The Importance of Third-Party Risk Assessments for Financial Institutions

CATHERINE TIBAAGA

TABLE OF CONTENTS

- Objectives and Target Audience
- What is Risk Management?
- What is Third-Party Risk Management (TPRM)?
- What is a Third-Party?
- Why do Organizations Choose to Outsource to Third-Parties?
- What are the Different Type of Risks associated with Third-Parties?
- What is the TPRM Process?
- Who are the Various Stakeholders Involved in the TPRM Process?

TABLE OF CONTENTS

Objectives and Target Audience

- Objectives: Explain the importance of third-party risk assessments to financial institutions that are subject to the following regulations below.
  - OCC 2013-29
  - FDIC Guidance on Third-Party Risk Management
  - FRB SR 13-19

- Target Audience:
  - Third-Party Risk Management (TPRM) Analysts, Managers and Executives
  - Enterprise/Operational Risk Management (ERM/ORM) analysts, managers, and executives
  - Vendors, Suppliers and Third-Parties
  - Procurement and Legal professionals that work with TPRM

What is Risk Management?

- **What is Risk?**
    - Risk is defined as the probability or likelihood that an event will lead to material and monetary losses or produce adverse effects for the organization.
        - Inherent Risks- The probability or likelihood of material and monetary losses without taking into consideration compensating controls in place to protect the organization.
        - Residual Risk- The probability or likelihood of material and monetary losses taking into consideration compensating controls in place to protect the organization.
- **What is Risk Management?**
    - Risk management is the process of controlling and managing the events that could lead to material and monetary losses or produce adverse effects.

What is Third-Party Risk Management (TPRM)?

- **What is Third-Party Risk?**
  - Third-party risk is the probability or likelihood that outsourcing specific business functions and processes to an external entity (i.e. vendor or supplier) will lead to material and monetary losses or produce adverse effects. Third-party risk is also referred to as vendor or supplier risk.

- **What is Third-Party Risk Management (TPRM)?**
  - Third-party risk management (TPRM) is the process of controlling and managing activities associated with outsourcing specific business functions and processes to an external entity that could lead to material and monetary losses or produce adverse effects. Third-party risk management (TPRM) is also referred to as vendor or supplier risk management.

What is a Third-Party?

- **What is third-party?**
  - A third-party is a private, public or quasi-government entity that provides services or products to other private, public or quisi-government institutions. Examples of third-parties are listed below.
    - A financial technology firm that provides software to corporate financial firms.
    - A software company that leases its technology to corporations or government entities.
    - A company that performs check processing for non-profits.

Why do Organizations Choose to Outsource to Third-Parties?

- Organizations choose to outsource business processes and functions to third-parties for the following reasons:
  - Reduce costs since the cost of outsourcing may be significantly lower than performing the services in-house or internally.
  - Improve efficiency with their business processes and functions by outsourcing to a third-party.
  - Gain competitive advantage in their respective markets by engaging with third-parties that possess expertise within their respective markets.
  - Maintain compliance with regulations and industry standards that govern the organization.

What are the Different Risks Associated with Utilizing Third-Parties?

- When firms choose to outsource to vendors, suppliers and third-parties, they expose themselves to third-party risks.
  - Third-party risk is the probability and likelihood of material and monetary losses due to outsourcing specific business functions and processes to external entities.
  - As a subset of enterprise and operational risk, third-party risks include the following risk areas below:
    - Information Security Risk
    - Privacy Risk
    - Business Continuity Risk
    - Disaster Recovery Risk
    - Compliance/Regulatory Risk
    - Reputational Risk
    - Financial Risk

What are the Different Type of Risks associated with Third-Parties?

- Enterprise Risk: The probability or likelihood that specific events will have a positive or negative impact on the ability of an organization to earn income and capital.
    - Financial Risk: The probability or likelihood of material and monetary losses due to the inability of an organization to earn adequate income, to pay its debts and to reward its shareholders.
    - Strategic Risk: The probability or likelihood of material and monetary losses that a third-party supplier is providing products/services that are not in alignment with the goals of the organization and that do not provide an adequate Return On Investment (ROI).
    - Operational Risk: The probability or likelihood of material and monetary losses due to inadequate processes, procedures, systems or people within an organization. Third-party risk is a subset of operational risk.
        - Third-Party Risk: Third-party risk is the probability or likelihood that outsourcing specific business functions and processes to an external entity will lead to material and monetary losses or produce adverse effects. Third-party risk is also referred to as vendor or supplier risk.
            - Information Security Risk: The probability or likelihood of material and monetary losses as a result of an organization lacking adequate controls to prevent the unauthorized access, use, disclosure, disruption, modification, inspection, recording or destruction of information. As a result, it is the probability or likelihood of material and monetary losses due to an organization's inability to protect the the confidentiality, integrity and availability of information (CIA Triad) due to inadequate internal controls.
            - Privacy Risk: The probability or likelihood of material and monetary losses as a result of an organization lacking adequate controls to prevent the unauthorized access, use, disclosure, disruption, modification, inspection, recording or destruction of consumer personal data. As a result, it is the probability or likelihood of material and monetary losses due to an organization's inability to protect the the confidentiality, integrity and availability of consumer personal data (CIA Triad) due to inadequate internal controls.

What are the Different Type of Risks associated with Third-Parties?

- Operational Risk: The probability or likelihood of material and monetary losses due to inadequate processes, procedures, systems or people within an organization. Third-party risk is a subset of operational risk.
    - Business Continuity Risk: The probability or likelihood of material and monetary losses due to an organization lacking the controls in place to ensure that they can continue to provide services or products to the organization in the event of a business disruption or interruption.
        - Disaster Recovery Risk: The probability or likelihood of material and monetary losses due to an organization lacking the controls to ensure that vital technological systems, infrastructure and information is recoverable after to a natural and man-made disaster.
    - Contract and/or Legal Risk: The probability or likelihood of material and monetary losses due to an organization not meeting their legal obligations as dictated by a contractual agreement with a third-party.
    - Regulatory/Compliance Risk: The probability or likelihood of material and monetary losses due to an organization not adhering to regulations, laws or industry standards.
    - Reputational Risk: The probability or likelihood of material and monetary losses due to poor public opinion as a result of a business event that compromises the ability of an organization to meet its regulatory and strategic objectives.

What is the TPRM Process?

- *Identify* inherent risks associated with the outsourced function or process.
    - The third-party risk analyst should work with the appropriate business department to identify the inherent risks associated with the outsourced function or process utilizing the inherent risk questionnaire. Refer to the Sample Inherent Risk Questionnaire at www.catherinetibaaga.com/resources.

    - To complete the Inherent Risk Questionnaire, the third-party risk analyst should leverage any Risk and Controls Self-Assessments (RCSAs) performed on the function or process when performed in-house or internally within the organization.
        - RCSAs are tools that helps identify risks associated with functions or processes within an organization and any controls in place to help manage and control those risks.

        - The third-party risk analyst should utilize RCSAs to complete the inherent risk questionnaire. Leveraging the RCSA to complete the inherent risk questionnaire helps capture all aspects of the function/process that the business department wants to outsource.

    - The inherent risk questionnaire should produce an inherent risk score for the outsourced function or process.
        - The inherent risk score determines the level of risk associated with outsourcing a specific function or process.

        - The inherent risk score should help determine the type of third-party risk assessments required.

        - The third-party risk analyst should document all inherent risk scores in the inherent risk register. Refer to the Sample Inherent Risk Register at www.catherinetibaaga.com/resources.

What is the TPRM Process?

- *Identify* preliminary residual risk utilizing the preliminary due diligence questionnaire (DDQ).
  - Work with the third-party (vendor/supplier) to complete the preliminary DDQ. Refer to the Sample Preliminary Due Diligence Questionnaire (DDQ) at www.catherinetibaaga.com/resources.
  - The preliminary DDQ should produce a preliminary residual risk score which determines the level of potential residual risk associated with utilizing a third-party.
  - The preliminary residual risk score also determines whether utilizing the third-party to support the outsourced function/process is within the third-party risk appetite for the organization.

- *Determine* the type of third-party risk assessments to send to the third-party based on the inherent and preliminary residual risk scores.
  - The inherent risk score determines the type of risk assessments required since it represents the level of criticality/risk associated with outsourcing a specific function or process.
  - The preliminary residual risk score should be taken into consideration as it will determine how to tailor the third-party risk assessment based on the information provided from the third-party. For example, the preliminary DDQ should help determine which questions within the third-party risk assessments apply to the third-party.
  - Utilizing the inherent and preliminary residual risk scores to determine the type of third-party risk assessments needed represents a risk-based approach to TPRM.

The vendor, supplier or third-party risk analyst could function as the risk SME.

Note: If an automated solution is utilized, all parties involved in the vendor, supplier or third-party risk process should use the automated interface to help identify preliminary residual risks and determine the type of third-party risk assessments that need to be sent to the third-party.

What is the TPRM Process?

- *Send* the third-party risk assessments to the third-party to complete with a list of supporting documentation that the third-party can provide to support responses provided in the third-party risk assessments. Refer to the document checklist on Slide 28.
  - Information Security Risk Assessment: Determines if the third-party possesses adequate controls to protect the organization from the unauthorized access, use, disclosure, disruption, modification, inspection, recording or destruction of information. It also determines if the third-party's IT infrastructure protects the confidentiality, integrity and availability of information (CIA Triad).

  - Privacy Risk Assessment: Determines if the third-party possesses adequate controls to protect the organization from the unauthorized access, use, disclosure, disruption, modification, inspection, recording or destruction of consumer personal data as defined by privacy laws (i.e. GLBA, GDPR). It also determines if the third-party's IT infrastructure protects the confidentiality, integrity and availability (CIA Triad) of consumer personal data.

  - Business Continuity Risk Assessment: Determines if the third-party possesses adequate controls to provide services or products to the organization and meet their contractual Service Level Agreements (SLAs) in the event of a business disruption.

  - Disaster Recovery Risk Assessment: Determines if the third-party possesses adequate controls to ensure that vital technological systems, infrastructure and information is recoverable after a natural or man-made disaster.

  - Financial Risk Assessment: Determines if the third-party possesses the ability to earn adequate income, pay its debts and reward its shareholders. A financial risk assessment consists of performing fundamental analysis using a third-party's financial statements (i.e. income statement, balance sheet, statement of capital).

  - Compliance Risk Assessment: Determines if the third-party adheres to applicable regulations, laws or industry standards.

  - Reputational Risk Assessment: Determines if the health of the third-party's brand and reputation and if any public events have compromised the ability of an organization to meet its regulatory requirements and strategic objectives.

  - *The vendor, supplier or third-party risk analyst could function as the risk SME.

Note: If an automated solution is utilized, all parties involved in the vendor, supplier or third-party risk process should use the automated interface to send the third-party risk assessments to the third-party to complete with a list of supporting documentation that needs to be sent to the third-party.

What is the TPRM Process?

- The third-party should send the completed third-party risk assessments along with the supporting documentation as required in the document checklist back to the third-party risk analyst to analyze.
    - The third-party risk analyst should perform the first-level review by checking to ensure all answers have been completed and that there do not exist any discrepancies in the answers provided. If discrepancies exist, the third-party risk analyst should check with the third-party to correct any discrepancies prior to submitting the third-party risk assessments to the risk SMEs.

    - The third-party risk analyst should ensure that the correct supporting documentation was provided by the third-party.

- *Analyze and evaluate* the third-party risk assessments to determine the residual risks associated with the third-party.
    - After the first-level review, the third-party risk analyst should send the third-party risk assessments to the respective risk subject-matter experts (SMEs) for the second-level review of the third-party's controls.

    - The third-party risk analyst/Risk SME should utilize the supporting documentation provided by third-party to support the evaluation of the third-party's controls.

    - Once the third-party risk analyst/risk SME completes the second-level review, the third-party risk analyst/Risk SME should provide a Risk Mitigation Action Plan (R-MAP) to the relationship manager/owner. The R-MAP contains all of the information security, business continuity, disaster recovery, financial, compliance and reputational risks identified.

    - Refer to the Sample Risk Mitigation Action Plan (R-MAP) at www.catherinetibaaga.com/resources.

Note: If an automated solution is utilized, all parties involved in the vendor, supplier or third-party risk process should use the automated interface to analyze risks utilizing the third-party risk assessments and supporting documentation provided by the third-party.

What is the TPRM Process?

- *Mitigate* residual risks found during third-party risk assessment evaluation by working with relationship manager/owner and third-party to review the R-MAP with all parties.
    - The third-party analyst/risk SME should work with the relationship manager and third-party to determine which risks can be mitigated using the R-MAP. The third-party should commit to remediating high risks in 90 days, medium risks in 180 days and low risks in 365.
    - The third-party analyst/risk SME should utilize the R-MAP to discuss the risk findings along with recommended mitigation steps and dates with the vendor, supplier or third-party.
    - Work with the third-party relationship manager and procurement to ensure that correct language regarding TPRM is included in the contracts. Contract language should include information security, business continuity, disaster recovery, financial and compliance standards.
    - For the correct contract language, refer to OCC 2013-29.
    - For risks that cannot be mitigated, TPRM should work with third-party relationship manager to undergo a risk acceptance process or choose an alternative third-party.
    - Risk acceptance process should be determined and approved by Enterprise/Operational Risk.

Note: If an automated solution is utilized, all parties involved in the vendor, supplier or third-party risk process should use the automated interface to mitigate risks found during third-party risk assessment evaluation.

What is the TPRM Process?

- Monitor all residual risks found during the third-party risk assessment process using a residual risk register.
    - The Residual Risk Register should capture whether risks were accepted, mitigated or are in the process of being mitigated.
    - TPRM should leverage the Residual Risk Register to perform data analytics.
    - Performing data analytics on the Residual Risk Register enables TPRM to produce reports that communicate and model risk trends.
    - Reports produced as a result of performing data analytics allow TPRM and Enterprise/Operational Risk to make decisions that ensure that the TRPM program is in alignment with the strategic objectives of the organization.
    - Refer to the Sample Residual Risk Register at www.catherinetibaaga.com/resources.
    - Provide reporting to enterprise/operational risk and senior management on inherent and residual risk trends.
    - Hold monthly and quarterly meetings with departmental executives that utilize third-parties and enterprise/operational risk management to discuss reporting.

Note: If an automated solution is utilized, all parties involved in the vendor, supplier or third-party risk process should use the automated interface to monitor risks.

Who are the Various Stakeholders Involved in the TPRM Process?

- **1st Line of Defense: Business Units, Lines and Department**
  - Vendor, Supplier or Third-Party Relationship Manager: Responsible for working with the third-party risk analyst/risk SMEs to complete the third-party risk assessments. Utilizes the policies, processes and procedures as defined by the TPRM team in conjunction with the risk SMEs.

- **2nd Line of Defense: Third-Party Risk Management**
  - Third-Party Risk Management ((TPRM) Group: Works with the other risk SME groups to create and implement the policies, processes and procedures that govern the third-party risk assessment process.

  - The risk SME groups include information security, business continuity, disaster recovery, finance, compliance, and legal. Other risk SME groups include operational/enterprise risk management.

  - The TPRM group or the Risk SMEs may conduct third-party risk assessments.

- **3rd Line of Defense: Auditors (Internal and External)**
  - Internal Auditors: A group within the organization that provides objective and independent assurance of the first, and second line of defense to ensure that vendor, supplier or third-party risk management is in alignment with industry best practices and regulations. They report back to Senior Management and the Board.

  - External Auditors: An entity outside the organization that provides objective and independent assurance of the first, and second line of defense to ensure that vendor, supplier or third-party risk management is in alignment with industry-best practices and regulations. They report back to Senior Management and the Board.

What is a Third-Party Risk Assessment?

- A third-party risk assessment evaluates the effectiveness and maturity of the internal controls of a third-party.
  - The purpose of the third-party risk assessment is to determine if the controls in place are sufficient to protect the organization from the following risks below:
    - Information Security
    - Privacy
    - Business Continuity
    - Disaster Recovery
    - Financial
    - Regulatory/Compliance
    - Reputational

Information Security Risk Assessment

- An information security risk assessment determines if the third-party possesses adequate controls to protect the organization from the unauthorized access, use, disclosure, disruption, modification, inspection, recording or destruction of information. It also determines if the third-party's IT infrastructure protects the confidentiality, integrity and availability of information (CIA Triad).
- To assess information security controls, risk SMEs and third-party risk analysts should assess the following control areas:
  - Enterprise Risk Management (ERM) Policies and Procedures
  - Operational Risk Management (ORM) Policies and Procedures
  - Third-Party Risk Management (TPRM) Policies and Procedures
  - Information Security Policies and Procedures
  - Asset Management
  - Human Resources Security
  - Physical and Environmental Security
  - Network Management, Communications and Operational Security

**The control areas are based on ISO 27001 and 27002. Please visit www.iso.org. Also visit Shared Assessments at www.sharedassessments.org/sig/*

**For a sample information security risk assessment, please refer to Appendix A.*

Information Security Risk Assessment

- An information security risk assessment determines if the third-party possesses adequate controls to protect the organization from the unauthorized access, use, disclosure, disruption, modification, inspection, recording or destruction of information. It also determines if the third-party's IT infrastructure protects the confidentiality, integrity and availability of information (CIA Triad).
- To assess information security controls, risk SMEs and third-party risk analysts should assess the following control areas:
  - Access Controls
  - Systems Acquisition, Development and Maintenance
  - Incident Response and Notification
  - Compliance
  - Mobile Security
  - Software Security
  - Cloud Security

**The control areas are based on ISO 27001 and 27002. Please visit www.iso.org. Also visit Shared Assessments at www.sharedassessments.org/sig/*

**For a sample information security risk assessment, please refer to Appendix A.*

Privacy Risk Assessment

- A privacy risk assessment determines if the third-party possesses adequate controls to protect the organization from the unauthorized access, use, disclosure, disruption, modification, inspection, recording or destruction of consumer personal data. It also determines if the third-party's IT infrastructure protects the confidentiality, integrity and availability of consumer personal data (CIA Triad).
- To assess privacy risk controls, risk SMEs and third-party risk analysts should determine the following information below when conducting a privacy risk assessment:
  - Does the third-party have documented privacy policies and procedures?
  - Who is responsible for approving privacy policies and procedures?
  - Does the third-party have Chief Privacy Officer or Privacy Manager?
  - Does the Chief Privacy Officer or Privacy Manager approve privacy policies and procedures?
  - Are privacy policies and procedures reviewed on annual basis?
  - Is the third-party organization subject to privacy laws such as Gramm Leach Bliley Act (GLBA), EU Privacy Act, General Data Protection Regulation (GDPR), etc? If so, which privacy laws?
  - Does the third-party conduct privacy risk assessments?
  - Does the organization provide privacy training to employees and contingent workers?
  - Does the organization provide privacy training to employees and contingent workers on an annual basis?

**Third-party risk analyst/Risk SME should leverage the information security risk assessment to complete the privacy risk assessment. The questions above do not represent the full list of questions related to privacy risk.*

Business Continuity Risk Assessment

- A business continuity risk assessment determines if the third-party possesses adequate controls to provide services or products to the organization in the event of a business disruption or interruption.
- To assess whether a third-party possesses adequate internal controls to meet their SLAs in the event of a business disruption, the risk SMEs and third-party risk analysts should determine the following information below when conducting a business continuity risk assessment:
    - Does the third-party have a business continuity plan?
    - Does the third-party perform Business Impact Analysis (BIA)?
    - Is the business continuity plan reviewed and updated once a year?
    - Who is responsible for reviewing the business continuity plan?
    - Does the third-party conduct business continuity tests once per year?

**The questions above do not represent the full list of questions related to business continuity risk.*

Disaster Recovery Risk Assessment

- A disaster recovery risk assessment determines if the third-party possesses adequate controls to ensure that vital technological systems, infrastructure and information is recoverable after a natural or man-made disaster.
- To assess whether a third-party possesses adequate internal controls to ensure that vital technological systems, infrastructure and information is recoverable after a natural or man-made disaster, the risk SMEs and third-party risk analysts should determine the following information below when conducting a ddisaster recovery risk assessment:
    - Does the third-party have a disaster recovery plan?
    - Is the disaster recovery plan reviewed and updated once a year?
    - Who is responsible for reviewing the disaster recovery plan?
    - Does the third-party conduct disaster recovery tests once per year?
    - Does the third-party have a business continuity or disaster recovery site? If so, what is the location?
    - If the third-party does have a business continuity or disaster site, is the location outside of the United States?

**The questions above do not represent the full list of questions related to disaster recovery risk.*

Financial Risk Assessments

- A financial risk assessment determines if the third-party can earn adequate income, pay its debts and reward its shareholders. A financial risk assessment consists of performing fundamental analysis using a third-party's financial statements (i.e. income statement, balance sheet, statement of capital).
- To assess the financial health of an organization, third-party risk analysts should work with the finance department or utilize a tool to analyze financial statements using ratio analysis as listed below. Please refer to the ratios below to complete financial statement analysis on the third-party.
  - **Profitability Ratios**
    - Profit Margin= Net Income/Sales
    - Return on Assets (ROA)= Net Income/Total Assets
    - Return on Equity (ROE)= Net Income/Total Equity
  - **Leverage Ratios**
    - Total Debt Ratio= Total Assets-Total Equity/Total Assets
    - Debt-Equity Ratio= Total Debt/Total Equity
    - Equity Multiplier= Total Assets/Total Equity
    - Long-term Debt Ratio= Long-Term Debt/Long-Term Debt + Total Equity
    - Times Interest Earned Ratio= EBIT/Interest
  - **Liquidity Ratios**
    - Current Ratio= Current Assets/Current Liabilities
    - Quick Ratio= Current Assets-Inventory/Current Liabilities

**The questions above do not represent the full list of questions related to financial risk.*

Financial Risk Assessments

- A financial risk assessment determines if the third-party can earn adequate income, pay its debts and reward its shareholders. A financial risk assessment consists of performing fundamental analysis using a third-party's financial statements (i.e. income statement, balance sheet, statement of capital).
- To assess the financial health of an organization, third-party risk analysts should work with finance department or utilize a tool to analyze financial statements using ratio analysis as listed below. Please refer to the ratios below to complete financial statement analysis on the third-party.
  - **Asset Utilization Ratios**
    - Inventory turnover= Cost of Goods Sold/Inventory
    - Days' Sales in Inventory= 365 Days/Inventory turnover
    - Receivables Turnover= Sales/Accounts Receivable
    - Days' Sales in Receivables= 365 Days/ Receivables Turnover
    - Net Working Capital Turnover=Sales/Net Working Capital
    - Fixed Assets Turnover= Sales/Net Fixed Assets
    - Total Assets Turnover= Sales/Total Assets

**The questions above do not represent the full list of questions related to financial risk.*

Reputation Risk Assessments

- A reputational risk assessment determines the health of the third-party's brand, public image and reputation.
- To assess whether the reputation and brand whether an organization is in compliance with industry regulations, laws and standards, third-party risk analysts should research the following below utilizing a news database (i.e. Factiva, LexisNexis, Google News, Yahoo News) :
    - Does the organization have any bankruptcies in the last three to five years?
    - Has the organization experienced any information security or cyber security incidents such as data breaches in the last three to five years?
    - Has the organization engaged in any activities that demonstrate lack of compliance with laws, regulations or industry standards in the last three to five years?
    - Has the organization experienced any law suits or legal issues in the last three to five years?
    - Has the organization experienced financial difficulties within the past five years? *(*Leverage the financial risk assessment along with any financial news events)*

**The questions above do not represent the full list of questions related to reputation risk.*

Compliance Risk Assessments

- A compliance risk assessment determines if the third-party adheres to applicable regulations, laws and industry standards.

- To assess whether an organization is in compliance with industry regulations, laws and standards, risk SMEs and third-party risk analysts should work with the compliance department to answer the following questions below:

    - Complete an OFAC Scan to determine if a third-party is not in compliance with anti-money laundering (AML) laws and regulations. An OFAC scan also checks if an organization is listed on a sanctions list. To conduct OFAC scan, the third-party risk analyst should leverage software tool that enables OFAC searches.

    - Is the third-party following mandatory industry laws, regulations and standards? To determine if an organization complies with mandatory industry regulations and standards, the third-party risk analyst should research laws, regulations and standards that apply to the third-party.

    - Is the third-party compliant with global industry standards such as ISO 9001 or ISO 27001?
    - Does the third-party have an internal audit, compliance or enterprise/operational risk management function that identifies and tracks whether regulatory issues have been resolved?
    - Does the third-party have a compliance and ethics department where employees and contingent workers can report compliance issues?
    - Does the third-party have policies and procedures to ensure compliance with intellectual property rights on the use material and proprietary software?

**Third-party risk analysts should leverage reputational risk assessments to determine if third-party has experienced regulatory penalties due to lack of compliance with applicable laws and regulations.*

**The questions above do not represent the full list of questions related to compliance risk.*

Documentation Required

- To perform the third-party risk assessment, the third-party should provide the following documentation as supporting evidence to answers provided in third-party risk assessment.
  - SSAE18/SOC Reports including SOC 2 Report
  - ISO 27001certificate if available
  - ISO 9001 certificate if available
  - PCI DSS Compliance certificate if available
  - Information Security Policies and Procedures
    - Access Controls Policies and Procedures
    - Asset Management Policies and Procedures
    - Anti-Virus/Malware Policy or Program
    - Password Management Policies and Procedures: Provide screenshot that shows password complexity and configuration settings
    - Encryption Policies and Procedures: Provide screenshot of encryption key algorithm
    - Screenshot of encryption key algorithm
    - Network Management Policies and Procedures
    - Incident Management and Event Notification Policies and Procedures
    - Human Resources Security Policies and Procedures
    - Physical and Environmental Security Policies and Procedures

**The questions above do not represent the full list of documents required from the vendor, supplier or third-party. Please work with the information security department to determine if further documentation is required.*

Documentation Required

- To perform the third-party risk assessment, the third-party should provide the following documentation as supporting evidence to answers provided in third-party risk assessment.
  - SSAE18/SOC Reports including SOC 2 Report
  - ISO 27001certificate if available
  - ISO 9001 certificate if available
  - PCI DSS Compliance certificate if available
  - Information Security Policies and Procedures
    - Software/Systems Development Policies and procedures
    - Network Configuration Diagrams for internal and external networks
    - Application Security Policies and Procedures: Provide screenshot that shows that network logic is required to access applications
    - System Backup Policies and Procedures
    - Offsite Storage policies and Procedures
    - Change Control Policies and Procedures
    - Privacy Policies and Procedures
    - Threat management policies and procedures
    - Information Security and Privacy Training Program
    - Data Loss Prevention Program
    - System an network configuration standards

**The questions above do not represent the full list of documents required from the vendor, supplier or third-party. Please work with the information security department to determine if further documentation is required.*

Documentation Required

- To perform the third-party risk assessment, the third-party should provide the following documentation as supporting evidence to answers provided in third-party risk assessment.
  - Vulnerability Scans and Penetration Tests
  - Vulnerability assessments of systems, applications and networks
  - Application Security Scans
  - Enterprise/Operational Risk Management (ERM/ORM) Policies and Procedures
  - ERM/ORM Training Program
  - Third-Party Risk Management (TPRM) Policies and Procedures: Include any third-party risk assessments completed
  - Compliance Policies and Procedures
  - Business Continuity Policies and Procedures
  - Business Continuity Plan
  - Business Continuity Tests
  - Disaster Recovery Policies and Procedures
  - Disaster Recovery Plan
  - Disaster Recovery Tests
  - Three Years of Audited Financial Statements

**The questions above do not represent the full list of documents required from the vendor, supplier or third-party. Please work with the information security department to determine if further documentation is required.*

Conclusion

Summary

- Overall, it is important that financial institutions ensure that vendors, suppliers and third-parties implement and maintain internal controls that protect them from risks that could potentially undermine them.

- Ultimately regulators hold financial institutions responsible for any business incidents and events as a result of inadequate vendor, supplier or third-party controls.

- To protect themselves financial institutions should perform vendor, supplier and third-party risk assessments when choosing to outsource business processes and functions to vendors, suppliers or third-parties.

- By performing vendor, supplier or third-party risk assessments, financial institutions ensure that utilizing vendors, supplier or third-parties does not compromise their strategic objectives.

very strong income performance well ahead of prior year
Projected sales of main products in 2013
Distribution marketing participation in the securities market.
Analysis of total income
Share of market activity
Final Sales
Sales by Category
Distribution of the securities market key players
Revenue growth divisions
TYU division
FRT division
Passive market share
DAT
BID
ASK
PRO
QUA

Appendix A: Sample Information Security Risk Assessment

Information Security Risk Assessment

- To perform the third-party risk assessment, the third-party should answer the following questions:

- **Information Security Policies and Procedures**
  - Does the organization have information security policies and procedures to ensure that the organization protects the confidentiality, integrity and availability (CIA) triad of information within the organization?
  - Does the Chief Technology Officer (CTO), Chief Information Security Officer (CISO), or information Security Manager review the information security policies and procedures?
  - Who in the organization is responsible for reviewing information security policies and procedures?
  - How often are the information policies and procedures reviewed?
  - Are information security policies and procedures reviewed on annual basis?
  - Does the organization have any independent attestations? (i.e. ISO 27001, PCI DSS, SOC Reports)?

- **Privacy Policies and Procedures**
  - Does the organization have privacy policies and procedures?
  - Does the Chief Privacy Officer (CPO), Privacy Manager or legal review the privacy policies and procedures?
  - Who in the organization is responsible for reviewing the privacy policies?
  - How often are the privacy policies and procedures reviewed?
  - Are privacy policies reviewed on an annual basis?

- **Enterprise/Operational Risk Management**
  - Does the organization have enterprise/operational risk management (ERM/ORM) frameworks?
  - Does the organization have ERM/ORM policies and procedures?
  - Does the Chief Risk Officer (CRO), Operational and/or Enterprise Risk Manager review the ERM/ORM policies and procedures?
  - How often are the ERM/ORM policies and procedures reviewed?
  - Are ERM/ORM policies and procedures reviewed on an annual basis?
  - Is the ERM framework based on and internationally recognized standard (i.e. COSO Framework or ISO 30001)?

**The questions above do not represent the full list of documents required from the vendor, supplier or third-party. Please work with the information security, privacy and third-party risk departments to determine if further questions or documentation are required.*

Information Security Risk Assessment

- To perform the third-party risk assessment, the third-party should answer the following questions:

- **Vendor, Supplier or Third-Party Risk Management**
  - Does the organization outsource key business processes and functions to vendors, suppliers or third-parties ?
  - Does the organization have vendor, supplier or third-party risk policies and procedures?
  - Does the Chief Risk Officer (CRO), Operational and/or Enterprise Risk Manager, or Procurement Manager review the vendor, supplier or third-party risk management policies and procedures?
  - How often are the vendor, supplier or third-party risk management policies and procedures reviewed?
  - Are the vendor, supplier or third-party risk management policies and procedures reviewed on an annual basis?
  - Is the organization subject to OCC 2013-29 regulations?
  - Does the organization perform risk assessments on vendors, suppliers or third-parties?
  - Does the organization execute and maintain contracts with vendors, suppliers or third-parties?
  - Do contracts contain right-to-audit language that grants the organization permission to perform audits on vendors, suppliers or third-parties?
    - *Have the vendor, supplier or third-party provide a copy of the right-to-audit language if possible.*
  - Do contracts contain information security language that require vendors, suppliers and third-parties to maintain specific information security standards
    - *Have the vendor, supplier or third-party provide a copy of the information security language if possible.*
  - Do contracts contain information security language that require vendors, suppliers and third-parties to maintain specific business continuity and disaster recovery standards?
  - Does the organization require vendors, suppliers and third-parties to sign non-disclosure agreements (NDAs) and confidentiality agreements in order to protect company confidential information?

**The questions above do not represent the full list of documents required from the vendor, supplier or third-party. Please work with the information security, privacy and third-party risk departments to determine if further questions or documentation are required.*

Information Security Risk Assessment

- To perform the third-party risk assessment, the third-party should answer the following questions:

- **Asset Management**
  - Does the organization have asset management policies and procedures that ensure that hardware and software assets utilized during the information life cycle are properly identified and classified?
  - Does the Chief Technology Officer (CTO), Chief Information Security Officer (CISO), or Information Security Manager review the asset management policies and procedures?
  - Who in the organization is responsible for reviewing the asset management policies and procedures?
  - How often are the asset management policies and procedures reviewed?
  - Are asset management policies and procedures reviewed on annual basis?
  - Does there exist an information classification scheme for hardware and software assets?
  - Does there exist an inventory system for hardware and software assets?

- **Human Resources Security**
  - Does the organization have human resources policies and procedures that employees and contingent workers
  - Does the Chief Technology Officer (CTO), Chief Information Security Officer (CISO), Information Security Manager, review the human resources security policies and procedures?
  - Does human resources review the human resources security policies and procedures?
  - How often are the human resources security policies and procedures reviewed?
  - Are human resources security policies and procedures reviewed on annual basis?
  - Are employees and contingent workers required to undergo information security training?
  - How often are employees and contingent workers to complete information security training?
  - Are employees and contingent workers required to complete information security training on annual basis?
  - Are employees and contingent workers required to undergo privacy training?
  - How often are employees and contingent workers to complete privacy training?
  - Are employees and contingent workers required to complete privacy training on annual basis?

**The questions above do not represent the full list of documents required from the vendor, supplier or third-party. Please work with the information security, privacy and third-party risk departments to determine if further questions or documentation are required.*

Information Security Risk Assessment

- To perform the third-party risk assessment, the third-party should answer the following questions:

- **Human Resources Security (Cont)**
  - Are employees and contingent workers required to undergo background checks prior to accessing company networks and systems?
  - Are employees and contingent workers required to sign the following agreements below as part of the on boarding process?
    - Non-disclosure Agreement (NDAs)
    - Confidentiality Agreement
    - Code of Conduct/Ethics
  - Are employees and contingent workers subject to disciplinary action due to non-compliance with information security policies and procedures?
  - Does there exist a process to ensure that when the employment status of an employee or contingent worker changes, human resources notifies information security?
  - How often does information security review the "change of status/termination" process on an annual basis?
  - Are employees and contingent workers requires to return all company hardware and software assets (i.e. computers, laptops, PDAs,) as part of the termination process?

- **Physical and Environmental Security (Operating Facility)**
  - Does the organization have physical and environmental policies and procedures to prevent the unauthorized physical access and damage to the information and information processing facilities of the organization?
  - Does the Chief Technology Officer (CTO), Chief Information Security Officer (CISO), or information Security Manager review the physical and environmental policies and procedures?
  - Who in the organization is responsible for reviewing physical and environmental policies and procedures?
  - How often are the physical and environmental policies and procedures reviewed?
  - Are physical and environmental policies and procedures reviewed on annual basis?
  - Does the operating facility have a defined security perimeter?
  - Does the organization require employees and contingent workers to use scan cards, biometric scans, keys to enter the building?
  - Does the data center have a process to report stolen scan cards, keys to the appropriate personnel?
  - Does the organization require visitors to sign-in and out?
  - Does the organization require visitors to wear badges that distinguish them form employees and contingent workers?
  - Does the organization escort visitors through secure areas?
  - Are visitor logs kept for at least 90 days?
  - How long are visitor logs maintained?
  - Does the premise have a defined security perimeter?
  - Does the premise have security guards that at points of entry?
  - Does the premise have entry and exit door alarms or monitored by security guards?
  - Does the premise have CCTV with video?
  - Is CCTV video stored for 90 days?
  - How long is CCTV video stored?
  - Does the premise have heat detection?
  - Does the premise have smoke detection?
  - Does the premise have a monitored fire alarm system?
  - Does the premise have a fire suppression (i.e. dry, chemical, wet pipe)system?
  - Are access logs reviewed on a semi-annual basis?
  - How often are access logs reviewed?
  - Does the organization have procedures and mechanism to avoid tailgaiting/piggybacking into the operating facility?
  - Does the operating facility have generators?
  - Does the generator have the capability to supply power for at least 48 hours?

**The questions above do not represent the full list of documents required from the vendor, supplier or third-party. Please work with the information security, privacy and third-party risk departments to determine if further questions or documentation are required.*

Information Security Risk Assessment

- To perform the third-party risk assessment, the third-party should answer the following questions:

- **Physical and Environmental Security (Data Center)**
  - Does the data center have a defined security perimeter?
  - Does the data center require employees and contingent workers to use scan cards, biometric scans, keys to enter the data center?
  - Does the data center have a process to report stolen scan cards, keys to the appropriate personnel?
  - Does the data center require visitors to sign-in and out?
  - Does the data center require visitors to wear badges that distinguish them form employees and contingent workers?
  - Does the data center escort visitors through secure areas?
  - Are visitor logs kept for at least 90 days?
  - How long are visitor logs maintained?
  - Does the premise have security guards that at points-of-entry?
  - Does the premise have entry and exit door alarms or monitored by security guards?
  - Does the premise have CCTV with video?
  - Is CCTV video stored for 90 days?
  - How long is CCTV video stored?
  - Does the premise have heat detection?
  - Does the premise have smoke detection?
  - Does the premise have a monitored fire alarm system?
  - Does the premise have a fire suppression (i.e. dry, chemical, wet pipe) system?
  - Are access logs reviewed on a semi-annual basis?
  - How often are access logs reviewed?
  - Does the data center have procedures and mechanism to avoid tailgating/piggybacking into the operating facility?
  - Does the operating data center have generators?
  - Does the generator have the capability to supply power for at least 48 hours?

**The questions above do not represent the full list of documents required from the vendor, supplier or third-party. Please work with the information security, privacy and third-party risk departments to determine if further questions or documentation are required.*

Information Security Risk Assessment

- To perform the third-party risk assessment, the third-party should answer the following questions:

- **Network, Operations and Communication Management**
  - Does the organization have change management policies and procedures?
  - Who in organization is responsible for reviewing the change management policies and procedures?
  - How often are change management policies and procedures reviewed?
  - Are change management policies and procedures reviewed on an annual basis?
  - Does the organization have data loss prevention system?
  - Does the organization have an anti-virus/malware policy or program?
  - Does the organization have a backup policy or process?
  - Is the backup policy and process tested annually?
  - How often is the process tested?
    - Does the organization store backups?
    - Does organization store backup media offsite?
    - When stored offsite, does the organization have a process to ensure that data stored offsite is transported securely, that shipments are tracked and that there exists verification that data received by the appropriate parties?
  - Does the organization utilize firewalls for internal and external connections?
  - Are connections to external networks terminated at a firewall?
  - Are firewall used to segment internal networks?
  - Does the organization perform vulnerability assessments, scans and penetration tests on internal and external networks on an annual basis?
    - Are risks ranked for importance to the system for internal and external networks?
    - Are vulnerabilities identified for internal and external networks?
    - Are risks documented and tracked to remediation for internal and external networks?
  - Does the organization have wireless networking policies and procedures?
  - Who is responsible for approving wireless networking policies and procedures?
  - How often are wireless networking policies and procedures reviewed?
  - Are wireless networking policies and procedures reviewed annually?
  - Is split-tunneling allowed?
  - Does the organization utilize multi-factor authentication to authenticate wireless connections?
  - Does the organization utilize encryption that is WPA2 or higher for wireless networking technology?
  - Are wireless access points SNMP community strings changed?
  - Are quarterly scans performed for rogue wireless access points?
  - Does the organization have removable media policies and procedures?
  - Who is responsible for reviewing the removable media policies and procedures?
  - How often are removable policies and procedures reviewed?
  - Are removable policies and procedures reviewed on an annual basis?

*The questions above do not represent the full list of documents required from the vendor, supplier or third-party. Please work with the information security, privacy and third-party risk departments to determine if further questions or documentation are required.

Information Security Risk Assessment

- To perform the third-party risk assessment, the third-party should answer the following questions:

- **Network, Operations and Communication Management**
    - Are emails encrypted?
    - Does the organization utilize intrusion detection/prevention systems within its networks?
    - Does there exist external network connections (i.e. internet, intranet, extranet)?
    - Does organization review and monitor of network devices for compliance to security requirements?

*The questions above do not represent the full list of documents required from the vendor, supplier or third-party. Please work with the information security, privacy and third-party risk departments to determine if further questions or documentation are required.

Information Security Risk Assessment

- To perform the third-party risk assessment, the third-party should answer the following questions:

- **Access Controls**
  - Does the organization have documented access control policies and procedures?
  - Are access control policies and procedures reviewed and updated once a year?
  - Who is responsible for reviewing the access controls policies and procedures?
  - Is user access to networks and systems based on job duties?
  - Does the organization discourage the sharing of user IDs and passwords to gain access to networks and systems?
  - Does the organization require that access to networks and systems undergo a request and an approval process?
  - Are user access rights reviewed every 90 days?
  - How long does it take for a workstation to lock when inactive?
  - Does the organization have a password management policies and procedures?
  - Does the organization require that employees and contingent workers utilize complex password schemes?
  - Are employees and contingent workers required to change passwords every 90 days?
  - Are employees and contingent workers required to change default and temporary passwords to unique passwords using complex password schemes?
  - Are employees and contingent workers required to change passwords when a system interruption occurs that compromises user access?
  - Does the organization have remote access policies and procedures?
  - Who reviews, updates and approves the remote access policies and procedures?
  - Are the remote access policies and procedures reviewed and updated annually?
  - Does the organization use multi-factor authentication when accessing company network onsite and remotely?
  - Does the organization use FIPS 140-2 encryption methods for all onsite and remote connections?
  - Does the organization allow non-company devices to connect to company devices to access networks and systems onsite and remotely?
  - Does the organization allow onsite and remote users to connect to company network and systems using personal equipment?
  - Are employees and contingent worker user IDs deleted from user access logs after 90 days of termination?

*The questions above do not represent the full list of documents required from the vendor, supplier or third-party. Please work with the information security, privacy and third-party risk departments to determine if further questions or documentation are required.

Information Security Risk Assessment

- To perform the third-party risk assessment, the third-party should answer the following questions:

- **Access Controls**
  - Does the organization have documented access control policies and procedures?
  - Are access control policies and procedures reviewed and updated once a year?
  - Who is responsible for reviewing the access controls policies and procedures?
  - Is user access to networks and systems based on job duties?
  - Does the organization discourage the sharing of user IDs and passwords to gain access to networks and systems?
  - Does the organization require that access to networks and systems undergo a request and an approval process?
  - Are user access rights reviewed every 90 days?
  - How long does it take for a workstation to lock when inactive?
  - Does the organization have password management policies and procedures?
  - Does the organization require that employees and contingent workers utilize complex password schemes?
  - Are employees and contingent workers required to change passwords every 90 days?
  - Are employees and contingent workers required to change default and temporary passwords to unique passwords using complex password schemes?
  - Are employees and contingent workers required to change passwords when a system interruption occurs that compromises user access?
  - Does the organization have remote access policies and procedures?
  - Who reviews, updates and approves the remote access policies and procedures?
  - Are the remote access policies and procedures reviewed and updated annually?
  - Does the organization use multi-factor authentication when accessing company network onsite and remotely?
  - Does the organization use FIPS 140-2 encryption methods for all onsite and remote connections?
  - Does the organization allow non-company devices to connect to company devices to access networks and systems onsite and remotely?
  - Does the organization allow onsite and remote users to connect to company network and systems using personal equipment?
  - Are employees and contingent worker user IDs deleted from user access logs after 90 days of termination?

*The questions above do not represent the full list of documents required from the vendor, supplier or third-party. Please work with the information security, privacy and third-party risk departments to determine if further questions or documentation are required.

Information Security Risk Assessment

- To perform the third-party risk assessment, the third-party should answer the following questions:

- **Systems Development, Acquisition and Maintenance**
  - Are business information systems used to transmit, process or store systems and data?
  - Does organization engage in application development?
    - Does the organization have an authenticated and maintained state for every data transaction?
    - Does the organization have a process of secure session management?
    - Does the organization have a comprehensive secure error handling process?
    - Does the system generate audit log failures and alerts?
    - Are the application development, testing and staging environment separate from production environment?
    - Does there exist a formal software development lifecycle (SDLC) process?
    - Are change control procedures required for all changes to the production environment?
    - Is scoped system and data used in the testing, development or QA environment?
      - Does there exist an approval process when production data is is used in the testing environment?
      - Are developers allowed to access production environments including read-only access?
      - Are developers allowed to access systems and applications based on profiles that define responsibilities or job functions?
      - Are developers allowed to request or gain access to a role outside of what is allowed for emergency purposes?
    - Are system, vendor, or service accounts disallowed for normal operations and monitored for usage?
    - Prior to implementation, do applications go through a risk assessment and approval process by information or cybersecurity?
    - Do systems and applications undergo a patch management process?
      - Does the patch management process include evaluating, accessing and prioritizing vulnerabilities?
      - Do high-risk systems undergo patching first before other medium and low-risk systems?
    - Does the organization have a website?
      - Does the organization perform penetration tests on web-based applications?
  - Does the organization encrypt data-at-rest?
  - Does it encrypt data-in-transit?
  - Does the organization encrypt data-in-storage?

*The questions above do not represent the full list of documents required from the vendor, supplier or third-party. Please work with the information security, privacy and third-party risk departments to determine if further questions or documentation are required.

Information Security Risk Assessment

- To perform the third-party risk assessment, the third-party should answer the following questions:

- **Mobile**
  - Does the organization allow employees and contingent workers to access company networks and systems using their personal mobile devices?
  - Does the organization provide company mobile devices to employees and contingent workers?
  - Does the organization allow employees and contingent workers to access company networks and systems using company mobile devices?
  - Does there exist policies and procedures for mobile devices?
  - How often are policies and procedures for mobile devices reviewed?
  - Are policies and procedures for mobile devices reviewed on annual basis?
  - Who is responsible for reviewing policies and procedures for mobile devices?
  - Does the organization have a process for the mobile device life cycle?
  - Does the organization review mobile devices as part of its IT Risk Management Program?
  - Does the organization require employees and contingent workers to sign legal documentation which outline their rights and responsibilities regarding the mobile devices?
  - In the event of a data breach, does the organization perform the following actions?
    - Remotely wipe the mobile device?
    - Remotely access data on the mobile device?
  - Can the organization view scoped data and systems from the mobile device directly?
  - Is access to scoped data limited to a clean room?

*The questions above do not represent the full list of documents required from the vendor, supplier or third-party. Please work with the information security, privacy and third-party risk departments to determine if further questions or documentation are required.

Information Security Risk Assessment

- To perform the third-party risk assessment, the third-party should answer the following questions:

- **Incident Event and Notification Management**
  - Does the organization have an incident event and notification management program?
  - Does the organization have a documented incident event and notification management policies and procedures?
  - Does the organization have a formal incident response plan?
  - Does the information security and privacy training include incident event and notification management for employees and contingent workers?

- **Software Security**
  - Does the organization provide software to its client?
  - If yes, does the organization use the Software Developer Lifecycle (SDLC) to create and maintain software?
  - If yes, does the organization have software development lifecycle policies and procedures?
  - Does the organization review secured code?
  - If yes, how often is secured code reviewed?
  - Does the organization have a QA_UAT process?
  - Does the organization perform full secure code reviews for each release?
  - Does the organization monitor hosted production applications for vulnerabilities?
  - Does the organization review third-party code before releasing to production?
  - Are applications tested to determine vulnerabilities against attacks?

*The questions above do not represent the full list of documents required from the vendor, supplier or third-party. Please work with the information security, privacy and third-party risk departments to determine if further questions or documentation are required.

Information Security Risk Assessment

- To perform the third-party risk assessment, the third-party should answer the following questions:

- **Other**
    - Does the organization provide products and services in the cloud?
    - Is the cloud private, public or hybrid?

*The questions above do not represent the full list of documents required from the vendor, supplier or third-party. Please work with the information security, privacy and third-party risk departments to determine if further questions or documentation are required.

very strong income performance well ahead of prior year
Projected sales of main products in 2013
Distribution marketing participation in the securities market.
Share of market activity
Distribution of the securities market key players
Revenue growth divisions
TYU division
FRT division
Analysis of total income
Final Sales
Sales by Category
Passive market share
DAT
BID
ASK
PRO
QUA

Appendix B: List of Vendor Risk Management Tools

List of Vendor Risk Management Tools

- Please refer to the list of tool below

Name of Tool	Description	Website
Prevalent	Vendor Risk Management Tool	www.prevalent.com
ProcessUnity	Vendor Risk Management Tool	www.processunity.com
Hiperos	Governance, Risk and Control Tool	www.hiperos.com
MetricStream	Governance, Risk and Control Tool	www.metricstream.com
Rapid Ratings	Financial Risk Tool	www.rapidratings.com
LexisNexis	Reputational Risk Tool	www.lexisnexis.com
Factiva	Reputational Risk Tool	www.factiva.com
Thomson Reuters	Reputational Risk Tool	www.thomsonreuters.com