is evaluating the risk posed by obtaining services from another entity or delegating a function to a third party. The third party is an independent or un-affiliated entity. The outsourcer is often considered the data controller as the entity that determines the purpose and means of data processing.

- **Second Party**: An entity, typically called an Affiliate is an organization under the

Organizational Entity Terms and Definitions

The terms used to describe different entities are always defined from the perspective of the entity that is being as

SHARED ASSESSMENTS
© 2024. Shared Assessments LLC. All Rights Reserved.

CTPRA Reference Material

Resource	Purpose and Location
Shared Assessments Glossary	Shared Assessments Website
CTPRA Candidate Handbook	CTPRA Candidate Handbook
Papers and Studies	https://sharedassessments.org/papers-and-studies/
Risk Rundown Podcast	https://sharedassessments.org/podcasts/series/shared-assessments/
TPRM Webinars	https://sharedassessments.org/on-demand-events/

Shared Assessments TPRM Recommended Reading

Curriculum Alignment	Type of Study Resource
Course I: Third Party Risk Program Management	White Paper: Guide To Risk Domains For Vendor Risk Management White Paper: Complex Supply Chains – Gaining Visibility into Nth Party Governance White Paper: TPRM Risk Basics White Paper: Fourth Party Risk Management Paper White Paper: Partnering With Procurement – Part 1: Supplier/Vendor Lifecycle Risk Rundown Podcast: Episode One: It Isn't Easy Being Green White Paper: GDPR Privacy Guidelines and Checklists White Paper: CCPA Privacy Guidelines and Checklists White Paper: Executive Summary: The Role of ERM in Managing Risks Related to New Technologies
Course II: Performing Risk-Based Due Diligence	White Paper: Partnering With Procurement – Part 2: Supplier/Vendor Contracts Blog Post: Third Party Onsite Assessment Best Practices: Practitioner Guide White Paper: Tone at the Top Paper White Paper: Building Best Practices In Third Party Risk Management: Involving Procurement Paper

	White Paper: Framework For Managing Third Party Reputation Risk: Identifying, Assessing, Reporting, Mitigating, And Monitoring White Paper: Risk Quantification: Techniques For The Extended Enterprise White Paper: Complex Supply Chains – Gaining Visibility into Nth Party Governance Risk Rundown Podcast: Episode Two: Unpacking the Layers of Third-Party Risk: From Vendor Lists to ISO Certifications Blog Post: Unmasking Inherent Risk: Setting The Stage For Due Diligence Blog Post: Relationship Between Contracts, Vendor Management, And Privacy White Paper: Adaptive Risk Management For Complex Supply Chains White Paper: Risk Quantification: Techniques For The Extended Enterprise
Course III: **Governance and Information Protection**	Blog Post: Cybersecurity Vs. Information Security White Paper: Internet of Things (IoT): A New Era of Third Party Risk White Paper: Evaluating Cloud Risk for the Enterprise – An Updated Shared Assessments Guide White Paper: Assessment of Public Cloud Computing Vendors White Paper: Incident Response Briefing Paper

	Blog Post: Crisis Management And Communications: Prepared Makes Perfect White Paper: Guide To Risk Domains For Vendor Risk Management White Paper: Complex Supply Chains – Gaining Visibility into Nth Party Governance Blog Post: Internet Of Things (Iot) And Third-Party Risk Blog Post: AI Risk: Advanced Technology Adoption Requires Stronger Data Governance Blog Post: Third Party Business Continuity And Disaster Recovery Programs Blog Post: When Business Resilience Falters: The Criticality Of Incident Management Blog Post: Crisis Management And Communications: Prepared Makes Perfect White Paper: A Unified Third Party Continuous Monitoring Cybersecurity Taxonomy
Course IV: Technology Management and Operation Risk	White Paper: Building TPRM Resources in Light of Increasing Risks & Regulatory Change: Tools to Align with Business Goals White Paper: Creating a Unified Continuous Monitoring Taxonomy: Gaining Ground by Saying What's What White Paper: Innovations in Third Party Continuous Monitoring White Paper: Continuous Monitoring of Third Party Vendors: Building Best Practices Blog Post: KPIs And KRIs For Your Risk Management Program