BITS

FINANCIAL SERVICES ROUNDTABLE

BITS KEY CONSIDERATIONS FOR MANAGING SUBCONTRACTORS

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

TABLE OF CONTENTS

EXECUTIVE SUMMARY

As financial institutions and primary service providers have developed more mature sourcing practices, use of subcontractors (i.e., dependent service providers) has increased. Financial institutions benefit from the specialization of subcontractors, but must address the risks associated with the distribution of services among parties with whom they have no direct relationship. This paper will assist financial institutions as they expand their risk assessment processes to evaluate the effect of subcontractors on their own contracted services.

This paper is organized into six main sections, reflecting the importance of managing subcontractor risk through the supplier risk lifecycle:

- Regulatory Requirements
- Policy Considerations
- Due Diligence Considerations
- Contracting Considerations
- Subcontractor Approval Considerations
- Monitoring Considerations

Financial institutions and primary service providers should selectively apply the guidelines in this *BITS Key Considerations for Managing Subcontractors* based on their risk assessment results and the nature of their outsourcing engagement. This document should be used as a reference, not a checklist. The content should stimulate firms to ask relevant questions about their subcontractors.

For the purposes of this paper, a subcontractor is defined as a party on which a primary service provider relies to provide all or part of the contracted service. Examples of subcontractors can span a large range of services including: data center hosting, shredding services, printing services, call center functions, software development, etc.

This paper is written from the perspective of financial institutions for the purpose of sharing risk management experiences as it relates to subcontracting arrangements. Both financial institutions and primary service providers are encouraged to also review the *BITS Framework for Managing IT Service Provider Relationships*. The *Framework* provides detailed considerations for financial institutions establishing a program to select and manage primary service providers.

REGULATORY REQUIREMENTS

The following references are excerpts from the noted regulation or guidance.

Agency	Guidance	Page	Subcontractor Reference
FFIEC	June 2004 IT Outsourcing Technology Handbook	15	**Sub-contracting and Multiple Service Provider Relationships.** Some service providers may contract with third parties in providing services to the financial institution. Institutions should be aware of and approve all subcontractors. To provide accountability, the financial institution should designate the primary contracting service provider in the contract. The contract should also specify that the primary contracting service provider is responsible for the services outlined in the contract regardless of which entity actually conducts the operations. The institution should also consider including notification and approval requirements regarding changes to the service provider's significant subcontractors.
FFIEC	June 2004 IT Outsourcing Technology Handbook	16	**Assignment.** The institution should consider contract provisions that prohibit assignment of the contract to a third party without the institution's consent. Assignment provisions should also reflect notification requirements for any changes to material subcontractors.
FFIEC	June 2004 IT Outsourcing Technology Handbook	29	An institution can select from two techniques to manage this relationship, but remains responsible for understanding and monitoring the control environment of all servicers that have access to the financial institution's systems, records, or resources. The first technique involves the use of a lead service provider to manage the institution's various technology providers. The second technique, which may present its own set of implementation challenges, involves the use of operational agreements between each of the service providers or stand-alone contracts. If the first technique is employed, management should ensure its primary service provider has a contractual obligation to notify the financial institution of any concerns (controls / performance) associated with any of its outsourced activities. Management should also ensure the service provider's control environment meets or exceeds the institution's expectations, including the control environment of organizations that the primary service provider utilizes.

Agency	Guidance	Page	Subcontractor Reference
FFIEC	June 2004 IT Outsourcing Technology Handbook	A-3	Determine whether due diligence requirements encompass all material aspects of the service provider relationship, such as the provider's financial condition, reputation (e.g., reference checks), controls, key personnel, disaster recovery plans and tests, insurance, communications capabilities and use of subcontractors. Consider whether [r]equired contract clauses address significant issues, such as financial and control reporting, right to audit, ownership of data and programs, confidentiality, subcontractors, continuity of service, etc.
FFIEC	June 2004 IT Outsourcing Technology Handbook	A-5, 6	Evaluate whether the institution's due diligence considers [t]he service provider's proposed use of third parties, subcontractors, or partners to support the outsourced activities.
FFIEC	June 2004 IT Outsourcing Technology Handbook	A-8	Review any material subcontractor relationships identified by the service provider or in the outsourcing contracts. Ensure [m]anagement has reviewed the control environment of all relevant subcontractors for compliance with the institution's requirements definitions and security guidelines; and [t]he institution monitors and documents relevant service provider subcontracting relationships including any changes in the relationships or control concerns.
FDIC	Offshore Outsourcing of Data Services by Insured Institutions and Associated Consumer Privacy Risks, June 2004	3-4	Part of a standardized procedure should include [d]etermining if the financial institution has procedures for monitoring all outsourcing arrangements to ensure adequate controls are in place or the service provider has proper procedures and controls to monitor their outsourcing arrangements.
FDIC	Financial Institution Letter FIL-52-2006 Guidance for Financial Institutions on the Use of Foreign-Based Third-Party Service Providers	1	U.S.-based third-party service providers are subcontracting substantial portions of their operations to entities located outside of the United States. In its 2004 study of offshore outsourcing of data services to identify both consumer and safety and soundness risks associated with offshore data processing, the FDIC learned that financial institutions may be unaware of such subcontracting arrangements or, if they are aware, are not adequately monitoring the relationship.

Agency	Guidance	Page	Subcontractor Reference
FDIC	Financial Institution Letter FIL-52-2006 Guidance for Financial Institutions on the Use of Foreign-Based Third-Party Service Providers	6	***Undisclosed Foreign-Based Subcontracting Arrangements*** Undisclosed foreign-based subcontracting arrangements occur when a domestic third-party service provider subcontracts all or part of the work for a financial institution to an offshore company without prior notice to or consent from the financial institution. Third-party service provider contracts often permit subcontracting. However, the transfer of data overseas without any notification to the financial institution may increase risk in an outsourcing relationship. Standard Federal Financial Institutions Examination Council (FFIEC) examination procedures include a review of outsourcing arrangements to determine whether: • subcontracting is employed either under or outside the terms of the contract; • the financial institution is aware of the subcontracting and the vendor's location; and • the financial institution has procedures for monitoring all outsourcing arrangements to ensure adequate controls are in place or the third-party service provider has proper procedures and controls to monitor its subcontracting arrangements. The financial institution should consider including contract provisions that require a third-party service provider to notify the financial institution of and obtain approval for changes to significant subcontracting relationships, whether the subcontracted entity is domestic or foreign-based. Further, contract provisions allowing the financial institution to monitor the primary contractor's risk management activities related to foreign-based subcontractors should be considered.

Agency	Guidance	Page	Subcontractor Reference
FDIC	Financial Institution Letter FIL-44-2008 Guidance for Managing Third-Party Risk	5-6	***Due Diligence in Selecting a Third Party*** Comprehensive due diligence involves a review of all available information about a potential third party, focusing on the entity's financial condition, its specific relevant experience, its knowledge of applicable laws and regulations, its reputation, and the scope and effectiveness of its operations and controls. The evaluation of a third party may include the following items: • Use of other parties or subcontractors by the third party.
FDIC	Financial Institution Letter FIL-44-2008 Guidance for Managing Third-Party Risk	6-7	***Contract Structuring and Review*** After selecting a third party, management should ensure that the specific expectations and obligations of both the financial institution and the third party are outlined in a written contract prior to entering into the arrangement. Board approval should be obtained prior to entering into any material third-party arrangements. Appropriate legal counsel should also review significant contract prior to finalization. Any material or significant contract with a third party should prohibit assignment, transfer or subcontracting by the third party of its obligations to another entity, unless and until the financial institution determines that such assignment, transfer, or subcontract would be consistent with the due diligence standards for selection of third parties. <u>Scope.</u> The contract should clearly set forth the rights and responsibilities of each party to the contract, including the following: • Permissibility/prohibition of the third party to subcontract or use another party to meet its obligations with respect to the contract, and any notice/approval requirements.

Agency	Guidance	Page	Subcontractor Reference
OCC	OCC Bulletin 2001-47 Risk Management Principles for Third Party Relationships	8-9	***Selecting a Third Party and Due Diligence.*** Due diligence should involve a thorough evaluation of all available information about the third party, and may include reliance on and success in dealing with sub-contractors (the bank may need to consider whether to conduct similar due-diligence activities for material subcontractors).
OCC	OCC Bulletin 2001-47 Risk Management Principles for Third Party Relationships	10	*Scope of arrangement.* The contract should specify the scope of the relationship. For example, outsourcing contracts should specifically identify the frequency, content, and format of the service or product to be provided. The contract should also include, as applicable, such services to be performed by the service provider as software support and maintenance, training of employees, and customer service. Contracts should detail which activities the third party is permitted to conduct, whether on or off the bank's premises, and should describe the terms governing the use of the bank's space, personnel, and equipment. When dual employees are used, their duties and responsibilities should be clearly articulated. The agreement should also indicate whether the service provider is prohibited from assigning any portions of the contract to subcontractors or other entities.
OCC	OCC Bulletin 2001-47 Risk Management Principles for Third Party Relationships	10-11	*The right to audit.* Banks should make certain that they have the right to audit third parties (and their subcontractors) as needed to monitor performance under the contract. Generally, in an outsourcing contract, banks should ensure that periodic internal and/or external audits are conducted at intervals and scopes consistent with in-house functions. Banks should generally include in the contract the types and frequency of audit reports the bank is entitled to receive from the service provider (e.g., financial, internal control, and security reviews). The bank may reserve the right to conduct its own audits of the function, or it may engage an independent auditor. The bank should consider whether to accept independent internal audits conducted by the third-party provider's audit staff or external audits and reviews (e.g., SAS 70 reviews). In any event, audit reports should include a review of the third party's internal control environment as it relates to the service or product being provided to the bank. Reports should also include a review of the third party's security program and business continuity program.

Agency	Guidance	Page	Subcontractor Reference
OTS	Thrift Bulletin TB-82a Third Party Arrangements	10	*Subcontractor reliance.* You should assess the third party's use of other parties or partners to support the third party's activities. You should determine whether the third party understands that it is its responsibility to ensure that its subcontractors are in compliance with all regulatory requirements including the GLBA and the USA PATRIOT Act, as it relates to the work being done for the association, and the security of and handling of confidential nonpublic information that the association may provide.
OTS	Thrift Bulletin TB-82a Third Party Arrangements	11	A contract should typically include [terms that] [a]ddress a third party's use of subcontractors or other entities. You should require that the third party provide you notice of its use of subcontractors, and that you give approval.
OTS	Thrift Bulletin TB-82a Third Party Arrangements	15-16	*Ongoing oversight of third parties.* The degree of oversight activities will vary depending upon the nature of the services. Consider if the third party conducts its own similar oversight activities for any of its significant subcontractors, and whether you may need to perform such oversight of subcontractors.

POLICY CONSIDERATIONS

In cases where primary service providers choose to subcontract, the goal of both financial institutions and their primary providers should be the successful delivery of the contracted service without introduction of undue risk to either party. Financial institutions should review their internal policies to ensure that they enable meeting this objective.

The relevant internal policies should address risks and outline requirements that span the entire supplier lifecycle. Risks inherent to subcontracting vary, but may include:

- Subcontract language that does not provide the financial institution with the same controls and protections as those specified in the agreement with the primary service provider;
- Subcontractor control weaknesses that may compromise data security and result in breaches of confidential information; or
- Subcontractor failure that may lead to failure by the primary vendor to fulfill service level agreements with the financial institution.

Financial institutions should address several foundational considerations before examining the specifics of a particular proposed or existing primary service provider or subcontractor relationship. Among the most important of these broad policy considerations are the:

- Determination of what is considered a material subcontractor relationship for the purpose of subcontractor oversight. Criteria may include such things as:
    - Whether a new service provider or financial institution activity is involved;
    - Volume or percentage of work performed by the service provider, or the potential effect on earnings or capital;
    - Primary service provider reliance on the subcontractor to provide mission-critical services, such that the failure of the subcontractor would render the primary service provider unable to provide services to the financial institution;
    - Subcontractor access to confidential or personal information;
    - Services involved in the marketing of financial institution products or services;
    - Services related to subprime lending or card payment transactions; or
    - Measurement against a risk threshold.
- Due diligence requirements and ongoing monitoring appropriate to service engagements based on the nature of the engagement (e.g., location requirements, scorecard reporting, controls reviews);
- Risk assessment method, frequency, and measurement to be applied to proposed or ongoing primary service providers and material subcontractors;
- Notification or approval requirements when new subcontractors are engaged;
- Level of direct contact the financial institution requires with the subcontractor; and
- Definition of an exception process for those cases where management is willing to accept missing controls or controls not functioning effectively. This should include a risk-based review by a defined management team so the variations are accepted or mitigated appropriately.

Management should review the relevant sections of this document for specifics related to due diligence, contracts, subcontractor approval, and monitoring to determine which of these considerations should be included in their policies.

INITIAL DUE DILIGENCE CONSIDERATIONS

When a financial institution is considering forming a relationship with a new service provider, the financial institution should include in its due diligence an evaluation of the primary service provider's reliance on subcontractors, as well as controls implemented by the primary service provider to oversee and manage its subcontractors. Reliance on the primary service provider's risk management can aid in reducing the costs of managing subcontractors.

Elements of due diligence related to subcontractor management fall into two broad categories: risk assessment and control activities. The financial institution's appraisal of the primary service provider's risk management practices may include some or all of the following:

- Whether the service provider's due diligence review of the particular subcontractor included the following:
  - Security and data handling practices;
  - Business continuity planning;
  - Operational controls relevant to the subcontracted work;
  - Hiring/screening practices; and
  - Financial strength and viability;
- Whether the primary service provider conducts its own location risk assessment prior to engaging a subcontractor and when the subcontractor adds or changes locations, and the ongoing monitoring of location risk;
- Whether the primary service provider performed a site visit of subcontractor(s); and
- Whether the primary service provider's risk assessment included consideration of whether law enforcement is effective to contain risks, such as those associated with identity theft, in the subcontractor's location.

The financial institution should also appraise the primary supplier's subcontractor controls as related to the service or product being provided to the financial institution. This appraisal may take into account whether the primary service provider has done, or has established, acceptable procedures to do some or all of the following:

- Implement and appropriately review, update and approve a corporate policy to manage their subcontractors;
- Evaluate the sufficiency of its subcontractor controls;
- Perform acceptable due diligence in the selection of subcontractors;
- Identify the potential disruptions in their service delivery due to disruptions at the subcontractors, and their additional resiliency plans to address the risk of subcontractor disruption;
- Maintain current exit strategies for its material subcontractor relationships;
- Require notification of security breaches and significant changes (e.g., ownership, key personnel, infrastructure) at the subcontractor;
- Execute a supplier monitoring program with criteria for subcontractor inclusion and review frequency;
- Design contingency plans to ensure delivery of subcontracted services in the event of subcontractor failure;

- Obtain copies supporting documentary evidence of subcontractor's controls (e.g., SAS70 reports, Shared Assessments SIG/AUP reports[1], penetration testing reports);
- Manage access to systems that store financial institution data;
- Implement controls to manage and monitor remote access by subcontractors, where such access is acceptable to the financial institution;
- Map financial institution data related to the proposed contract to all subcontractors;
- Establish data handling requirements applicable to subcontractors (e.g., whether the subcontractor is required to inform the service provider about offsite storage); and
- Manage service provider background check practices in light of the nature of background checking in the subcontractor location(s).

If the due diligence and controls review of the primary service provider does not bring confidence, the financial institution should consider withholding approval for the primary service provider to engage the subcontractor(s). In certain limited circumstances (keeping in mind costs and potential liability issues), the financial institution may wish to directly review subcontractor(s) itself.

CONTRACTING CONSIDERATIONS

When contracting with a primary service provider who presently uses or may use subcontractors to perform portions of the contracted work, the financial institution's fundamental objective is to hold the primary service provider to the same standard regardless of who performs the work. Therefore, the primary service provider contract should require their subcontractors to meet the same obligations as they are required to meet. Key considerations include the following:

- Security and Confidentiality, including definition, ownership and requirements for protection of confidential information, and requirements that subcontractors adhere to the financial services institution's security requirements;
- Business continuity recovery, including recovery time objectives, testing/joint testing requirements, and prioritization of recovery efforts.
- Compliance with laws and regulations, including GLBA, Patriot Act, etc.;
- Compliance with applicable financial institution policies, including requirements for background checks, records retention policies, data handling/encryption requirements, change management policies, etc.;
- Audit rights, including:
  - On-site reviews by the primary service provider;
  - On-site reviews by the financial institution; and
  - Right to review internal and external audit reports;
- Right to inspection by relevant regulators; and
- Primary service provider's right to approve the subcontractor's use of other subcontractors.

[1] The Financial Institution Shared Assessment Program is an industry program for evaluating the security controls of service providers. Informaiton is available at http://www.bitsinfo.org/FISAP/index.php.

Additionally, to ensure appropriate governance over outsourced activities, the financial institution may wish to:

- Require written approval before the primary service provider may engage a subcontractor, particularly if the subcontractor is foreign based;
- Establish the governance framework as part of the primary service provider contract, to ensure the financial institution has the ability to evaluate the service levels associated with the subcontracted work, as well as the related control environment; and
- Spell out the circumstances under which the financial institution may or may not contract directly with the subcontractor(s).

SUBCONTRACTOR APPROVAL CONSIDERATIONS

As previously noted, financial services institutions should consider requiring primary service providers to obtain approval prior to subcontracting. When a primary service provider requests the financial institution's approval to subcontract a portion of the work, the institution should explore factors detailed in both the Initial Due Diligence Considerations and Contracting Considerations sections above. In addition, the financial institution may consider the following:

- Determine materiality of the subcontracted work, based on criteria similar to that used by the financial institution when assessing the risk of primary service providers (e.g., new relationship, new financial institution activity, volume or percentage of work, criticality of the service provided by the subcontractor, level of data sensitivity, marketing of financial institution products or services, service related to subprime lending or card payment transactions, potential effect on earnings or capital);
- Identify the level of due diligence and ongoing monitoring required based on the risk analysis performed, and validate that the service provider has performed appropriate due diligence on the subcontractor (see Initial Due Diligence Considerations);
- Establish a subcontractor oversight framework (i.e., due diligence and ongoing monitoring activities and responsibilities) with the primary service provider, including periodic reporting requirements (if not already defined in the primary service provider agreement);
- Review the service provider's framework or process for ongoing monitoring and oversight of their subcontractors and validate conformance with the financial institution's requirements;
- If the subcontractor is foreign-based, review the service provider's framework for identification and monitoring of foreign risk; and
- Review relevant terms and conditions of the subcontractor agreement (if possible), in order to ensure that terms and conditions of the financial institution's contract with the primary service provider are reflected in the contract between the primary service provider and its subcontractor.

ONGOING MONITORING CONSIDERATIONS

A financial institution is responsible for understanding and monitoring the control environment of all primary service providers that perform processing or have access to the financial institution's information or systems. Two methods may be used to ensure appropriate understanding and monitoring of the control environment. The financial institution may rely on a lead or primary service provider to manage the subcontractors; or the institution may establish separate agreements between each of the contractors involved in providing the service. While contracting for services using a primary service provider may lessen the need for the financial institution to become directly involved in monitoring, it does not eliminate their responsibility for monitoring performance and controls through the primary service provider relationship.

Financial institutions should have an ongoing program in place to monitor their primary service provider's management of subcontractors. The level and depth of monitoring may vary based on the risk ranking and criticality of service. The financial institution may elect to monitor the primary service provider's oversight of key subcontractors via review of documentation (e.g. policies, procedures, assessment reports) or directly oversee, monitor and/or audit the subcontractor (assuming that the relevant contracts allow this).

Considerations for ongoing monitoring include:

- Identification of any new subcontractor relationships that have been formed by the primary service provider during the monitoring period;
- Ongoing information security and privacy assessments to ensure data security, including understanding what data is shared with subcontractors, what assessments are conducted, and whether controls have been implemented similar to those the financial institution has in place for primary service providers with a similar risk profile (e.g., access control, perimeter security controls, vulnerability/penetration testing);
- Evidence of an end-to-end business continuity test, including any subcontractor involved in providing a product or service to the financial institution;
- Ongoing monitoring of location risk (applicable if subcontracted work is to be performed offshore or in any location deemed to be risky);
- Evaluation of the subcontractor's financial strength and viability;
- Active monitoring of contract compliance (e.g., SLAs) and quality;
- Verification of the adequacy of the subcontractor's insurance coverage;
- Evaluation of other internal controls applicable to the services provided (e.g. change control, records destruction);
- Periodic contract reviews to ensure that vendor contracts obligate subcontractors to meet the same requirements that the primary service provider is required to meet;
- Review and evaluation of any available independent third party reviews;
- Periodic evaluation of any potential changes to the relationship required due to the external environment (e.g., regulations, technology, economic, competition); and
- Evidence that primary service provider conducts periodic status reviews for any identified issues or outstanding remediation activities.

CONCLUSION

Because of the risk associated with the distribution of services among parties with whom the financial institution has no direct relationship, institutions may need to expand their risk assessment processes to evaluate the effect of subcontractors on their own contracted services.
Financial institutions should also consider:

- Ensuring that the primary service provider understands that it is responsible for the services outlined in the contract regardless of whether a subcontractor actually conducts the operations;
- Either ensuring that the primary service provider has proper procedures and controls to monitor its subcontracting arrangements, or directly reviewing the control environment of all material subcontractors; and
- Ensuring that the primary service provider understands that it is responsible for ensuring that its subcontractors are in compliance with all regulatory requirements related to the work being done for the financial institution.

Guidelines included in this white paper should be selectively applied based on the financial institution's own risk assessment results and judgments of materiality.