Professional Certificate in Third-Party Risk Management

Governance And Policy Development

Access Control: Access control refers to the procedures and mechanisms used to control who has access to an organization's assets, including data, systems, and facilities. Related terms include authentication, authorization, and identity management. In the context of third-party risk management, access control is critical to ensure that third-party vendors and service providers only have access to the necessary assets and data. For example, an organization may implement role-based access control to restrict access to sensitive data based on a user's job function. Accountability: Accountability refers to the state of being answerable for one's actions and decisions. In the context of governance and policy development, accountability is critical to ensure that individuals and organizations are responsible for their actions and decisions. Related terms include transparency, responsibility, and oversight. For example, an organization may establish an accountability framework to ensure that employees are held accountable for their actions and decisions. Assessment: An assessment is a systematic evaluation of an organization's risks, vulnerabilities, and controls. In the context of third-party risk management, assessments are used to evaluate the risks associated with third-party vendors and service providers. Related terms include risk assessment, vulnerability assessment, and control evaluation. For example, an organization may conduct a risk assessment to identify potential risks associated with a third-party vendor. Audit: An audit is a systematic examination of an organization's processes, procedures, and controls to ensure compliance with regulatory requirements and internal policies. In the context of governance and policy development, audits are used to evaluate the effectiveness of an organization's governance and policy framework. Related terms include internal audit, external audit, and compliance audit. For example, an organization may conduct an internal audit to evaluate the effectiveness of its internal controls. Authentication: Authentication refers to the process of verifying the identity of users, systems, or entities. In the context of third-party risk management, authentication is critical to ensure that only authorized users and systems have access to an organization's assets and data. Related terms include authorization, identity management, and access control. For example, an organization may implement multi-factor authentication to verify the identity of users. Authorization: Authorization refers to the process of granting users, systems, or entities access to an organization's assets and data. In the context of third-party risk management, authorization is critical to ensure that only authorized users and systems have access to an organization's assets and data. Related terms include authentication, identity management, and access control. For example, an organization may implement role-based authorization to restrict access to sensitive data based on a user's job function. Board of Directors: A board of directors is a group of individuals elected or appointed to oversee and govern an organization. In the context of governance and policy development, the board of directors is responsible for establishing and overseeing an organization's governance and policy framework. Related terms include governance, leadership, and oversight. For example, an organization's board of directors may establish a governance committee to oversee the development and implementation of the organization's governance and policy framework.

Cloud Computing: Cloud computing refers to the delivery of computing services over the internet. In the context of third-party risk management, cloud computing is a critical area of focus, as organizations increasingly rely on cloud-based services and vendors. Related terms include cloud security, cloud governance, and data protection. For example, an organization may implement cloud security measures to protect its data and assets in the cloud. Compliance: Compliance refers to the state of being in accordance with regulatory requirements, internal policies, and industry standards. In the context of governance and policy development, compliance is critical to ensure that an organization operates within the bounds of regulatory requirements and internal policies. Related terms include regulatory compliance, internal compliance, and audit. For example, an organization may establish a compliance program to ensure that it is in compliance with regulatory requirements. Control: A control is a procedure, policy, or mechanism used to mitigate or manage risks. In the context of third-party risk management, controls are critical to ensure that risks associated with third-party vendors and service providers are mitigated or managed. Related terms include internal control, external control, and risk management. For example, an organization may implement a control to restrict access to sensitive data. Data Protection: Data protection refers to the procedures and mechanisms used to protect an organization's data from unauthorized access, use, or disclosure. In the context of third-party risk management, data protection is critical to ensure that an organization's data is protected when shared with third-party vendors and service providers. Related terms include data security, data privacy, and information protection. For example, an organization may implement data encryption to protect its data. Due Diligence: Due diligence refers to the process of conducting a thorough evaluation of a third-party vendor or service provider to assess its risks and vulnerabilities. In the context of third-party risk management, due diligence is critical to ensure that an organization thoroughly evaluates the risks associated with a third-party vendor or service provider. Related terms include risk assessment, vendor assessment, and vetting. For example, an organization may conduct due diligence on a third-party vendor to assess its financial stability and security controls. Governance: Governance refers to the framework of rules, policies, and procedures used to oversee and manage an organization. In the context of governance and policy development, governance is critical to ensure that an organization operates within the bounds of regulatory requirements and internal policies. Related terms include corporate governance, IT governance, and leadership. For example, an organization may establish a governance framework to oversee and manage its operations. Incident Response: Incident response refers to the procedures and mechanisms used to respond to and manage security incidents, such as data breaches or system compromises. In the context of third-party risk management, incident response is critical to ensure that an organization is prepared to respond to security incidents involving third-party vendors and service providers. Related terms include incident management, disaster recovery, and business continuity. For example, an organization may establish an incident response plan to respond to security incidents. Information Security: Information security refers to the procedures and mechanisms used to protect an organization's information assets from unauthorized access, use, or disclosure. In the context of third-party risk management, information security is critical to ensure that an organization's information assets are protected when shared with third-party vendors and service providers. Related terms include data security, network security, and cybersecurity. For example, an organization may implement a firewall to

protect its network. IT Service Management: IT service management refers to the processes and procedures used to manage and deliver IT services to an organization. In the context of third-party risk management, IT service management is critical to ensure that IT services provided by third-party vendors and service providers are managed and delivered in a secure and reliable manner. Related terms include ITIL, service management, and outsourcing. For example, an organization may establish an IT service management framework to manage and deliver IT services. Leadership: Leadership refers to the individuals or groups responsible for overseeing and managing an organization. In the context of governance and policy development, leadership is critical to ensure that an organization operates within the bounds of regulatory requirements and internal policies. Related terms include governance, management, and oversight. For example, an organization's leadership may establish a governance framework to oversee and manage its operations. Monitoring: Monitoring refers to the ongoing evaluation and review of an organization's processes, procedures, and controls to ensure that they are operating effectively and efficiently. In the context of third-party risk management, monitoring is critical to ensure that the risks associated with third-party vendors and service providers are identified and mitigated. Related terms include continuous monitoring, risk monitoring, and audit. For example, an organization may conduct regular monitoring of its third-party vendors and service providers to identify and mitigate risks. Network Security: Network security refers to the procedures and mechanisms used to protect an organization's network from unauthorized access, use, or disclosure. In the context of third-party risk management, network security is critical to ensure that an organization's network is protected when connected to third-party vendors and service providers. Related terms include firewall, intrusion detection, and access control. Outsourcing: Outsourcing refers to the practice of contracting with a third-party vendor or service provider to perform a specific function or service. In the context of third-party risk management, outsourcing is critical to ensure that the risks associated with outsourcing are identified and mitigated. Related terms include offshoring, nearshoring, and vendor management. For example, an organization may outsource its IT services to a third-party vendor. Policy: A policy is a statement of intent or a set of rules used to guide an organization's decisions and actions. In the context of governance and policy development, policies are critical to ensure that an organization operates within the bounds of regulatory requirements and internal policies. Related terms include procedure, standard, and guideline. For example, an organization may establish a policy to guide its decisions and actions. Procedure: A procedure is a detailed description of the steps used to perform a specific task or function. In the context of governance and policy development, procedures are critical to ensure that an organization's policies are implemented and enforced. Related terms include policy, standard, and guideline. For example, an organization may establish a procedure to implement its policies. Regulatory Compliance: Regulatory compliance refers to the state of being in accordance with regulatory requirements. In the context of governance and policy development, regulatory compliance is critical to ensure that an organization operates within the bounds of regulatory requirements. Related terms include internal compliance, audit, and enforcement. For example, an organization may establish a regulatory compliance program to ensure that it is in compliance with regulatory requirements. Risk Assessment: A risk assessment is a systematic evaluation of an organization's risks, vulnerabilities, and controls. In the context of third-party risk management, risk assessments are used to evaluate the risks

associated with third-party vendors and service providers. Related terms include risk management, vulnerability assessment, and control evaluation. Risk Management: Risk management refers to the processes and procedures used to identify, assess, and mitigate risks. In the context of third-party risk management, risk management is critical to ensure that the risks associated with third-party vendors and service providers are identified and mitigated. Related terms include risk assessment, risk monitoring, and control evaluation. For example, an organization may establish a risk management framework to identify and mitigate risks. Security: Security refers to the procedures and mechanisms used to protect an organization's assets, including data, systems, and facilities, from unauthorized access, use, or disclosure. In the context of third-party risk management, security is critical to ensure that an organization's assets are protected when shared with third-party vendors and service providers. Related terms include information security, network security, and cybersecurity. For example, an organization may implement security measures to protect its assets. Service Level Agreement: A service level agreement (SLA) is a contract between an organization and a third-party vendor or service provider that outlines the expected service levels, including availability, performance, and support. In the context of third-party risk management, SLAs are critical to ensure that the services provided by third-party vendors and service providers meet the organization's requirements. Related terms include contract, agreement, and vendor management. For example, an organization may establish an SLA with a third-party vendor to outline the expected service levels. Standard: A standard is a set of requirements or guidelines used to ensure consistency and quality. In the context of governance and policy development, standards are critical to ensure that an organization's policies and procedures are consistent and effective. Related terms include policy, procedure, and guideline. For example, an organization may establish a standard to ensure consistency and quality. Third-Party Risk Management: Third-party risk management refers to the processes and procedures used to identify, assess, and mitigate the risks associated with third-party vendors and service providers. In the context of governance and policy development, third-party risk management is critical to ensure that an organization's risks are identified and mitigated. Related terms include risk management, vendor management, and outsourcing. For example, an organization may establish a third-party risk management framework to identify and mitigate risks. Vendor Management: Vendor management refers to the processes and procedures used to manage and oversee third-party vendors and service providers. In the context of third-party risk management, vendor management is critical to ensure that the risks associated with third-party vendors and service providers are identified and mitigated. Related terms include contract management, supplier management, and outsourcing. For example, an organization may establish a vendor management program to manage and oversee its third-party vendors and service providers. Vulnerability: A vulnerability is a weakness or flaw in an organization's assets, including data, systems, and facilities, that can be exploited by unauthorized users or systems. In the context of third-party risk management, vulnerabilities are critical to identify and mitigate, as they can be exploited by unauthorized users or systems. Related terms include risk assessment, vulnerability assessment, and penetration testing. For example, an organization may conduct a vulnerability assessment to identify potential vulnerabilities. Vulnerability Assessment: A vulnerability assessment is a systematic evaluation of an organization's assets, including data, systems, and facilities, to identify vulnerabilities and weaknesses. In the context of third-party risk management,

vulnerability assessments are used to evaluate the vulnerabilities and weaknesses associated with third-party vendors and service providers. Related terms include risk assessment, penetration testing, and control evaluation. For example, an organization may conduct a vulnerability assessment to identify potential vulnerabilities associated with a third-party vendor.