SHARED
ASSESSMENTS

CTPRP

CERTIFIED THIRD-PARTY RISK PROFESSIONAL (CTPRP) EXAM PREP GUIDE

Table of Contents

Introduction

About the CTPRP Credential

The Certified Third-Party Risk Professional (CTPRP) designation is a professional credential designed to validate knowledge, experience, and proficiency in designing, structuring, and implementing a comprehensive Third-Party Risk Management (TPRM) program.

The CTPRP 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 CTPRP 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 CTPRP 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

This guide serves as a study and preparation guide for anyone planning to take the Shared Assessments CTPRP certification examination. This guide is not intended to replace course materials, instructor, or self-study training, and using this guide does not guarantee that you will pass the examination. CTPRP candidates often apply for the credential with varying backgrounds or years of experience in third-party risk. Each candidate should prepare for the examination based on their experience, competency in taking exams, and their educational and professional background.

This guide is broken into four sections:

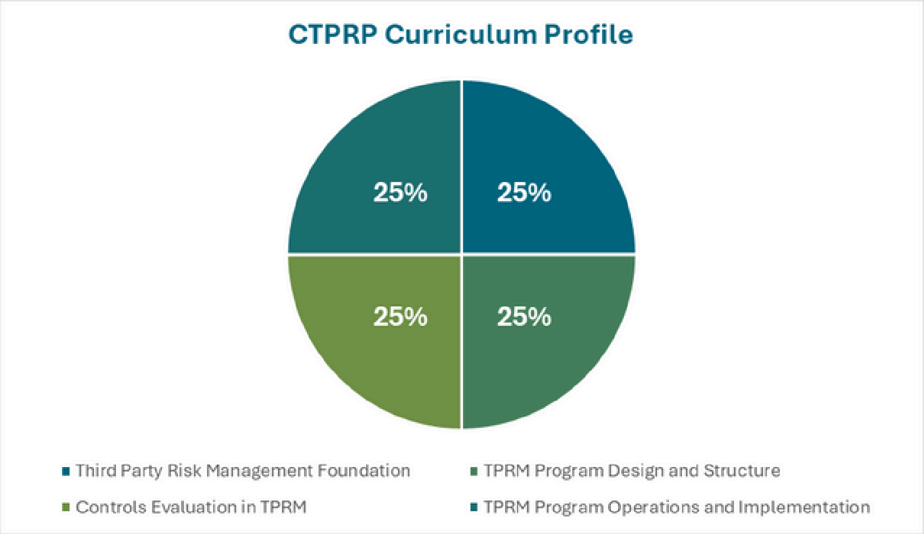
A. CTPRP Curriculum Content Review
B. Curriculum Content Validation
C. Examination Preparation and Practice Test
D. Supplemental Study Materials

Section A: CTPRP Curriculum Content Review

Understanding the Curriculum Structure

The CTPRP 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



The CTPRP certification includes the processes for third-party risk identification, structuring a risk-based vendor classification structure, and risk assessment. The curriculum summarizes the information technology, governance, resilience, and cybersecurity risk and control factors used in third-party risk assessments. The program incorporates best practices for TPRM program metrics, management reporting, and evaluating the operational performance of the program.

Course I. Third Party Risk Management Foundation

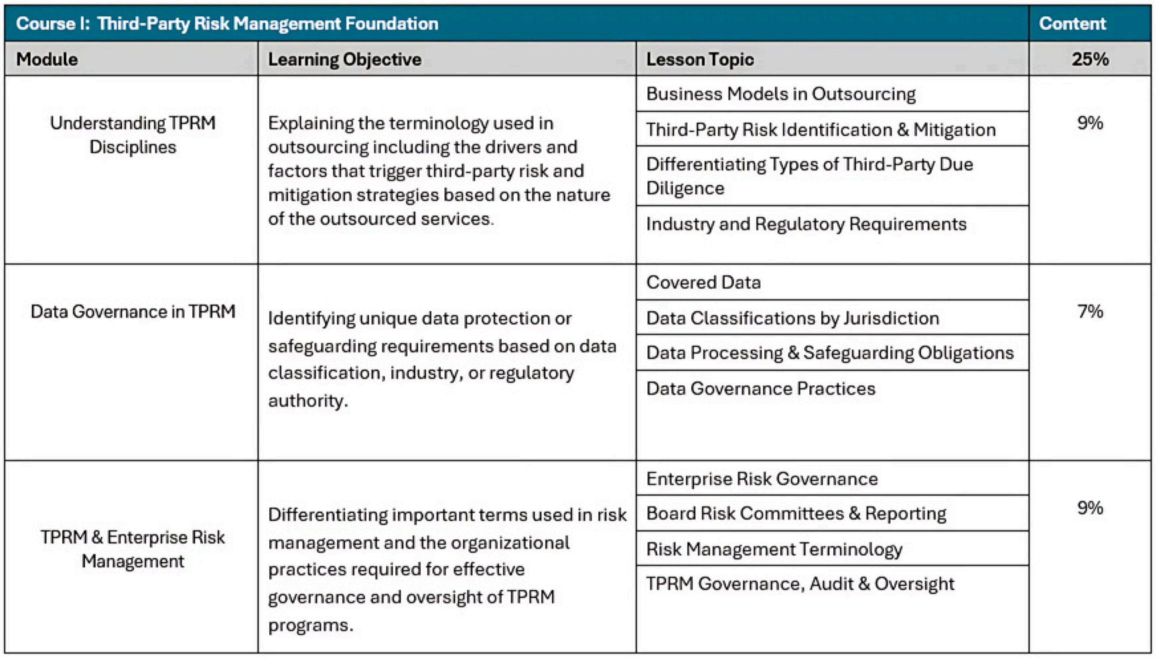
Learning Objectives

The purpose of **Course I, Third-Party Risk Management Foundation**, is to enable learners to 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.

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

- 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.
- Identifying unique data protection or safeguarding requirements based on data classification, industry, or regulatory authority.
- Differentiating essential terms used in risk management and the organizational practices required for effective governance and oversight of TPRM programs.

Content Distribution



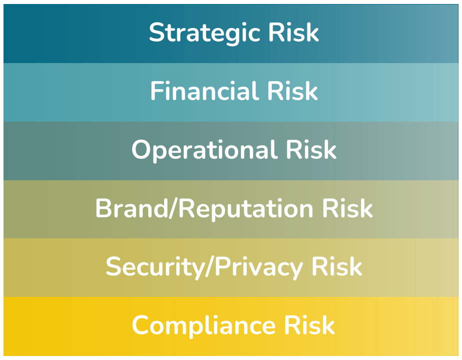
Course I: Third-Party Risk Management Foundation			Content
Module	**Learning Objective**	**Lesson Topic**	**25%**
Understanding TPRM Disciplines	Explaining the terminology used in outsourcing including the drivers and factors that trigger third-party risk and mitigation strategies based on the nature of the outsourced services.	Business Models in Outsourcing	9%
		Third-Party Risk Identification & Mitigation	
		Differentiating Types of Third-Party Due Diligence	
		Industry and Regulatory Requirements	
Data Governance in TPRM	Identifying unique data protection or safeguarding requirements based on data classification, industry, or regulatory authority.	Covered Data	7%
		Data Classifications by Jurisdiction	
		Data Processing & Safeguarding Obligations	
		Data Governance Practices	
TPRM & Enterprise Risk Management	Differentiating important terms used in risk management and the organizational practices required for effective governance and oversight of TPRM programs.	Enterprise Risk Governance	9%
		Board Risk Committees & Reporting	
		Risk Management Terminology	
		TPRM Governance, Audit & Oversight	

Content Description

Understanding TPRM Disciplines

Effective risk management requires analysis of each type of third-party relationship and the nature of the business relationship. Third party risks can be organized into common categories based on the risk impact or negative outcome that could be triggered by the relationship. Each risk category provides an input to the risk rating process when quantifying the risk posed by utilizing the third party's services.

Categorizing Risk in Third Party Relationships



In TPRM, the outsourcer owns all risks associated with any outsourced functions. TPRM requirements may be triggered by specific regulations that increase focus on vendor oversight. Third-party obligations can be defined by law, company policy, industry sector, or technology frameworks. Technology providers, vendors and suppliers of a third party are considered indirect relationships and external dependencies. Mitigating these risks is known as Fourth-Nth party management. Managing different types of third-party due diligence activities requires the integration of processes for compliance, procurement, vendor relationship management, and ongoing risk assessments. These processes may include supply chain risk management, ethical sourcing, sanctions screening, or supplier codes of conduct.

TPRM professionals must understand how multiple types of third-party risk activities are performed within the organization to align expectations. TPRM professionals must understand the industry segments their organization operates in to appropriately align the level of due diligence with external expectations. There are unique frameworks to address industry sector requirements. Outsourcers and service organizations need to monitor emerging risks and evolving threats to update TPRM program requirements.

Data Governance in TPRM

Data classification starts by identifying the data subject or data owner. Each regulation, jurisdiction, or industry standard may define Personally Identifiable Information (PII) differently. Different industry sectors have varying levels of confidentiality. The concept of “target data” or “client-scoped” data is the narrowing of the scope of any assessment to solely that data that lies within the scope of the product or service being delivered. TPRM programs develop requirements for due diligence based on the type of data and its level of sensitivity.

Data processing is any operation or set of operations performed on personal data or on sets of personal data, by manual or automated methods. Data processing may be performed by a third party or by a fourth-nth Party. The data flow helps TPRM professionals understand the people, systems, applications, and authorizations involved in the collection, use, transfer, and storage of data between parties.

Effective data governance requires understanding the exchange of information between parties, networks, systems, and locations. TPRM professionals need to understand the different classifications of data and the appropriate safeguarding techniques to establish the right data processing expectations or agreements with third parties. TPRM programs need to be able to categorize which third-party relationships require a more thorough due diligence process if the services involve significant data processing, analytics, or the use of algorithms.

TPRM and Enterprise Risk Management

Company risk culture, appetite, and tolerance set the tone for TPRM. TPRM professionals must understand how their organization addresses third-party risk and the methodologies used to identify and quantify these risks. It is essential to understand the differences in the meaning and nature of risk in TPRM. Risk can be measured qualitatively and quantitatively based on impact or likelihood. Risk appetite and risk tolerance are a balancing act between the organization’s propensity to take risks or exercise control. TPRM uses multiple risk techniques to address inherent and residual risks in third-party relationships. Inherent risk is assessed before implementing controls, while residual risk is evaluated after considering those controls. Differentiating these terms is essential to identify the set of requirements used for assigning risk ratings.

TPRM may be a part of Enterprise Risk Management (ERM) functions or committees with executive oversight. Enterprise risk functions and TPRM programs should have clearly defined definitions for risk treatment course of action along with the approved level of authority for each risk decision. TPRM risks are routinely, and in certain industries required to be reported to the company Board of Directors or a Board-Level Risk Committee. The TPRM program structure and performance may be evaluated either internally or externally. TPRM professionals must understand the separation of duties within the organization that assure the effectiveness of governance, risk management, and internal controls.

Course II. TPRM Program Design and Structure

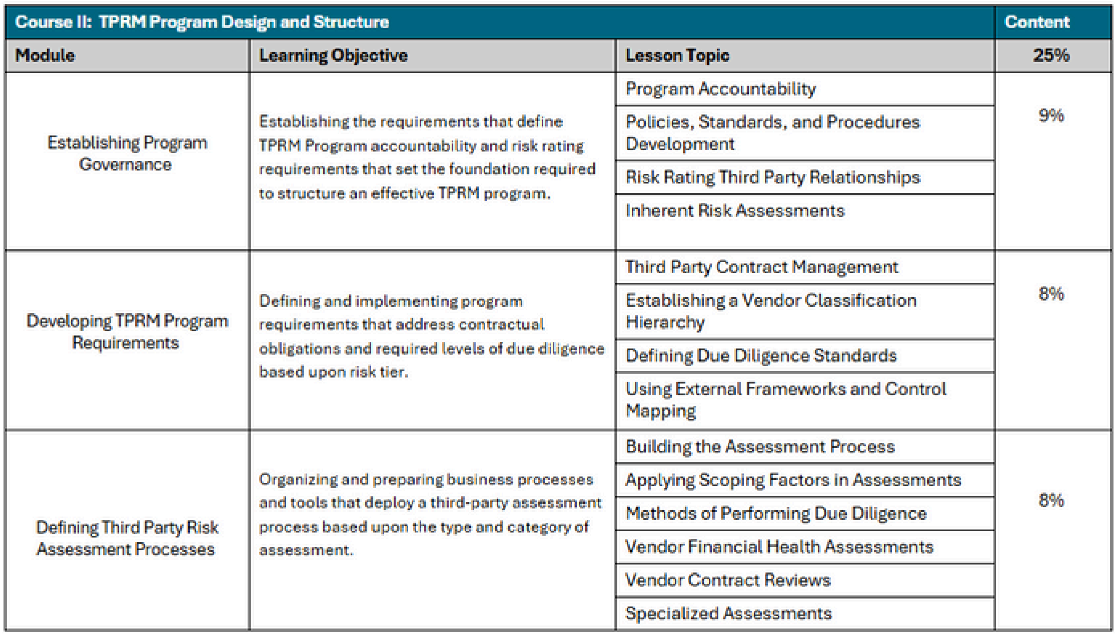
Learning Objectives

The purpose of **Course II TPRM Program Design and Structure** is to enable learners to recognize and interpret the set of program components required to structure and operate an effective TPRM program based upon organizational requirements and contractual obligations.

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

1. Establishing the requirements that define TPRM program accountability and risk rating requirements that set the foundation required to structure an effective TPRM program.
2. Defining and implementing program requirements that address contractual obligations and required levels of due diligence based on risk tier incorporating external frameworks and organizational requirements.
3. Organizing and preparing business processes and tools that deploy a third-party assessment process based upon the type and category of assessment.

Content Distribution



Course II: TPRM Program Design and Structure			Content
Module	**Learning Objective**	**Lesson Topic**	**25%**
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.	Program Accountability	9%
		Policies, Standards, and Procedures Development	
		Risk Rating Third Party Relationships	
		Inherent Risk Assessments	
Developing TPRM Program Requirements	Defining and implementing program requirements that address contractual obligations and required levels of due diligence based upon risk tier.	Third Party Contract Management	8%
		Establishing a Vendor Classification Hierarchy	
		Defining Due Diligence Standards	
		Using External Frameworks and Control Mapping	
Defining Third Party Risk Assessment Processes	Organizing and preparing business processes and tools that deploy a third-party assessment process based upon the type and category of assessment.	Building the Assessment Process	8%
		Applying Scoping Factors in Assessments	
		Methods of Performing Due Diligence	
		Vendor Financial Health Assessments	
		Vendor Contract Reviews	
		Specialized Assessments	

Content Description

Establishing Program Governance

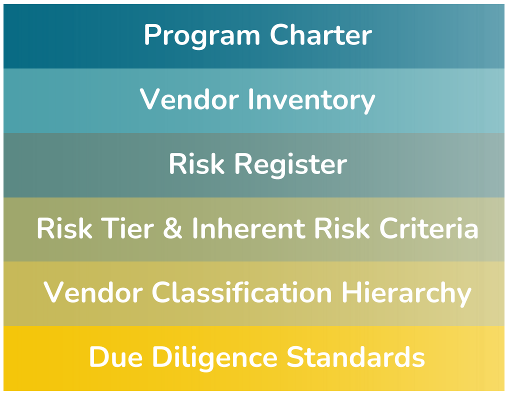
Designating program accountability starts with establishing program ownership with the position of authority to provide effective oversight of TPRM functions. The organization establishes the governance model for implementing and adhering to TPRM program requirements. Program governance includes creating policies, standards, and procedures to define requirements for risk-based due diligence. Compliance and ethics programs, ESG commitments, and goals for supplier diversity can impact program requirements. TPRM programs may operate at an enterprise level or be structured within more regulated lines of business. It is not uncommon for organizations to manage different categories of third parties with distinct processes.

Governance policies establish a repeatable process for identifying and categorizing the risks posed by third parties. The evaluation process includes identifying specific risk factors, inherent risk criteria, and the level of criticality or materiality of the services for certain relationships. Risk scoping factors can be defined from business, operational, or technology perspectives. Each risk category identified specific areas of focus to be evaluated during controls evaluation. Within each risk category, there may be distinct considerations based on company policy, regulation, or customer impact.

Developing TPRM Program Requirements

TPRM program requirements tie back to the foundational principles of type of risk, business, model, industry sector, or nature of the outsourced product, service, or activity.

TPRM Program Components



Program Charter

Vendor Inventory

Risk Register

Risk Tier & Inherent Risk Criteria

Vendor Classification Hierarchy

Due Diligence Standards

TPRM programs use a vendor inventory and risk-tracking system, typically called risk registers. TPRM professionals need to understand the difference between tracking risks at an individual third- party relationship and the overall risk level across the portfolio of relationships at the organization. To efficiently address the inventory of third parties, TPRM programs stratify the relationships using risk ratings and risk tiers to structure a vendor classification hierarchy. The risk tier establishes the scope of due diligence requirements, including more robust oversight of outsourced critical activities.

The contract defines the entire relationship based on the business model and includes mandatory contract provisions to enforce TPRM program policies. TPRM professionals need to understand how third-party contract management works within their organization and establish the sets of policies, standards, and procedures that apply to each stage of the relationship lifecycle from onboarding to termination. Contractual terms, required provisions, and type of contract may be impacted by the regulatory jurisdiction, industry sector, or classification of services.

TPRM due diligence standards include a definition of the tools, templates, and instruments to collect Vendor information and mechanisms to track and store assessment results. TPRM programs should also identify the in-scope regulations, statutes, or authoritative guidance that need to be considered in assessments.

Effective TPRM programs define assessment requirements by mapping control objectives to industry standards and frameworks. Control mapping identifies the set of control families or domains to be included in the assessment process. TPRM professionals may or may not be directly performing the controls evaluation but may be accountable for identifying, defining, and supporting how the risk assessment process addresses TPRM program requirements.

Defining Third-Party Risk Assessment Processes

TPRM professionals need to understand how to organize and prepare business processes that effectively manage and deploy third-party assessment risk intake, information gathering, scoping, and communication protocols. Risk-based due diligence may be performed at the entity or the product/service/activity level. Each TPRM program will utilize different processes based on the level of due diligence, the type of assessment, and how the assessment information was collected. Planning for effective due diligence involves determining the assessment's type and scope, including methods or platforms to collect and review evidence.

Scoping narrows the focus of evaluating the control environment based on specific parameters. External assurance reports provide evidence of independent testing of controls. Controls can be assessed by inquiry, observation, inspection of relevant documentation, and re-performance of a control. Third-party assessments are conducted using a set of requirements, tools, and templates defined by the TPRM program's due diligence standards.

Third-party assessments may also include periodic reviews of financial health, contract reviews, or compliance requirements. The frequency of these reviews should be aligned to risk ratings.

Course III. Controls Evaluation in TPRM

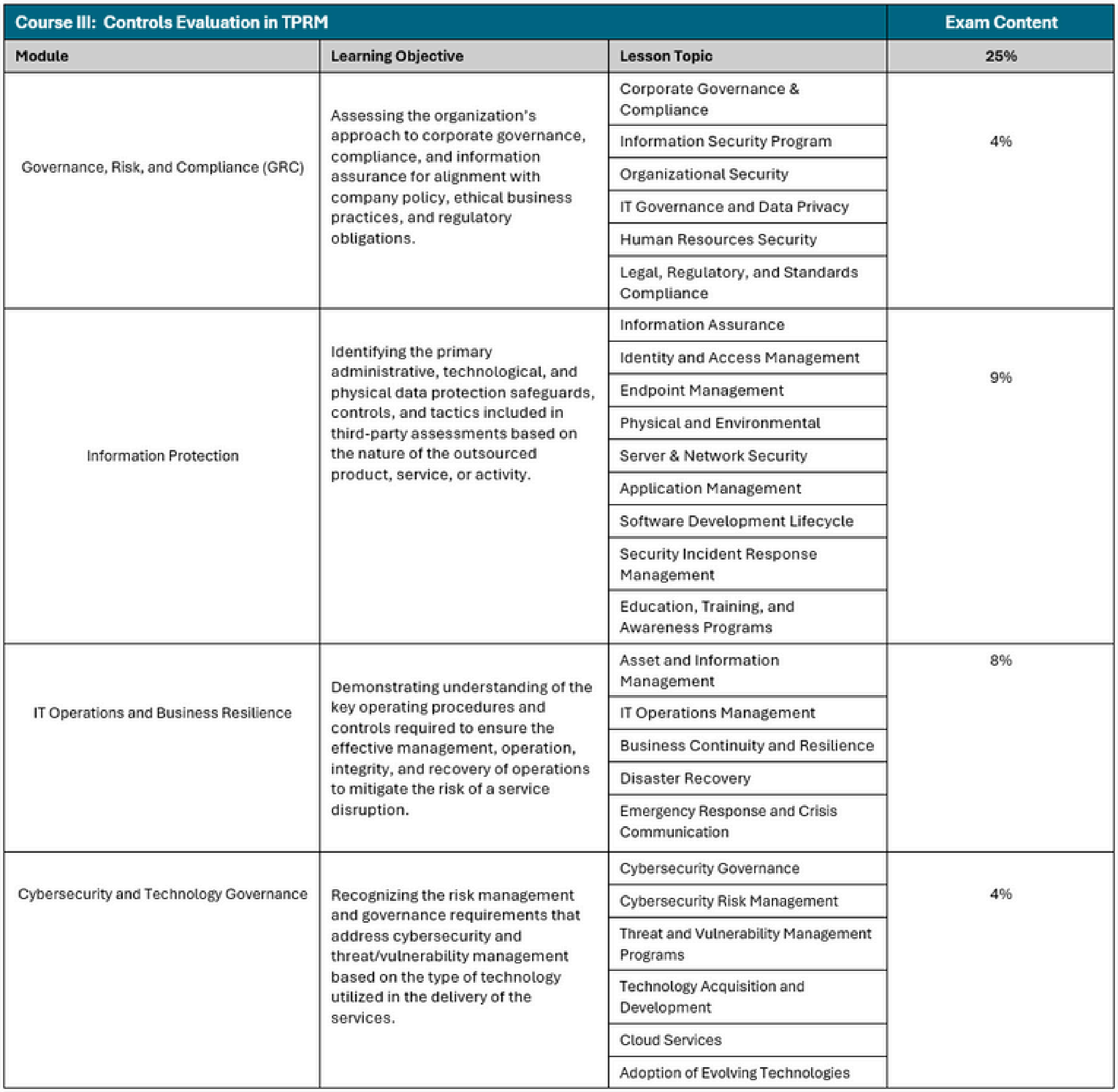
Learning Objectives

The purpose of **Course III: Controls Evaluation in TPRM** is to enable learners to interpret knowledge of the control objectives for evaluating distinct types of risk by identifying control domains to define TPRM program requirements or conduct third party assessments.

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

1. Assessing the organization's approach to corporate governance, compliance, and information assurance for alignment with company policy, ethical business practices, and regulatory obligations.
2. 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.
3. Demonstrating understanding of the critical operating procedures and controls required to ensure the effective management, operation, integrity, and recovery of operations to mitigate the risk of a service disruption.
4. 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.

Content Distribution



Course III: Controls Evaluation in TPRM			Exam Content
Module	**Learning Objective**	**Lesson Topic**	**25%**
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.	Corporate Governance & Compliance	4%
		Information Security Program	
		Organizational Security	
		IT Governance and Data Privacy	
		Human Resources Security	
		Legal, Regulatory, and Standards Compliance	
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.	Information Assurance	9%
		Identity and Access Management	
		Endpoint Management	
		Physical and Environmental	
		Server & Network Security	
		Application Management	
		Software Development Lifecycle	
		Security Incident Response Management	
		Education, Training, and Awareness Programs	
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.	Asset and Information Management	8%
		IT Operations Management	
		Business Continuity and Resilience	
		Disaster Recovery	
		Emergency Response and Crisis Communication	
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.	Cybersecurity Governance	4%
		Cybersecurity Risk Management	
		Threat and Vulnerability Management Programs	
		Technology Acquisition and Development	
		Cloud Services	
		Adoption of Evolving Technologies	

Content Description

Governance, Risk, and Compliance (GRC)

Evaluating a third party's approach to corporate governance provides insights into the maturity of their processes and can mitigate the potential risk of gaps in compliance obligations. Organizations with less maturity in GRC functions may pose a greater risk to the outsourcer based on the nature of the outsourced function.

TPRM assessment requirements in GRC focus on understanding how the third party provides management direction and support for information security, privacy, and IT Governance in accordance with business requirements and relevant laws and regulations. TPRM professionals need to understand the framework for how the third party addresses information security programs. Information Technology functions may be centralized or decentralized based on company culture and organizational design. Either approach can be effective in managing and mitigating risk. The critical factor in TPRM is to understand the interactions and structures for the various types of roles involved in organizational security and IT governance functions.

Data privacy policies outline the measures an organization takes to process and handle personal data in the scope of outsourced services. These privacy obligations may be described as data processing requirements that address data privacy, safeguards, security, and governance.

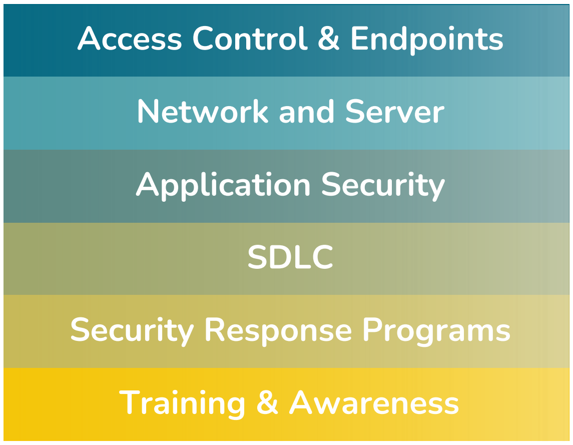
Certain third-party relationships may require the evaluation of specific compliance functions or programs. Business ethics, acceptable behaviors, and compliance requirements may be based on business model, industry, geography, or type of product/service. Understanding the nature of regulatory and standards compliance for each industry sector can assist professionals in understanding how to identify, translate, and apply TPRM requirements in different situations.

The Human Resource Security discipline is designed to examine key controls applied before, during, and after human resource hiring. Human resources play a critical role in addressing personnel risk and enforcing organizational policies. TPRM professionals need to be familiar with GRC functions to ensure that third-party risk assessments adequately address corporate, legal, regulatory, and standards compliance.

Information Protection

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. Assessments may also include physical and environmental security measures to validate that third parties are taking appropriate steps to prevent unauthorized physical access or damage to systems, facilities, and resources.

TPRM Program Components



Access Control & Endpoints

Network and Server

Application Security

SDLC

Security Response Programs

Training & Awareness

A third-party risk assessment evaluates technology and system controls from perspectives of server, network, application, and technical environment. The extent of system-to-system integration, network connectivity, or data exchange impacts the depth and breadth of the evaluation of controls. For third parties that develop and host applications used by the outsourcer or its customers, each type of software application will prompt different assessment requirements. Application security involves the use of software, hardware, development, and security practices to protect applications from external threats. Managing security and quality within the application SDLC process requires TPRM professionals to differentiate defects and vulnerabilities and their mitigation strategies. Applications that include application programming interfaces (API) for integration to external party applications pose greater risks and should be evaluated with greater scrutiny in the due diligence process. Logging and monitoring are critical and vital to help detect active breaches.

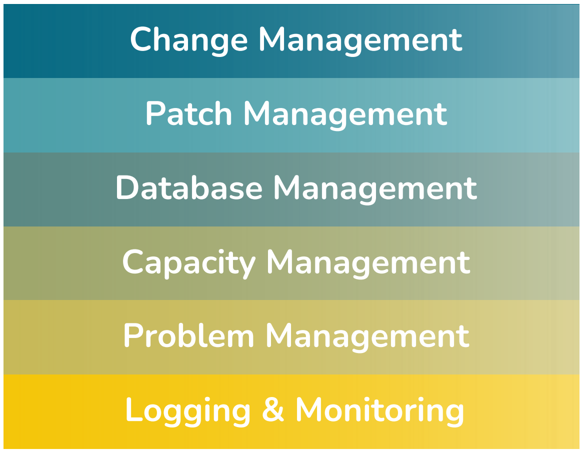
TPRM assessments include evaluating how a third party addresses security incidents and events. Incidents follow an incident lifecycle from detection, containment, response, and notification. Incident Response Management requires well-defined and regularly tested escalation, reporting, notification, and resolution procedures.

Third-party risk assessments evaluate the extent and effectiveness of training programs to ascertain how the organization is mitigating the personnel risk that could result in either a breach of data or an operational impact on the services being delivered.

IT Operations and Business Resilience

Mitigating third-party risk is not limited to cybersecurity controls. Third parties may prompt operational risk that needs to be evaluated. TPRM professionals need to understand the IT operational functions performed by the third party that directly impact service delivery to the outsourcer or the outsourcer's customers. Evaluating the operational functions starts with ensuring a mutual understanding of the physical and information assets that are in the scope of the service. Asset management includes managing the inventory of assets and deploying data loss prevention. Protecting information assets requires the deployment and execution of defined controls using cryptography.

TPRM Program Components



Change Management

Patch Management

Database Management

Capacity Management

Problem Management

Logging & Monitoring

IT Operational risk is the risk of failure or loss resulting from inadequate or failed people, processes or technology. IT operations management focus areas emphasize change management controls and patch management. Operations functions are critical in managing risk based on system hardening and configuration management. Management of infrastructure and performance uses processes and tools for logging, monitoring, and planning to ensure efficient use and operations of databases, systems, networks, and applications.

Third-party service organizations should be able to prepare, respond, and adapt to operational disruptions. Operational resilience is based on defining and deploying Disaster Recovery and Business Continuity plans to minimize disruption. Assessment requirements involving reviewing the scope and scale of recovery testing, including testing for impact to customers. Disaster recovery testing uses written plans, processes, and procedures to validate the ability of the organization's ability to resume business operations.

Business continuity is operational while resilience is strategic. Continuity is required to achieve resilience. Continuity and resilience allow an organization to continue to serve its customers within acceptable impact tolerances regardless of the business disruption. TPRM professionals need to be able to differentiate the resilience metrics including RTO/RPO validated in assessments map back to service level agreements and contractual obligations.

Operational resilience includes the identification of vendors and external dependencies to company operations that impact the availability of services. Availability requirements, service levels, and recovery times should be based on the risk tier and criticality of the product/service/activity. Minimal viable service levels are defined as the lowest level of service delivery where the services are still useable and valuable to customers and company operations.

Certain incidents or events may be of a scale to cause a crisis. Effective crisis management combines incident response from multiple processes, including emergency preparedness, disaster recovery, breach response, and privacy notification procedures.

Cybersecurity Governance and Technology Management

Technological changes, nation-state attacks, cyber-criminal activity, and ransomware have accelerated the threat landscape. A cybersecurity plan focuses on proactive measures to prevent attacks, while a Security Incident Response Plan focuses on reactive measures to minimize damage once an attack is detected. The Cybersecurity Risk Assessment process should also identify the linkages between other risks such as privacy, supply chain risk, or risk from emerging technologies

TPRM assessments include reviewing threat and vulnerability management programs. TPRM professionals need to differentiate a threat from a vulnerability to ensure that the appropriate controls are in place based on the type of technology, application, or software development process.

TPRM programs should define requirements that address the governance approach to acquiring, developing, and maintaining technology for certain categories of third parties. Increased technology risk often arises from greater operational or technological complexity, newer or different types of relationships, or potentially inferior performance by the third party.

Assessing evolving technologies starts with identifying the technological use and implementation in the outsourced services and the risk mitigation options. Service model and contract terms define cloud services accountabilities. TPRM professionals need to understand how the adoption of innovative technology impacts both requirements and the third-party risk assessment process.

Course IV. TPRM Program Operations and Implementation

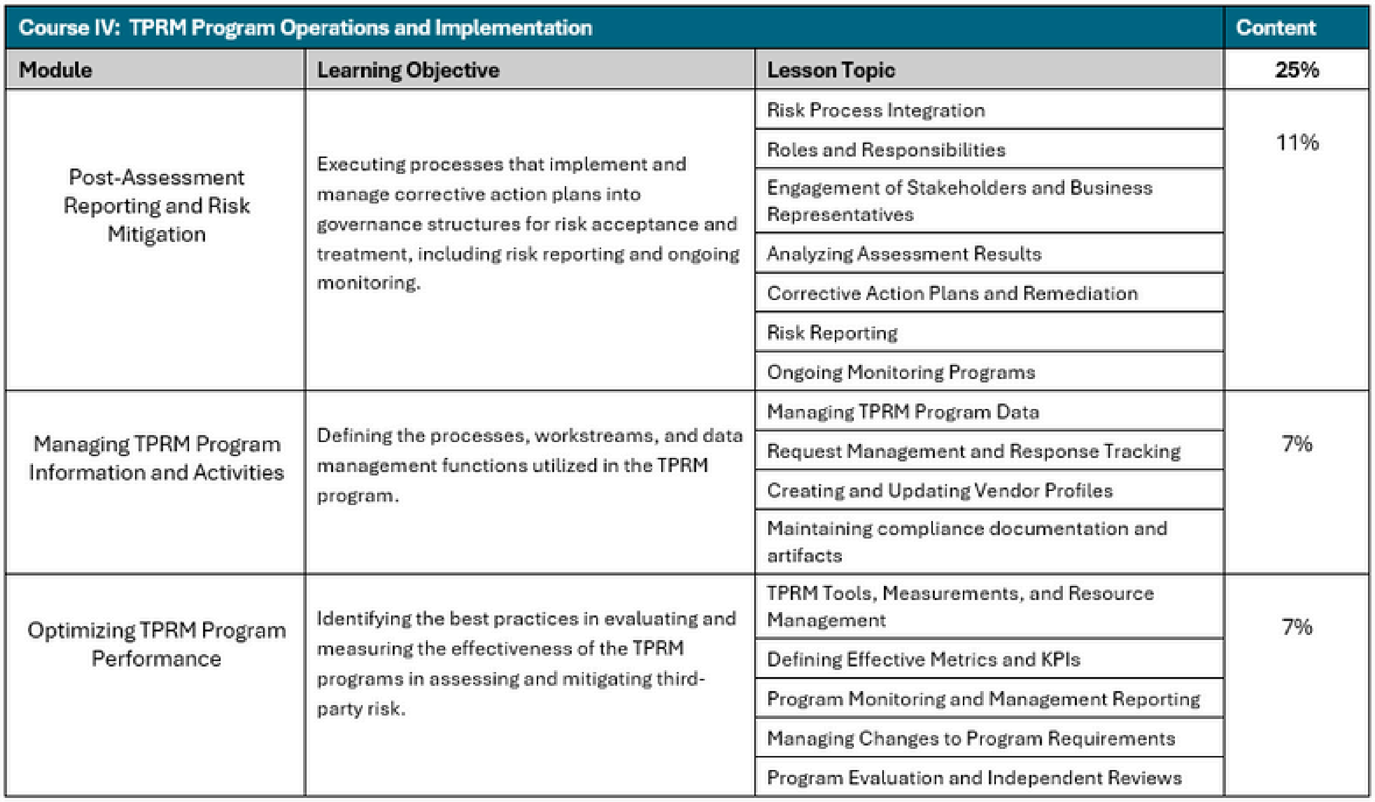
Learning Objectives

The purpose of **Course IV: TPRM Program Operations and Implementation** is to enable learners to implement the TPRM processes and infrastructure required to operate and maintain an effective TPRM program that enables risk-based management decision-making.

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

- Executing processes that integrate TPRM gaps and findings into company governance structures by engaging stakeholders with risk acceptance and treatment accountabilities.
- Implementing and managing corrective action plans, including periodic management reports and status of risk remediation for the TPRM program.
- Summarizing the process, workstreams, and data management functions utilized in the TPRM program.
- Identifying the best practices in deploying continuous monitoring and measuring the effectiveness of TPRM programs.

Content Distribution



Course IV: TPRM Program Operations and Implementation			Content
Module	**Learning Objective**	**Lesson Topic**	**25%**
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.	Risk Process Integration	11%
		Roles and Responsibilities	
		Engagement of Stakeholders and Business Representatives	
		Analyzing Assessment Results	
		Corrective Action Plans and Remediation	
		Risk Reporting	
		Ongoing Monitoring Programs	
Managing TPRM Program Information and Activities	Defining the processes, workstreams, and data management functions utilized in the TPRM program.	Managing TPRM Program Data	7%
		Request Management and Response Tracking	
		Creating and Updating Vendor Profiles	
		Maintaining compliance documentation and artifacts	
Optimizing TPRM Program Performance	Identifying the best practices in evaluating and measuring the effectiveness of the TPRM programs in assessing and mitigating third-party risk.	TPRM Tools, Measurements, and Resource Management	7%
		Defining Effective Metrics and KPIs	
		Program Monitoring and Management Reporting	
		Managing Changes to Program Requirements	
		Program Evaluation and Independent Reviews	

Content Description

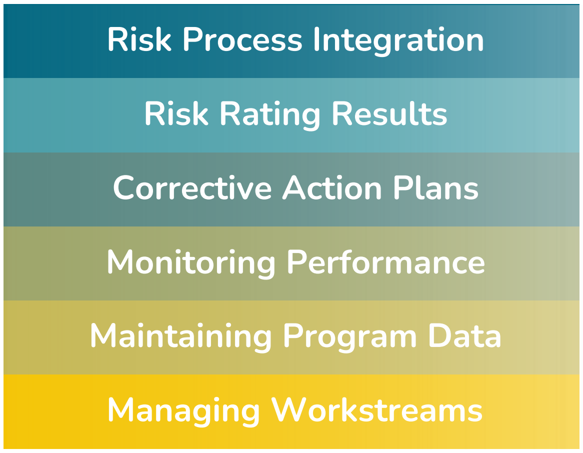
Process Execution and Integration

TPRM programs define both the processes and the organizational responsibilities for reviewing, assigning ownership, and approving risk treatment approaches. The TPRM process involves the engagement of both stakeholders and business representatives to collaborate and negotiate on solutions that address the identified risks.

Post-Assessment Reporting and Remediation

TPRM programs function using processes defined within the program but also require integration into other organizational governance processes. Risks identified by assessments may be included in enterprise risk management reports, shared with auditors, or included in updates to the Board of Directors. A TPRM program should define the processes, enablers, and resources needed to implement program requirements and manage risk mitigation activities.

TPRM Program Components



Risk Process Integration

Risk Rating Results

Corrective Action Plans

Monitoring Performance

Maintaining Program Data

Managing Workstreams

The Controls Evaluation Process identified and classified the findings from the assessment. These findings or control gaps are now risk rated by severity level to quantify the risk to the organization based upon the potential impact or likelihood of the risk. Analyzing assessment results focuses on risk quantification and assigning severity levels to findings. Corrective action plans are defined by the outsourcer and executed by the third party as part of the remediation process. Identified control owners or subject matter experts may need to be consulted to validate results or the assessor's analysis of the controls. Organizations may have different approval levels for corrective action plans based on either the severity of the risk or the criticality of the relationship. Ongoing status of managing findings closure or escalation is part of management reporting. An effective TPRM program provides business owners and management reports based on the status of assessments and identified risks. Risk reports need to provide management with the appropriate level of information to understand the risks associated to third parties. TPRM risk reporting should focus on not only operational metrics but report the status of the organization's ability to identify and mitigate risk from third party relationships. Escalation processes for outstanding items or changes in risk should be documented.

TPRM professionals need to articulate how identified risks are managed and the extent of monitoring required based on the level of risk. Periodic, continuous, or real-time monitoring strengthens but does not replace TPRM processes. TPRM programs should include defining the criteria for escalation, performance management metrics, and using risk visualization dashboards/scorecards.

Managing TPRM Program Information and Activities

Managing and maintaining a TPRM program requires the collection of vast amounts of data used in multiple processes. The TPRM organizational structure may be divided into different job roles for distinct coordination or data governance responsibilities. These functions manage assessment logistics, workstreams, due diligence artifacts, and TPRM program information.

TPRM professionals need to be able to identify the data, processes, and resources required to operate and maintain their program. Workstreams include both work product and activity for concurrent third-party assessments. Third-party risk assessments require collecting and maintaining confidential reports and compliance artifacts. The TPRM program establishes the procedures, systems, and roles for collecting and maintaining vendor information based on the assigned risk rating and vendor classification hierarchy. CTPRP candidates may provide leadership direction to personnel performing these functions or develop business cases for process improvements.

Each step in the process is performed by personnel who may be using tools or systems to automate the workflows. Most companies have one or more systems that support their program, such as a Governance, Risk, & Compliance (GRC) system, TPRM system, Contract Management System (CMS), and/or workflow management system. TPRM program information may need to be updated based on changes in requirements or triggered by the onboarding of new categories of third parties.

Optimizing TPRM Program Performance

Managing TPRM operations requires team members to collect metrics, manage workflows and create operational metrics that monitor program performance. TPRM programs may include manual and automated processes based on the organization's size, the number of relationships, and the complexity of the ecosystem. Risk professionals should be familiar with the methods used to develop operational reporting to inform management of the status of risk mitigation activities and allocation of resources.

Establishing staffing models that can support the work effort defined in policies and sufficient to meet TPRM goals and objectives is essential. The program needs to change over time, requiring a review of the skills, expertise, and training needed to run the program. TPRM professionals need to understand how TPRM metrics and tools measure the effectiveness of the overall program.

TPRM programs should ensure repeatable and consistent approaches using standardized documentation request lists, questionnaire templates and document repositories. TPRM programs should maintain documented risk scoring methodologies and scoring criteria to be used in the risk assessment process.

TPRM programs utilize monitoring solutions, independent scorecards or rating services. Leveraging external data sources can improve event identification and analysis. Use of outside data for geopolitical events can enable TPRM programs to anticipate the impact of events, promoting early intervention and risk mitigation strategies. These external inputs serve as a mechanism to provide additional information to inform metrics and management reporting. The goal of using external data is to anticipate future risks and be able to respond proactively.

TPRM professionals need to understand how Management reporting provides top-down/bottom-up work product at each of an organization's three levels. Changes to the internal or external environment may trigger updatesto TPRM policies, standards, and procedures. Organizations should undertake a regular review of their TPRM program based on changes in scope, operational challenges, and an analysis of the effectiveness of TPRM processes. Periodic program evaluations should carefully examine the effectiveness of due diligence methods, metrics, and reporting on a regular basis. TPRM professionals should develop criteria for triggering a periodic independent evaluation of the TPRM program.

Recommendations for TPRM program updates should be based on the analysis of the results of actual assessments, new risks, monitoring insights, and self-assessments.

TPRM Skills and Competencies

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

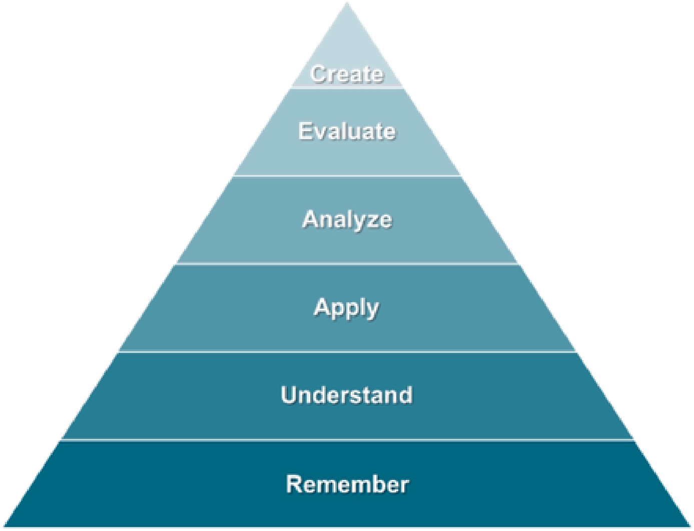
- **JUDGEMENT**: TPRM disciplines require strong analytical and systems thinking to enable risk-based decision-making
- **TECHNICAL APTITUDE**: TPRM involves analyzing controls across diverse risk domains using broad knowledge of the control environment.
- **COMMUNICATION**: TPRM professionals use effective 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 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 the hierarchy and type of knowledge for each item.

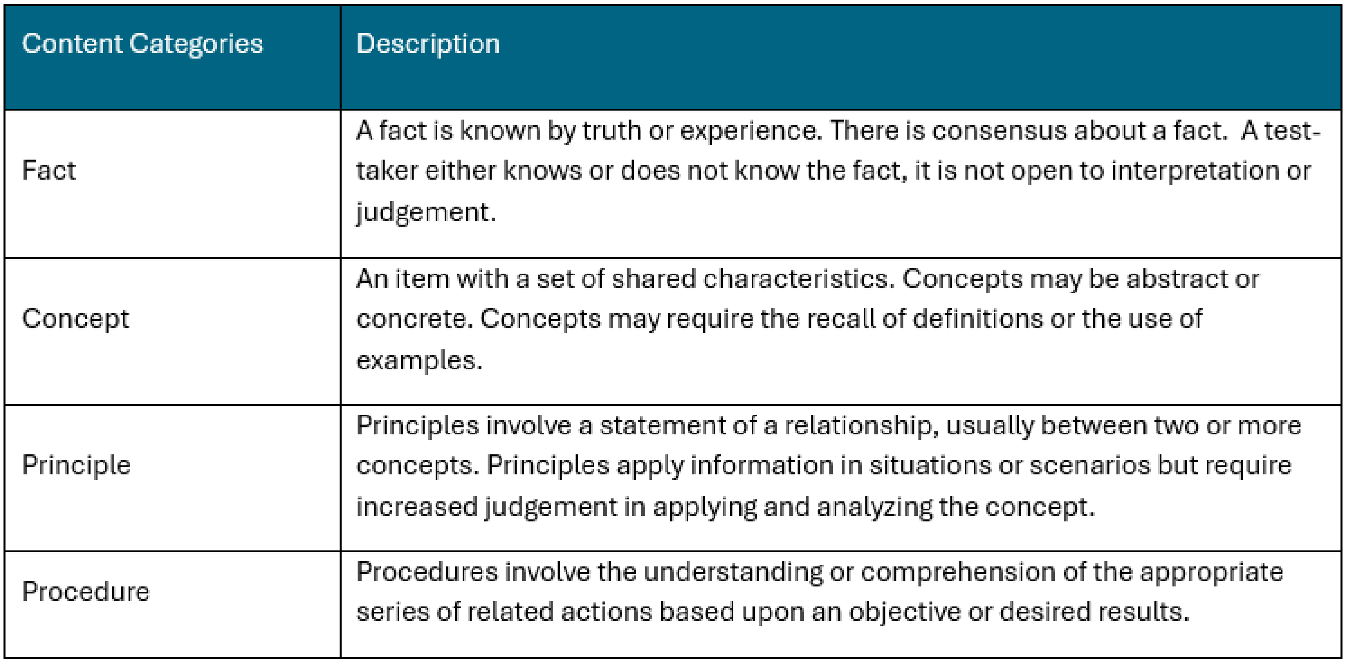
Figure1: Bloom's Taxonomy Knowledge Level Hierarchy



Type of Knowledge

The type of knowledge categorizes CTPRP curriculum content 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 judgement.
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 level of difficulty of the question, the item is assigned both an Item Knowledge Level and the Type of Knowledge. The distribution of the overall knowledge level requirements is part of the examination and content blueprint.

Chart 1: CTPRP Item Knowledge Level Breakdown

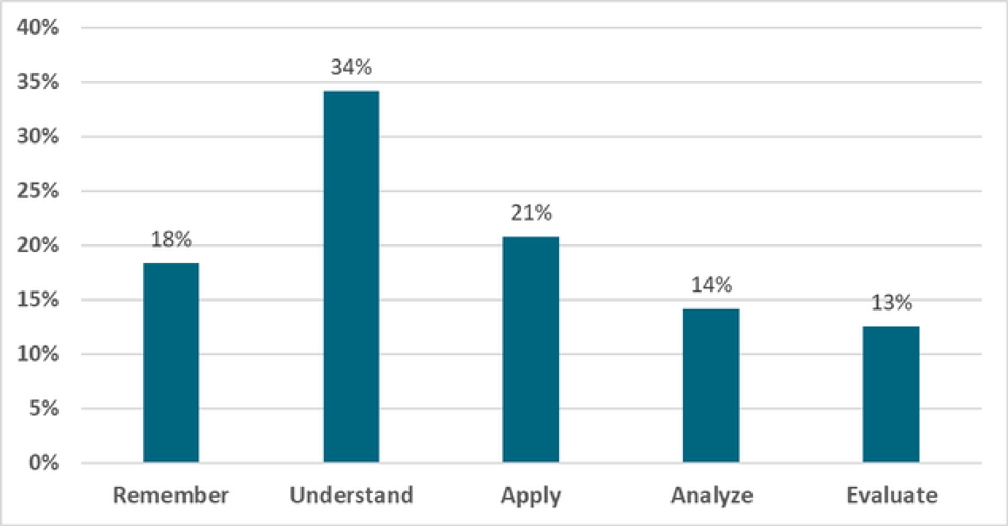
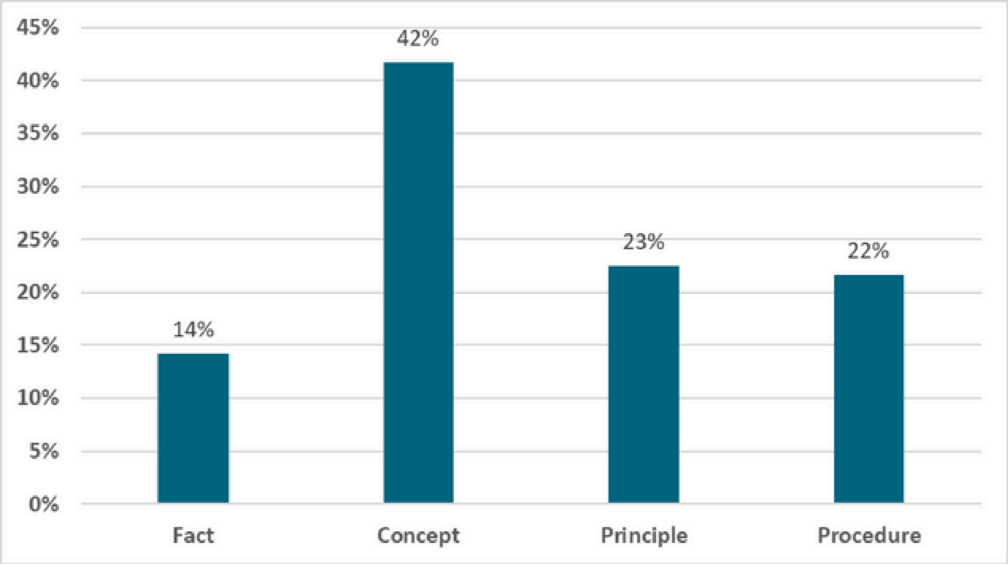


Chart 2: CTPRP Type of Knowledge Breakdown

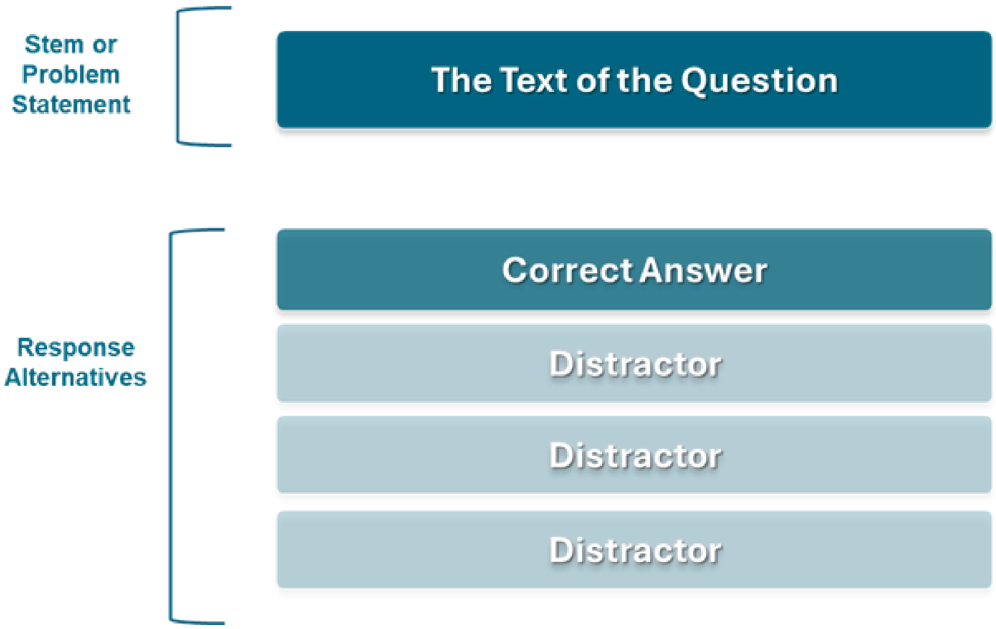


Section C: Practice Test and Examination Preparation

Questions and Response Formats

In a c***ertification*** program, testing is performed to assess knowledge and validate competency of prior knowledge, experience, and abilities. Holders of a certification demonstrate a mastery of knowledge and application that knowledge in a specific topic. The examination utilizes multiple choice question formats that follow a standard educational hierarchy that assesses the knowledge of a test taker on a specific topic; but will require judgement and experience to differentiate between the proposed solutions. Examination questions in a credentialing program follow a standard question hierarchy, which includes concepts of the STEM, the Key, Alternatives, and Distractors.

Figure 3: Structure of an Exam Question



Shared Assessments maintains documented item rationales for both the correct answer and incorrect 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 materials 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 tips help analyze and improve your ability to respond to the questions accurately:

1. **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.**

    - Develop a study timeline for the identified topic areas

2. **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 or come back to questions and change your response. However, testing trends suggest that first instincts are more closely related to a correct response.

3. **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 the first response with words that relate to the topic identified in the question.

4. **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 or gaps in the relationship between the responses.
    - Look for qualifying words like LEAST, STRONGEST, or MOST to identify the response with the greater potential to address the risk management question.

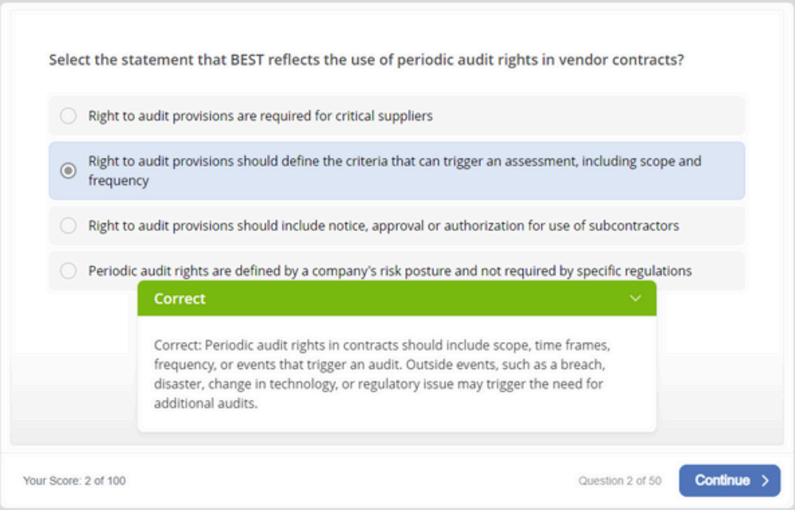
Using the Practice Exams

The practice exams include two separate exams each structured with 40 multiple-choice questions designed to reflect the types of questions you may encounter during the actual exam. The questions are distributed according to the CTPRP exam profile as follows:

- Third-Party Risk Management Foundation: 25%
- TPRM Program Design and Structure: 25%
- Controls Evaluation in TPRM: 25%
- TPRM Program Operations and Implementation: 25%

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 justification for your selected option to help you understand.



Select the statement that BEST reflects the use of periodic audit rights in vendor contracts?

○ Right to audit provisions are required for critical suppliers

● Right to audit provisions should define the criteria that can trigger an assessment, including scope and frequency

○ Right to audit provisions should include notice, approval or authorization for use of subcontractors

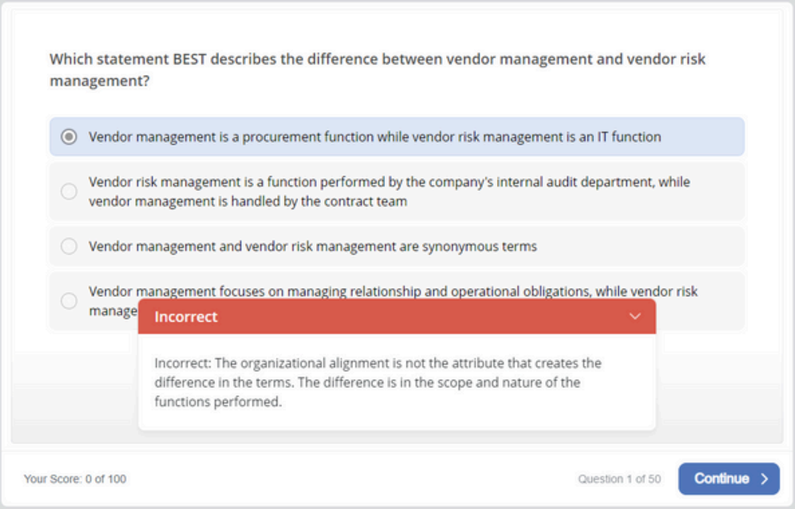
○ Periodic audit rights are defined by a company's risk posture and not required by specific regulations

Correct

Correct: Periodic audit rights in contracts should include scope, time frames, frequency, or events that trigger an audit. Outside events, such as a breach, disaster, change in technology, or regulatory issue may trigger the need for additional audits.

Your Score: 2 of 100

Question 2 of 50



Which statement BEST describes the difference between vendor management and vendor risk management?

● Vendor management is a procurement function while vendor risk management is an IT function

○ Vendor risk management is a function performed by the company's internal audit department, while vendor management is handled by the contract team

○ Vendor management and vendor risk management are synonymous terms

○ Vendor management focuses on managing relationship and operational obligations, while vendor risk manage

Incorrect

Incorrect: The organizational alignment is not the attribute that creates the difference in the terms. The difference is in the scope and nature of the functions performed.

Your Score: 0 of 100

Question 1 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 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 on completing 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 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 see your name and photo clearly.
- Show your desk and workspace. The proctor will ask you to complete a 360˚ room pan and desk sweep with your webcam 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 technical issues.

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. You will receive final exam results and next steps via email within two weeks of completing the exam, along with information on the application process or re-testing options.

Exam Retake

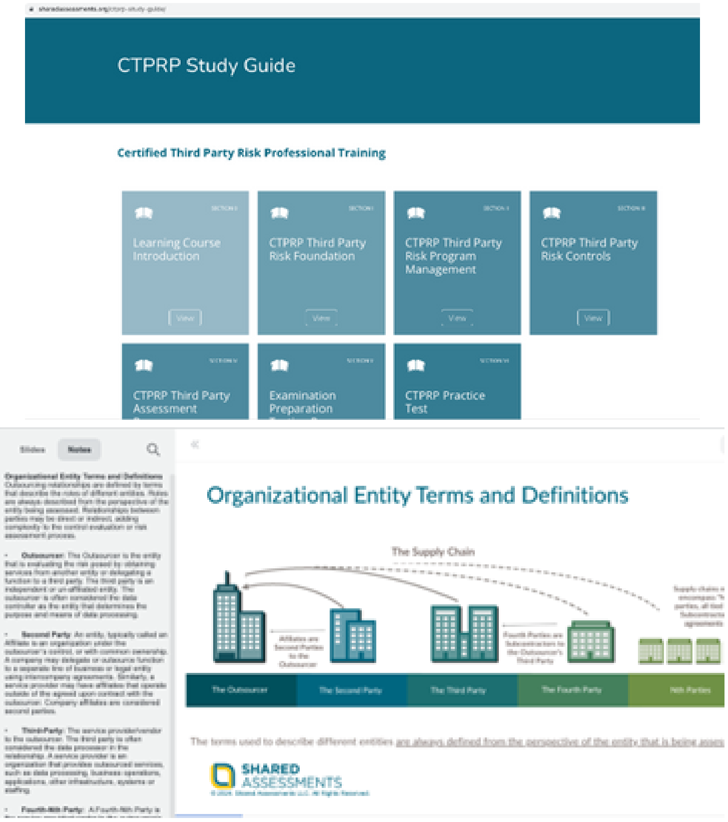
If you do not pass the exam with a minimum score of 70%, you may retake it. There is a $150 USD fee to retake the exam. You may re-take the exam up to three (3) times. After the third attempt, you must re-take the class at your expense. Individuals who wish to retake the class will receive a 50% discount on the program.

Section D: Supplemental Study Materials

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 the content for each slide and additional content for slides with additional notes to provide t further clarification, terms, explanations, or narrative.

Figure 4: Example of Study Guide & Notes View



CTPRP Study Guide

Certified Third Party Risk Professional Training

Learning Course Introduction

CTPRP Third Party Risk Foundation

CTPRP Third Party Risk Program Management

CTPRP Third Party Risk Controls

CTPRP Third Party Assessment

Examination Preparation

CTPRP Practice Test

Organizational Entity Terms and Definitions
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 outsourcer's control, or with common ownership. A company may delegate or outsource function to a separate line of business or legal entity using intercompany agreements. Similarly, a service provider may have affiliates that operate outside of the agreed upon contract with the outsourcer. Company affiliates are considered second parties.
- **Third-Party:** The service provider/vendor to the outsourcer. The third party is often considered the data processor in the relationship. A service provider is an organization that provides outsourced services, such as data processing, business operations, applications, other infrastructure, systems or staffing.
- **Fourth-Nth Party:** A Fourth-Nth Party is

Organizational Entity Terms and Definitions

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

© 2024 Shared Assessments LLC. All Rights Reserved.

Slides
Notes
View
The Supply Chain
Affiliates are Second Parties to the Outsourcer
Fourth Parties are Subcontractors to the Outsourcer's Third Party
Supply chains encompass parties, all Subcontract agreements
The Outsourcer
The Second Party
The Third Party
The Fourth Party
Nth Parties
SHARED ASSESSMENTS

CTPRP Reference Material

Resource	Purpose and Location
Shared Assessments Glossary	Shared Assessments Website
CTPRP Candidate Handbook	CTPRP 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: Introduction to Third Party Risk 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: TPRM Program Design and Structure	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: Controls Evaluation in TPRM	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: TPRM Program Operations and Implementation	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