Understanding your vendor management risks

an independent member of
BAKER TILLY
INTERNATIONAL

Baker Tilly refers to Baker Tilly Virchow Krause, LLP,
an independently owned and managed member of Baker Tilly International.

BAKER TILLY

Candor. Insight. Results.

Agenda

BAKER TILLY

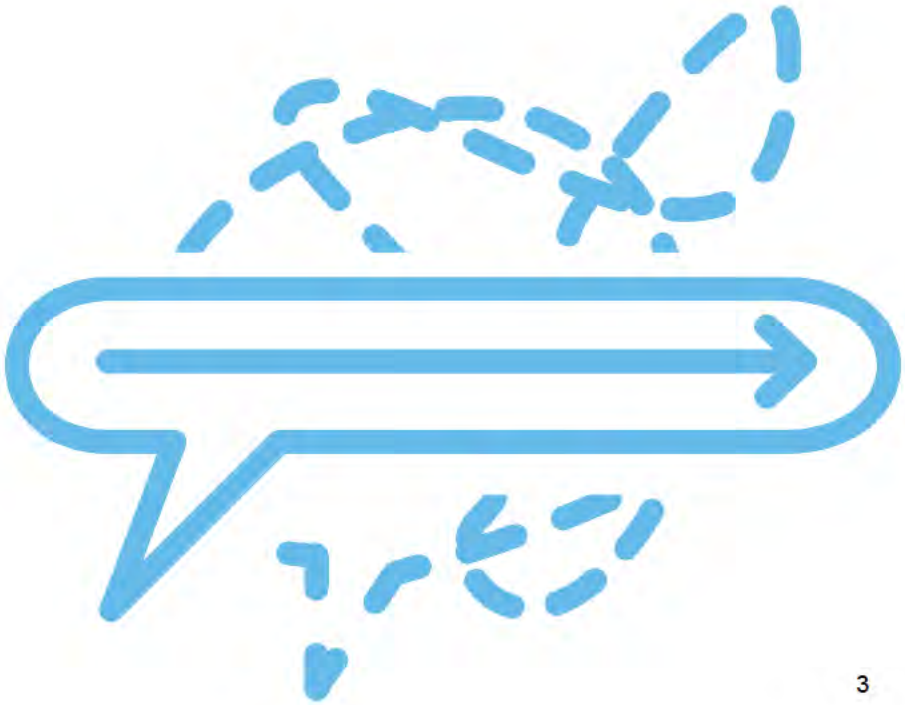
Candor. Insight. Results.

1) Drivers for vendor management
2) Effective vendor management
3) Vendor management life cycle
4) Ongoing monitoring
5) Key takeaways
6) Questions

BAKER TILLY

Candor. Insight. Results.

DRIVERS FOR VENDOR MANAGEMENT



Increasing focus

BAKER TILLY

Candor. Insight. Results.

Two-thirds of companies 'extensively or significantly' rely on vendors

(IIARF)

40% of CEOs expect to develop majority of upcoming innovations with strategic partners

(PwC 2011 Annual Global CEO Survey)

IT is outsourced more than any other function

(Outsourcing Institute)

63% of data breaches in 2013 involved a third-party

(2013 Trustwave Global Security Report)

Increased Risk

BAKER TILLY

Candor. Insight. Results.

Case study: Multi-billion dollar financial institution

Vendor reliance

- Over 400 vendors
- More than 30 were identified as critical
- Approximately 160 “Critical Applications” identified (operational, financial, security, etc.)
- Approximately 60% hosted onsite (35% running at an offsite hot site)
- 40% Software as a Service (SaaS)

BAKER TILLY

Candor. Insight. Results.

National Archive and Records Administration (NARA)

Fall 2008: A NARA hard drive containing the names and Social Security Numbers of 76 million U.S. military veterans was sent to a government contractor for repair after it stopped functioning. The vendor determined the drive could not be repaired — so it was sent it out to be scrapped. However, no evidence exists to confirm whether the drive was actually destroyed.

TD Bank

Spring 2012: Vendors lost two unencrypted tapes in transit containing customers' personally identifiable information (PII)

Capital One

Summer 2012: Call-center contractors used deceptive marketing practices to pressure customers into purchasing credit card 'add-on' products over a multi-year period. As a result, the company paid out $150 million in customer refunds and $60 million in fines.

Drivers for vendor risk management

BAKER TILLY

Candor. Insight. Results.

Business Factors

- Increased number and complexity of vendor relationships
- Informal vendor selection process
- Inability to identify relevant risks by vendor relationship
- Insufficient knowledge of vendor universe
- Inconsistent risk assessment and monitoring practices

Regulatory Focus

- *NAIC*: Annual Financial Reporting Model Regulation, Implementation Guide, Appendix G
- *OCC*: Bulletin 2013-29, Third Party Relationships
- *FINRA*: Rule 3190: Third Party Service Providers
- COSO 2013 Internal Control – Integrated Framework

Drivers for vendor risk management

BAKER TILLY

Candor. Insight. Results.

Outsourcing business operations does *not* absolve organizations of their responsibilities to manage risk!

BAKER TILLY

Candor. Insight. Results.

EFFECTIVE VENDOR MANAGEMENT

Effective vendor risk management

BAKER TILLY

Candor. Insight. Results.

Effective vendor management programs

should…

- Consider organizational strategy
- Evaluate the degree of risk and complexity of each relationship
- Align activities based on evaluation
- Define roles and responsibilities
- Develop reporting mechanisms to facilitate monitoring
- Involves relevant stakeholders

BAKER TILLY

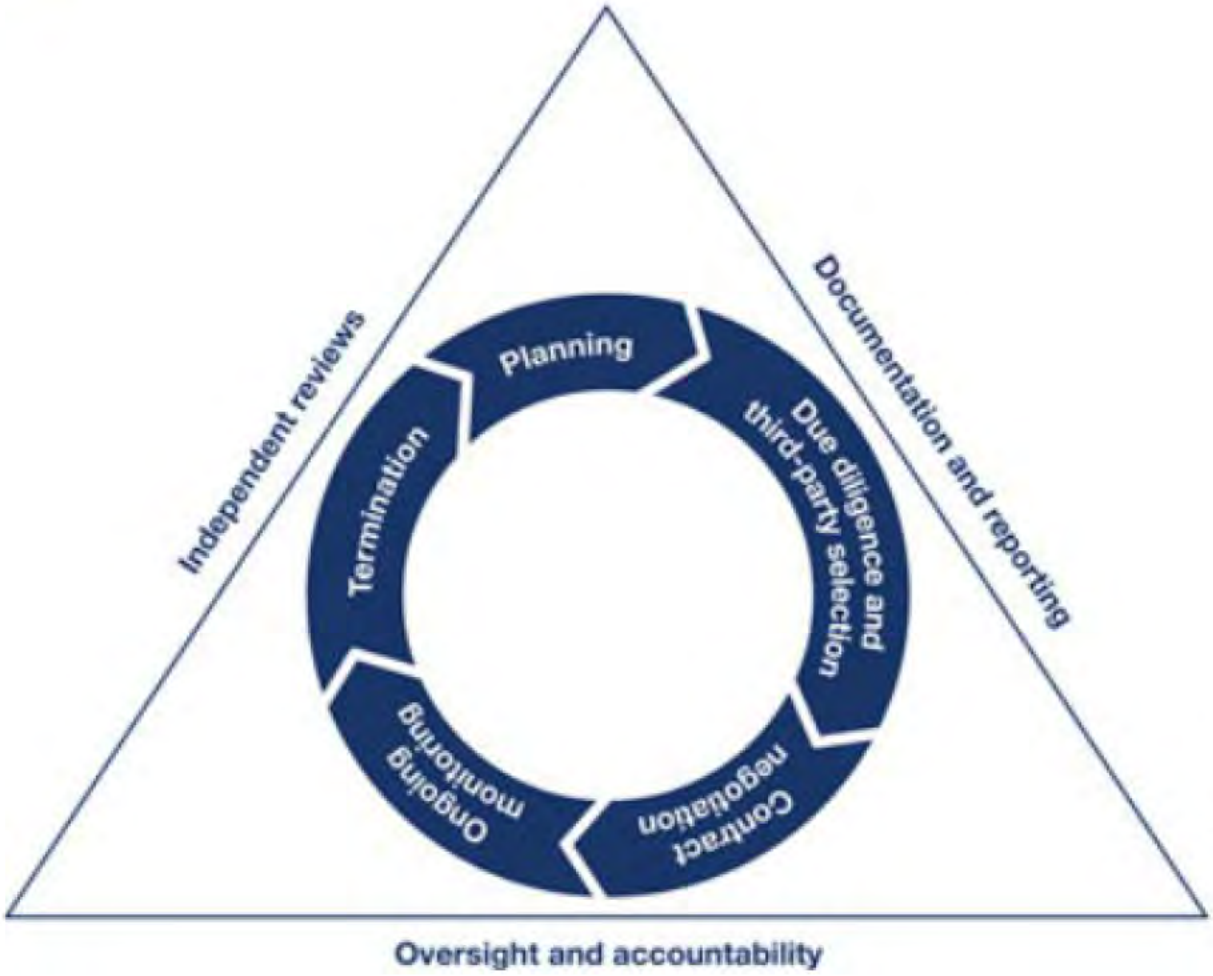
Candor. Insight. Results.

VENDOR MANAGEMENT LIFE CYCLE

Vendor management life cycle

BAKER TILLY

Candor. Insight. Results.



Source: OCC

Vendor management life cycle

BAKER TILLY

Candor. Insight. Results.

Planning | **Due Diligence** | **Contract Negotiation** | **Ongoing Monitoring** | **Termination**

- Determine the scope of services to be provided
- Assess related vendor risks
- Identify potential vendors
- Issue a Request for Proposal (RFP) or equivalent
- Involve relevant stakeholders:
  - Business Process/Relationship Owner;
  - Subject Matter Expert;
  - IT/Information Security

Vendor management life cycle

BAKER TILLY

Candor. Insight. Results.

Planning | Due Diligence | Contract Negotiation | Ongoing Monitoring | Termination

> Scale activities based on risk and complexity

> Obtain organizational information for each vendor
- Company history
- Reputational and financial standing
- Risk management program
- Information security practices
- Business continuity / recovery plan
- Any use of sub-contractors (“fourth-party vendors”)

> Evaluate and select chosen service provider

Vendor management life cycle

BAKER TILLY

Candor. Insight. Results.

Planning | Due Diligence | **Contract Negotiation** | Ongoing Monitoring | Termination

- Use clear, unambiguous language
- Define scope, timing and fees for the arrangement
- Document data confidentiality responsibilities
- Determine any performance measures and/or benchmarks
- Incorporate internal control monitoring requirements (e.g., SOC report, right to audit)

BAKER TILLY

Candor. Insight. Results.

ONGOING MONITORING

Vendor management life cycle

BAKER TILLY

Candor. Insight. Results.

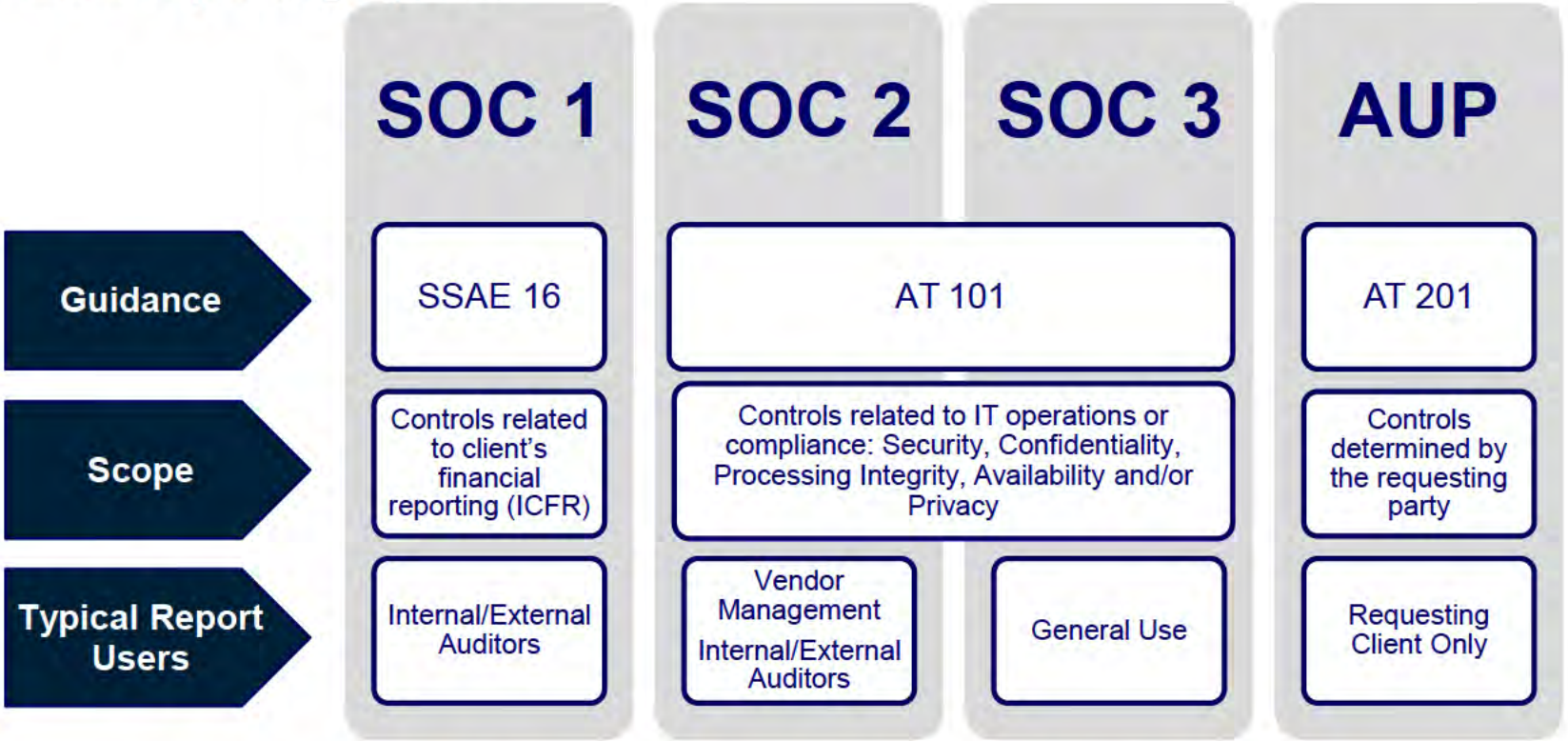
Planning | Due Diligence | Contract Negotiation | Ongoing Monitoring | Termination

- Continue to monitor the same areas evaluated during due diligence
  - Periodic risk assessment questionnaires
  - Service-level agreement monitoring
  - Service Organization Control (SOC) examination reports
- Establish criteria for ‘critical vendors’ and increase the frequency and depth of monitoring activities

BAKER TILLY

Candor. Insight. Results.

SOC reporting options



Remember: the 'best' option is subjective, and based on the services performed and related third-party risks

BAKER TILLY

Candor. Insight. Results.

SOC report considerations

- Does the scope of the report address the services provided by the vendor?
- Is the examination period sufficient to provide assurance over the control activities? (Type 1 vs. Type 2)
- How are the Complementary User Entity Controls included by the service organization addressed within your organization?
- Do identified control findings, if any, result in risk to your organization? If so:
  - What actions has the service organization taken to address the findings?
  - What mitigating controls exist either at the service organization or within your organization to address those risks?

Vendor management life cycle

BAKER TILLY

Candor. Insight. Results.

Planning | Due Diligence | Contract Negotiation | Ongoing Monitoring | Termination

- Understand and document the services performed by the vendor
- Develop a plan to transfer activities to another provider (or bring in-house)
- Evaluate the degree of difficultly and specific risk factors of transition
- Define and monitor data transmission, retention and destruction actions

BAKER TILLY

Candor. Insight. Results.

KEY TAKEAWAYS

Key takeaways

BAKER TILLY

Candor. Insight. Results.

- Develop a formal, standardized process for vendor management
- Identify risk considerations by vendor, including criteria for critical vendors
- Tailor due diligence activities based on risk
- Continue risk management for existing vendors through ongoing monitoring
- Determine whether a SOC report will effectively meet monitoring needs

Disclosure

BAKER TILLY

Candor. Insight. Results.

The information provided here is of a general nature and is not intended to address the specific circumstances of any individual or entity. In specific circumstances, the services of a professional should be sought.

Baker Tilly refers to Baker Tilly Virchow Krause, LLP, an independently owned and managed member of Baker Tilly International. © 2015 Baker Tilly Virchow Krause, LLP