Third Party Risk: Comply with Confidence, Execute with Efficiency

Orus Dearman, Director
Johanna Terronez, Sr. Manager
Advisory Services
Grant Thornton, LLP
Core Competencies – C21

AGENDA

1. OVERVIEW
2. DEVELOPING A RISK MANAGEMENT FRAMEWORK
3. VALUE-ADD FROM INTERNAL AUDIT
4. KEYS TO IMPLEMENTING FRAMEWORK SUCCESSFULLY
5. CASE STUDY EXAMPLES

AGENDA

1. **OVERVIEW**
2. DEVELOPING A RISK MANAGEMENT FRAMEWORK
3. VALUE-ADD FROM INTERNAL AUDIT
4. KEYS TO IMPLEMENTING FRAMEWORK SUCCESSFULLY
5. CASE STUDY EXAMPLES

3rd Party Risk Management
Defined

Vendor Management is a discipline that enables organizations to control and optimize their costs, drive service excellence and mitigate risks to gain increased value from their third parties throughout the Source to Pay lifecycle

– Gartner 2013

A Third Party is a company that is **not under direct business control** of the organization that engages it. A third-party relationship is any business arrangement between a company and another entity, by contract or otherwise.

– OCC 2013-29

3rd Party Risk Management

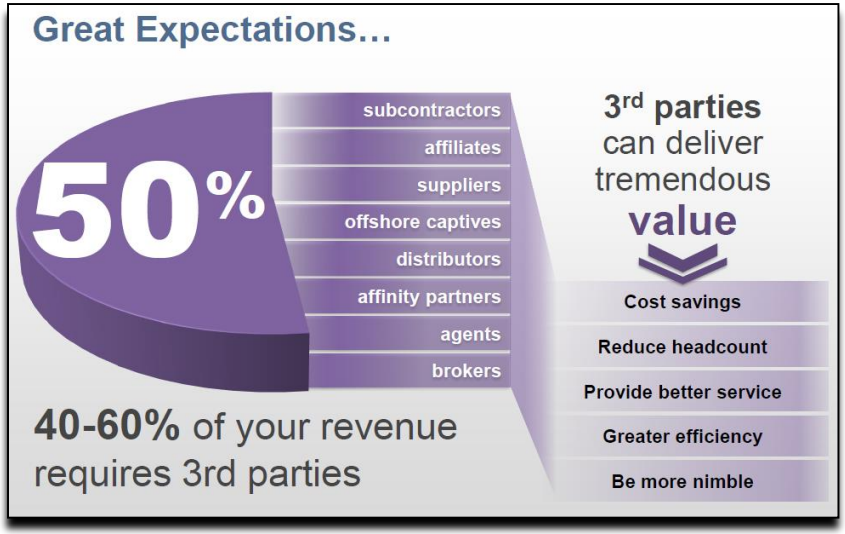
Key Drivers of Third Party Use

Companies are seeing third parties **as a means to gain a competitive edge:**

- Cost Savings, Reduced Headcount
- New or Improved Service offerings
- Greater efficiencies

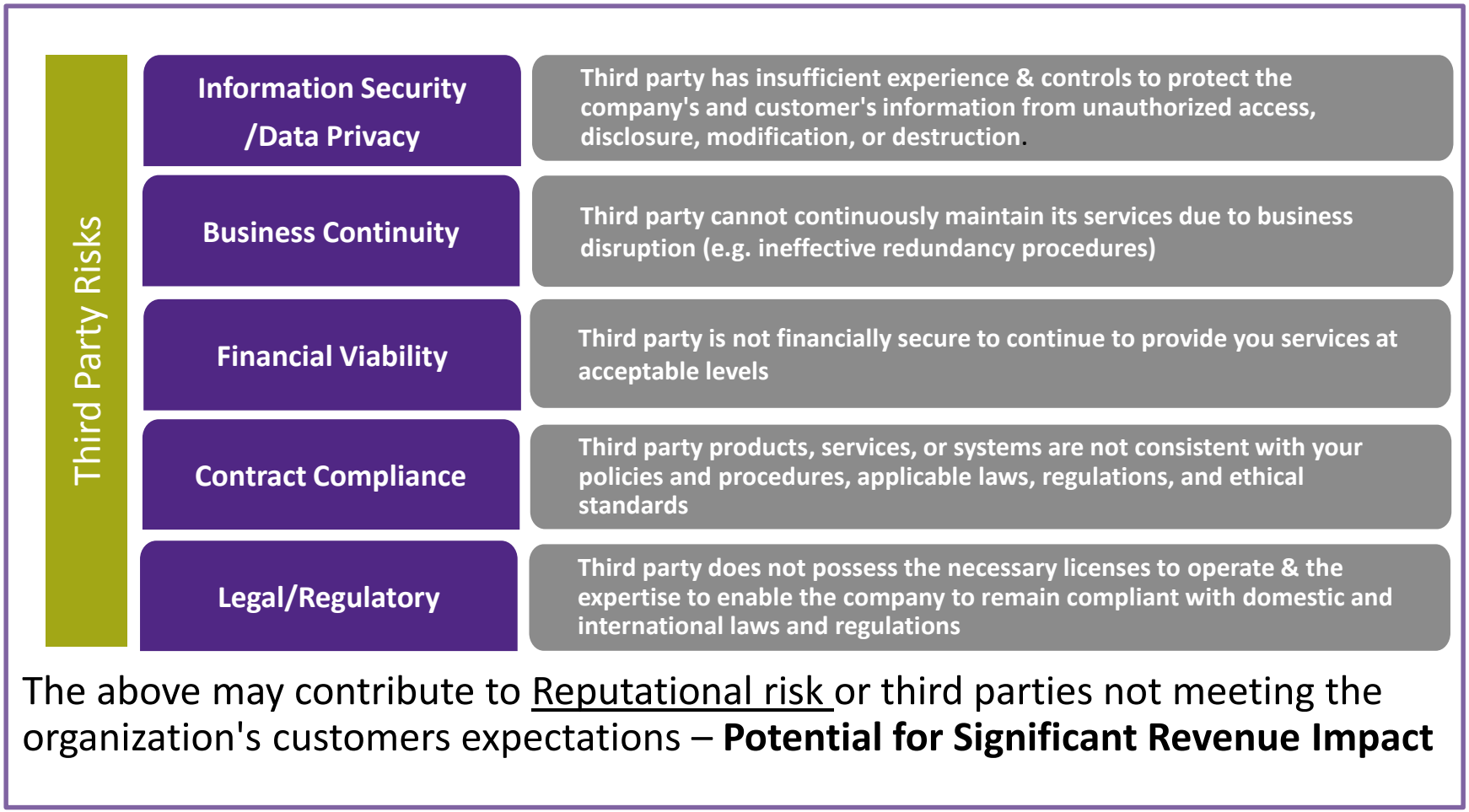
- 40% of CEOs expect the majority of innovations over the next three years to be co-developed with partners

- Roughly a third of CEOs indicated their companies plan to complete a cross-order merger or acquisition, or outsource a business process or function in the next year



3rd Party Risk Management

Key Risk Summary



The above may contribute to Reputational risk or third parties not meeting the organization's customers expectations – **Potential for Significant Revenue Impact**

3rd Party Risk Management
Recent Examples – The risk is real…

- **Info Security: Target** – 40 million stolen credit card numbers, 70 million stolen addresses, 90 lawsuits, $61 million spent remediating to date.
  Bloomberg, 3/13/2014

Reputational Risk: Amex fines $10M, $60M refunded to customers – 3rd party call centers involved in deceptive tactics to sell the company's credit card products.
CFPB - 12/23/2013

Info Security: - FundTech Corp - Operating without effective procedures to identify and address information security vulnerabilities effecting their clients.
OCC, 12/7/2013

BCM Risk: OCC and FDIC identified unsafe and unsound practices relating to Jack Henry and Associates disaster recovery and business continuity planning.
OCC – 3/24/2014

3rd Party Risk Management

Regulators View of Third Parties

Quality of risk management over third-party relationships may not be keeping pace with the level of risk and complexity these relationships cause

- working with third parties that engage directly with customers
- outsourcing entire internal functions to third parties, such as tax, legal, audit, or information technology operations
- outsourcing lines of business or products
- relying on a single third party to perform multiple activities, often to such an extent that the third party becomes an integral component of the company's operations
- contracting with third parties that subcontract activities to other foreign and domestic providers

3rd Party Risk Management

Defining the What

3rd Party Risk management is a comprehensive plan for identifying, and mitigating potential business uncertainties and legal liabilities regarding the hiring of third party services. The plan should oversee the full lifecycle of a third party relationship including:

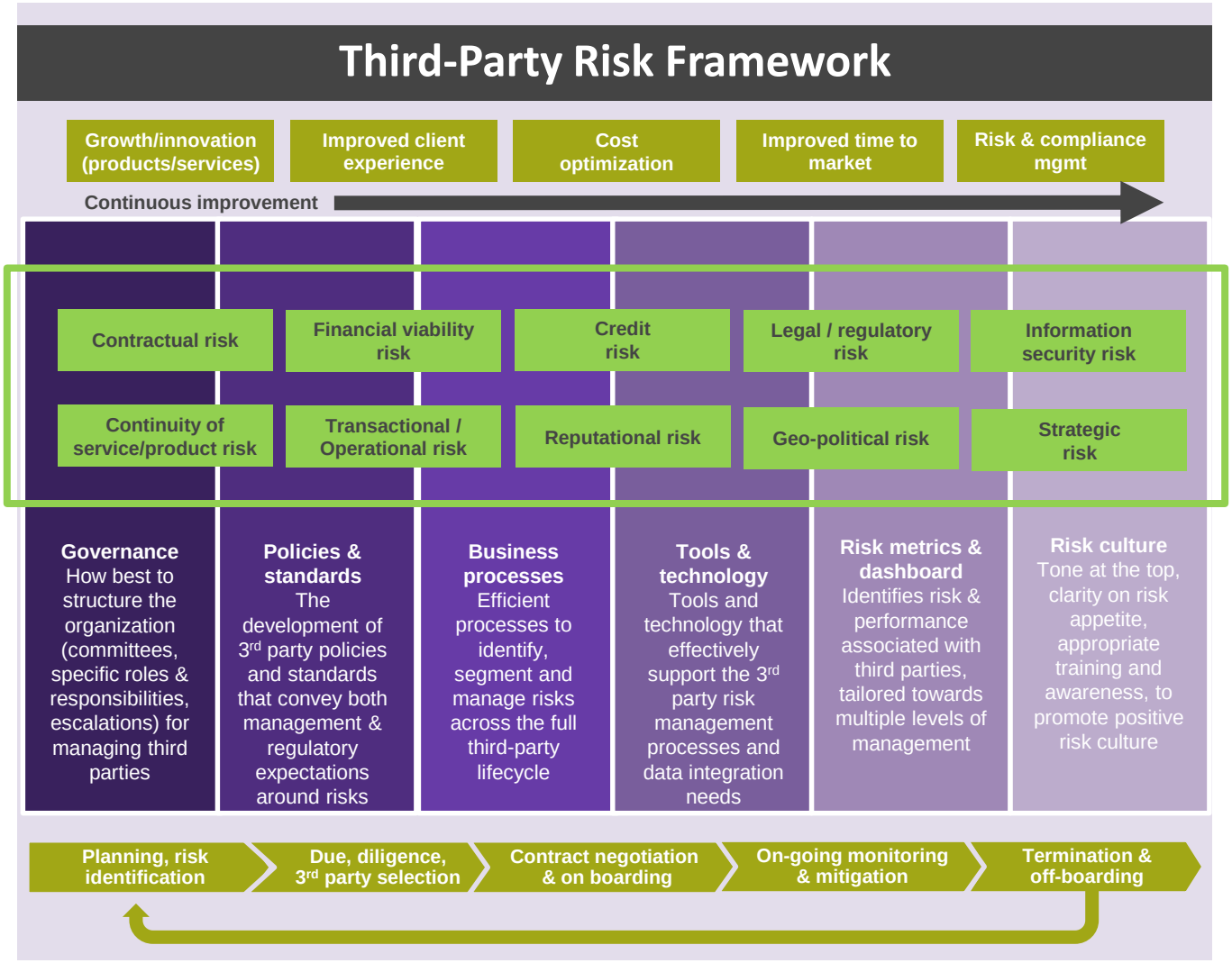
- company's strategy for why it is using the third party, and the inherent risks the relationship presents
- proper due diligence in selecting the third party
- written contracts that outline the rights and responsibilities of all parties
- ongoing monitoring of the third party's activities and performance
- contingency plans for terminating the relationship in an effective manner
- clear roles and responsibilities for overseeing and managing the relationship and risk management process
- Documentation and reporting that facilitates oversight, accountability, monitoring, and risk management
- Independent reviews that allow organization's management to determine that processes align with its strategy and effectively manages risks.

AGENDA

1. OVERVIEW
2. **DEVELOPING A RISK MANAGEMENT FRAMEWORK**
3. VALUE-ADD FROM INTERNAL AUDIT
4. KEYS TO IMPLEMENTING FRAMEWORK SUCCESSFULLY
5. CASE STUDY EXAMPLES

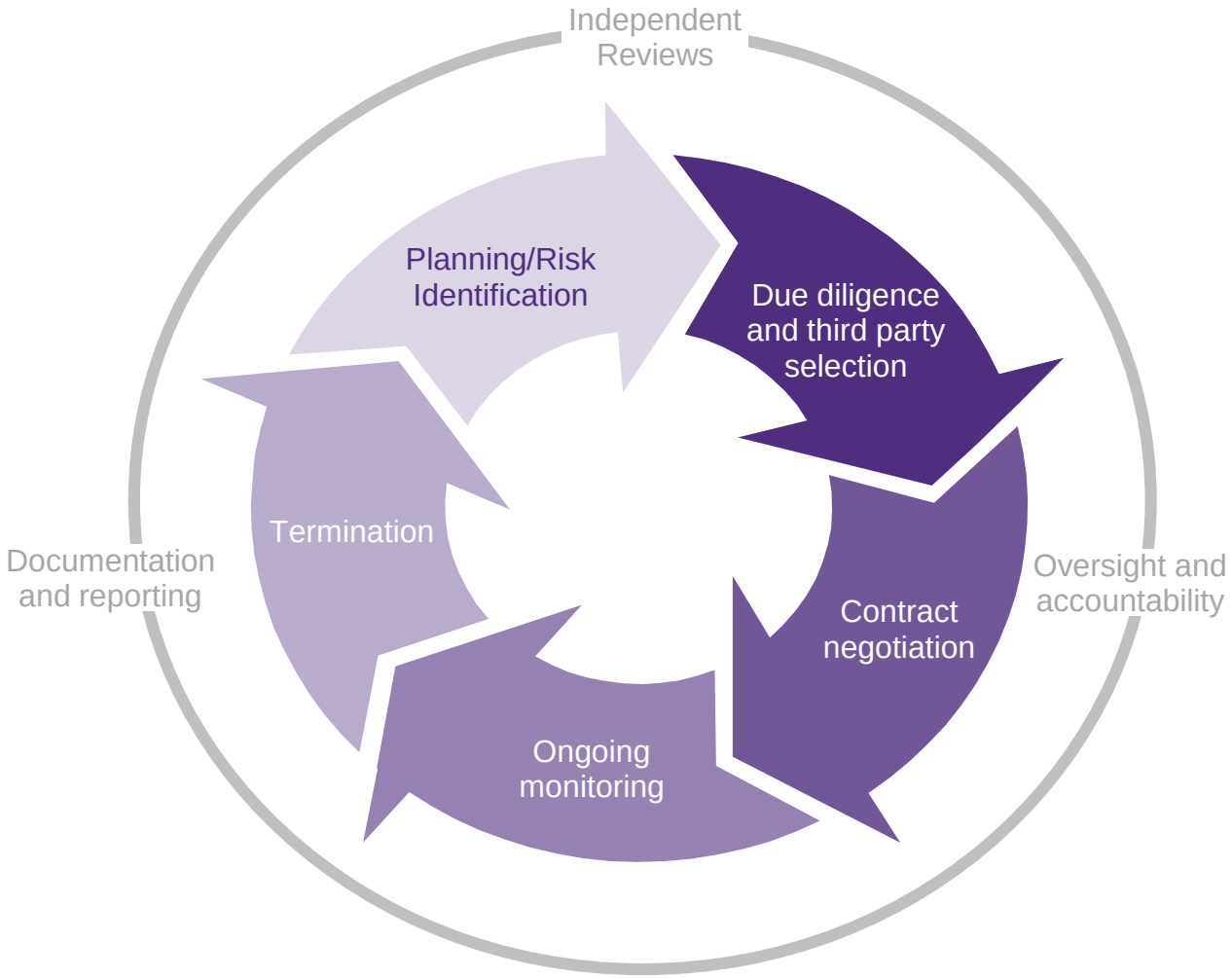
3rd Party Risk Management

Developing Risk Management Framework

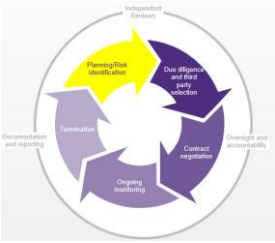


3rd Party Risk Management
Third Party Risk Management Framework

It is expected that companies have risk management processes that are commensurate with the level of risk and complexity of its third-party relationships and their organizational structures.



3rd Party Risk Management
Planning/Risk Identification

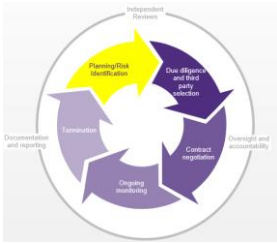


- List of all third party vendors and services they provide (start with vendor master)
- Catalog vendor risks third party relationships may cause
- Segment your supply based on risk criticality

- Regulators define "**critical activities**" as those that…
  - have significant customer impacts
  - cause significant risks to operations if the third party fails to meet expectations – e.g. data privacy, business continuity,
  - requires significant investments in resources to implement the third party relationship and manage the risk (outsource a business function)
  - could have a major impact on the company's operations if an alternative third party is needed or if the outsourced activity has to be brought in house

Note: The planning phase cannot just focus on the current list of third parties but involves risk identification of newly on-boarded third parties before contracts are being signed

3rd Party Risk Management
Planning/Risk Identification

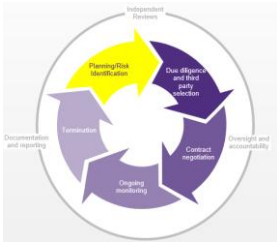


Vendor Tier	Definition
1	A supplier whose products/services provide "critical activities" to a company's operations and revenues and include: • Complex contracts that details specific roles/responsibilities from both parties • Significant customer impacts • Proactive supplier relationship management • Detailed monthly supplier performance reporting
2	A supplier whose products/services are important to a company's operations and revenues and require: • Complex contracts • Proactive supplier relationship management • Detailed quarterly supplier performance reporting
3	A supplier whose products/services are not critical to a company's operations & revenue but require • Standard contracts • Annual supplier performance reporting
4	A supplier whose products/services are not critical to a company's revenue and • Falls within a non-procurement managed category • May utilize standard purchase order terms and conditions

3rd Party Risk Management

Planning/Risk Identification

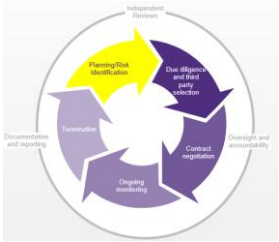
Example of how to define the risk universe



Vendor	Vendor type	Nature of service being provided	Contractual details	Geographic/ global consideration	Applicable regulatory requirements (e.g., HIPAA, FCPA)	Primary relationship owner within organization	Provides an audit report such as SOC 1	Right to audit clause
ABC Payroll	Payroll provider	Payroll processor	Five-year agreement approved by legal department	Payroll processed in Kansas City, Kan.	IRS, Department of Labor	Bob Peoples, Human Resources	Yes, SOC 1	No
IT Help	Help desk support	IT support contractors	One-year auto-renewing contract	Local to each company site and headquarters	N/A	Martin Technology, CIO	No	No
Quick Print	Printing/ mail service provider	Prints/mails invoices and marketing materials	Six-year agreement, approved by legal department	Local to headquarters	N/A	Sally Accountant, CFO	No	No

3rd Party Risk Management

Planning/Risk Identification

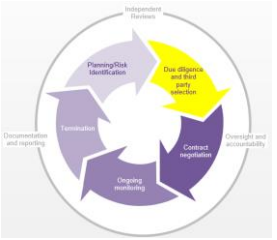


Example - continued: Weighting Risk Factors

Vendor	Significance of the data handled by the vendor	Potential magnitude of a financial loss	Potential magnitude of a reputational loss	Potential magnitude of an operational loss	The frequency of interaction	Expense of vendor in relation to income of the business unit supporting it	Significance of financial risk	Significance of operational risk	Significance of strategic risk
ABC Payroll	3	1	1	5	5	4	3	5	2
IT Help	3	1	1	3	5	2	1	4	1
Quick Print	2	1	4	2	4	1	1	1	1

Rating is from low (1) to high (5). Source: Grant Thornton LLP

3rd Party Risk Management
Due Diligence & Third Party Selection



Degree of Due Diligence should be commensurate with

- ❖ level of risk
- ❖ complexity of the third-party relationship.

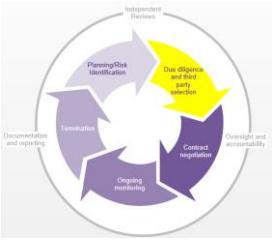
Organizations need to **focus their efforts** on the areas that present the **greatest risks**.

On-site visits may be useful to understand fully the third party's operations and capability to serve

Due Diligence Assessment Criteria:

- Audited Financial Statements
- Business reputation, complaints, and litigation
- Qualifications, backgrounds, and reputation of company's officials
- Risk management procedures
- Compliance capabilities
- Internal Audit coverage
- Internal controls
- Technology and MIS sufficiency, business contingency plans
- Information Security
- Physical Security
- Reliance on sub-contractors
- Insurance coverage

3rd Party Risk Management
Due Diligence & Third Party Selection



3rd Party Risk Assessment Survey

Materiality Assessment

Response Triggers Additional Due Diligence

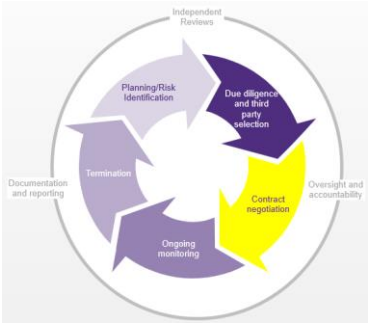
1) Will the provider support a critical business process ?
2) Will the provider have direct interaction with our customers ?
3) Will the provider have access to our network ?
4) Will the provider process, store, transmit or have access to customer or employee data ?
5) Will the provider impact our ability to comply with government or bank regulations ?
6) Is the provider headquartered outside of the United States?
7) Will any services be provided from a non-US location ?
8) Is the spend (one time or annual) greater than $100,000 USD?
9) Will the provider use subcontractors?
10) Does the provider have an existing relationship with us ?

Low Risk Score & Rank Result | **Medium Risk Score & Rank Result** | **High Risk Score & Rank Result**

Score & Rank Outcome

Rank Appropriate Compliance Routines Automatically Launched

3rd Party Risk Management
Contract Negotiations



The board and management should ensure that the expectations and obligations of each party are clearly defined, understood, and enforceable.

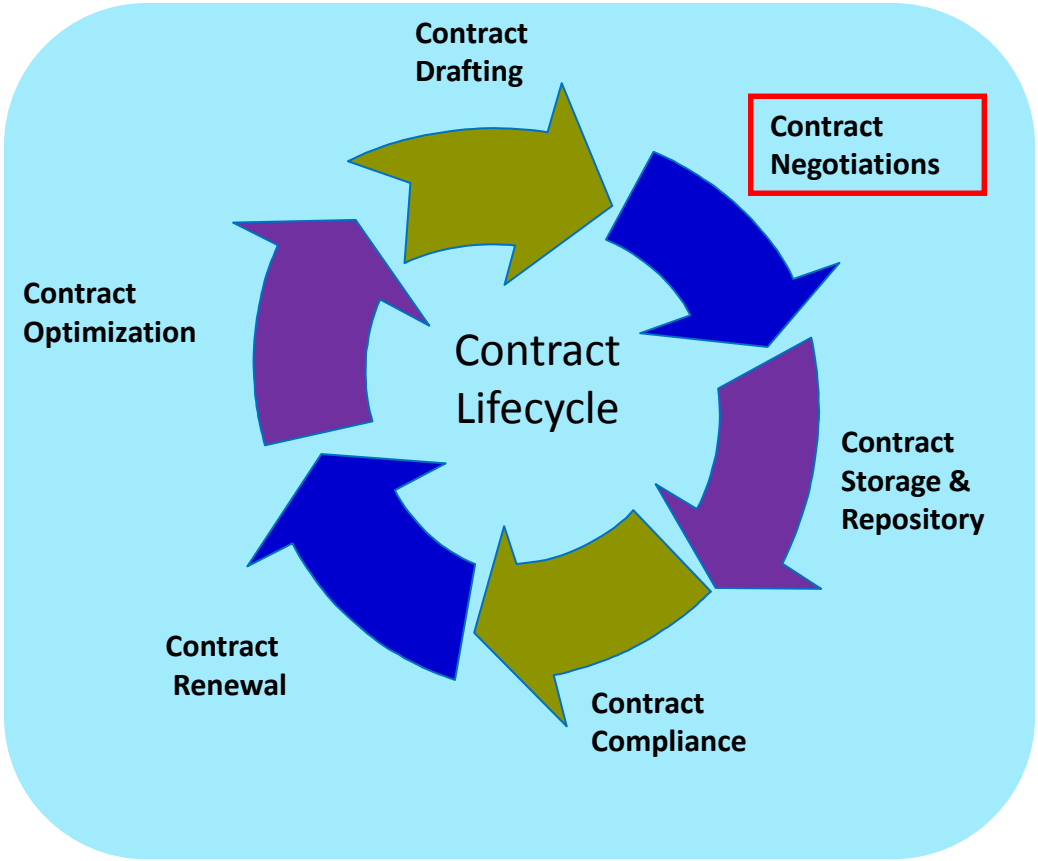
Note: There tends to be time pressure to sign vendors so performing third party DD and contracting cannot be rushed at the expense of a good deal. Have **contract templates** designed with key terms addressing identified risks

Common topics that should be included in contracts are:

- Scope of the arrangement
- Performance measures or benchmarks
- Responsibilities - providing/receiving info
- Regulatory compliance requirements
- Costs and compensation
- Insurance
- Limits on liability
- Business resumption/contingency
- Default and termination
- OCC Supervision
- Sub-contracting
- Foreign Based third parties
- Handling of Customer complaints
- Confidentiality and security
- Indemnification
- Right-to-audit
- "Balanced Scorecard"

3rd Party Risk Management
Contract Negotiations

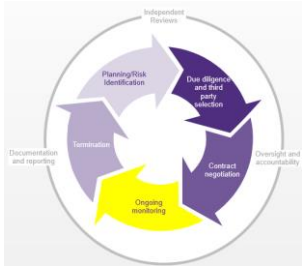
Strong contracts are at the center of good risk management practices, however…



- Lack **central repository** and visibility to in-process contracts
- **Limited standards** on contract types making tracking and reporting on key terms difficult
- Poor compliance practices
- **Lack of automated notifications** on contract expirations and contract non compliance

"4.6 million in contract leakage per billion in spend on average"
- The Hackett Group

3rd Party Risk Management
On-going Monitoring



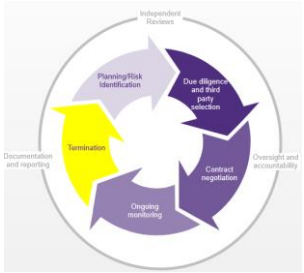
After entering into a contract with a third party, organization management should dedicate sufficient staff with the necessary expertise, authority, and accountability to oversee and **monitor the third party** with respect to its **activities and performance**.

Tier 1 Vendors will be reviewed **at least annually**.

Performance monitoring may include:

- Financial reviews for viability
- Ability to recover from service disruptions (resiliency)
- Ability to maintain confidentiality & integrity company's information (PII)
- Physical security procedures
- Insurance coverage
- Agreements with other entities that may pose a conflict of interest or introduce reputation, operational, or other risks to the organization
- Ability to appropriately remediate customer complaints
- Reliance on & performance of subcontractors
- Changes in key personnel; ability to retain essential knowledge to perform
- Changes to risk management procedures

3rd Party Risk Management
Termination



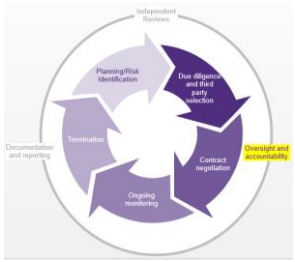
Management should ensure that third party relationships **terminate in an efficient manner**, whether activities are transitioned to another party, brought in-house, or discontinued.

In the event of contract default or termination, the company should **have a plan** in place that brings the service in-house, if there are no alternate third parties.

The Plan should cover:

- capabilities, resources, and the time frame required to transition the activity while still managing legal, regulatory, customer, and other impacts that might arise.
- risks associated with data retention and destruction, information system connections and access control issues, or other control concerns that require additional risk management and monitoring during and after the end of the third-party relationship.
- handling of joint intellectual property developed during the course of the arrangement.
- reputation risks to the organization if the termination happens as a result of the third party's inability to meet expectations.

3rd Party Risk Management
Oversight & Accountability



The organization's board of directors (or a board committee) and senior management are responsible for overseeing the organization's overall risk management processes. There needs to be distinct roles and responsibilities set and escalation procedures communicated.

Illustrative Structure

Board of Directors

- Approve risk-based policies
- Approve contracts that involve critical activities
- Review and take action on significant deficiencies involving critical activities

Enterprise Risk Committee

3rd Party Risk Management

- Policies for 3rd party risk
- Sets structure for risk program and escalation activities
- Oversee risk assessments and remediation activity

Lines of Business

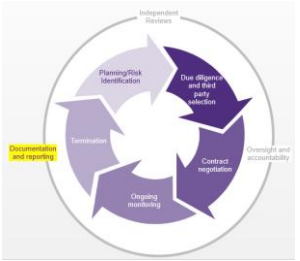
- Owns the risk
- Self assessments
- Risk Remediation

Internal Audit

- Perform periodic reviews
- Highlight and discuss material risks and any deficiencies
- Recommend improvement opportunities

Note: Prepares company for Regulatory Reviews

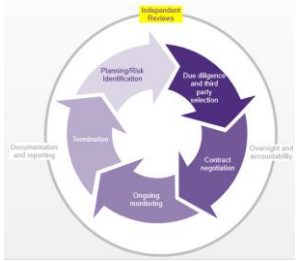
3rd Party Risk Management Documentation & Reporting



A company should properly document and report on its third-party risk management process and arrangements throughout the life cycle. Documentation and reporting facilitates the **accountability, monitoring, and risk management** associated with third parties and typically includes:

- a current inventory of all third-party relationships, which should clearly identify those relationships that involve critical activities and delineate the risks posed by those relationships across the company.
- approved plans for the use of third-party relationships.
- due diligence results, findings, and recommendations.
- analysis of costs associated with each activity or third-party relationship, including any indirect costs assumed by the company.
- executed contracts.
- regular risk management and performance reports required and received from the third party (e.g., audit reports, security reviews, and reports indicating compliance with service-level agreements).
- regular reports to the board and senior management on the results of internal control testing and ongoing monitoring of third parties involved in critical activities.
- regular reports to the board and senior management on the results of independent reviews of the organization's overall risk management process.

3rd Party Risk Management
Independent Reviews



Independent reviews should be conducted on the third-party risk management process, particularly when a company involves third parties in ***critical activities***.

The IA or independent 3rd Party may perform the reviews, and results should be reported to the Board.

A review should consider the following:

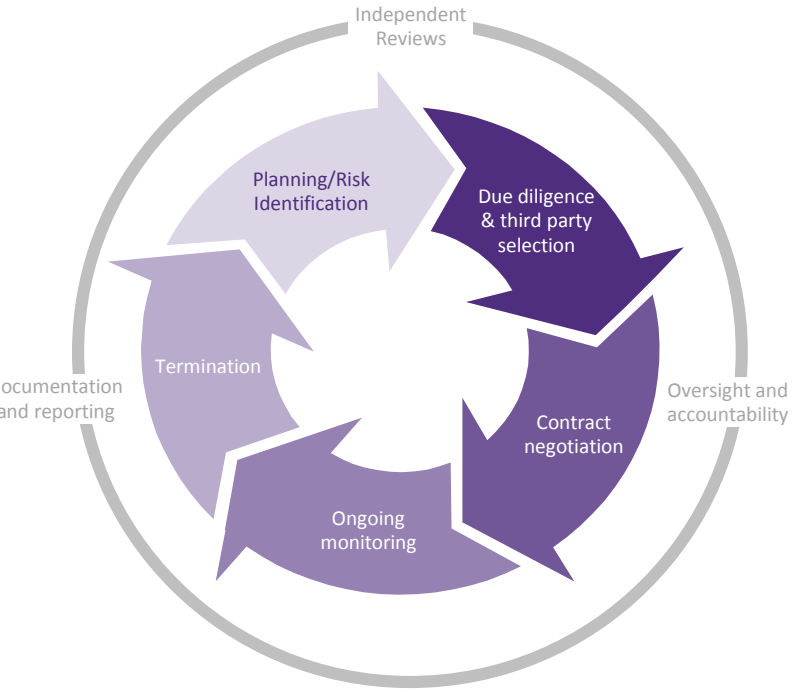
- ensuring third-party relationships continue to align with the company's business strategy
- ensuring proper oversight and accountability for managing third-parties (e.g. roles and responsibilities clear, possess the requisite expertise, resources, and authority).
- ensuring appropriate staffing and expertise to perform due diligence and ongoing monitoring and management of third parties
- identifying and managing third party risks, including foreign-based third parties and subcontractors
- ability to report, track and mitigate identified material breaches, service disruptions, or other material issues.
- ensuring conflicts of interest or appearances of conflicts do not exist
- identifying and managing concentration risks that may arise from relying on a single third party for multiple activities

AGENDA

1. OVERVIEW
2. DEVELOPING A RISK MANAGEMENT FRAMEWORK
3. **VALUE-ADD FROM INTERNAL AUDIT**
4. KEYS TO IMPLEMENTING FRAMEWORK SUCCESSFULLY
5. CASE STUDY EXAMPLES

3rd Party Risk Management
The Value Add from Internal Audit

Audit Strategy: As 3rd party risk management is an enterprise risk, internal audit is in a unique situation to report on its sufficiency across the organization. Remember that many business lines only see their own set of vendors.

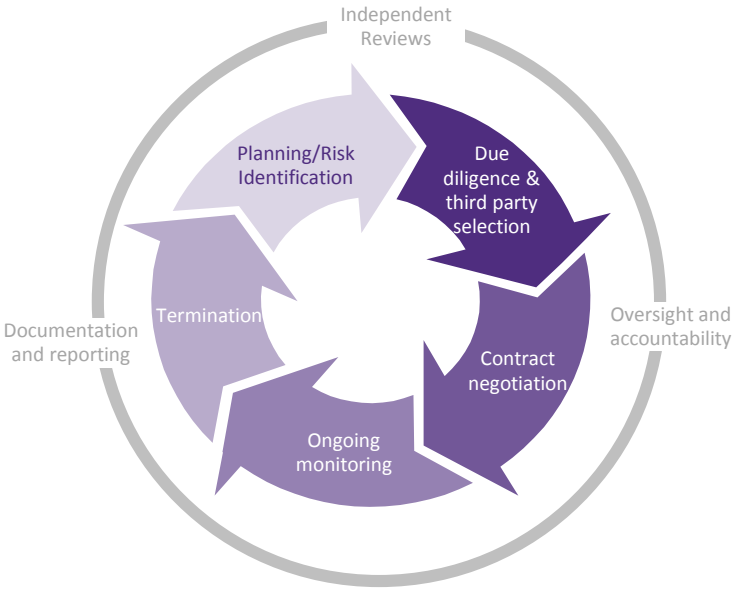


Leading Practice

1. Appoint a "central point of contact" (CPC) in internal audit to face off with vendor management similar to other enterprise risks
2. Sets the audit standard for vendor audit programs
3. Serves as SME on vendor risk management within audit
4. Conducts reviews and identifies potential risks and required remediation
5. Influences/coaches business and control functions audits
6. Develops a point of view on the overall design and operating effectiveness of vendor risk management procedures
7. Communicates and reports that point of view to management and the Chief Audit Executive

3rd Party Risk Management
Summary

- **Plan and Identify** inherent risks associated with the third-party activity
- Perform the proper **due diligence and 3rd party selection**
- **Negotiate contracts** defining rights and responsibilities of all parties specific to your identified risks
- **Continually monitor** third parties' activities and performance – focus on critical activities



- **Terminate** 3rd party relationships if certain criteria are not met, have transitions plans ready
- Provide senior **Oversight and Monitoring**
- Maintain proper **Documentation and Reporting**
- Conduct **Independent Reviews** of the risk management process

AGENDA

1. OVERVIEW
2. DEVELOPING A RISK MANAGEMENT FRAMEWORK
3. VALUE-ADD FROM INTERNAL AUDIT
4. **KEYS TO IMPLEMENTING FRAMEWORK SUCCESSFULLY**
5. CASE STUDY EXAMPLES

3rd Party Risk Management

Keys to Implementing Program Successfully

The following are a sample of areas where we feel make a difference to a successful third party risk deployment

STRONG TONE AT THE TOP	SUPPORTING TONE AT THE MIDDLE	PROPER STRATEGY & GOVERNANCE	COMPREHENSIVE TRAINING	NETWORK OF SUPPPORT	RISK MANAGEMENT REPORTING
• Build a culture and individual ownership for risk management • Define and communicate importance & obligation • Engage in ongoing conversations with key leaders , Influencers about the program • Ensure consistent communications from leadership to all employees	• Reinforce risk culture and ownership from the top • Identify key users impacted • Develop discussion-based program to be included in pre-standing meetings • Reinforce benefits and impact users can have on the company • Allow business input to select risk scenarios most applicable to their staff • Equip the business with all necessary materials	• Don't boil the ocean - take a risk-based approach; focus on most critical services • Develop a strong project governance • Define clear roles and responsibility and importance of accountability with tone from top • Articulate what constitutes program success • Incorporate use of technology to drive accuracy and efficiency	• Important part of building risk based culture • Embed risk as part of company wide training programs • Include role based training, including critical third parties • Make as part of supplier onboarding program – what service what risks may be posed	• Develop a strong change management program • Identify your critical influencers of change and develop compliance champions • Establish key roles/ responsibilities, have champions actively sell the benefits of the program • Provide assistance with program barriers	• Identify critical data elements for 3RD Party risk reporting • Develop standard add repeatable dashboards - by region/area of responsibility • Provide effectively program monitoring

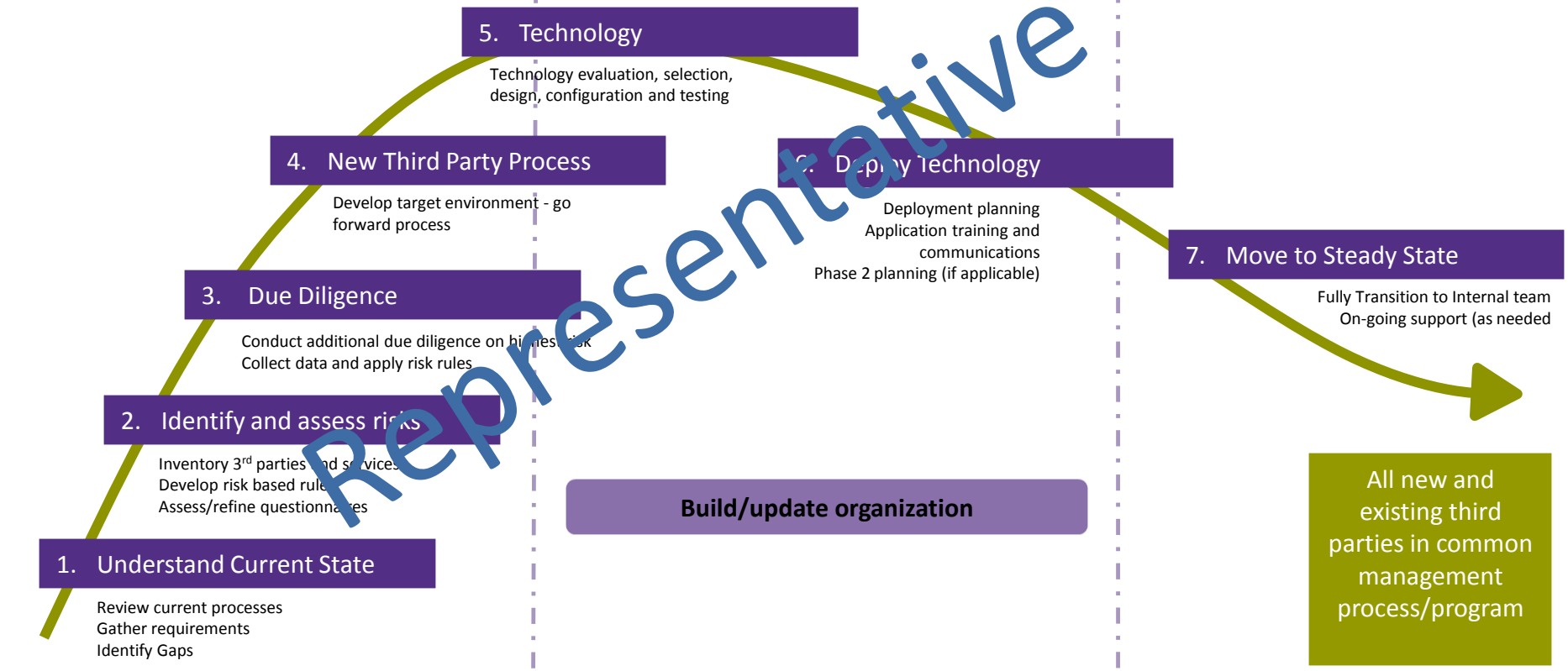
Third-Party Management

Implementation Strategy – Key Progression

Develop:
- Understand current state.
- Build approach and provide external expertise (where needed)

Operationalize:
- Roll out all elements of program.
- Finish all "existing third party" work.

Maintain:
- Integrate all processes into business-as-usual



AGENDA

1. OVERVIEW
2. DEVELOPING A RISK MANAGEMENT FRAMEWORK
3. VALUE-ADD FROM INTERNAL AUDIT
4. KEYS TO IMPLEMENTING FRAMEWORK SUCCESSFULLY
5. **CASE STUDY EXAMPLES**

Case Study 1

The issue:

- A Global Fortune 500 Corporation
- More than 110,000 employees
- Operates in over 60 countries
- Self-disclosed FCPA violations to the Department of Justice
- Had to get better and more adaptive

Case Study 1 – continued -

The Solution:

- Develop and implement a FCPA-based Third Party Program
- Implement new onboarding process
- Identify and assess legacy relationships
- Implement automated vendor management solution
- Implement requirements for certain third party relationships, including the generation of a written agreement and a training process.
- Enable ongoing vendor reviews and assessments

Case Study 1 – continued -

Benefits:

- Developed a centralized solution for the client that is a single source of compliance related Third-Party data
- Standardized the review and acceptance of a new third party business relationship
- Provided insight and seamless transparency into the third party relationships retained that would otherwise be unseen
- This Third Party data was used to validate the creation of a new customer master or vendor master file within the Client's local ERP system.
- With the written agreement process, the program also resulted in:
  - the reviewing, updating, and\or creating of approximately 10,000 agreements; and
  - an overall more efficient process of creating valid agreements helping to further protect the Client from any unforeseen risks
- To date, the Client's third party population has exceeded 80,000 relationships and is continually growing

Case Study 2

The issue:

- A primary provider of electronic payment solutions for more then 1,300 banks (11,900 customers)
- Subject to OCC/FDIC oversight of Vendor Risk Management Practices.
- Hurricane Sandy severely flooded its NJ processing center
- $13.7 million in damages and rendering it inoperable
- Data processing transferred to its Oklahoma City processing center
- Hundreds of its core banking clients were impacted with processing backlogs
- The OCC, FDIC and FRB of St. Louis identified unsafe and unsound practices relating to its DR and BCP (and fined)

Case Study 2 – continued -

The Solution:

- Maintain an active Compliance Committee of at least three (3) directors
- Provide progress updates to depository clients
- Prepare potential impacts on its customers as a result of business disruptions and mitigation strategies
- Identification of legal and regulatory requirements for business functions and processes
- Estimation of the maximum allowable operational downtime
- Estimation of recovery time objectives
- Gaps analysis of new Business Continuity Management procedures compared to existing and actions to close gaps
- Assessing the testing program and test results on at **least an annual basis by an independent party**

Case Study 2 – continued -

Benefits:

- Revamped procedures to meet compliance requirements with OCC/FDIC for BC/DRP
- Established oversight and accountability functions within the business
- Renegotiated contracts with specific terms for BC/DRP and monitoring
- Developed monitoring and reporting procedures
- Required an independent assessment of BC/DRP and monitoring and reporting procedures with results for customers, regulators and the Board

Questions?

Third Party Risk: Comply with Confidence, Execute with Efficiency

Orus Dearman, Director
Advisory Services
P 415.318.2240
E Orus.Dearman@us.gt.com

Johanna Terronez, Senior Manager
Advisory Services
P 415.318.2228
E Johanna.Terronez@us.gt.com

Grant Thornton LLP
101 California Street, Suite 2700
San Francisco, CA 94103
www.GrantThornton.com

Core Competencies – C21