Professional Certificate in Third-Party Risk Management

# Compliance And Regulatory Requirements

Access Certification is the process of verifying that users have the necessary permissions and access rights to perform specific tasks or access certain resources, it is a critical component of compliance and regulatory requirements in third-party risk management, related terms include identity and access management, it involves regular reviews and audits to ensure that access is granted based on the principle of least privilege, where users are given only the minimum levels of access necessary to perform their jobs.

Accountability refers to the state of being responsible for one's actions, in the context of compliance and regulatory requirements, accountability involves ensuring that individuals and organizations are held responsible for their actions and decisions, related terms include compliance and governance, it involves establishing clear lines of authority and decision-making processes, as well as implementing mechanisms for monitoring and reporting on compliance.

Anti-Bribery and Anti-Corruption refer to the laws and regulations that prohibit the offering or accepting of bribes or other corrupt practices, related terms include foreign corrupt practices act, it involves implementing policies and procedures to prevent bribery and corruption, such as due diligence on third-party vendors and agents, and training employees on anti-bribery and anti-corruption laws.

Assessment is the process of evaluating the risks and vulnerabilities associated with a particular system, process, or third-party vendor, related terms include risk and mitigation, it involves identifying potential risks and evaluating the likelihood and potential impact of those risks, as well as developing strategies for mitigating or managing those risks.

Audit Committee is a group of individuals responsible for overseeing the audit process and ensuring that the organization is in compliance with relevant laws and regulations, related terms include governance and compliance, it involves reviewing audit reports and providing recommendations for improving internal controls and compliance.

Audit Trail refers to the record of all changes, additions, or deletions made to a system, process, or data, related terms include security and compliance, it involves maintaining a secure and tamper-evident record of all changes, to ensure that the integrity of the system or data is maintained.

Authentication is the process of verifying the identity of users, devices, or systems, related terms include identity and access management, it involves using various methods such as passwords, biometrics, or smart cards to verify the identity of users and ensure that only authorized users have access to systems or data.

Authorization is the process of granting users the necessary permissions and access rights to perform

specific tasks or access certain resources, related terms include access and identity management, it involves evaluating the user's role and responsibilities and granting the necessary permissions and access rights to ensure that the user can perform their job functions.

Business Continuity Planning refers to the process of developing and implementing plans to ensure that an organization can continue to operate in the event of a disaster or other disruption, related terms include disaster recovery and business interruption, it involves identifying critical business processes and developing plans to maintain or restore those processes in the event of a disruption.

Certification is the process of verifying that a system, process, or individual meets certain standards or requirements, related terms include compliance and regulatory requirements, it involves conducting audits and assessments to ensure that the system, process, or individual meets the necessary standards or requirements.

Cloud Computing refers to the delivery of computing resources and services over the internet, related terms include cloud security and data protection, it involves using cloud-based services to store, process, and manage data, and ensuring that the necessary security and compliance controls are in place to protect that data.

Compliance refers to the state of being in accordance with relevant laws, regulations, and standards, related terms include regulatory requirements and governance, it involves implementing policies and procedures to ensure that the organization is in compliance with relevant laws and regulations, and conducting regular audits and assessments to ensure ongoing compliance.

Compliance Officer is the individual responsible for overseeing and ensuring compliance with relevant laws and regulations, related terms include governance and regulatory requirements, it involves developing and implementing compliance policies and procedures, and conducting regular audits and assessments to ensure ongoing compliance.

Compliance Program refers to the set of policies, procedures, and processes used to ensure compliance with relevant laws and regulations, related terms include compliance and governance, it involves developing and implementing a compliance program that includes policies, procedures, and training to ensure that employees understand and comply with relevant laws and regulations.

Compliance Risk is the risk of non-compliance with relevant laws and regulations, related terms include risk and mitigation, it involves identifying and assessing compliance risks, and developing strategies for mitigating or managing those risks.

Conflict of Interest refers to a situation in which an individual's personal interests may conflict with their professional responsibilities, related terms include ethics and governance, it involves disclosing and managing conflicts of interest to ensure that they do not compromise the individual's professional

responsibilities.

Control Environment refers to the overall attitude and awareness of an organization's management and employees regarding internal controls, related terms include internal controls and compliance, it involves establishing a control environment that promotes a culture of compliance and internal controls.

Corporate Governance refers to the system of rules, practices, and processes by which an organization is directed and controlled, related terms include governance and compliance, it involves establishing a framework for corporate governance that includes a clear organizational structure, roles and responsibilities, and decision-making processes.

Data Protection refers to the process of safeguarding personal and sensitive data from unauthorized access, disclosure, or destruction, related terms include data security and privacy, it involves implementing policies and procedures to protect data, such as encryption, access controls, and incident response plans.

Due Diligence is the process of conducting a thorough and systematic review of a third-party vendor or business partner, related terms include risk and mitigation, it involves evaluating the vendor's or partner's financial, operational, and compliance risks, and developing strategies for mitigating or managing those risks.

Ethics refers to the principles and values that guide an individual's or organization's behavior, related terms include compliance and governance, it involves establishing a code of ethics that promotes a culture of integrity, honesty, and transparency.

Financial Reporting refers to the process of preparing and disclosing financial information to stakeholders, related terms include financial statements and compliance, it involves ensuring that financial reports are accurate, complete, and comply with relevant laws and regulations.

Governance refers to the system of rules, practices, and processes by which an organization is directed and controlled, related terms include corporate governance and compliance, it involves establishing a framework for governance that includes a clear organizational structure, roles and responsibilities, and decision-making processes.

Information Security refers to the process of protecting information from unauthorized access, disclosure, or destruction, related terms include data security and compliance, it involves implementing policies and procedures to protect information, such as access controls, encryption, and incident response plans.

Internal Audit is the process of conducting audits and assessments to evaluate an organization's internal controls and compliance, related terms include audit committee and compliance, it involves conducting regular audits and assessments to ensure that the organization is in compliance with relevant laws and regulations, and identifying areas for improvement.

Internal Controls refer to the policies, procedures, and processes used to manage and mitigate risks, related terms include risk and mitigation, it involves establishing internal controls to ensure that the organization is in compliance with relevant laws and regulations, and that financial reporting is accurate and reliable.

IT Security refers to the process of protecting information technology systems and data from unauthorized access, disclosure, or destruction, related terms include information security and compliance, it involves implementing policies and procedures to protect IT systems and data, such as access controls, encryption, and incident response plans.

Materiality refers to the concept that a particular issue or risk is significant enough to impact the organization's financial condition or compliance, related terms include risk and mitigation, it involves evaluating the materiality of a particular issue or risk, and developing strategies for mitigating or managing that risk.

Monitoring is the process of regularly reviewing and evaluating an organization's compliance and internal controls, related terms include compliance and internal controls, it involves conducting regular audits and assessments to ensure that the organization is in compliance with relevant laws and regulations, and identifying areas for improvement.

Operational Risk refers to the risk of loss or disruption resulting from inadequate or failed internal processes, related terms include risk and mitigation, it involves identifying and assessing operational risks, and developing strategies for mitigating or managing those risks.

Outsourcing refers to the process of contracting with a third-party vendor to perform specific tasks or services, related terms include third-party risk and compliance, it involves evaluating the risks and benefits of outsourcing, and developing strategies for mitigating or managing those risks.

Privacy refers to the protection of personal and sensitive information from unauthorized access, disclosure, or destruction, related terms include data protection and compliance, it involves implementing policies and procedures to protect personal and sensitive information, such as access controls, encryption, and incident response plans.

Regulatory Compliance refers to the process of ensuring that an organization is in compliance with relevant laws and regulations, related terms include compliance and governance, it involves implementing policies and procedures to ensure that the organization is in compliance with relevant laws and regulations, and conducting regular audits and assessments to ensure ongoing compliance.

Regulatory Requirements refer to the laws, regulations, and standards that an organization must comply with, related terms include compliance and governance, it involves staying up-to-date with changing regulatory requirements, and implementing policies and procedures to ensure that the organization is in compliance with those requirements.

Reporting refers to the process of providing information to stakeholders, related terms include financial reporting and compliance, it involves ensuring that reports are accurate, complete, and comply with relevant laws and regulations.

Risk Assessment is the process of identifying and evaluating potential risks, related terms include risk and mitigation, it involves identifying potential risks, evaluating the likelihood and potential impact of those risks, and developing strategies for mitigating or managing those risks.

Risk Management refers to the process of identifying, assessing, and mitigating risks, related terms include risk and compliance, it involves implementing policies and procedures to identify, assess, and mitigate risks, and conducting regular audits and assessments to ensure that risk management processes are effective.

Segregation of Duties refers to the concept of separating duties and responsibilities to prevent a single individual from having too much control, related terms include internal controls and compliance, it involves separating duties and responsibilities to ensure that no single individual has too much control, and to prevent fraud and errors.

Supply Chain Risk refers to the risk of disruption or loss resulting from a failure or disruption in the supply chain, related terms include risk and mitigation, it involves identifying and assessing supply chain risks, and developing strategies for mitigating or managing those risks.

Third-Party Risk refers to the risk of loss or disruption resulting from a failure or disruption of a third-party vendor or business partner, related terms include risk and mitigation, it involves identifying and assessing third-party risks, and developing strategies for mitigating or managing those risks.

Training and Awareness refer to the process of educating employees on compliance and regulatory requirements, related terms include compliance and governance, it involves providing regular training and awareness programs to ensure that employees understand and comply with relevant laws and regulations.

Vendor Management refers to the process of managing and overseeing third-party vendors, related terms include third-party risk and compliance, it involves evaluating the risks and benefits of using third-party vendors, and developing strategies for mitigating or managing those risks.