



**BITS VENDOR MANAGEMENT
RISK ASSESSMENT SURVEY
EXECUTIVE SUMMARY**

BITS
1001 PENNSYLVANIA AVENUE, NW
SUITE 500 SOUTH
WASHINGTON, DC 20004
202-289-4322
WWW.BITS.ORG

TABLE OF CONTENTS

INTRODUCTION..... 2

SURVEY METHODOLOGY 3

KEY FINDINGS 4

Tiering..... 4

Due Diligence and Ongoing Monitoring Assessments..... 4

Resource Allocation..... 6

IMPLICATIONS 7

Areas of consensus 7

Areas for consideration 8

APPENDIX 1: SURVEY QUESTION RESPONSE ANALYSIS 9

Tiering Questions..... 9

Assessment Questions 11

Ongoing Monitoring Questions..... 15

Resource Allocation Questions 17

APPENDIX 2: SURVEY QUESTION RESPONSE DETAIL..... 18

Tiering Questions..... 18

Ongoing Monitoring Questions..... 48

Resource Allocation Questions 53

APPENDIX 3: SURVEY DEFINITIONS 56

APPENDIX 4: SHARED DOCUMENTS..... 57

INTRODUCTION

Financial institutions are utilizing ever more vendor relationships to expedite product offerings, leverage industry expertise and best practices, concentrate internal resources on core businesses, and reduce costs. The demands associated with managing these relationships are driven by industry best practices as well as a variety of regulatory requirements. However, each financial institution has unique business environments and risk profiles. The vendor risk assessment practices for each financial institution reflect the complexity of their own vendor activities, the materiality of related risks, and the financial institution's ability to manage those risks. As a result, vendor risk assessment practices vary by financial institution, though there may be elements of their risk assessment practices that are similar.

The intent of this survey is to identify how financial institutions have implemented vendor risk assessment practices, to evaluate where the industry may be able to leverage similar practices, and to highlight practices that may be more appropriately customized to individual financial institution needs.

SURVEY METHODOLOGY

The online survey was anonymous and distributed to all members of the BITS Vendor Management Working Group. It was developed by a team of BITS Vendor Management Working Group members. The survey focuses on vendor tiering practices, risk assessment practices, and resource allocation. The table below provides an overview of the survey sections and how many questions comprised each section.

Survey Section	Number of Questions
Tiering Questions	12
Assessment Questions	24
Ongoing Monitoring Questions	7
Resource Allocation Questions	3

A total of nineteen financial institutions responded to the survey, although the number of respondents to individual questions varies as some respondents skipped questions. Percentages provided within the analysis were determined based on the number of respondents who answered the relevant question.

Key findings from the survey are summarized in the following section of this document. Additionally, more detailed information is provided in the appendices of this document.

Appendix	Content Description
APPENDIX 1: SURVEY QUESTION RESPONSE ANALYSIS	A detailed question by question analysis of the survey results
APPENDIX 2: SURVEY QUESTION RESPONSE DETAIL	Question by question detailed responses presented in bar or pie charts and detailed respondent comments where provided
APPENDIX 3: SURVEY DEFINITIONS	Definitions for terms used within the survey including: Risk Assessment, Due Diligence and Ongoing Monitoring

KEY FINDINGS

Tiering

Financial institutions typically stratify their vendor population into tiers based on risk and other factors. Half of survey respondents use four or more tiers to stratify their vendor population (Question 11). The breadth, depth, and frequency of review requirements are based on the level of risk (i.e., tier). Higher risk tiers have greater review requirements and may be assessed as frequently as every six months to one year.

More than three quarters of survey respondents use some form of limited risk assessment to determine what vendor population requires further analysis (Question 5). Approximately half of the survey respondents evaluate all tiers and/or services, while others will exclude certain vendors from the assessment process based on low inherent risk. Factors indicating a low inherent risk may include lack of sensitive or confidential data, non-mission critical services, or the ability to easily replace the service (Question 10). Personal Information (PI) or Non-Public Personal Information (NPPI) is the most prevalent factor used to evaluate risk. Other key factors used by the majority of the survey respondents, listed in descending order of use include: legal/regulatory compliance, information classification, business resiliency, cost for products/services, financial viability, operations, and country risk (Question 2). The identification of control issues or gaps for a vendor directly impacts the risk assessment and changes the frequency of due diligence and ongoing monitoring for approximately half of the respondents (Question 3).

The majority of survey respondents assess vendors against the tiers at least annually (Question 6) and also re-evaluate the overall tiering process annually (Question 8). Additionally, most respondents re-assess a vendor against the tiers when there are changes to the related product or service (Question 7).

There does not appear to be a consensus for the level of a vendor relationship for which a risk assessment should be completed. Some organizations complete a risk assessment for each product or service provided, while others complete a risk assessment based on the vendor's overall relationship. Only one-quarter of the respondents complete a risk assessment at both levels of the vendor relationship (Question 12).

In addition to tiering vendors by risk, one-third of the survey respondents tier vendors by services/commodities (e.g., office supplies, temporary staffing, software services, IT infrastructure, printing services). Another one-third of the survey respondents do not tier by services/commodities (Question 1).

Due Diligence and Ongoing Monitoring Assessments

All review activities included in the survey are performed by the majority of the respondents (typically based on the tier or level of risk). These review activities, listed in descending order of performance include: contract reviews, security breaches and incidents, on-site reviews, resiliency/pandemic preparedness reviews, relationship management meetings, financial condition,

questionnaires/surveys, Service Level Agreement (SLA) reviews, invoice reviews, and vendor management scorecards (Question 13).

Questionnaires/surveys provide the most value for three-quarters of survey respondents. Other assessment activities identified by more than half of the respondents as providing the most value include: on-site reviews, relationship management meetings, and SLA reviews (Questions 29 and 30).

The majority of the survey respondents use some form of risk analysis to determine which vendors are subject to site visits, and only the highest risk vendors require a site visit (Question 39). The following specific control areas are assessed during a site visit by more than half of the survey respondents, listed in descending order of performance: Physical and environmental security, resiliency, backup and offsite storage, encryption, policies and standards, network communications, logical access, monitoring, operations, change control, application and development, incident response, subcontractors, asset management, and standard builds (Question 41).

Almost two-thirds of survey respondents involve Audit or a corporate group (e.g., Corporate IT Risk, Corporate Security, Corporate Information Security, or Enterprise Research) in conducting site visits (Question 43).

A majority of survey respondents spend more than ten percent of the entire review process to clarify a vendor's response to questions. One-sixth of the respondents spend more than half of their time clarifying responses to questions (Question 16).

Almost eighty-five percent of survey respondents assign a score to indicate the level of risk associated with their vendors (Question 24), although almost half of the respondents have not developed or purchased a risk scoring tool/software to assist in determining the level of risk associated with their vendors (Question 25).

Most survey respondents at least sometimes validate information provided by the vendors in questionnaires, but only one-sixth of the respondents always validate information provided by vendors (Question 14). The most common validation method is to obtain copies of documentation from the vendor or to review documentation while on-site with the vendor (Question 15).

Almost two-thirds of survey respondents complete a risk acceptance/exception for vendors who refuse to complete due diligence or ongoing monitoring activities. Most of these respondents automatically rate these vendors as high risk and attempt to get additional control related information through alternate means such as third party reviews or internal controls (Question 18). The majority of respondents approve the risk acceptance/exception at the business level, and document and report the risk acceptance/exception at the corporate level (Question 19 and 20).

A majority of survey respondents follow-up with the vendor to address issues and concerns identified outside of the normal review process (e.g., security breaches, incidents). Less than one-quarter of the respondents may perform an out-of-cycle review (Question 23).

There does not appear to be a consensus related to the level of the assessment for initial due diligence versus ongoing monitoring. Some organizations indicated both assessments are consistent, while others indicated the initial due diligence assessment is more robust (Question 37).

All of the survey respondents will accept a SAS 70 Type II review in lieu of their company's assessment, though supplemental work may need to be performed depending on the scope of the review. Additionally, more than half of the respondents will accept a BITS Shared Assessment SIG/AUP or ISO 27001/27002 review (Question 22).

Half of survey respondents indicated that vendor management tracking and reporting is performed through both, central governance and reporting, as well as line of business governance and reporting. When not performed both centrally and by line of business, most respondents perform central governance and reporting (Question 34). Management reporting generated by more than half of the respondents include: high risk issues, compliance with review requirements, and risk by vendor (Question 35). Half of respondents perform vendor management reporting on a quarterly basis and another one-quarter report on a monthly basis (Question 36).

Forty percent of the survey respondents that perform site reviews did not or were not able to identify the average cost and how many hours are typically spent at the vendor's site for an on-site review. Of those who identified the cost of vendor reviews, the cost ranged between \$1,000 and \$25,000. The average on-site review time ranged between eight hours and twenty-four hours (Questions 40 and 42).

Resource Allocation

All but two of the survey respondents indicated that twenty or fewer Full Time Equivalents (FTEs) are aligned with performing and evaluating risk assessments (Question 45). Almost two-thirds of the respondents have dedicated resources for performing and evaluating risk assessments (Question 46).

The largest portion of the survey respondents, forty-seven percent, indicated that business relationship management typically participates in an on-site visit. The next most prevalent response, forty-one percent, was Corporate Security (Question 44).

IMPLICATIONS

Areas of consensus

This survey identified various areas of consensus related to the vendor risk assessment process. Those areas where more than half of the survey respondents agreed are identified below.

- Vendor stratification (i.e., tiers) is based on risk (Question 11).
- Limited initial risk assessments determine the level of analysis required (Question 5).
- Key risk assessment factors include: Personal Information (PI) or Non-Public Personal Information (NPPI), legal/regulatory compliance; information classification; business resiliency, cost for products/services, financial viability, operations, and offshoring/country risk (Question 2).
- Residual risk (i.e., issues identified) changes the assessment frequency (Question 3).
- Annual risk assessments are performed (Question 6).
- Annual tier rationalization is performed (Question 8).
- Re-assessments are required when there are changes to a product/service (Question 7).
- Key due diligence/ongoing monitoring activities include: contract reviews, security breaches and incidents, on-site reviews, resiliency/pandemic preparedness reviews, relationship management meetings, financial condition, questionnaires/surveys, Service Level Agreement (SLA) reviews, invoice reviews, and vendor management scorecards (Question 13).
- Most valuable assessment activities include: Questionnaires/surveys, on-site reviews, relationship management meetings, and SLA reviews (Questions 29 and 30).
- Site visits are required for high risk vendors (Question 39).
- Control areas evaluated during site visits include: Physical and environmental security, resiliency, backup and offsite storage, encryption, policies and standards, network communications, logical access, monitoring, operations, change control, application and development, incident response, subcontractors, asset management, and standard builds (Question 41).
- Corporate groups are involved in site visits (Question 43).
- Clarifying vendor responses to questionnaires is time consuming (Question 16).
- Risk scores are assigned to vendors (Question 24).
- Controls are sometimes validated (Question 14).
- Vendors who refuse to be reviewed require a risk acceptance/exception (Question 18).
- Exceptions are approved by the business (Question 19).
- Exceptions are documented and reported by corporate (Question 20).
- Off-cycle issues require follow-up with the vendor (Question 23).
- SAS 70 Type II reviews (supplemental work may be performed), BITS Shared Assessment SIG/AUP, and ISO 27001/27002 reviews are accepted in lieu of proprietary assessments (Question 22).
- Vendor management tracking and reporting is performed through both central and line of business governance and reporting (Question 34).
- Vendor management reporting is done on a quarterly basis (Question 36).

Areas for consideration

Based on the responses to the survey questions, the following areas have been identified as possibly requiring additional research or understanding to add value to the BITS membership. As a result, the BITS Vendor Management Working Group will be evaluating these topics for potential future activities.

- Vendor stratification (i.e., tiering) by services/commodities may represent a way to identify and perform appropriate limited assessment activities (Question 1)
- The impact and probability associated with risk assessment risk factors often only has a subjective influence on the level of risk. There may be opportunities to explore how to apply an explicit impact on the level of risk (Question 4)
- Limited risk assessments are used to determine what vendor population requires further analysis. This survey did not explore what factors are typically evaluated within the limited risk assessment (Question 5).
- There was no consensus on which level of a vendor relationship a risk assessment is completed; based on each specific product/service, the overall vendor relationship, or both (Question 12).
- There may be opportunities to explore process enhancements that may help reduce the time required to clarify responses to questionnaires (Question 16).
- There may be opportunities to standardize a process and the number of attempts to reach out to a vendor to complete due diligence or ongoing monitoring before taking alternate actions (Question 17).
- There may be opportunities to standardize how to determine when it is appropriate to perform an out-of-cycle review (Question 23).
- While most institutions seem to be scoring the level of risk associated with vendors, there does not appear to be any standard process or tool in use (Question 24 and 25).
- Performance metrics do not appear to be a standard part of the risk assessment process. However, they may have a substantial impact on the overall vendor risk profile (Question 26).
- Other than tiering, there does not appear to be a consensus on how the frequency and scope of due diligence and ongoing monitoring should be scaled (e.g., residual risk, relationship history, vendor reputation) (Question 27).
- While the survey respondents indicated that they have a way to measure the more subjective risks such as strategic risk, credit risk, transaction risk, and reputation risk, this survey did not explore the detail associated with measuring those risks (Question 33).
- The survey responses indicated that quarterly reporting was performed. The survey did not explore the type of reporting performed on a quarterly basis versus the reporting performed on a monthly basis (Question 36).
- There was no consensus on the level of assessment activities performed for initial due diligence versus ongoing monitoring. There may be opportunities to identify best practices in this area, including the appropriateness of sharing prior responses to assessments (Question 37).

APPENDIX 1: SURVEY QUESTION RESPONSE ANALYSIS

Tiering Questions

Q1 – In addition to tiering vendors by risk, some institutions may tier vendors by services/commodities (e.g., office supplies, temporary staffing, software services, IT infrastructure, printing services) based on the associated risk. Select all that apply:

- 6 of 18 (33.3%) survey respondents do not tier by services/commodities.
- 6 of 18 (33.3%) survey respondents tier by services/commodities and by risk.
- 8 of 18 (44.4%) survey respondents tier based on the risk associated with the vendor relationship.

Q2 – What factors are used to establish tiers/risk categories? Select all that apply:

- 17 of 18 (94.4%) survey respondents use Personal Information or Non-Public Personal Information (NPPI) as a factor to evaluate risk associated with vendors.
- The following factors were used by more than 50% of the survey respondents:
 - Personal Information or NPPI (17 of 18 or 94.4%);
 - Legal/Regulatory Compliance (16 of 18 or 88.9%);
 - Information Classification (16 of 18 or 88.9%);
 - Business Resiliency (15 of 18 or 83.3%);
 - Cost for products/services (12 of 18 or 66.7%);
 - Financial viability (11 of 18 or 61.1%);
 - Operations (11 of 18 or 61.1%); and
 - Offshoring/country or geographic location (10 of 18 or 55.6%).

Q3 – How does the implementation of controls and identification of related control issues/gaps impact the risk assessment process?

- 9 of 19 (47.4%) survey respondents indicated that control implementation and related issues directly impact the risk assessment process. This includes two survey respondents who indicated that the control implementation and related issues would impact both the risk assessment and change the frequency of review activities.
- 10 of 19 (52.6%) survey respondents indicated that control implementation and related issues change the frequency of due diligence and ongoing monitoring. This includes two survey respondents who indicated that the control implementation and related issues would impact both the risk assessment and change the frequency of review activities.

Q4 – Is the impact and probability of risk factors included in the risk assessment?

- 10 of 18 (55.6%) survey respondents indicated that the impact and probability of at least some risk factors have an explicit impact on the risk assessment.
- 4 of 18 (22.2%) survey respondents indicated that the impact and probability of risk factors have a subjective impact on the risk assessment.

Q5 – How do you determine the population of vendors for which a risk assessment must be performed?

- 4 of 19 (21.1%) survey respondents require a complete risk assessment for all vendors.

- 15 of 19 (78.9%) survey respondents require some form of limited risk assessment to determine what vendor population requires further analysis. The risk assessment may include the service provider's ability to handle confidential or personal information, or to provide mission critical services.

Q6 – How often are the vendors reassessed against the tiers?

- 12 of 19 (63.2%) survey respondents reassess vendors against the tiers at least annually.

Q7 – In addition to the standard frequency identified above, is risk reassessed when there are changes to the product/service?

- 17 of 19 (89.5%) survey respondents indicated that, in addition to the standard reassessment frequency, vendors are reassessed against the tiers when there are changes to the product/service.

Q8 – How often does your company reevaluate the overall tiering process (e.g., factors/criteria associated with the tiers)?

- 15 of 19 (78.9%) survey respondents reevaluate the overall tiering process annually.

Q9 – If evaluating services/commodities based on risk, how often is risk evaluated for each commodity?

- 8 of 10 (80%) of survey respondents that evaluate the risk associated with commodities, reevaluate the risk for each commodity annually.

Q10 – Are there certain tiers or services that are not evaluated?

- 10 of 19 (52.6%) survey respondents indicate that all tiers and/or services are evaluated. Those respondents who indicated there are tiers and/or services that are not evaluated generally highlighted the lack of sensitive or confidential data related to the service, non-mission critical services or the ability to easily replace the service as the reason that no assessment is performed.

Q11 – Please describe the number of tiers your institution uses and what due diligence/ongoing monitoring requirements are associated with each tier (include any impact on frequency and scope of reviews).

- 7 of 16 (43.8%) respondents use 5 or more tiers.
- 1 of 16 (6.3%) respondent uses 4 tiers.
- 5 of 16 (31.3%) respondent uses 3 tiers.
- 1 of 16 (6.3%) respondent uses 2 tiers.
- 2 of 16 (12.5%) respondents do not use tiers.
- The breadth, depth, and frequency of various requirements are based on the level of risk (i.e., tier). Higher risk tiers have greater review requirements and may be required as frequently as every 6 months to 1 year. Lower risk tiers have no or limited review requirements.

Q12 – At what level of a vendor relationship does your institution complete a risk assessment?

- 6 of 19 (31.6%) survey respondents complete a risk assessment for each product/service provided.

- 7 of 19 (36.8%) survey respondents complete a risk assessment based on a vendor's overall relationship.
- 5 of 19 (26.3%) survey respondents complete a risk assessment for both each product/service provided and based on a vendor's overall relationship.

Assessment Questions

Q13 – What review activities are included in the due diligence/ongoing monitoring process? How are these functions performed? Please respond to all that apply.

- 17 of 17 (100%) survey respondents perform contract reviews.
- The following were performed by more than 75% of the survey respondents:
 - Contract reviews (17 of 17 or 100%);
 - Security breaches and incidents (16 of 17 or 94.1%);
 - On-site reviews (16 of 17 or 94.1%);
 - Resiliency / pandemic preparedness reviews (16 of 17 or 94.1%);
 - Relationship management meetings (16 of 17 or 94.1%);
 - Financial condition (16 of 17 or 94.1%);
 - Questionnaires/surveys (15 of 17 or 88.2%);
 - SLA reviews (15 of 17 or 88.2%);
 - Invoice reviews (15 of 17 or 88.2%); and
 - Vendor management scorecards (13 of 17 or 76.5%).
- Responsibility of the reviews and level of obligation (e.g., required versus discretionary) varies by respondent and type of review. Lines of Business (LOBs) may be responsible for the following types of reviews: on-site review; SLA review; relationship management; invoice review; and financial condition. Where the LOB is responsible for the review activity, consistency across LOBs may be a concern.

Q14 – To what extent is the information provided by vendors in questionnaires validated?

- 16 of 17 (94.1%) survey respondents at least sometimes validate information provided by vendors in questionnaires.
- 3 of 17 (17.6%) survey respondents always validate information provided by vendors in questionnaires.

Q15 – How do you validate the information provided by vendors in questionnaires? Select all that apply.

- 14 of 17 (82.4%) obtain copies of documentation to validate the information provided by vendors in questionnaires.
- The following methods are used to validate the information provided by vendors in questionnaires by more than 50% of the survey respondents:
 - Obtain copies of documentation (14 of 17 or 82.4%);
 - Review documentation while on-site (13 of 17 or 76.5%);
 - Observation (12 of 17 or 70.6%);
 - Interviews with personnel (12 of 17 or 70.6%); and
 - Process or data flow walk-through (10 of 17 or 58.8%).
- At least two of the respondents also indicated that they will leverage third party reviews to validate the information provided by vendors in questionnaires.

Q16 – When supplemental information is required to clarify a vendor’s response to a question, how much time is spent on vendor follow up relative to the entire review?

- 5 of 17 (29.4%) survey respondents spend more than 25% of the time related to the entire review process to clarify a vendor’s response to questions.
- 7 of 17 (41.2%) survey respondents spend less than 10% of the time related to the entire review process to clarify a vendor’s response to questions.

Q17 – How many times will you reach out to a vendor to complete due diligence or ongoing monitoring before you take alternate action?

- 15 of 17 (88.2%) survey respondents will reach out to a vendor 4 or fewer times to complete due diligence or ongoing monitoring before they take alternative actions.
- 2 of 17 (11.8%) survey respondents will reach out to a vendor more than 4 times to complete due diligence or ongoing monitoring before they take alternative actions.

Q18 – How are vendors who refuse to complete due diligence or ongoing monitoring activities handled? Select all that apply.

- 11 of 17 (64.7%) survey respondents will complete a risk acceptance/exception for vendors who refuse to complete due diligence or ongoing monitoring activities.
- 10 of 17 (58.8%) survey respondents will automatically rate a vendor high risk when vendors refuse to complete due diligence or ongoing monitoring activities.
- 10 of 17 (58.8%) survey respondents will try to get information through other means, such as third party reviews or related internal controls, for vendors who refuse to complete due diligence or ongoing monitoring activities.
- 6 of 17 (35.3%) survey respondents will terminate the relationship for vendors who refuse to complete due diligence or ongoing monitoring activities.
- 6 of 17 (35.3%) survey respondents will rely on the vendor’s requirement to comply with laws/regulations for vendors who refuse to complete due diligence or ongoing monitoring activities.

Q19 – How does the risk acceptance/exception process work when the internal business or vendor refuses to follow vendor review requirements? Select all that apply.

- A majority of survey respondents (13 vs. 8) approve the risk acceptance/exception at the business level when a vendor refused to complete due diligence or ongoing monitoring.
- A majority of survey respondents (13 vs. 6) document the risk acceptance/exception at the corporate level when a vendor refused to complete due diligence or ongoing monitoring.
- A majority of survey respondents (14 vs. 8) report the risk acceptance/exception at the corporate level when a vendor refused to complete due diligence or ongoing monitoring.

Q20 – Does issue acceptance (i.e., residual risk remaining after reviews) reside within the line of business and, if so, does a risk management governance and oversight function exist that reports risk acceptances to management?

- The majority of respondents indicate that acceptance of vendor related issues resides within the associated line of business, and governance reporting is in place to inform management.

Q21 – Are alternative assessments accepted in lieu of your institution’s control assessment?

- 4 of 17 (23.5%) survey respondents will not accept alternative assessments in lieu of their company’s assessment.
- 12 of 16 (70.6%) survey respondents will accept alternative assessments in lieu of their company’s assessment, indicating that supplemental work may be required based on the scope of the review.

Q22 – If you answered yes to the previous question, what types of reviews are accepted? Select all that apply.

- 100% of the respondents (15 of 15) will accept a SAS 70 Type II review (supplemental work may need to be performed) in lieu of their company’s assessment.
- The following types of reviews are accepted in lieu of their company’s assessment (supplemental work may need to be performed) by more than 50% of the survey respondents:
 - SAS 70 Type II (15 of 15 or 100%);
 - BITS Shared Assessment SIG (8 of 15 or 53.3%);
 - BITS Shared Assessment AUP (8 of 15 or 53.3%); and
 - ISO 27001/27002 (8 of 15 or 53.3%).

Q23 – How does your company address issues and concerns identified outside of the normal review process (e.g., security breaches, incidents)?

- The majority of respondents indicated they will follow up with the vendor to address issues and concerns identified outside of the normal review process (e.g., security breaches, incidents).
- 4 of 17 (23.5%) survey respondents indicated they may perform an out-of-cycle review of the vendor to evaluate controls subsequent to identification of issues and concerns outside of the normal review process.

Q24 – If your institution uses a “scorecard” to evaluate questionnaire and ongoing monitoring activity and assign a level of risk to the vendor, how is the overall risk scored?

- 11 of 13 (84.6%) survey respondents assign a score to the level of risk associated with their vendors.
- 7 of 13 (53.8%) survey respondents assign an objective overall score to their vendors based on a score to each question response.

Q25 – If your institution has developed or purchased a risk scoring software tool to help determine the level of risk, please indicate the vendor and tool or, if internally developed, describe.

- 7 of 15 (46.7%) survey respondents have not developed or purchased a risk scoring tool/software to assist in determining the level of risk associated with their vendors.
- Of the remaining respondents, 4 of 15 (26.7%) have developed their own risk scoring tool/software and the other 4 of 15 (26.7%) have purchased a risk scoring tool/software.
- 3 of 4 (75%) of respondents who purchased a risk scoring tool/software, have indicated they use an Archer solution.

Q26 – Are performance metrics (e.g., SLAs) included in your vendor risk assessment process?

- 9 of 17 (52.9%) survey respondents at least sometimes include performance metrics in their vendor risk assessment process.
- 8 of 17 (47.1%) survey respondents seldom or never include performance metrics in their vendor risk assessment process.

Q27 – Are the frequency and scope of the due diligence and ongoing monitoring scaled in any way beyond the tier assigned (e.g., residual risk, relationship history, vendor reputation)?

- 9 of 17 (52.9%) survey respondents at least sometimes use factors beyond the tiering process to define the frequency and scope of the due diligence and ongoing monitoring activities.
- 8 of 17 (47.1%) survey respondents seldom or never use factors beyond the tiering process to define the frequency and scope of the due diligence and ongoing monitoring activities.

Q28 – If programmers and consultants are not included in your third party service provider assessment process, what is the process for vetting contract programmers and consultants?

- 7 of 11 (63.6%) survey respondents indicated that programmers and consultants are not included in their third party service provider process (i.e., a separate vetting process exists for programmers and consultants).

Q29/30 – What specific vendor assessment activities have provided the most value? What about the items you selected above has made them most valuable?

- 13 of 17 (76.5%) survey respondents indicated that questionnaires/surveys (e.g., remote reviews) have provided the most value relative to vendor assessment activities.
- The following types of vendor assessment activities were identified as providing the most value by at least 47% of the survey respondents:
 - Questionnaires/surveys (12 of 17 or 76.5%);
 - On-site reviews (11 of 17 or 64.7%);
 - Relationship management meetings (10 of 17 or 58.8%);
 - SLA reviews (9 of 17 or 52.9%);
 - Contract reviews (8 of 17 or 47.1%); and
 - Financial condition (8 of 17 or 47.1%).
- Additional comments indicated that the questionnaires/surveys and on-site reviews provide the most effective way to evaluate and validate the vendor's control environment and their overall commitment to address risk.

Q31/32 – What specific vendor assessment activities have provided the least value? What about the items you selected above has made them least valuable?

- 4 of 13 (30.8%) survey respondents indicated that invoice reviews (e.g., completeness/accuracy) have provided the least value relative to vendor assessment activities.
- 3 of 13 (23.1%) survey respondents indicated that SLA reviews have provided the least value relative to vendor assessment activities.
- Of those respondents that indicated the financial condition review provided the least value, there were concerns about the timeliness of the reviews, especially during tough economic times.

Q33 – Aside from the typical risk assessment categories (e.g., privacy, information classification, business continuity) does your institution have a way to measure the more subjective risks such as strategic risk, credit risk, transaction risk, and reputation risk?

- 10 of 16 (62.5%) survey respondents indicated they do have some way to measure at least some of the more subjective risks.
- At least one respondent indicated that they have a questionnaire that is completed to address all of the risks identified in OCC 2001-47.

Q34 – How is all vendor management tracking and reporting performed within your institution?

- 9 of 16 (52.9%) survey respondents indicated that vendor management tracking and reporting is performed through both central governance and reporting, as well as through line of business governance and reporting.
- 6 of 7 (85.7%) of those survey respondents who indicated vendor management tracking and reporting is done either centrally or at the line of business, but not both, are using central governance and reporting.

Q35 – What kind of management reporting exists? Select all that apply.

- The following types of management reporting were identified as being used by more than 50% of the survey respondents:
 - High risk issues (15 of 17 or 88.2%);
 - Compliance with review requirements (10 of 17 or 58.8%); and
 - Risk by vendor (10 of 17 or 58.8%).
- A couple of respondents indicated that reporting was done for the highest risk (e.g., Tier 1) vendors only.

Q36 – How often is management reporting shared?

- 9 of 17 (52.9%) survey respondents indicated that vendor management reporting is performed on a quarterly basis.
- 5 of 16 (29.4%) survey respondents indicated that vendor management reporting is performed on a monthly basis.

Ongoing Monitoring Questions

Q37 – If the assessment process is different for initial due diligence versus ongoing monitoring, how do they differ? Select all that apply.

- 4 of 13 (30.8%) survey respondents indicated that their assessment process is not different for initial due diligence versus ongoing monitoring.
- 4 of 13 (30.8%) survey respondents indicated that prior responses to questions during initial due diligence and ongoing monitoring are provided to the vendor for subsequent reviews.
- 3 of 13 (23.1%) survey respondents indicated that their initial due diligence process is more robust than ongoing monitoring, and the scope of ongoing monitoring changes based on residual risk.

Q38 – What area is typically responsible to pay the costs incurred as part of the site visit?

- 10 of 17 (58.8%) survey respondents indicated that the line of business typically is responsible to pay the costs incurred as part of a site visit.

Q39 – How does your organization determine which vendors are subject to site visit?

- The majority of respondents indicated they use some form of risk analysis to determine which vendors are subject to site visits, and only the highest risk vendors require a site visit. In some cases, lower risk vendors may require a periodic site visit with lower frequency.

Q40 – What is the average cost of a site visit and how many hours do you typically spend on a site visit? Please identify by tier, if appropriate.

- 5 of 12 (41.7%) survey respondents that perform site reviews did not or were not able to identify the average cost and how many hours were typically spent on a site visit.
- Of those respondents that provided an average cost associated with a site visit (6), the minimum cost was \$1,000 and the maximum cost was \$25,000. The overall unweighted average cost of all respondents was estimated to be \$6,800.
- Of those respondents that provided a typical time spent on a site visit (4), the minimum time was eight hours and the maximum time was twenty-four hours. The overall unweighted average time of all respondents was estimated to be fourteen hours.

Q41 – What specific control areas are assessed during a site visit? Select all that apply.

- 13 of 15 (86.7%) of the respondents assess physical and environmental security, resiliency, backup and offsite storage, and encryption during a site visit.
- The following specific control areas are assessed during a site visit by more than 50% of the survey respondents:
 - Physical and environmental security (13 of 15 or 86.7%);
 - Resiliency (13 of 15 or 86.7%);
 - Backup and offsite storage (13 of 15 or 86.7%);
 - Encryption (13 of 15 or 86.7%);
 - Policies and standards (12 of 15 or 80.0%);
 - Network communications (12 of 15 or 80.0%);
 - Logical Access (12 of 15 or 80.0%);
 - Monitoring (12 of 15 or 80.0%);
 - Operations (12 of 15 or 80.0%);
 - Change control (11 of 15 or 73.3%);
 - Application and development (11 of 15 or 73.3%);
 - Incident response (11 of 15 or 73.3%);
 - Subcontractors (10 of 15 or 66.7%);
 - Asset management (10 of 15 or 66.7%); and
 - Standard builds (8 of 15 or 53.3%).

Q42 – How many days on site are usually required for an on-site review?

- 7 of 14 (50.0%) survey respondents indicated that they usually spend one day at the vendor's site for an on-site review.
- 7 of 14 (50.0%) survey respondents indicated that they usually spend two to three days at the vendor's site for an on-site review.
- The unweighted average number of hours spent actually at the vendor's site is estimated to be fourteen hours.

Q43 – What area within your organization actually conducts site visits?

- 4 of 17 (23.5%) survey respondents indicated that more than one area within their organization actually conducts site visits.
- 11 of 17 (64.7%) survey respondents indicated that Audit or a corporate group (e.g., Corporate IT Risk, Corporate Security, Corporate Information Security, or Enterprise Research) is involved in conducting site visits.
- 5 of 17 (29.4%) survey respondents indicated that the line of business may conduct site visits.

Resource Allocation Questions

Q44 – What areas within your organization typically participate in an on-site visit? Select all that apply.

- The following areas within your organizations typically participate in an on-site visit by at least 25% of the survey respondents:
 - Business relationship management (8 of 17 or 47.1%);
 - Corporate security (7 of 17 or 41.2%);
 - Audit (5 of 17 or 29.4%) ; and
 - Sourcing or vendor management (5 of 17 or 29.4%).

Q45 – How many FTEs are aligned with performing and evaluating risk assessment? What are their specific roles?

- An average of approximately twenty FTEs are aligned with performing and evaluating risk assessments based on those respondents that provided an estimated FTE figure.

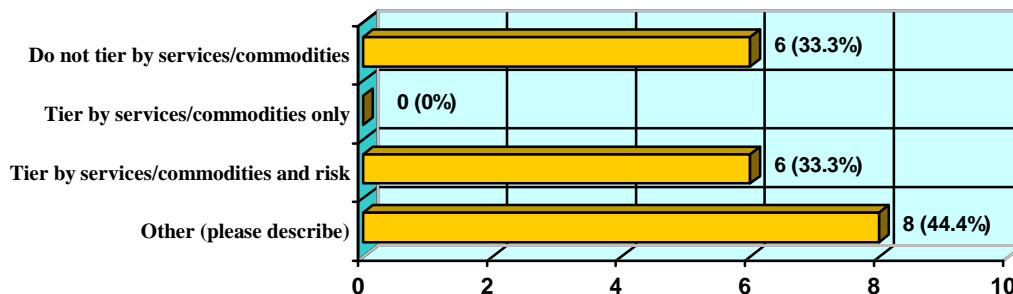
Q46 – Within your organization, are there dedicated resources for performing and evaluating risk assessments?

- 11 of 17 (64.7%) survey respondents indicated that they have dedicated resources for performing and evaluating risk assessments.
- 6 of 17 (35.3%) survey respondents indicated that the resources used for performing and evaluating risk assessments are not dedicated.

APPENDIX 2: SURVEY QUESTION RESPONSE DETAIL

Tiering Questions

Q1. In addition to tiering vendors by risk, some institutions may tier vendors by services/commodities (e.g., office supplies, temporary staffing, software services, IT infrastructure, printing services) based on the associated risk. Select all that apply:

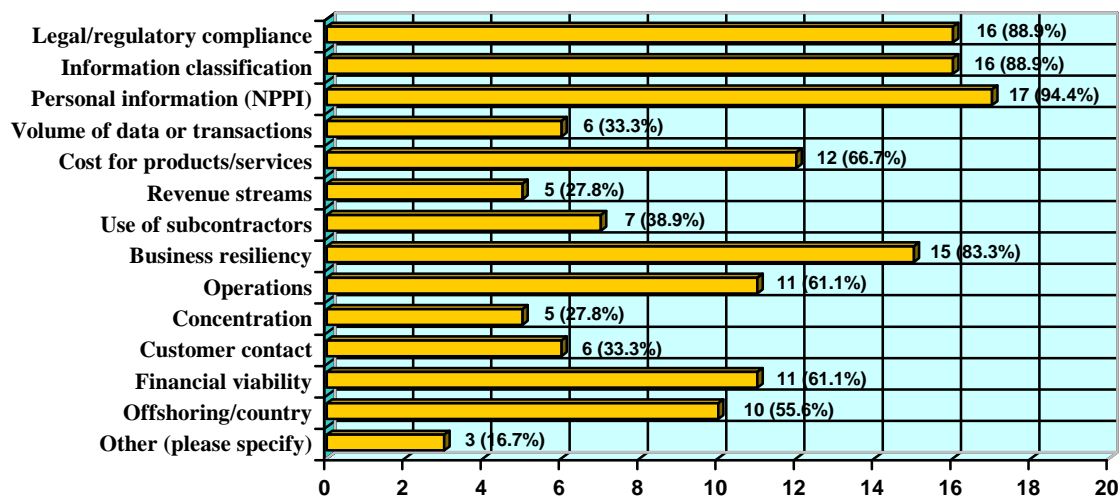


Answered question 18
 Skipped question 1

Other Comments:

1. Currently only tier by risk, but have categorizations in draft format to be used as baseline going forward. We will still however continue to require a risk rating.
2. Done by risk, spend and business criticality
3. Risk and spend
4. We tier IT-related ASPs only based on business criticality and data criticality.
5. Tiering (e.g. Tier 1, 2, 3, etc.) is no longer being used within our program. Inherent risk is evaluated in key risk areas (information security, BCP, legal/regulatory compliance, country risk), with “points” assigned based upon the level of inherent risk (e.g., higher points for higher volumes of records shared). Inherent risk across all areas of risk is also calculated and used to determine the overall inherent risk by vendor.
6. Currently we tier vendors based upon the amount of due diligence required to maintain the vendor relationship appropriately.
7. We used to tier by category, but now only focus on risk.
8. Dollar spend; market impact.

Q2. What factors are used to establish tiers/risk categories? Select all that apply:

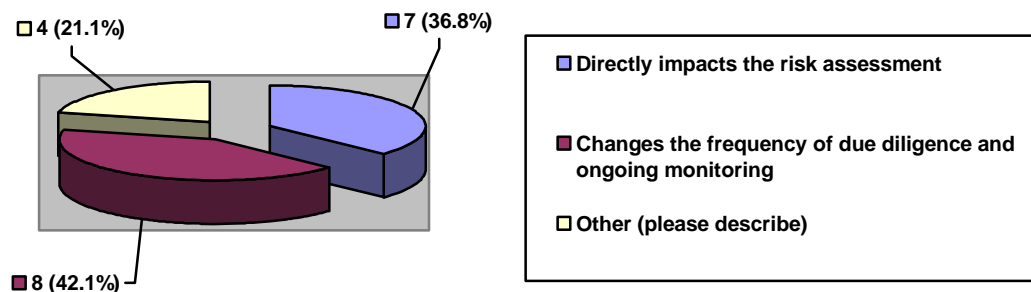


Answered question 18
Skipped question 1

Other Comments:

1. Legal/regulatory compliance risk
2. Insurance indemnification
3. Network or mainframe connectivity to our company

Q3. How does the implementation of controls and identification of related control issues/gaps impact the risk assessment process?



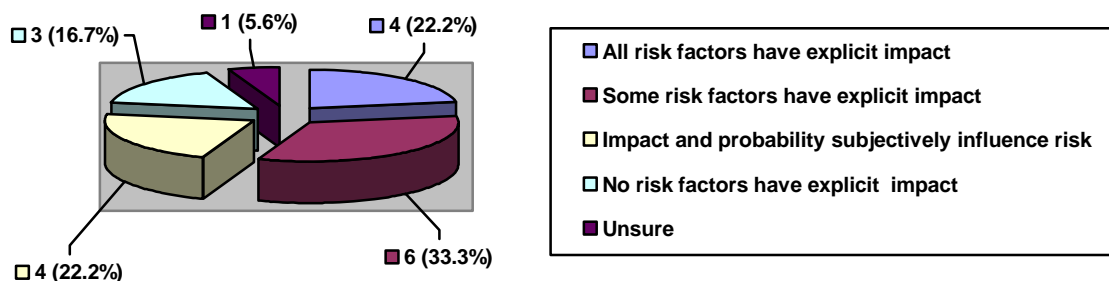
Answered question 19
Skipped question 0

Other Comments:

1. Gaps/control issues require remediation or acceptance, but do not change the base assessment requirements or frequency.

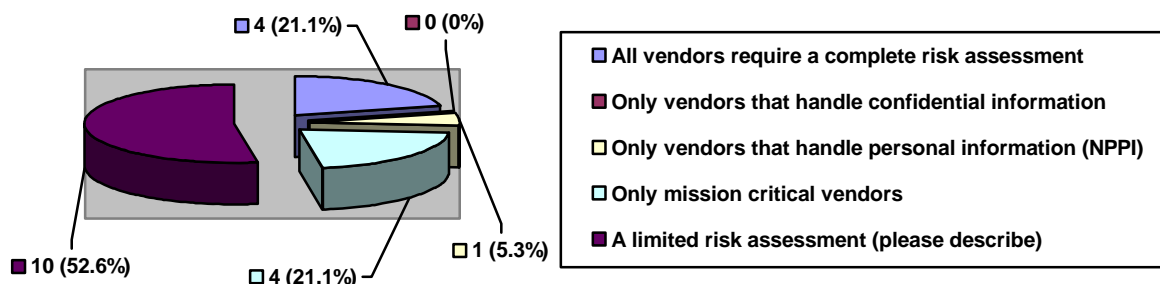
2. Both.
3. Depending on the severity of the control gap, additional controls will be implemented and monitored more quickly.
4. It both impacts the risk assessment AND changes the frequency of ongoing monitoring.

Q4. Is the impact and probability of risk factors included in the risk assessment?



Answered question 18
Skipped question 1

Q5. How do you determine the population of vendors for which a risk assessment must be performed?



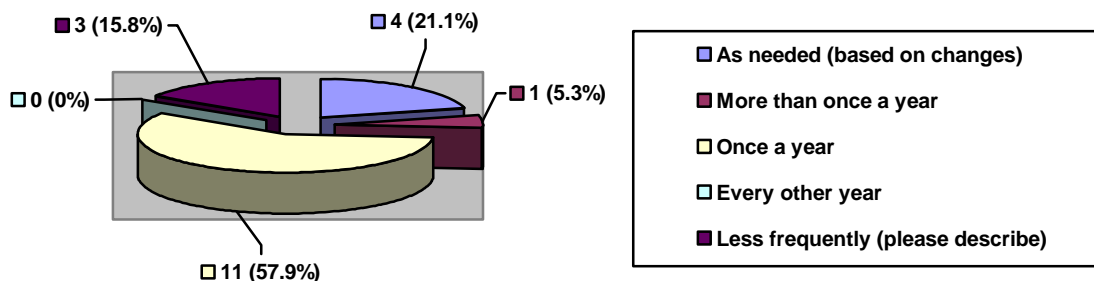
Answered question 19
Skipped question 0

Other Comments:

1. OTHER: Assessments are required based on risk rating, which includes both privacy and operational risk ratings.
2. Those vendors that are mission critical, handle NPI, and handle confidential information would be rated higher risk.
3. Options 2 through 4 are used.
4. The first step is the sponsor completes a Business Risk Assessment form and then appears before the Technology Outsourcing Committee. The vendor/ASP service is evaluated and tiered. The tier assigned to that vended relationship equates to the level of due diligence required to be performed and its frequency of re-review.

5. We have multiple forms of risk assessment, with requirements for each based upon inherent risk. I don't see a response that really fits . . . unless we were to consider the establishment of inherent risk scores a “limited risk assessment.”
6. We perform a preliminary review of all vendors to determine if a more thorough is required.
7. We risk assess vendors who receive/have access to sensitive info (including customer info) and/or are operationally critical
8. Risk assessment mechanism is determined by the inherent risk of the provider, including frequency of review.
9. Each vendor contract is scored based on the vendor and transaction to determine if additional assessments are required.

Q6. How often are the vendors reassessed against the tiers?

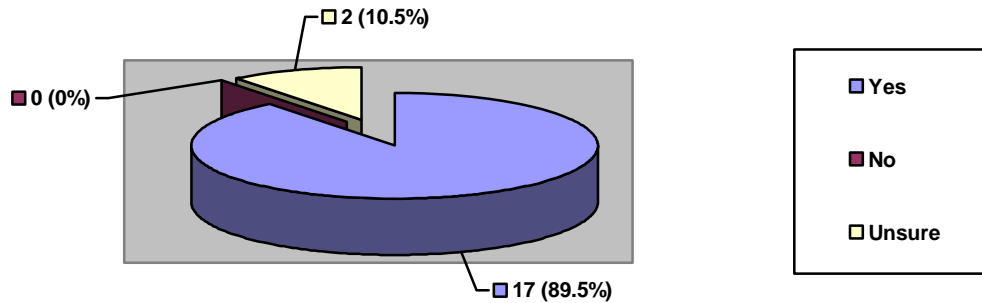


Answered question 19
Skipped question 0

Other Comments:

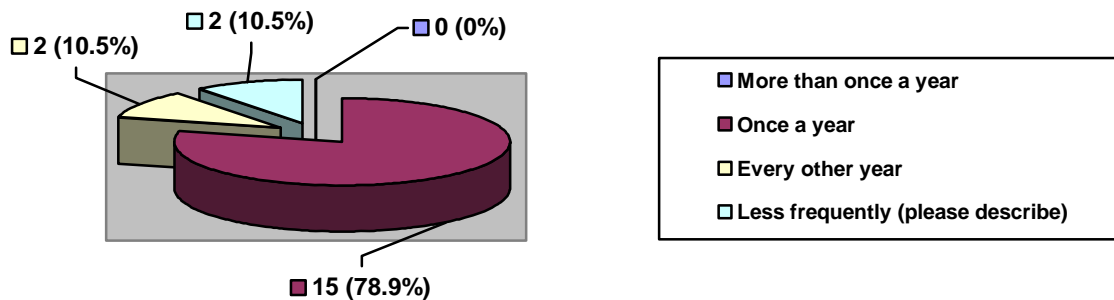
1. Vendors have not been reassessed against the tiers since the program was established 5 years ago. Reassessment is being considered as a goal for 2009.
2. Actually, not less frequently. The option I would have chosen but not there is based on tier. Tier 1 is annually, Tier 2 is every 18 months, Tier 3 is every 24 months, Tier 4 is every 36 months. Unless significant changes to the relationship arise, or issues with the relationship are identified (i.e., financial, breach, deterioration of service - not meeting SLA), etc.
3. Based on Residual risk 12 - 24 months.

Q7. In addition to the standard frequency identified above, is risk reassessed when there are changes to the product/service?



Answered question 19
 Skipped question 0

Q8. How often does your company reevaluate the overall tiering process (e.g., factors/criteria associated with the tiers)?

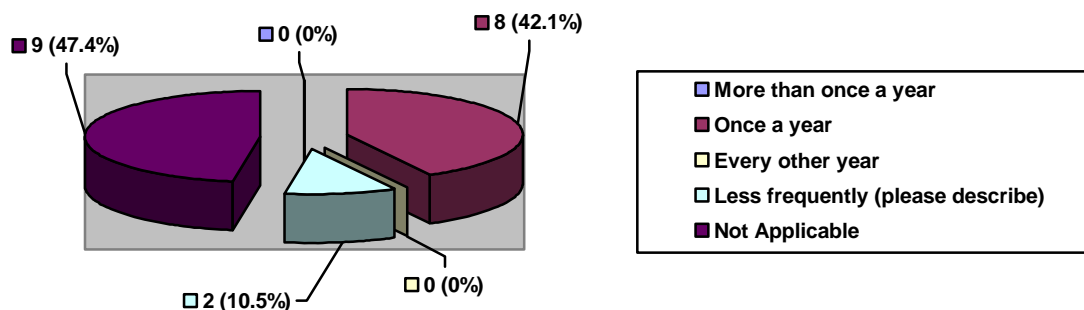


Answered question 19
 Skipped question 0

Other Comments:

1. Tiering process has not been reassessed since the program was implemented 5 years ago. Reevaluation is being considered as a goal for 2009.
2. Ongoing basis - I'm responding based upon questions used to establish inherent risk scores given that's the form of "tiering" we use.

Q9. If evaluating services/commodities based on risk, how often is risk evaluated for each commodity?

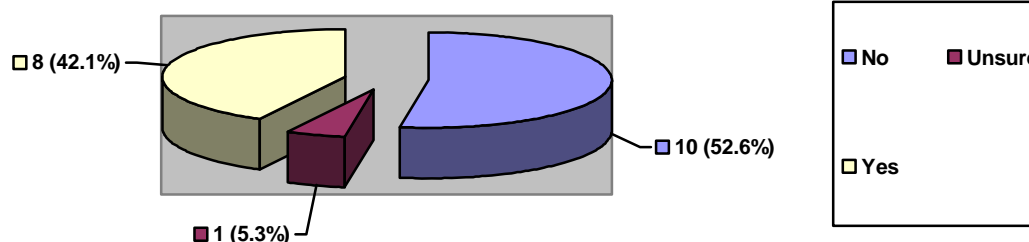


Answered question 19
Skipped question 0

Other Comments:

1. Reevaluation is being considered as a goal for 2009.
2. Prior to contract signing and after that either due to material changes or contract renewal.

Q10. Are there certain tiers or services that are not evaluated?



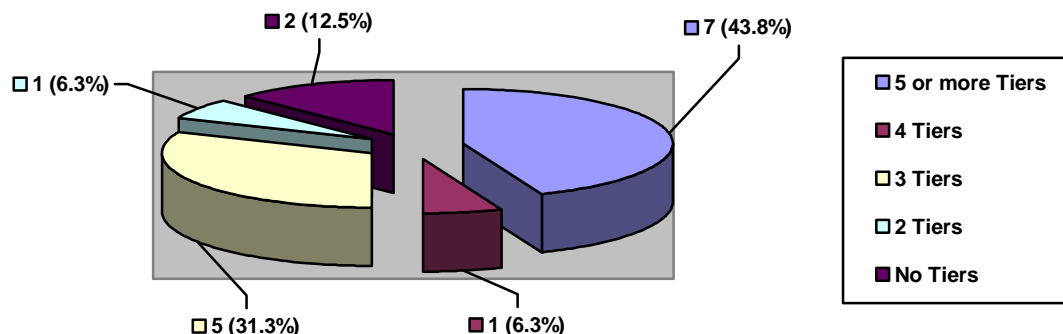
Answered question 19
Skipped question 0

Other Comments:

1. All suppliers get initial evaluation. Once a supplier has been considered for segmentation, it may be determined to be not mission critical and therefore not monitored.
2. Tier III relationships include the following types of third parties: loan and property brokers; originators; auto dealers; annuity companies; mutual fund companies; investment/insurance companies; and clearing firms. Affiliates and LOBs with 3rd party relationships that are subject to the Tier III requirements include the Investment Company, Capital Corp, Insurance, Mortgage Group, Direct Consumer Lending, Corporate Real Estate and Dealer Sales / Indirect Auto Lending. These affiliates and LOBs may also have other business relationships that are subject to the Tier I and Tier

- II processes. The affiliate or LOB has sole responsibility for managing the processes and relevant risks presented by each Tier II relationship.
3. Those that are not mission critical and they do not directly impact customers and they do not have access to customer data and they are easily replaced.
 4. We determine if a vended solution supporting our business meets the requirements through the Business Risk Assessment process. Every potential vended solution with an IT component is evaluated independently by the committee. In some cases it does not require further review as it does fit the definition of technology outsourcing. We do not look at Healthcare providers/DTC/Fed/SWIFT/ Consortiums of banking products such as CLS/Equilend/FXALL. Feds did not have a problem with that approach or rationale.
 5. Less than \$1M or that do not provide critical IT outsourcing services.
 6. Our lowest tier is not evaluated. These are vendors whose services are assumed to be low risk due to their overall tier. If services change, the tiering is dynamically changed if appropriate and risk assessments will be done as part of the contract change process and then annually
 7. They do not access sensitive data ever; their product/service is readily replaceable; their fees are relatively low
 8. Services that are the lowest inherent risk do not require a vendor assessment.

Q11. Please describe the number of tiers your institution uses and what due diligence/ongoing monitoring requirements are associated with each tier (include any impact on frequency and scope of reviews).



Answered question 16
Skipped question 3

Other Comments:

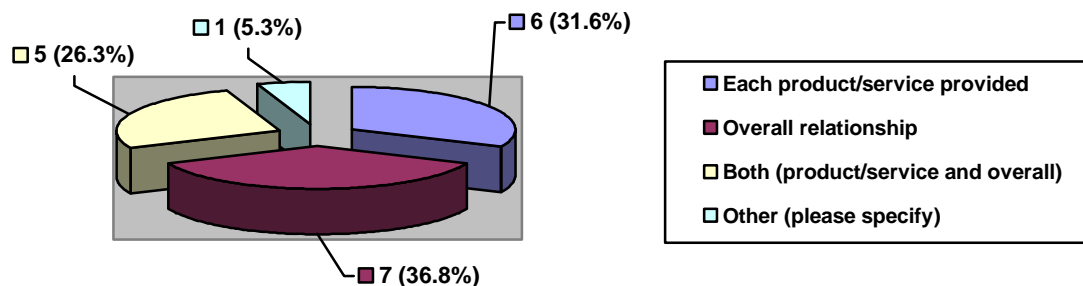
1. 16 tiers with operational and information risk ratings. Some form of Financial, Operational, BCP and Info Sec reviews are required for 14 of the 16 tiers. Low Risk - review every 2 years, moderate risk - review each year, High risk - review every 6 months.
2. 5 tiers - 1 being the most business impactful and 5 being non-material. Monitoring requirements and due diligence based on the tier and the service they provide.
3. 5 Tiers or segments (1 through 4 and unsegmented)
 - a. Segment 1 (high risk./high spend) has the greatest requirements for ongoing monitoring, and participate in our Performance Management program. For

agreements with unsegmented suppliers LOB are only required to have a written contract, assign a supplier manager, approve invoices and/or P.O. Segments 1,2,4 fall in between.

4. We use three tiers. Tier I contracts involve a potential leverage opportunity and/or pose a larger overall risk to the bank. These relationships are managed through a partnership between the Line of Business and the Sourcing Team. Due diligence and ongoing monitoring is required for all of them, however, ongoing monitoring for the Tier I suppliers that are considered the highest risk category is facilitated by the dedicated 3PRM team. Tier II relationships are defined as independent, one-off contractual relationships with a total supplier contract value less than \$400,000, that do not involve a specified Tier II supplier and/or that do not involve a selected Tier I spend category. Tier II relationships are managed directly by the lines of business following established Tier II procedures. Due diligence is required and ongoing monitoring is the responsibility of the line of business. Tier III relationships generally fall into areas where we are reselling the third party's products and/or services that we do not originate and are not subject to the Tier I and Tier II established contract and risk management processes.
5. 3 Tiers.
6. Vendors are divided into four tiers. These tiers help determine the breadth, depth, and frequency of various requirements.
7. The chart I wanted to include was not user friendly so I used this. It does not represent the frequency. Tier 1-3 all require the Business Risk Assessment form, Technology Outsourcing Questionnaire, Financial Questionnaire, and SAS70 Type II, or equivalent. The need for on-site audits will be determined based on several factors.
 - a. Tier 1 service providers are those that are core to the bank's success and are provided data that is either sensitive or non-public. Tier 1 providers are subject to the highest level of due diligence, including financial analysis, independent third party verification of controls, disaster recovery and, where appropriate, business continuity planning, and require ongoing performance reviews on an annual basis.
 - b. Tier 2 service providers are either performing a core or client visible service with public data, or an ancillary service with sensitive data. These providers require a more stringent review at startup, and may require more frequent third party reviews and performance reviews once established.
 - c. Tier 3 service providers are performing a client visible service with non-public data. These providers require a more stringent review at startup, but may not require frequent third party reviews and performance reviews once established.
 - d. Tier 4 service providers are either performing a service directly visible by a client with public data, or provide an ancillary service with non-public data. Tier 4 providers do not require periodic independent verification of controls.
 - e. Tier 5 service providers do not fall into the FFIEC definition of technology outsourcing (i.e., client information housed offsite or transactions taking place). In the case of Tier 5, the Outsourcing Committee would recommend to the business sponsor they follow proper due diligence steps, but there will be no review of the due diligence by the Outsourcing Committee.
 - f. Tier 6 service providers are those who have had some initial review by the Outsourcing Committee but have been canceled by the business sponsor prior to final implementation.

- g. Tier 9 service providers are those who had a relationship with The Northern Trust, had been reviewed and tiered by the Outsourcing Committee in the past, but are no longer being actively used.
- 8. No tiers are used. Approach described in Q1. Assessment requirements are based on inherent risk (e.g. information security, BCP, legal/regulatory compliance, country risk). Ongoing monitoring requirements (e.g. performance, contract compliance) are also defined based upon inherent risks.
- 9. 3 tiers: Top 10, not top 10 but material, lesser impact
- 10. No tiers defined. Only risk scores for service providers within the scope of the policy.
- 11. Five Tiers:
 - a. Tier 1 - Highly critical vendors, yearly reviews;
 - b. Tier 2 - Moderately critical vendors, every other year reviews;
 - c. Tier 3 - Important vendors - monitoring if requested by LoB;
 - d. Tier 4 - Low risk vendors - no monitoring; and
 - e. Tier 5 - Terminated vendors - unique due diligence related to contract terminations.
- 12. Five tiers - and all require comparable due diligence and monitoring
- 13. High Information Security Inherent Risk and outsourced
- 14. Five basic tiers:
 - a. 1 -- Full proprietary assessment;
 - b. 2 with NPPI -- Full proprietary assessment;
 - c. 2 without NPPI -- SIG Level 2 type assessment;
 - d. 3/4 with NPPI -- SIG level 2 type assessment;
 - e. 3/4 without NPPI -- SIG Lite assessment; and
 - f. 5 - No assessment required (lowest risk).
- 15. High/Medium/Low vendor risk tiers. Scorecard completed for each contract to determine if GLBA/Third Party/Finance assessment required. Those assessments lead to tier classification. Annually thereafter each contracted vendor is rescored/classified.
- 16. Low Risk - review every 2 years, moderate risk - review each year, High risk - review every 6 months.

Q12. At what level of a vendor relationship does your institution complete a risk assessment?



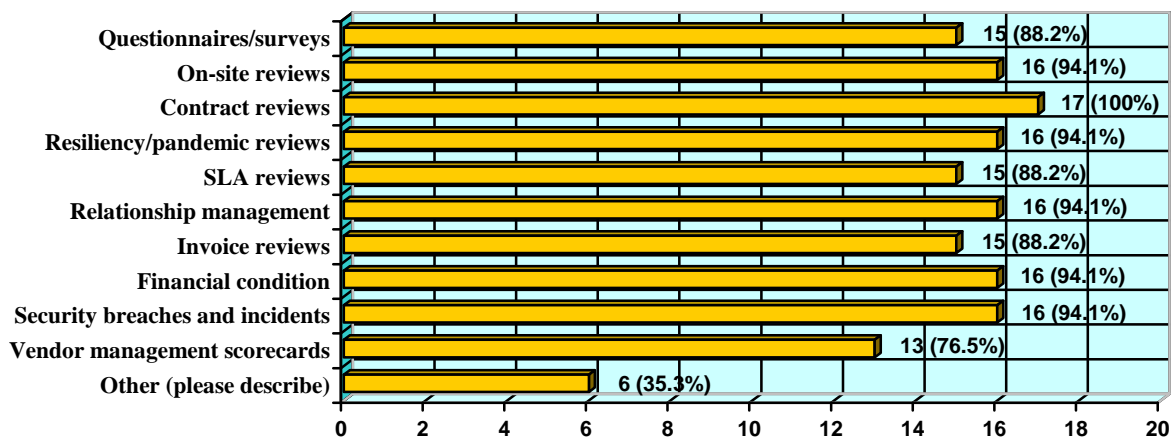
Answered question 19
 Skipped question 0

Other Comments:

- 1. Highest risk gets assessment.

Assessment Questions

Q13. What review activities are included in the due diligence/ongoing monitoring process? How are these functions performed? Please respond to all that apply.



Answered question 16
Skipped question 2

Other Comments:

Review Activity	Comments
Questionnaires/surveys	<ol style="list-style-type: none"> 1. Annual questionnaires completed by vendor and returned to bank. 2. As needed based on risk. 3. RFP; Info Security performs both remote reviews and on-site reviews based on the nature and risk of the supplier. 4. Risks are identified based on product/service being provided. Individual risk questionnaires are sent to the suppliers based on applicable risk. 5. Yes. 6. Yes. 7. Used for IS/BCP - may be used for other monitoring activities as well. 8. Both a Technology Outsourcing proprietary questionnaire and a financial questionnaire. 9. Yes. 10. Use SIG Lite and full SIG as needed. 11. Yes. 12. Yes; they are emailed to vendor. 13. Yes for the provider controls, including information security and business continuity . 14. Line of Business Rep required to score each transaction to

Review Activity	Comments
	determine level of risk and contract review required 15. Yes, sent to vendor.
On-site reviews	1. Only upfront, not ongoing. 2. As needed based on risk. 3. Info Security performs both remote reviews and on-site reviews based on the nature and risk of the supplier. 4. We do not perform on site reviews. 5. Yes. 6. Yes. 7. Used for IS for vendors with higher inherent risk. 8. Based on Tier and is determined if issues are seen in evaluation of proprietary questionnaire, or SAS70 Type II, or no SAS70 Type II for Tier 1 vended solutions. 9. Yes. 10. Conducted for all vendors requiring access to sensitive or proprietary data or materials. 11. Use appropriate sections of Full SIG. 12. Sometimes. 13. Yes; may require technology team too. 14. Limited. 15. Line of Business Rep may need to conduct on-site reviews for high-risk vendors to mitigate risks. 16. Yes, visits.
Contract reviews	1. At time of purchase. 2. As needed based on term of contract. 3. Sourcing manager checks to see if there are existing agreements. 4. All contracts are reviewed by our on-staff attorney as part of the contract authorization process. Contracts may also be reviewed in the event of a service issue with the supplier. 5. Yes. 6. Yes. 7. We have reviewed all existing contracts; new contracts are reviewed, with any gaps in expected coverage identified, prior to execution. If gaps are identified, they are accepted by the LOB as part of the contract execution process. 8. Required and governed by Global IT Procurement. IT Procurement partner is on the Technology Outsourcing Committee. 9. Yes. 10. Conducted before signing, thereafter conducted whenever contracts come up for renewal. 11. Only done as part of vendor billing audits and limited to payment and pricing terms only. 12. Yes. 13. Yes; sourcing.

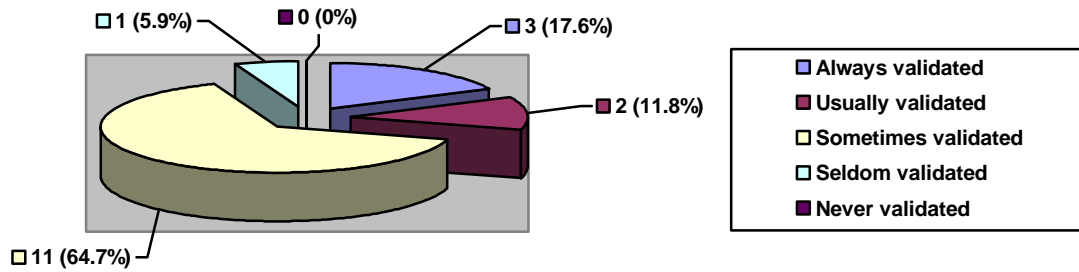
Review Activity	Comments
	<ul style="list-style-type: none"> 14. All. 15. Included, but rely on legal and sourcing. 16. Legal Dept or Contract Office will review every contract during negotiation and prior to execution. 17. Yes, as services are engaged.
Resiliency/pandemic reviews	<ul style="list-style-type: none"> 1. Upfront and annual questionnaire. 2. As needed based on risk. 3. RFP; Supplier BCP and results of supplier's BCP test are collected annually. Pandemic Readiness questions are included in initial due diligence. 4. Identified and reviewed through the Enterprise Business Continuity Risk Assessment Questionnaire as part of ongoing monitoring and due diligence. 5. Yes BCP, just starting with pandemic. 6. Yes. 7. Is part of the questionnaire/survey. 8. Incorporated into our TO proprietary questionnaire. 9. Yes. 10. Conducted at the corporate level. 11. Currently only part of initial due diligence. Updates happening ad hoc only and is done by LOBs. 12. Not currently but will be included. 13. Rare. 14. Yes. 15. Reviewed initially before contract signed and annually thereafter. 16. N/A.
SLA reviews	<ul style="list-style-type: none"> 1. As deemed appropriate by business. 2. Performance management of suppliers is a daily task done by looking at quality reports or other indicators. 3. Quarterly performance scorecards for top segment of suppliers only; SLA review for all suppliers in program. 4. Supplier Performance Reviews are performed on an annual basis for several key or strategic suppliers. Review of SLAs are included in that process. 5. Yes. 6. Done via SLA reports and any independent monitoring activities conducted by the LOB. 7. Business Unit; however, Covered in our Guidelines for vendor managers. 8. Yes. 9. Conducted at the business unit level under the vendor relationship manager. Practice varies by manager. 10. Only required for Tier 1 and it is part of a monthly performance management report, suggested for other tiers as well.

Review Activity	Comments
	<ol style="list-style-type: none"> 11. Yes. 12. Yes; business units. 13. No, planned. 14. Reviewed initially before contract signed and annually thereafter. 15. Yes, ongoing as work with vendor continues.
Relationship management	<ol style="list-style-type: none"> 1. As deemed appropriate by business. 2. Based on type of product and importance of supplier done on quarterly, semi-annually or annual basis. 3. Quarterly Strategic Business Review meetings held with key suppliers and Executive Sponsor. 4. Performed at the discretion of the Sourcing Managers or Lines of Business. For a number of key or strategic relationships, weekly, bi-weekly, monthly or quarterly meetings are scheduled. 5. As required. 6. Done at the discretion of the LOB; recommended/not required and tracked/monitored. 7. Initially and then when reassessed. Covered in our Guidelines for vendor managers. 8. Yes. 9. Quarterly Council meetings for Top 10 vendor relationships, others vary by vendor relationship manager. 10. Suggested quarterly for Tier 1 and yearly for Tier 2. An executive summary is done quarterly for Tier 1 vendors and shared with senior leadership. 11. No - this is the responsibility of the business unit. 12. Yes; often quarterly. 13. All. 14. No. 15. Line of Business Rep responsible for managing vendors. 16. Yes, ongoing as work with vendor continues.
Invoice reviews	<ol style="list-style-type: none"> 1. As deemed appropriate by business. 2. Ongoing management as invoices are submitted. 3. Performed by LOB supplier managers as part of ongoing monitoring. Required for all payments not covered by a P.O. 4. The LOBs are responsible for invoice review. In the event of a potential problem with invoices, particularly those issues that are contract related, the LOB may engage their assigned Sourcing Manager. 5. As required. 6. Discretionary at LOB level. 7. Business unit. 8. Yes. 9. Conducted at the business unit level under the vendor.

Review Activity	Comments
	<p>relationship manager. Practice varies by manager.</p> <p>10. Currently done.</p> <p>11. No - this is the responsibility of the business unit.</p> <p>12. Rare.</p> <p>13. No.</p> <p>14. Accounts Payable is responsible for reviewing invoices and associated contract.</p> <p>15. N/A.</p>
Financial condition	<p>1. Up front and annual questionnaire.</p> <p>2. Quarterly to annually based on criticality of supplier.</p> <p>3. RFP and ongoing - review financial statements, ratios and trends of key suppliers; along with credit ratings, financial stability metrics and default probabilities to arrive at an assessment of a supplier's financial strength</p> <p>4. Financial Stability reviews are available for all suppliers, but are required as part of ongoing monitoring for Tier I "A", Offshore, or any other suppliers that have been selected for annual ongoing monitoring.</p> <p>5. Yes.</p> <p>6. Yes.</p> <p>7. Required annually for vendors with a moderate/significant financial or customer/operational impact of non-performance.</p> <p>8. Initially and then when reassessed. Covered in our Guidelines for vendor managers.</p> <p>9. Yes.</p> <p>10. Conducted at the business unit level under the vendor relationship manager. Practice varies by manager.</p> <p>11. Done quarterly for Tier 1 vendors and yearly for Tier 2 vendors.</p> <p>12. Yes.</p> <p>13. Yes; at least annually.</p> <p>14. Yes.</p> <p>15. Reviewed initially before contract signed and annually thereafter.</p> <p>16. Yes, via available information services.</p>
Security breaches and incidents	<p>1. Covered in contract and reviewed as part of the risk assessment process.</p> <p>2. RFP.</p> <p>3. Identified and reviewed through the Privacy and Information Security Risk Assessment Questionnaires as part of ongoing monitoring and due diligence. Sourcing Managers and LOBs are also responsible for monitoring their suppliers between risk assessments and notifying the appropriate persons if such an incident occurs.</p> <p>4. Yes.</p>

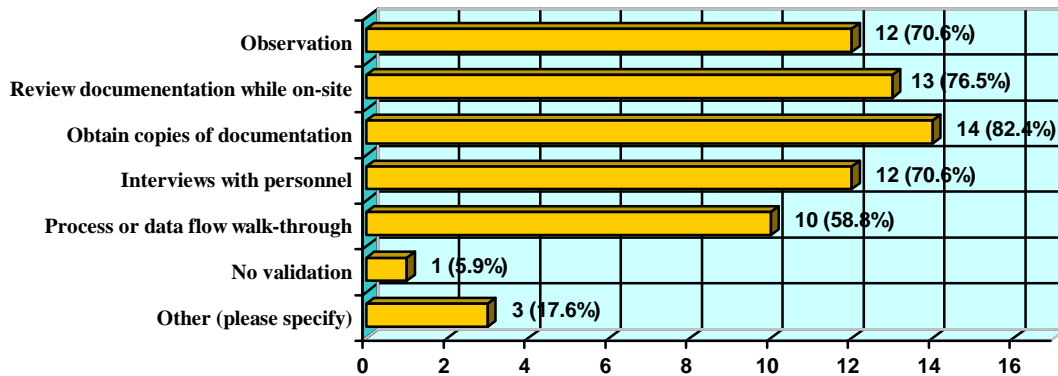
Review Activity	Comments
	<ol style="list-style-type: none"> 5. Yes. 6. Linked to incident reporting; ongoing monitoring of vendors also takes place via monitoring of news/press releases. 7. As needed. Covered in our guidelines for vendor managers. 8. Yes. 9. Oversight conducted at the corporate level. 10. Done as part of the financial analysis. 11. Yes, but limited to information included in SAS70 reports. 12. Yes; require vendor self reporting. 13. All. 14. No, planned. 15. Reviewed initially before contract signed and annually thereafter. 16. Yes, via reports.
Vendor management scorecards	<ol style="list-style-type: none"> 1. Up front and annually. 2. Quarterly to annually based on criticality of supplier. 3. We do not currently use a vendor management scorecard. 4. Yes. 5. Not a formal part of the program, but used selectively within some LOB. 6. Annually for Tier 1 vendors. 7. Yes. 8. Conducted before signing, thereafter conducted whenever contracts come up for renewal. 9. Currently only done for Tier 1 - Critical vendors and is done twice yearly. 10. Yes. 11. Yes; often quarterly. 12. No. 13. Yes, sourcing function.
Other (please describe)	<ol style="list-style-type: none"> 1. D&B reports when other info is not available; vendor's operations (any lawsuits, change in corporate strategy, etc.). 2. Other compliance internal controls requested via RFP. Monitoring covers change in product/service, insurance certification, regulatory compliance. 3. Yes. 4. Top 10 vendor relationships conducted on an annual basis at our quarterly vendor management council meetings. 5. Review of insurance policies. 6. Planning to include industry risk as well as country risk via data feeds.

Q14. To what extent is the information provided by vendors in questionnaires validated?



Answered question 17
Skipped question 2

Q15. How do you validate the information provided by vendors in questionnaires? Select all that apply.

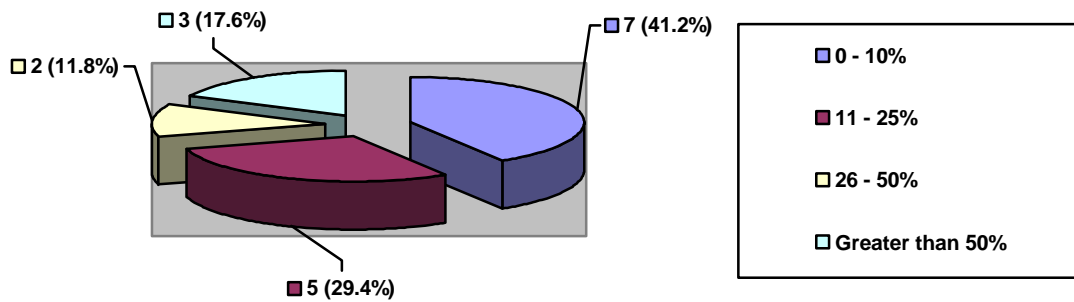


Answered question 17
Skipped question 2

Other Comments:

1. Interagency exams and SAS70s.
2. Re #14 - key risks are validated.
3. SAS70 audit reports.

Q16. When supplemental information is required to clarify a vendor’s response to a question, how much time is spent on vendor follow up relative to the entire review?

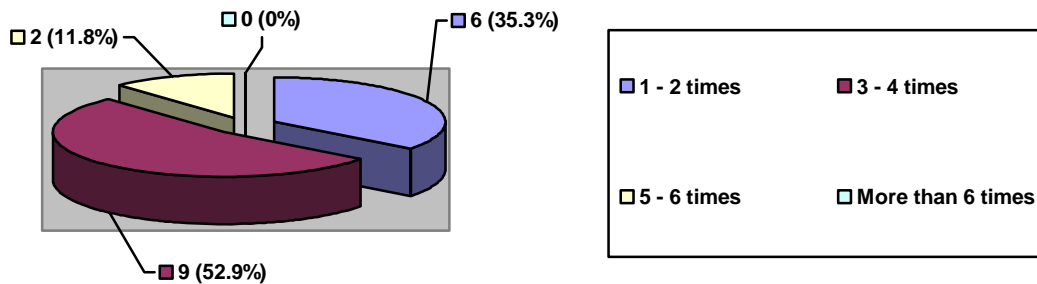


Answered question 17
Skipped question 2

Other Comments:

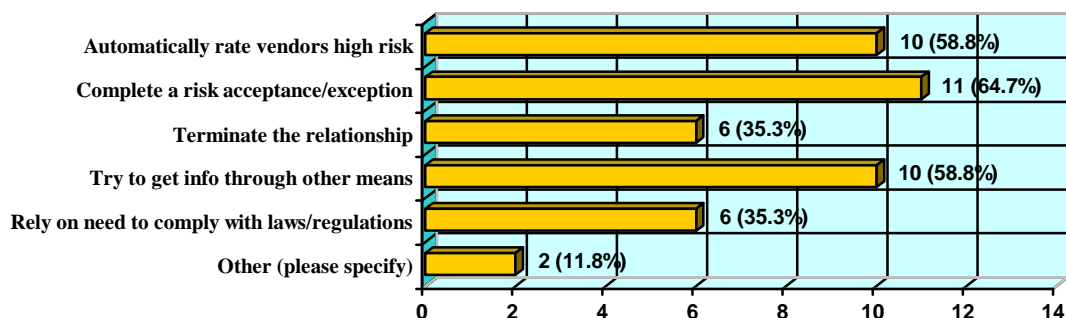
1. This response assumes both the initial interviews to issue a report and any subsequent risk closure assistance are both in scope.
2. When required, clarity is usually obtained through a 30-60 minute conference call between the supplier and the risk team.
3. Practice varies depending upon the specific situation.
4. This is one of the pain points.

Q17. How many times will you reach out to a vendor to complete due diligence or ongoing monitoring before you take alternate action?



Answered question 17
Skipped question 2

Q18. How are vendors who refuse to complete due diligence or ongoing monitoring activities handled? Select all that apply.



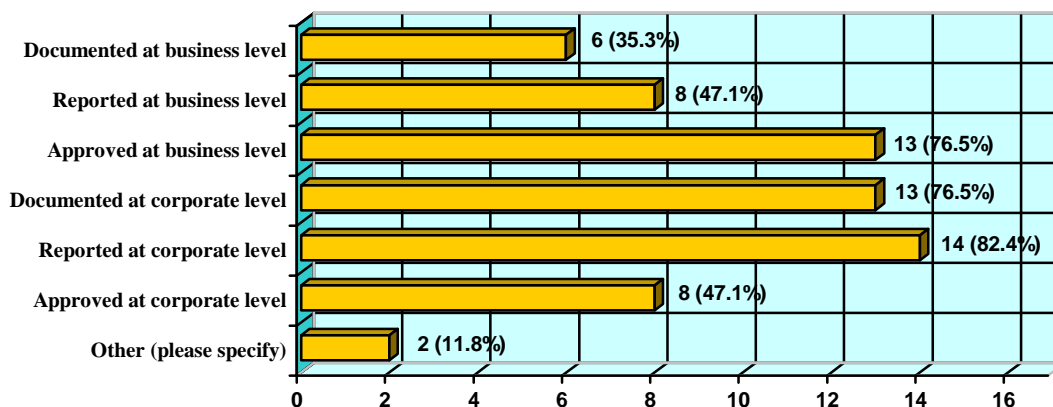
Answered question 17

Skipped question 2

Other Comments:

1. Notify Business Unit Senior partners. Report to various committees.
2. Vendor may be prohibited from being awarded any new work or current work may be stopped until vendor complies with requests.

Q19. How does the risk acceptance/exception process work when the internal business or vendor refuses to follow vendor review requirements? Select all that apply.



Answered question 17

Skipped question 2

Other Comments:

1. Varies by situation.
2. Notification to compliance.

Q20. Does acceptance of issues (i.e., residual risk remaining after reviews) reside within the line of business and, if so, does a risk management governance and oversight function exist that reports risk acceptances to management?

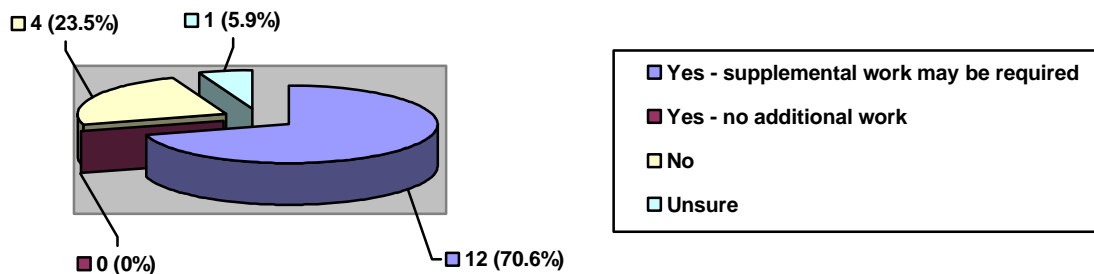
Answered question 16

Skipped question 3

Other Comments:

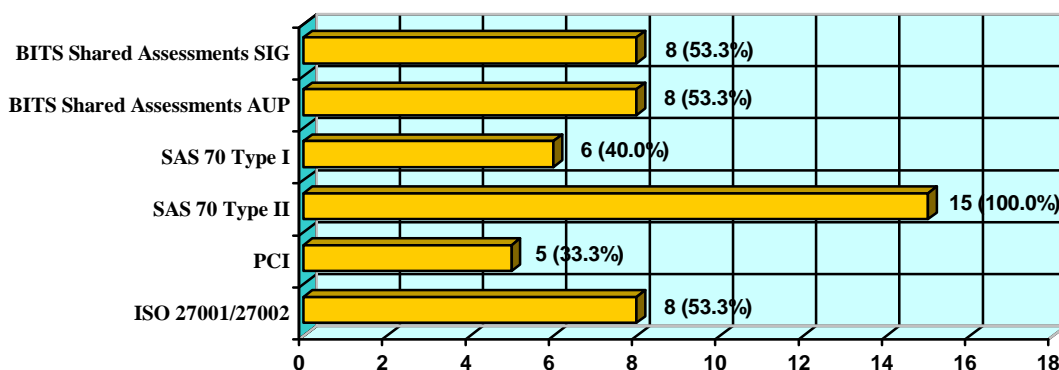
1. Acceptance resides with the business, but there is not regular reporting/oversight of these accepted risks.
2. Line of business accepts the risk. But an oversight function approves, tracks and reports risk acceptances.
3. See #19. Reported monthly.
4. Yes. The risk acceptance process is managed through the 3PRM Team, who also reports high risk issues through the appropriate management channels and follows up to ensure mitigation plans are followed.
5. Resides with the Risk Council.
6. Acceptance of issues does reside within the lines of business. Reporting and oversight of issues is handled at a corporate level.
7. Risk acceptance resides within the LOB, and is tracked and reported to management via the centralized VM function (contained in the vendor repository).
8. The process is currently being defined, as it was highlighted as an issue during our recent Fed review. The acceptance of risk resides with the business unit and is reported to various corporate committees.
9. Yes to both questions.
10. Responsibility for acceptance of issues ultimately resides with the executive who oversees the particular line of business.
11. This is a process that isn't working well today and needs to be tightened up.
12. Yes. Policy oversight is at the corporate level so any exceptions or issues will also be reported at the corporate level.
13. Yes.
14. Operational risk management coordinates the process and communicates overall and specific status to senior management
15. Yes. If a vendor is deemed high-risk the line of business is required to sign a High Risk Vendor Acknowledgement Form detailing the high risks and 1) accepting the risk(s) or 2) stating how it will mitigate the risk(s). These forms are routed up to the Executive Risk Committee for review/discussion.
16. Dual accountability at the business level and corporate level.

Q21. Are alternative assessments accepted in lieu of your institution's control assessment?



Answered question 17
Skipped question 2

Q22. If you answered yes to the previous question, what types of reviews are accepted? Select all that apply.



Answered question 15
Skipped question 4

Other Comments:

1. We don't accept alternatives to replace our own, but we do utilize things like a SAS70 to give us some information when all other requests are rejected.
2. Depends on supplier relationship and risk assessment.
3. Consideration is being given to develop an internal process that will allow us to accept the AUP and SIG.
4. OTS Examination Reports.
5. Note: reviews are accepted, however will not impact the scope of review conducted; viewed only as supplemental information.
6. BS7799 - These assessments are not accepted in lieu of but rather in addition to our control assessments.
7. BSR.

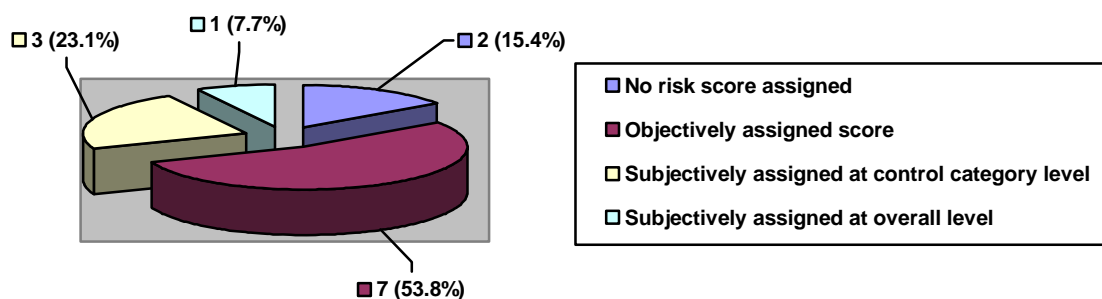
Q23. How does your company address issues and concerns identified outside of the normal review process (e.g., security breaches, incidents)?

Answered question 17
Skipped question 2

Other Comments:

1. They are channeled through another program (incident response).
2. They flow into our standard internal investigation and escalation processes and action plans are documented related to remediation activities.
3. Security Services department has established incident management and crisis management procedures to address a wide array of possible security incidents. Specific breach procedures as required by GLBA, Reg S-P, etc.
4. Such issues are documented as risk events and are reported to both the 3PRM Steering Committee monthly and the Operational Risk Committee quarterly.
5. We have breach notification process. We work with the vendor to determine the extent of the problem and mutually decide with vendor how to resolve. Issues or concerns may come from the audit or OTS exam finding resolution process or vulnerability assessments. Resolution may involve notification to regulators, letters to affected customers, notifying senior management for their review and comment, etc. We then work with the vendors to determine the cause, what controls were missing or not applied, and seek a resolution to prevent a re-occurrence.
6. All relationships are monitoring on an ongoing basis. Relationship managers would handle any issues and concerns out of normal reviews.
7. Treated and managed as critical incidents. We also monitor for other trigger events that might cause us to re-evaluate the vendor outside of the normal review cycle.
8. When advised of such incidents, a re-assessment of vendor is required to be performed.
9. Handled as part of the ongoing vendor relationship management function. Mechanisms exist to handle these types of operational issues as they occur.
10. Response varies dependent upon the particular situation.
11. Included in financial analysis and Quarterly Executive Summaries with recommended actions including transition away from the vendor and development of contingency plans
12. Contacting the vendor directly. We might also conduct onsite visits and interviews.
13. Directly.
14. We re-perform the entire review when an incident is reported. All vendors are contractually required to notify in case of breach.
15. Limited at this point.
16. Once notified the Line of Business rep will contact the vendor to discuss and proceed with an action plan.
17. Research and follow-up.

Q24. If your institution uses a “scorecard” to evaluate questionnaire and ongoing monitoring activity and assign a level of risk to the vendor, how is the overall risk scored?



Answered question 13

Skipped question 6

Other Comments:

1. Some objective data is used, but the category level score is subjective.
2. No scorecard used to evaluate ongoing monitoring. Eight categories of risk reviewed every 6-12 months. Vendors sorted into risk/spend categories annually
3. Scores are assigned, but the scoring process varies by risk area. Some risk areas scorecards are completely objective (Software, EBC), while others require some degree of subjectivity (Privacy, Compliance).
4. We don't use a scorecard per se, but do assign a level of residual risk to the vendor based upon the results of assessments. Residual risk is the difference between inherent risk and the effectiveness of vendor controls or the vendor environment.
5. While the scoring has not actively taken place it has been developed and scheduled to be instituted in 2009.
6. Top 10 vendors subject to annual scorecard review using BITS calculator and have appended to it an internally developed ERM scoring mechanism. Both subjective and objective factors are considered. Others use scorecards prior to contract initiation and during contract renewal periods. Still others may be flying below the radar.
7. What we do is to calculate a risk score for the Service Provider. If it is a High Risk provider we conduct the due diligence process. The due diligence process provide us information about the controls implemented by the service provider to manage our information. Based on this we decide if we can depend on this vendor.
8. I'm not understanding the question; we do require a quarterly qualitative score for each engagement under management, with that score being subjective to define guidelines

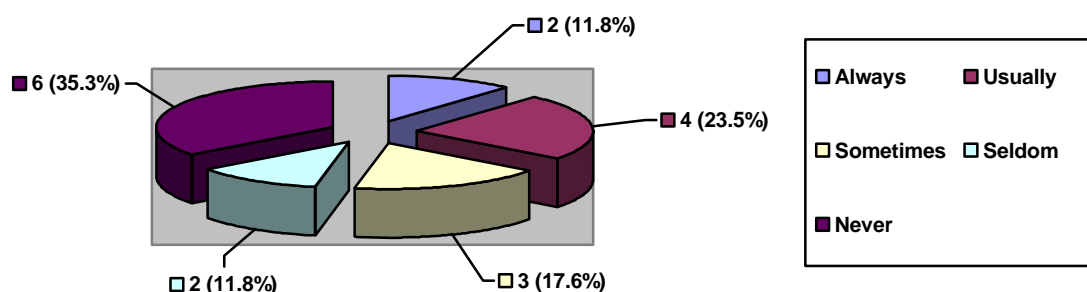
Q25. If your institution has developed or purchased a risk scoring software tool to help determine the level of risk, please indicate the vendor and tool or, if internally developed, describe.

Answered question 15
Skipped question 4

Other Comments:

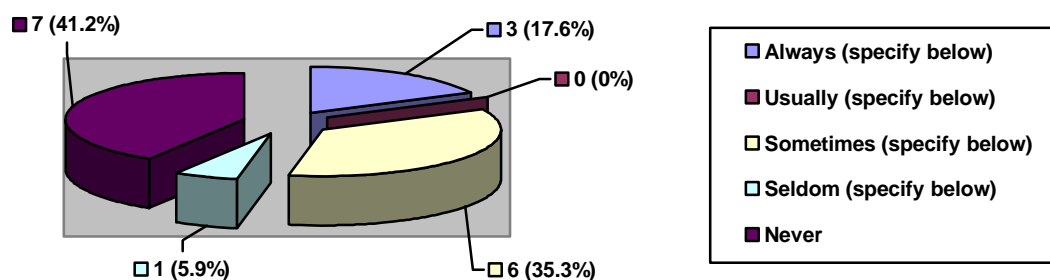
1. N/A.
2. N/A.
3. We have not purchased a risk scoring software tool.
4. We purchased the Archer SmartSuite software tool which includes a Vendor management module that we are developing for use with our oversight program. We also use the Citicus tool from ISF.
5. N/A.
6. Currently part of the Archer solution.
7. N/A.
8. We are using the BITS calculator and we have appended to it an internally developed ERM scoring mechanism to it.
9. We plan to use Archer and augment the capabilities that comes out of the box.
10. Tool internally developed using MS Excel.
11. Internally developed.
12. Internally developed.
13. Internally developed. Have ~10 defined categories with sub-questions. All categories and sub-questions have a value and a weight to create the overall inherent risk score.
14. None.
15. N/A.

Q26. Are performance metrics (e.g., SLAs) included in your vendor risk assessment process?



Answered question 17
Skipped question 2

Q27. Are the frequency and scope of the due diligence and ongoing monitoring scaled in any way beyond the tier assigned (e.g., residual risk, relationship history, vendor reputation)?



Answered question 17
Skipped question 2

Other Comments:

1. Can vary depending on information security risk assessment.
2. In addition to the periodic reviews we perform based on tier and commodity assignment, Ongoing Monitoring may be performed on a supplier if we become aware of a material change in that supplier's financial condition, business models or risk controls.
3. Frequency is based upon both the level of inherent risk (e.g., for info security - # of records the vendor has access to) AND the past assessment rating.
4. Our firm has developed an enterprise risk methodology that allows us to integrate risk scores from all sources, including vendor risks.
5. If there is a negative Financial Health assessment, if there is concern based on a change in control (M&A), if there are known changes in company direction.
6. Residual risk.
7. Scope is based on inherent risk frequency is based on residual risk.

Q28. If programmers and consultants are not included in your third party service provider assessment process, what is the process for vetting contract programmers and consultants?

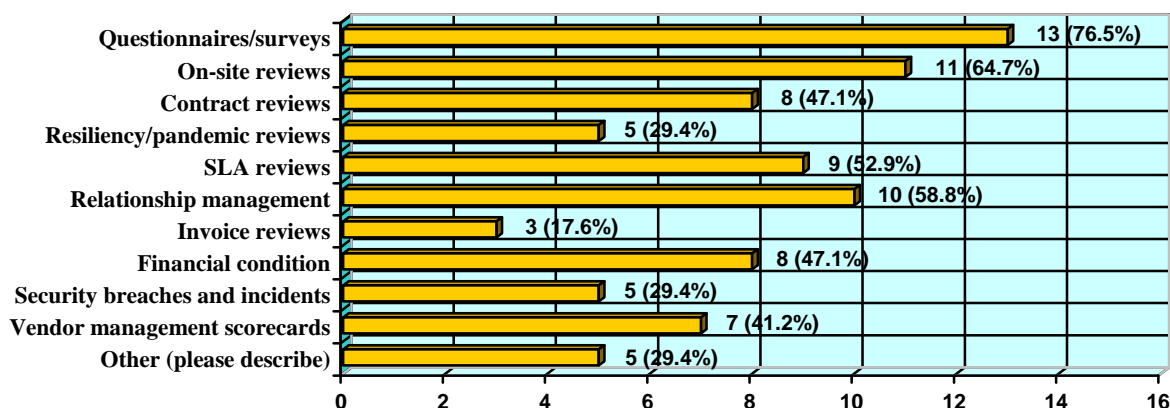
Answered question 11
Skipped question 8

Other Comments:

1. If consultants are not brought in through the contingent workforce process, they must go through the vendor risk process.
2. They are managed through our standard TPM program with a specific process defined for onsite resources.
3. External consulting and professional services are included in the supply chain program.
4. Programmers and consultants are supposed to be part of our assessment process.
5. We have a preferred vendor program for contractors; compliance is monitored through that program. In addition, Vendor Managers are expected to ensure that contractors have completed an appropriate background check.
6. Offshore consultants or programmers are vetted in a different risk based approach.
7. N/A.

8. Their companies are included.
9. A questionnaire with basic security controls is send to these providers to confirm that they have implemented good security controls.
10. Vet the dispensing firm and require they vet and evaluate the workers.
11. We have a contract administration policy for all contractors not covered by our Third Party Risk process.

Q29. What specific vendor assessment activities have provided the most value?



Answered question 17

Skipped question 2

Other Comments:

1. Monitoring questionnaires (we do not produce scorecards with this information).
2. OTS exam reports, SAS70.
3. SAS70 Type II.
4. Info that comes out from the RFP bid process.
5. We are moving away from a reactive approach to waiting for vendor data to gathering industry research and any associated data feeds to have a score and then use received information to refine the overall risk score of the provider.

Q30. What about the items you selected above has made them most valuable?

Answered question 15

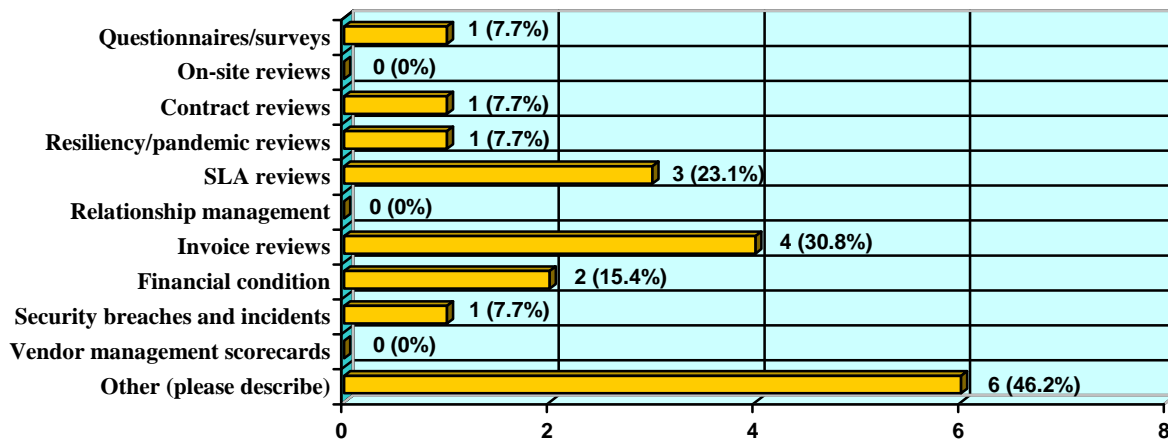
Skipped question 4

Other Comments:

1. You can cover a greater number of items in a questionnaire / site visit and they are tailored to your needs.
2. They provide a means to monitor critical controls.
3. Relationship management meetings are a forum for strategic dialogue with key suppliers and key internal stakeholders. All reviews are valuable because they allow us to examine

- and assess elements of risk and proactively alert stakeholders. Financial risk assessments also enable us to monitor mergers, acquisitions, and other corporate organizational changes that could impact our supplier relationships.
4. As we don't perform site visits, questionnaires are the most valuable tool we have to perform risk assessments. The Supplier Performance Review process creates an opportunity for lines of business to meet with supplier to drive process improvements. Resiliency reviews performed by EBC helps to identify mission critical vendors.
 5. The items selected above have provided an overall view of the vendor that has allowed us to develop a picture of the vendor. We have identified weaknesses, lack of policies, procedures and/or controls. We attempt to be involved in the vendor's BCP/DR exercises to provide a comfort level on the vendor's ability to recover from an incident. Site visits have uncovered significant gaps.
 6. Two are specific to risks. We believe we get the most value from an on-site review because there is greater opportunity to validate controls. The relationship management meetings, if done well, are an effective way to understand other aspects of vendor risk (e.g., use of sub-contractors, other controls in place).
 7. The consistency of the program being followed. Know what to look for.
 8. They all provide specific insight into the over all risk of the vendor. These items, if properly prepared, demonstrate the vendor's operational approach to addressing risk.
 9. The collection of the stated due diligence information allows us to develop an overall understanding of the risk each vendor relationship brings to our company.
 10. Best way to get updated information about the vendor and services provided to our company.
 11. Questionnaires and contract review.
 12. The obvious.
 13. Questionnaire provides basic information and indication of where to ask additional questions. On site reviews allow you to see the physical controls and make a judgment as to whether the attestations in the questionnaire are accurate.
 14. Allows internal reps to rate the vendor for a more objective determination.
 15. All important pieces of the vendor relationship.

Q31. What specific vendor assessment activities have provided the least value?



Answered question 13
Skipped question 6

Other Comments:

1. Each activity has provided some benefit, not sure how to quantify which provided the least.
2. Rely strictly on data provided by supplier.
3. Attempts to rate each agreement (product/service) as H/M/L risk.
4. SIG/AUP.
5. We use all of these.
6. N/A.

Q32. What about the items you selected above has made them least valuable?

Answered question 9
Skipped question 10

Other Comments:

1. Can be inaccurate (partly due to interpretation) and not comprehensive.
2. Process of risk rating agreements was subject to manipulation as people attempted to avoid increased monitoring requirements.
3. The assessment activities we do perform add value to our processes. This issue arises with the activities we do not perform, such as site visits or vendor management scorecards.
4. They are either used infrequently or are not developed enough to be of significant value to us.
5. SLA reviews are only as good as the SLAs and level of monitoring/validation. Some are done very well; many are not. Financial condition, while important to monitor, often does not give us the kind of timely information we need . . . particularly in tough economic times.

6. It was our assessment that the versions we looked at were not easy to read and too much information, hard to map back to our needs assessment/program requirements. Not a lot of vendors participating.
7. N/A.
8. It only gives us information available in the public sector and can be misleading in making us believe things are going well.
9. Haven't done them yet as we are just in the beginning stage of our process.

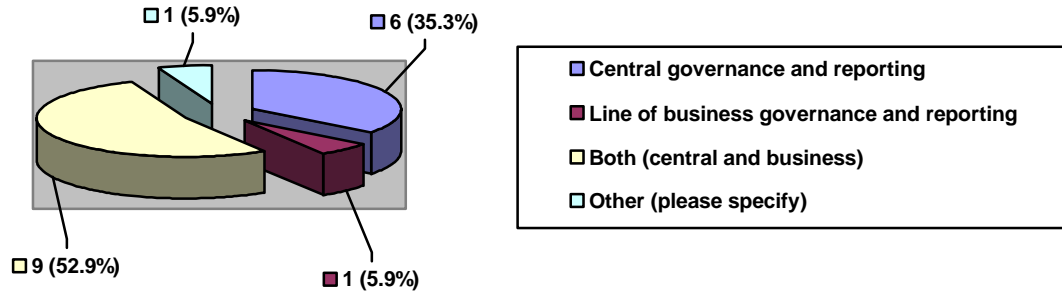
Q33. Aside from the typical risk assessment categories (e.g., privacy, information classification, business continuity) does your institution have a way to measure the more subjective risks such as strategic risk, credit risk, transaction risk, reputation risk, etc.?

Answered question 16
Skipped question 3

Other Comments:

1. No.
2. Not at this time.
3. No. We are attempting to develop this now.
4. No.
5. Request for proposal, financial analysis, measurement of service level agreements, etc.
6. Yes, some of these are measured.
7. Based on the Business Risk Assessment and discussions the committee has with the business sponsor, some of that (strategic, transaction and reputational) is assessed in those discussions. Credit risk is defined through an independent financial evaluation.
8. Yes, these are based on ongoing discussions with the vendor, their other customers, and review of publically available information on the vendor.
9. Yes, we are able to quantify the more subjective risk categories by categorizing reported criteria in a creative way that permits its quantification.
10. No.
11. Currently in process of implementing this process. The process is conducted but is fragmented as of today.
12. Yes - credit risk.
13. Financial risk is determined through our normal credit risk rating process
14. Strategic risk is included in the inherent risk scoring. Planning to use other control risks for financial scores, country and industry risk.
15. Yes, contract scorecard completed by the line of business rep asks series of questions regarding each risk in OCC 2001-47.
16. No.

Q34. How is all vendor management tracking and reporting performed within your institution?

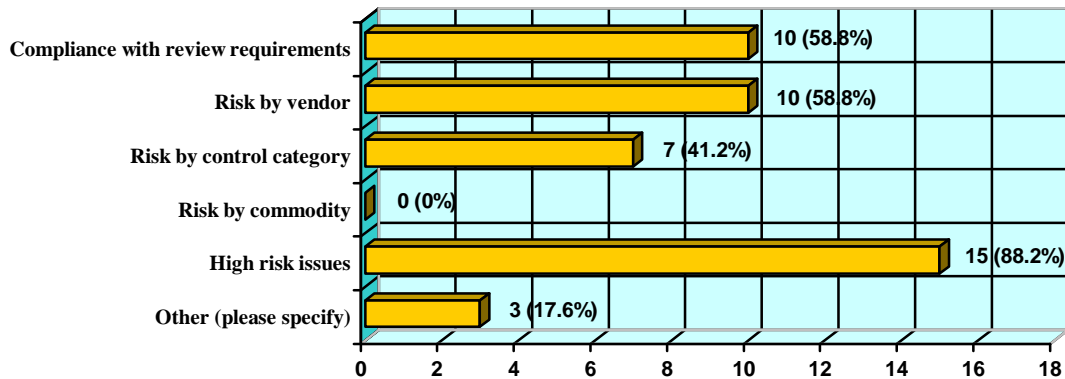


Answered question 17
Skipped question 2

Other Comments:

1. We are still in the process of developing a unified system.

Q35. What kind of management reporting exists? Select all that apply.

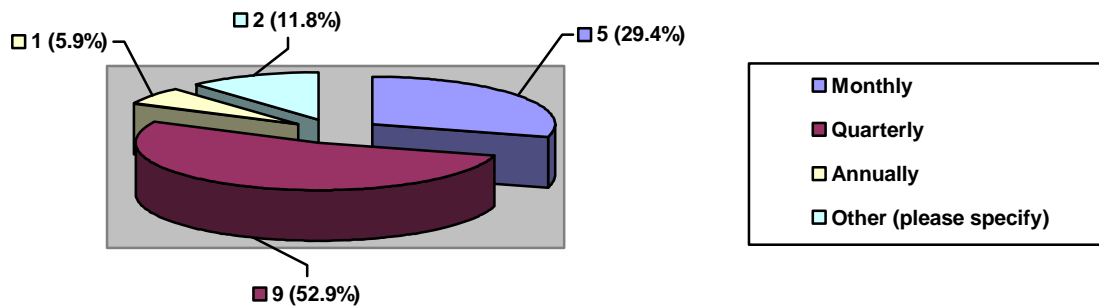


Answered question 16
Skipped question 2

Other Comments:

1. Risk by LOB.
2. Tier One Heat mapping/score card. Credit reviews reported separately.
3. Only done for Tier 1 vendors.

Q36. How often is management reporting shared?



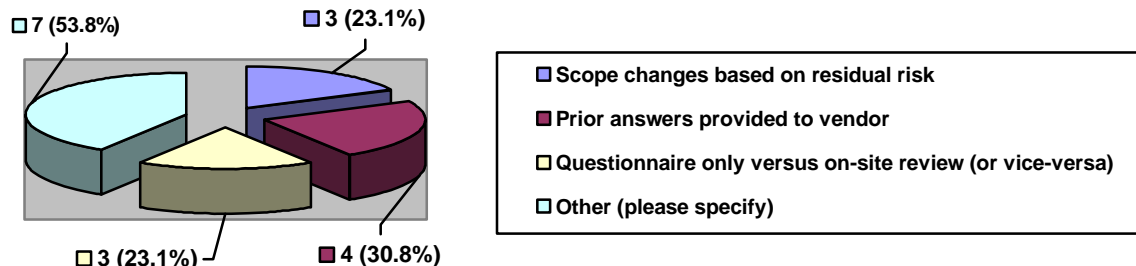
Answered question 17
Skipped question 2

Other Comments:

1. As issues are identified, but not on a regular basis.
2. We are still in the process of developing a unified system.

Ongoing Monitoring Questions

Q37. If the assessment process is different for initial due diligence versus ongoing monitoring, how do they differ? Select all that apply.

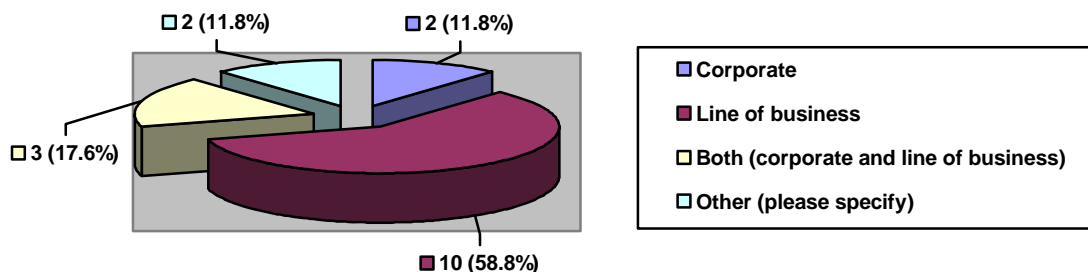


Answered question 13
Skipped question 6

Other Comments:

1. More financial and public records checks at initial stage than in ongoing stage.
2. An assessment is performed for all suppliers during due diligence. Ongoing monitoring is required only for agreements with segmented suppliers.
3. Due diligence is more robust. Ongoing monitoring generally consists of obtaining and reviewing updated risk questionnaires.
4. Assessment process does not change.
5. It is all a single process. There is no difference.
6. Is not different from initial process.
7. Same process for both.

Q38. What area is typically responsible to pay the costs incurred as part of the site visit?



Answered question 17
Skipped question 2

Other Comments:

1. We do not perform site visits.
2. Limited use today. If done, incur corporately.

Q39. How does your organization determine which vendors are subject to site visit?

Answered question 17

Skipped question 2

Other Comments:

1. Those who have data at their location.
2. Based on risk and/or line of business discretion
3. An inherent risk assessment questionnaire (7 questions) is answered by the LOB. Any risk assessments resulting in a score of High require a site visit.
4. We do not perform site visits.
5. Site visits are based on review of all information gathered about the vendor. We pay particular attention to findings in OTS exams and SAS70s. The nature and extent of the findings might lead to an on-site visit. We also will visit a vendor if they are unwilling to provide the information to us other than during an on-site visit. We will also increase the site visit frequency with a vendor if significant gaps were uncovered from the prior visit.
6. The tiered scoring model determines which vendors require a site visit.
7. Based upon results of a pre-assessment questionnaire and volume of records to which the vendor has access.
8. Based on tiers
 - a. Tier 1 vendors:
 - i. Full On-site Audit;
 - ii. Required if no SAS70 Type II;
 - iii. Reduced on-site audit if significant SAS70 Type II issues; and
 - iv. None if clean or minor SAS70 Type II issues.
 - b. Tier 2/3
 - i. On-site audit TBD based on SAS70 Type II and Outsourcing Questionnaire.
9. Based on initial risk assessment.
10. Vendors who will host or access protected sensitive information must either provide an accredited SAS 70 or are subject to a site visit.
11. Based on Tiers. Tier 1 requires a site visit every 2 years (or 4 years if they have an AUP completed by an approved 3rd party assessor) and Tier 2 site visits every three years (or six years if they have an AUP).
12. Based on risk score and financial implications of the contract.
13. Risk based.
14. Subjectively.
15. Planning to do based on the highest risk -- using a combination of the inherent and assessed risk.
16. Line of business determines.
17. Based on initial questionnaire.

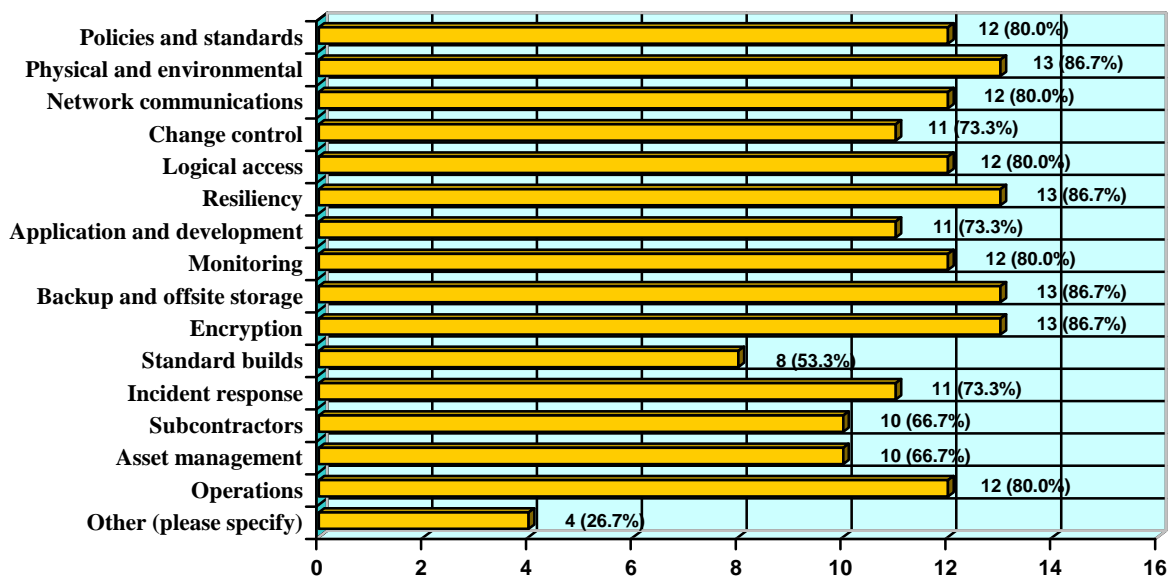
Q40. What is the average cost of a site visit and how many hours do you typically spend on a site visit? Please identify by tier, if appropriate.

Answered question 15
Skipped question 4

Other Comments:

1. 20k - takes less than one day.
2. 1,700 (plus travel) - can range from 8 to 16 hours depending on scope.
3. Average cost=\$1000, Average time spent = 8 hours.
4. We do not perform site visits.
5. \$4,000 - \$25,000 depending on the geographic location and the use of third party assessors.
6. ~\$7,000.
7. Average cost is about \$1800. Time ranges from 2-3 days for a single site; additional sites usually require an additional day per site when reviewed.
8. Unable to answer. Truly depends on location and scope of review.
9. No average cost. Depends upon distance to vendor facility.
10. Average costs are \$3500 for US based and \$10,000 for International. Only the Information Security group tracks hours and they estimate 20 hrs regardless of location
11. Do not know.
12. Costs dependent on number of employees and destination; first look generally more in depth with follow ups being under two days.
13. N/A.
14. N/A.
15. Unknown.

Q41. What specific control areas are assessed during a site visit? Select all that apply.

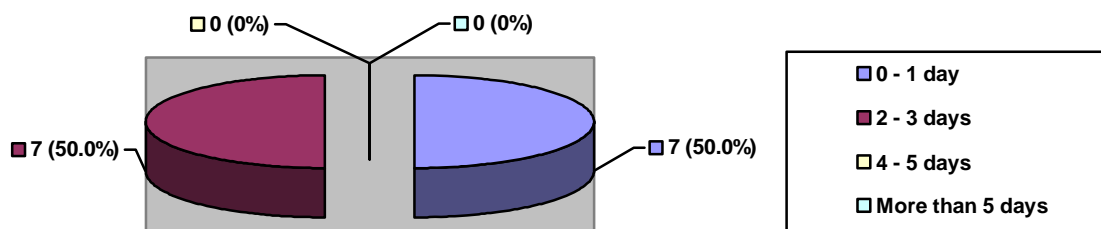


Answered question 15
Skipped question 4

Other Comments:

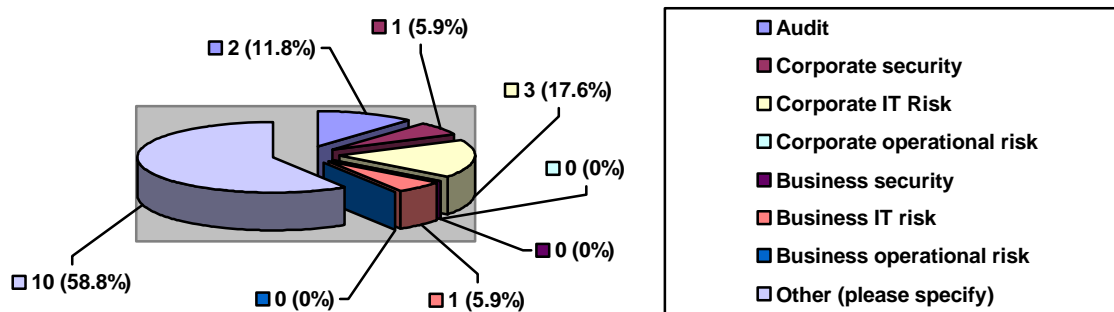
1. Evidence of proper execution of HR practices (e.g., background checks) and evidence of relevant certification (e.g., PCIDSS).
2. We do not perform site visits.
3. This is again defined more concretely when determined that an onsite is required.
4. We utilize the BITS calculator.

Q42. How many days on site are usually required for an on-site review?



Answered question 14
Skipped question 5

Q43. What area within your organization actually conducts site visits?



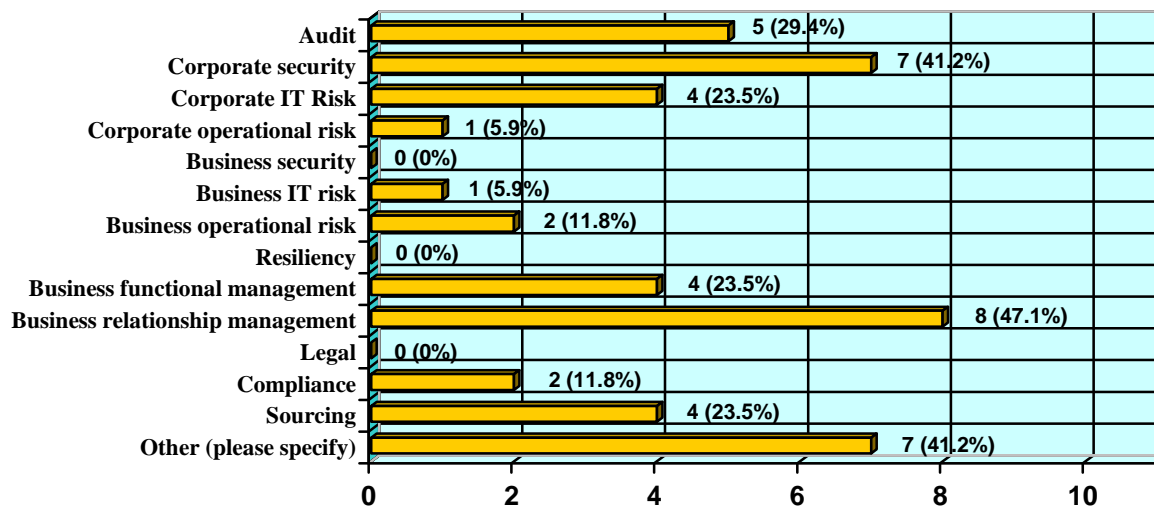
Answered question 17
 Skipped question 2

Other Comments:

1. Audit also conducts onsite visits, Corporate IT Risk represents Corporate Security, the business conducts site visits for operational concerns.
2. Enterprise Research; Some LOBs conduct site visits. Our standard contract language includes right to conduct or request audits.
3. We do not perform site visits.
4. Sourcing.
5. Corporate information security - not sure if security was meant to capture physical security so didn't select that response.
6. IT Risk Management.
7. Corporate security, Information Security (CISO) and Compliance. Occasionally Internal Audit.
8. Mostly is done by the business unit who will be contracting the service.
9. Two areas - Corporate Security and Corporate IT Risk.
10. Line of business.

Resource Allocation Questions

Q44. What areas within your organization typically participate in an on-site visit? Select all that apply.



Answered question 17
 Skipped question 2

Other Comments:

1. Enterprise research; LOB-specific site visits.
2. We do not perform site visits.
3. Corporate Information Security - see response to prior question.
4. Third party auditor, if internal audit is unable.
5. IT Risk Management.
6. Vendor Management and Information Security.
7. Information security.

Q45. How many FTEs are aligned with performing and evaluating risk assessment? What are their specific roles?

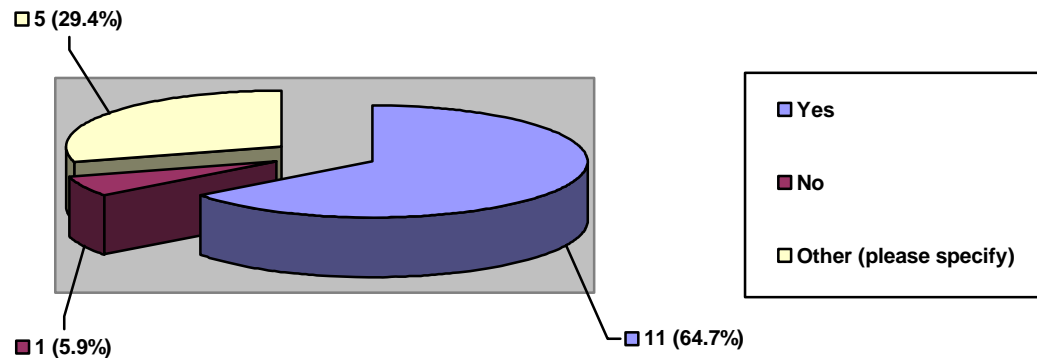
Answered question 16
 Skipped question 3

Other Comments:

1. Seven, and all have the same role (review all categories end to end).
2. 5.5 - conduct the Information Security, Physical Security and BCM assessments. Audit and Business - unable to quantify resources for these areas.
3. Hard to know. Includes sourcing teams of variable sizes, LOB supplier managers who do ongoing monitoring, information security (6 FTE) and supplier risk area (9 FTE).

4. 2.5 The 3PRM Manager has dual responsibilities with Sourcing. Two Business Analyst help to facilitate the manual process of distributing questionnaires to the supplier and the risk evaluation team, tracking the results, reporting the results and the high risks.
5. 3-4 FTE do the core pieces of the assessment. In addition, other parts of the organization contribute time and effort into evaluating results and providing input.
 - Risk ranking vendors – new and existing.
 - Requesting required documentation from Tier 1 vendors.
 - Request examination report from OTS, if available.
 - Contacting account manager at vendors to request and discuss requested information and timelines, BCPDR participation, SAS70s, on-site visits, etc.
 - Following up with vendors to obtain information.
 - Work with business lines on assessing potential new vendors and any vendor management issues.
 - Participating in BCP/DR exercises (where allowed).
 - Reviewing information received from vendors and assessing information.
 - Reviewing OTS exam reports received.
6. ~30.
7. 13.
8. The Technology Outsourcing Program is administered by Corporate Operational Risk and consists of membership by Corporate Operational Risk, Audit(IT) - Advisory, Corporate IT Risk Management, Technology Risk Management, Business Continuity and Disaster Recovery Services, Offshore Risk Management, Global IT Procurement, Technology Services, Legal - (Advisory).
9. 150.
10. 4 FTEs.
11. Unknown, they come from multiple departments.
12. About 10. These include managers and staff. Some are dedicated to operational risk and others are dedicated to the business.
13. The two departments have approx 10 FTEs who can perform.
14. 5 full time.
15. 7 FTEs. 1 atty/mgr, 1 contract analyst, 1 data analyst, 1 IT Technical Assessment SME, 1 Information Security SME, 1 GLBA/Third Party SME, 1 Credit SME.
16. 30?

Q46. Within your organization, are there dedicated resources for performing and evaluating risk assessments?



Answered question 17
Skipped question 2

Other Comments:

1. Evaluating only. Those performing risk assessments also have other responsibilities.
2. Each of our Risk Officers have full time job responsibilities in addition to the evaluation of risk assessment questionnaires.
3. In parts of our organization there are members dedicated to risk assessments. However, there are many more people involved in the assessment process that are have other responsibilities.
4. Dedicated; however, not full time to this program.
5. IT Risk Management.

Q47. Any additional thoughts or questions?

Answered question 4
Skipped question 15

Other Comments:

1. Interpretation of question intent was challenging given their broad nature. Without further discussion and clarification results may be skewed.
2. As is typical with BITS surveys, some questions are based on assumptions that do not apply for us. For instance, other than RFPs and questionnaires that are specific to data security, our questionnaires are usually completed by employees, not suppliers.
3. I look forward to seeing the results
4. Beyond the SIG and AUP, need a process to measure issues. Would be beneficial if the members could develop a method to rate providers and share that information to have a score of the providers based on the work of the institutions. Realize that some information will need to be made non-attributable, but this is a real struggle in the industry and we could likely manage our providers better if we shared more.

APPENDIX 3: SURVEY DEFINITIONS

Risk Assessment - A study of vulnerabilities, threats, likelihood, loss, or impact, and theoretical effectiveness of security measures; the process of evaluating threats and vulnerabilities, known and postulated, to determine expected loss and establish the degree of acceptability to system operations.

Due Diligence - The initial technical, functional, and financial review by the financial institution to verify the service provider's ability to deliver the requirements specified in its proposal. The intent is to verify that the service provider has a well-developed plan and adequate resources and experience to ensure acceptable service, controls, systems backup, availability, and continuity of service to its clients.

Ongoing Monitoring - Periodic technical, functional, and financial reviews by the financial institution to verify the service provider's ongoing ability to deliver the requirements specified in its agreement. The intent is to verify that the service provider has well developed processes and services, as well as adequate resources and experience to ensure acceptable service, controls, systems backup, availability, and continuity of service to its clients on an ongoing basis.

APPENDIX 4: SHARED DOCUMENTS

In advance of the Spring 2008 BITS Vendor Management Working Group Meeting, members submitted risk assessment related documents to be anonymously distributed at the meeting. Institutions may find these documents helpful as they continue to mature their risk assessment processes.

The chart below identifies and describes each document, listing the associated review activities and risks addressed. The referenced documents may be downloaded as a single ZIP file from the members-only section of the BITS website at www.bits.org. They are archived with the documents from the Spring 2008 BITS Vendor Management Working Group Meeting.

Shared Documents and Tools	Description	Associated Review Activities	Associated Risks
01 – Third Party Info Mgmt Agrmt (doc)	Contract - Third party agreement to outline control requirements to protect Company confidential and proprietary data.	<ul style="list-style-type: none"> • Contract review 	<ul style="list-style-type: none"> • Reputation Risk - Bank Confidential Info • Reputation Risk - Bus. Customer Confidential Info • Regulatory / Compliance Risk - NPPI or Personally Identifiable • Regulatory / Compliance Risk - Security Breach • Regulatory / Compliance Risk - Contract Provisions • Other Risk - Controls, Security & Training
02 – Vend Risk Mgmt Prep (doc)	Checklist/Risk Assessment - Third party checklist to document the vendor profile, risk management and performance management information, and risk assessment questionnaire (completed internally).	<ul style="list-style-type: none"> • Risk Assessment • Contract review • Relationship Management Meetings • Performance review • Questionnaire/survey • Resiliency/pandemic preparedness • Third party assessments 	<ul style="list-style-type: none"> • Strategic Risk - Mission Critical • Reputation Risk - Bank Branded (e.g., Web Site) • Reputation Risk - Internet Facing Customer Info • Reputation Risk - Bank Confidential Info • Reputation Risk - Bus. Customer Confidential Info • Reputation Risk - Account Mgmt Functions • Reputation Risk - Collect/Verify Customer Info • Operational Risk - Supports Financial Functions • Operational Risk - Transaction Complexity • Operational Risk - Subcontractors • Regulatory / Compliance Risk - NPPI or Personally Identifiable • Financial / Credit Risk - Vendor Cost/Spend • Financial / Credit Risk - Financial Analysis

BITS Vendor Management Risk Assessment Survey Executive Summary

Shared Documents and Tools	Description	Associated Review Activities	Associated Risks
03 – Risk Assmt Questions (xls)	Risk Assessment - Third party risk assessment questionnaire (completed internally).	<ul style="list-style-type: none"> • Risk Assessment 	<ul style="list-style-type: none"> • Strategic Risk - New Vendor • Reputation Risk - Bank Confidential Info • Reputation Risk - Bus. Customer Confidential Info • Reputation Risk - Customer Contact • Operational Risk - Resiliency and/or RTO • Operational Risk - Product/Service Concentration • Operational Risk - Experience • Operational Risk - Subcontractors • Regulatory / Compliance Risk - Regulatory Compliance • Regulatory / Compliance Risk - NPPI or Personally Identifiable • Regulatory / Compliance Risk - Foreign Entity or Location • Financial / Credit Risk - Vendor Cost/Spend • Financial / Credit Risk - Related Revenue • Financial / Credit Risk - Cost to Replace/Absorb Function • Other Risk - Potential Conflict of Interest
04 – Strengthen Risk Mgmt (ppt)	Presentation - Presentation on overall vendor management process (related to documents 5, 6 and 7 which provide details).		
05 – Checklist for Selection (xls)	Checklist - Checklist for selection of third parties (completed internally).	<ul style="list-style-type: none"> • Questionnaire/survey 	<ul style="list-style-type: none"> • Operational Risk - Resiliency and/or RTO • Operational Risk - Operational Concerns • Operational Risk - Technical Ability • Operational Risk - Subcontractors • Regulatory / Compliance Risk - Regulatory Compliance • Financial / Credit Risk - Financial Analysis • Other Risk - Controls, Security & Training • Other Risk - Insurance

BITS Vendor Management Risk Assessment Survey Executive Summary

Shared Documents and Tools	Description	Associated Review Activities	Associated Risks
06 – Checklist for Periodical Review (xls)	Questionnaire/Risk Assessment - Questions for the periodic review of third parties (completed internally).	<ul style="list-style-type: none"> • Risk Assessment • Performance review • Questionnaire/survey 	<ul style="list-style-type: none"> • Reputation Risk - Bus. Customer Confidential Info • Operational Risk - Resiliency and/or RTO • Operational Risk - Experience • Operational Risk - Subcontractors • Regulatory / Compliance Risk - Regulatory Compliance • Regulatory / Compliance Risk - NPPI or Personally Identifiable • Financial / Credit Risk - Financial Analysis
07 – Sheet for On-site Insp (xls)	Questionnaire - Questions for on-site inspection of third parties (completed internally).	<ul style="list-style-type: none"> • On-site review • Resiliency/pandemic preparedness • Questionnaire/survey 	<ul style="list-style-type: none"> • Operational Risk - Resiliency and/or RTO • Operational Risk - Operational Concerns • Other Risk - Controls, Security & Training
08 – GLBA Questions (xls)	Questionnaire - Questions to establish third party ranking which determines the level of ongoing monitoring required (completed internally).	<ul style="list-style-type: none"> • Risk Assessment • Contract review • Performance review • Resiliency/pandemic preparedness • Questionnaire/survey 	<ul style="list-style-type: none"> • Strategic Risk - Mission Critical • Strategic Risk - Service/Product Life Cycle • Reputation Risk - Bank Confidential Info • Reputation Risk - Bus. Customer Confidential Info • Reputation Risk - Customer Contact • Operational Risk - Resiliency and/or RTO • Operational Risk - Transaction Complexity • Operational Risk - Product/Service Concentration • Operational Risk - Operational Concerns • Operational Risk - Experience • Regulatory / Compliance Risk - Regulatory Compliance • Regulatory / Compliance Risk - NPPI or Personally Identifiable • Regulatory / Compliance Risk - Foreign Entity or Location • Regulatory / Compliance Risk - Security Breach • Regulatory / Compliance Risk - Contract Provisions • Regulatory / Compliance Risk - Active or Pending Litigation • Financial / Credit Risk - Adequate Return (ROI, ROA, IRR) • Other Risk - Controls, Security & Training • Other Risk - Incident Response Process

BITS Vendor Management Risk Assessment Survey Executive Summary

Shared Documents and Tools	Description	Associated Review Activities	Associated Risks
09 – Question (doc)	Questionnaire - Questions to evaluate overall control environment of third party (completed by third party).	<ul style="list-style-type: none"> • Questionnaire/survey 	<ul style="list-style-type: none"> • Reputation Risk - Bank Branded (e.g., Web Site) • Reputation Risk - Bank Confidential Info • Reputation Risk - Bus. Customer Confidential Info • Operational Risk - Operational Concerns • Operational Risk - Technical Ability • Operational Risk - Subcontractors • Regulatory / Compliance Risk - NPPI or Personally Identifiable • Other Risk - Controls, Security & Training • Other Risk - Incident Response Process
10 – 2007 Year-End Vendor Perf (ppt)	Scorecard - Annual performance assessment against goals (financial, customer, processes and learning and growth). (see documents 11 and 27).	<ul style="list-style-type: none"> • On-site review • Relationship Management Meetings • Performance review • Financial review 	<ul style="list-style-type: none"> • Strategic Risk - Service/Product Life Cycle • Operational Risk - Resiliency and/or RTO • Operational Risk - Operational Concerns • Regulatory / Compliance Risk - Regulatory Compliance • Financial / Credit Risk - Vendor Cost/Spend • Other Risk - Controls, Security & Training
11 – Vendor Exec Briefing (doc)	Scorecard - Quarterly assessment of successes, issues, performance and action plan.	<ul style="list-style-type: none"> • Performance review • Financial review 	<ul style="list-style-type: none"> • Operational Risk - Operational Concerns • Operational Risk - Technical Ability • Operational Risk - Experience • Financial / Credit Risk - Vendor Cost/Spend
12 – Corp VM Program (doc)	Presentation - Describes vendor management responsibilities and components of the vendor management program (see documents 13 through 19 for further detail).		
13 – Annual Relationship Review (doc)	Presentation - Describes annual relationship review process including responsibilities and components of the annual relationship review.	<ul style="list-style-type: none"> • Contract review • Relationship Management Meetings • Performance review • Financial review • Invoice review • Resiliency/pandemic preparedness 	<ul style="list-style-type: none"> • Strategic Risk - Service/Product Life Cycle • Operational Risk - Resiliency and/or RTO • Operational Risk - Operational Concerns • Regulatory / Compliance Risk - Contract Provisions • Financial / Credit Risk - Vendor Cost/Spend • Financial / Credit Risk - Financial Analysis • Other Risk – Insurance

BITS Vendor Management Risk Assessment Survey Executive Summary

Shared Documents and Tools	Description	Associated Review Activities	Associated Risks
14 – Annual Review of Company (doc)	Scorecard - Annual vendor relationship review form	<ul style="list-style-type: none"> • Questionnaire/survey • Relationship Management Meetings • Financial review • Invoice review • Resiliency/pandemic preparedness 	<ul style="list-style-type: none"> • Strategic Risk - Service/Product Life Cycle • Operational Risk - Resiliency and/or RTO • Operational Risk - Technical Ability • Financial / Credit Risk - Vendor Cost/Spend • Financial / Credit Risk - Financial Analysis
15 – Enterprise Scorecard Guidelines (doc)	Presentation - Guidelines for the completion of enterprise scorecard for top 50 vendor relationships, including a scorecard sample.	<ul style="list-style-type: none"> • Performance review • Invoice review 	<ul style="list-style-type: none"> • Operational Risk - Experience • Financial / Credit Risk - Vendor Cost/Spend
16 – Supplier Scorecard Detail (pdf)	Scorecard - Vendor scorecard	<ul style="list-style-type: none"> • Performance review • Invoice review 	<ul style="list-style-type: none"> • Operational Risk - Experience • Financial / Credit Risk - Vendor Cost/Spend
17 – Vend Scorecard Present (ppt)	Presentation - Describes scorecard objectives, meetings, and methodology, report and vendor responsibilities.	<ul style="list-style-type: none"> • Relationship Management Meetings • Performance review 	<ul style="list-style-type: none"> • Operational Risk - Experience
18 – Quarterly Scorecard Mtg Materials (ppt)	Scorecard - Meeting agenda, excerpt of scorecard and summary of health of the relationship.	<ul style="list-style-type: none"> • Relationship Management Meetings • Performance review 	<ul style="list-style-type: none"> • Operational Risk - Experience
19 – VM Responsibilities – Scorecards (ppt)	Presentation - Describes vendor management responsibilities related to scorecards.	<ul style="list-style-type: none"> • Relationship Management Meetings • Performance review 	<ul style="list-style-type: none"> • Operational Risk - Experience

BITS Vendor Management Risk Assessment Survey Executive Summary

Shared Documents and Tools	Description	Associated Review Activities	Associated Risks
20 – Vendor Risk Scorecard (hardcopy only)	Risk Assessment - Detailed analysis of various aspects of risk including the internal control environment.	<ul style="list-style-type: none"> • Risk Assessment 	<ul style="list-style-type: none"> • Strategic Risk - Mission Critical • Strategic Risk - New Vendor • Reputation Risk - Bank Branded (e.g., Web Site) • Reputation Risk - Bank Confidential Info • Reputation Risk - Bus. Customer Confidential Info • Operational Risk - Supports Financial Functions • Operational Risk - Resiliency and/or RTO • Operational Risk - Product/Service Concentration • Operational Risk - Experience • Operational Risk - Subcontractors • Regulatory / Compliance Risk - NPPI or Personally Identifiable • Regulatory / Compliance Risk - Foreign Entity or Location • Regulatory / Compliance Risk - Contract Provisions • Financial / Credit Risk - Vendor Cost/Spend • Financial / Credit Risk - Financial Analysis • Other Risk - Controls, Security & Training
21 – 2007 Annual Vendor Review Form (doc)	Checklist - Checklist and questions for annual review of vendors (completed internally).	<ul style="list-style-type: none"> • Contract review • Questionnaire/survey • Performance review • Financial review • Third party assessments • Resiliency/pandemic preparedness 	<ul style="list-style-type: none"> • Strategic Risk - Service/Product Life Cycle • Operational Risk - Resiliency and/or RTO • Operational Risk - Operational Concerns • Operational Risk - Experience • Regulatory / Compliance Risk - Regulatory Compliance • Regulatory / Compliance Risk - Foreign Entity or Location • Regulatory / Compliance Risk - Contract Provisions • Financial / Credit Risk - Financial Analysis • Other Risk - Controls, Security & Training • Other Risk – Insurance
22 – Vendor Perf Quarterly Scorecard (xls)	Scorecard - Quarterly performance scorecard for third parties.	<ul style="list-style-type: none"> • Performance review • Relationship Management Meetings • Invoice review • Resiliency/pandemic preparedness 	<ul style="list-style-type: none"> • Operational Risk - Resiliency and/or RTO • Operational Risk - Operational Concerns • Operational Risk – Experience • Regulatory / Compliance Risk - Contract Provisions • Financial / Credit Risk - Vendor Cost/Spend

BITS Vendor Management Risk Assessment Survey Executive Summary

Shared Documents and Tools	Description	Associated Review Activities	Associated Risks
23 – KPI Scores – Vendors of Choice (xls)	Scorecard - Summary of key performance indicators for third parties.	<ul style="list-style-type: none"> • Performance review • Financial review • Relationship Management Meetings 	<ul style="list-style-type: none"> • Operational Risk - Operational Concerns • Operational Risk - Experience • Financial / Credit Risk - Financial Analysis • Other Risk - Controls, Security & Training
24 – Vendor Scorecard (doc)	Scorecard - High level vendor risk scorecard.	<ul style="list-style-type: none"> • Contract review • Questionnaire/survey • Performance review • Financial review • Resiliency/pandemic preparedness 	<ul style="list-style-type: none"> • Operational Risk - Resiliency and/or RTO • Operational Risk - Operational Concerns • Operational Risk - Experience • Regulatory / Compliance Risk - Contract Provisions • Financial / Credit Risk - Financial Analysis • Other Risk - Controls, Security & Training
25 – 2008 Vendor Oversight Plan (doc)	Checklist - Checklist for vendor risk assessments.	<ul style="list-style-type: none"> • Risk Assessment • Contract review • On-site review • Questionnaire/survey • Performance review • Financial review • Resiliency/pandemic preparedness 	<ul style="list-style-type: none"> • Operational Risk - Resiliency and/or RTO • Operational Risk - Operational Concerns • Operational Risk - Experience • Regulatory / Compliance Risk - Foreign Entity or Location • Regulatory / Compliance Risk - Contract Provisions • Financial / Credit Risk - Financial Analysis • Other Risk - Controls, Security & Training
26 – Vendor Risk Mgmt On-Site Sec Ctrl Assmt (dot)	Questionnaire - Questionnaire to verify that authentication and access controls and procedures are adequate (completed internally).	<ul style="list-style-type: none"> • On-site review • Questionnaire/survey 	<ul style="list-style-type: none"> • Other Risk - Controls, Security & Training
27 – Privacy Survey (doc)	Questionnaire - High level questionnaire on privacy (completed by third party).	<ul style="list-style-type: none"> • Questionnaire/survey 	<ul style="list-style-type: none"> • Reputation Risk - Bank Confidential Info • Reputation Risk - Bus. Customer Confidential Info • Regulatory / Compliance Risk - Regulatory Compliance • Regulatory / Compliance Risk - NPPI or Personally Identifiable • Other Risk - Controls, Security & Training • Other Risk - Incident Response Process

BITS Vendor Management Risk Assessment Survey Executive Summary

Shared Documents and Tools	Description	Associated Review Activities	Associated Risks
28 – Contract Scorecard (xls)	Risk Assessment - Risk assessment associated with third party contracts.	<ul style="list-style-type: none"> • Risk Assessment • Contract review 	<ul style="list-style-type: none"> • Strategic Risk - Mission Critical • Reputation Risk - Bus. Customer Confidential Info • Operational Risk - Resiliency and/or RTO • Operational Risk - Transaction Complexity • Regulatory / Compliance Risk - Regulatory Compliance • Regulatory / Compliance Risk - NPPI or Personally Identifiable • Regulatory / Compliance Risk - Contract Provisions • Financial / Credit Risk - Vendor Cost/Spend • Financial / Credit Risk - Adequate Return (ROI, ROA, IRR)