Sample Risk Classification Schemes and Assessment Types

Sample Inherent and Residual Risk Classification Scheme

-Inherent Risk Score

Risk Classification	Description	Additional Information
Level 1	Critical Vendors	Vendors that provide products/services that support core business functions (i.e. loan processing).
Level 2	High Risk Vendors	
Level 3	Medium Risk Vendors	
Level 4	Low Risk Vendors	

-Residual Risk Score

Risk Classification	Description
Level 1	High Risk
Level 2	Medium Risk
Level 3	Low Risk

Sample Risk Classification Schemes and Assessment Types

Assessment Types with Sample Triggers

Assessment Types	Description	Assessment Criteria
Information Security	Assesses the vendor's or third-party's controls regarding the protection of data. The information security review may include understanding the access controls, network management, systems and application development, information security policies and procedures, physical and environmental security and other aspect of information security. The purpose is to ensure that the vendor has adequate controls in place to protect your company data from unauthorized access, use, disclosure, disruption, modification, inspection, recording or destruction.	All vendors with a data classification of non-public, confidential, highly confidential, PII and/or PHI and that will need to leave the organization's network. If the data will not be accessed outside the organization's network, then only certain aspects of an information security may apply.
Privacy	Assesses the vendor's and third-party's controls regarding the protection of sensitive data such as Personal Identifiable Information (PII) or Personal Health Information (PHI). Many institutions such as financial firms and healthcare companies are subject to specific regulations that require that they protect specific consumer information (i.e. SSN, bank account number, biometric identifiers). Regulations may include Gramm-Leach Bliley Act (GLBA) for financial institutions or Health Insurance Portability and Accountability (HIPAA) for health care companies. The purpose of a privacy risk assessment is to ensure that the vendor's controls are adequate to protect any PII or PHI and ensure compliance with regulations such as GLBA and/or HIPAA.	Data Classification: PII of PHI
Financial	Assesses the vendor's and third-party's financial health to ensure that the vendor is financially strong enough to stay in business and meet their contractual obligations to the organization. A financial risk assessment may include analyzing the vendor's financial statements using fundamental analysis and assigning a residual risk score based on a residual risk scoring scheme.	All vendors within the VRM program or utilize a risk-based approach (i.e tier 1, 2 and 3 vendors or only tier 1 and 2 vendors). The VRM program is responsible for establishing the criteria that determines whether a financial risk assessment is necessary.
Reputation	Assesses whether the firm has a positive reputation. The purpose is to ensure that the vendor does not undermine your company's brand. A reputation risk assessment may include analyzing news events regarding a company and assigning a residual risk score.	All vendors within the VRM program or utilize a risk-based approach (i.e tier 1, 2 and 3 vendors or only tier 1 and 2 vendors). The VRM program is responsible for establishing the criteria that determines whether a reputation risk assessment is necessary.

Sample Risk Classification Schemes and Assessment Types

Assessment Types	Description	Assessment Criteria
Compliance	Assesses whether the vendor or third-party has adequate program to ensure compliance with applicable regulations and industry standards. It also ensures that the vendor does not have a past history of violating regulations and industry standards. A compliance risk assessment may include an Anti-Money Laundering/OFAC scan.	All vendors within the VRM program or utilize a risk-based approach (i.e tier 1, 2 and 3 vendors or only tier 1 and 2 vendors). The VRM program is responsible for establishing the criteria that determines whether a compliance risk assessment is necessary.
Business Continuity	Assesses whether the vendor or third-party has adequate controls in place to ensure that an organization can continue to operate in case of serious incidents or disasters and is able to recover to an operational state within a specific time frame as required by contractually agreed-upon the Service Level Agreements (SLAs). For example, the contract may require the vendor or third-party to be operational within 24, 48, 72 or more hours after a business disruption. As a general rule, the lower the recovery time, the higher the criticality of the services involved. A business continuity assessment may include determining if the vendor has a business continuity plan that is tested, updated, and reviewed at least annually by the appropriate parties and assigning a residual risk score.	All vendors within the VRM program where they need to be fully operational within 24-72 hours after a business disruption. The VRM program along with the business continuity subject-matter expert/risk assessor are responsible for establishing the criteria that determines whether a business continuity assessment is necessary.
Disaster Recovery	Assesses whether the firm has adequate controls to recover key technological infrastructure in the event of a natural or other disaster (i.e. earthquake or nuclear bombing). Depending on your perspective, disaster recovery could be viewed as a subset of business continuity as a disaster could lead to a business disruption that affects the operations of an organization. There are many organizations where the business continuity and disaster recovery are combined into one assessment. A disaster recovery assessment may include determining if the vendor has a disaster recovery plan that is tested, updated, and reviewed at least annually by the appropriate parties and assigning a residual risk score.	All vendors within the VRM program where they need to be fully operational within 24-72 hours after a disaster where non-public information is involved. The VRM program along with the business continuity and/or disaster recovery subject-matter expert/risk assessor are responsible for establishing the criteria that determines whether a disaster recovery assessment is necessary.