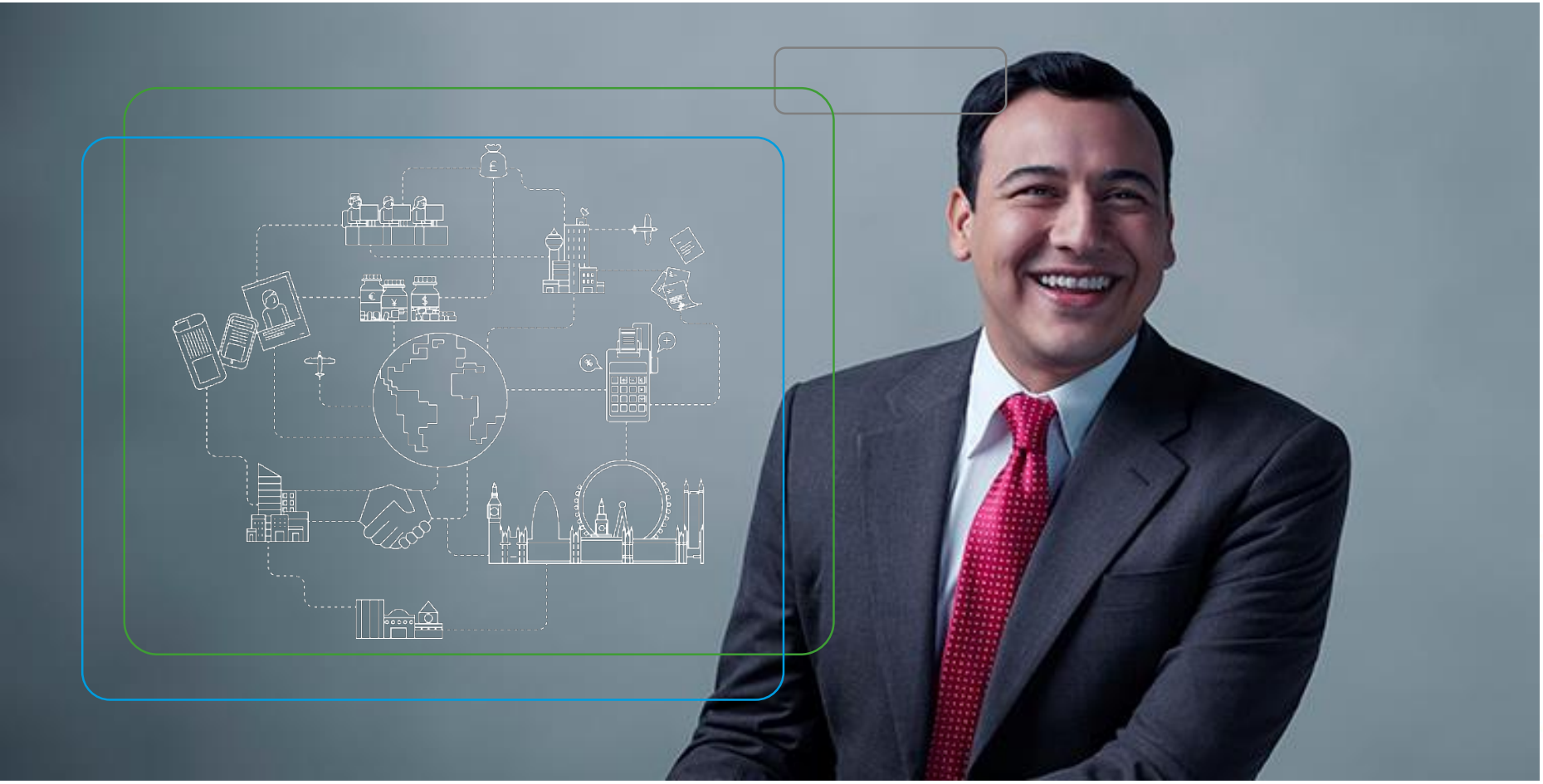

Cybersecurity, vendors and you—understanding and controlling your risks

December 2, 2015

THE POWER OF BEING UNDERSTOOD
AUDIT | TAX | CONSULTING

RSM

Agenda

- Introductions
- Regulator focus on IT vendor management
  - IT vendor management and cybersecurity
  - Regulatory letters/advisories
- IT vendor management program
  - IT vendor risk assessment
  - Risk management program
- Contacts
- Questions

Introductions

Your presenter:

Andy Ellsweig, CPA,
CGEIT, CITP
Director,
IT Risk Advisory Services
Andy.ellsweig@rsmus.com

- 30 + years performing financial, operational & IT audits
- Firm subject matter expert in performing audits of legacy environments
- Have led and performed many onsite vendor audits including off shore programming groups

REGULATOR FOCUS ON IT VENDOR MANAGEMENT

IT vendor management and cybersecurity

- Definition: for purposes of this webcast and presentation:
  - Vendor/IT vendor = outsourced third-party IT provider
  - Examples include:
    - Third-party IT support
    - Managed IT services—network monitoring, firewall monitoring, intrusion detection monitoring, etc.
    - Cloud services—SAAS, IAAS, etc.
    - Non-IT vendors with connections to networks and systems—heating and ventilation controls (HVAC), building security, etc.

RSM

IT vendor management and cybersecurity

- No bank is an “island” when it comes to information security, almost all use one IT vendor or another.

  Security is only as strong as the weakest link is a common statement that needs to be expanded to account for the vendors.

RSM

IT vendor management and cybersecurity

- Why the recent focus on IT vendor management?
  - Banks have been performing vendor management for years.
  - The vendors provide documents such as SSAE 16 SOC reports, insurance documents, etc.
  - Many vendors have worked with banks for years and are “trusted.”
  - The banks’ review of the documentation and information provided by the vendors has been limited; now a more critical review is needed.
  - The issue is heightened awareness of the fact that an IT vendor can significantly impact an organization’s system security.

RSM

IT vendor management and cybersecurity

- Recent regulatory advisories (Listed in order of usefulness):
  - FFIEC Cybersecurity Assessment Tool
  - FFIEC—http://ithandbook.ffiec.gov/it-booklets/business-continuity-planning/appendix-j-strengthening-the-resilience-of-outsourced-technology-services.aspx
  - http://www.occ.gov/news-issuances/bulletins/2013/bulletin-2013-29.html
  - https://www.fdic.gov/news/news/financial/2014/fil14013.pdf
  - http://www.federalreserve.gov/bankinforeg/srletters/sr1319a1.pdf

IT vendor management and cybersecurity

FFIEC Cybersecurity Assessment Tool

Mapping Baseline Statements to FFIEC IT Examination Handbook

Yes/No	FFIEC Cybersecurity Assessment Tool
	Relationship Management/Due Diligence: Risk-based due diligence is performed on prospective third parties before contracts are signed, including reviews of their background, reputation, financial condition, stability, and security controls. *Source: IS.B.69:* Financial institutions should exercise their security responsibilities for outsourced operations through appropriate due diligence in service provider research and selection. *IS.WP.I.5:* Evaluate the sufficiency of security-related due diligence in service provider research and selection. ** Operations, Outsourcing, E-Banking, Retail Payments*
	Relationship Management/Due Diligence: A list of third-party service providers is maintained. *Source: OT.B.19:* To increase monitoring effectiveness, management should periodically rank service provider relationships according to risk to determine which service providers require closer monitoring. *OT.WP.I.1.3:* Interview management and review institution information to identify…current outsourcing relationships, including cloud computing relationships, and changes to those relationships since the last examination. Identify any material service provider subcontractors; affiliated service providers; foreign-based third-party providers; current transaction volume in each function outsourced; any material problems experienced with the service provided; and service providers with significant financial- or control-related weaknesses.
	Relationship Management/Due Diligence: A risk assessment is conducted to identify criticality of service providers. *Source: OT.B.6:* Management should consider the following factors in evaluating the quantity of risk at the inception of an outsourcing decision, [including]…Risks pertaining to the function outsourced include… [and] Risks pertaining to the technology used. *OT.B.23:* Financial institutions must also consider which of their critical financial services rely on TSP services, including key telecommunication and network service providers.

Source: FFIEC

RSM

IT vendor management and cybersecurity

- Recent breaches due to IT vendor security issues:
  - Target—vendor party providing services was a managed HVAC provider
  - Zappos—vendor providing services was server hosting entity (cloud provider—IAAS)
  - Lowes—vendor, a third-party vendor called E-DriverFile inadvertently exposed personal employee information to the Internet as a whole

RSM

IT VENDOR MANAGEMENT PROGRAM

IT vendor management program

- Similar to other critical vendors, certain due diligence required when evaluating IT vendors

- Representative due diligence procedures
  - New IT vendors should have a risk assessment completed.
  - The vendor management program requirements for vendors is adjusted based on the risk assessment of the vendor.
  - The frequency of vendor review within the management program is dependent n the risk assessment of the vendor.

RSM

IT vendor management program

- IT vendor risk assessment
  - The risk assessment of the IT vendor is generally dependent on the classification of data or information that the vendor is exposed to.

    Common classes include:
    - Public*
    - Nonpublic (confidential)
    - Nonpublic (private)

**Public data is free to be released and does not require encryption.*

IT vendor management program

- IT vendor risk assessment
  - What the vendor does with the bank's data also factors into risk assessment:

    Common uses of data include:
    - Storing nonpublic data
    - Processing nonpublic data
    - Outputting nonpublic data

    (Nonpublic data requires encryption in transport.)

IT vendor management program

- IT vendor management program
  - The frequency of vendor review is dependent on the risk rating of the vendor. Typically the minimum review frequency is:
    - Critical or high risk—annual
    - Medium risk—annual to 18 months
    - Low risk—18 months to 24 months

IT vendor management program

- IT vendor management program
  - What are the typical items included in a review and what is minimal test?
    - Current contract
      - Review terms/identify when contract renewal period is.
      - Identify terms and conditions
        - Since some of these contracts may have been inked years ago—might be time for a “modifications to MSA, etc.”

RSM

IT vendor management program

- IT vendor management program
  - Financial reports
    - Determine whether the vendor is financially stable or if there are concerns.
    - Is the vendor’s financial strength improving/stable or weakening?
    - Has the vendor been acquired or have they made acquisitions?

IT vendor management program

- IT vendor management program
  - Privacy agreement/non-disclosure agreement (NDA)
    - Is there a separate privacy agreement or NDA in place with the vendor?
    - If not, validate the an equivalent is in the terms and conditions of the contract.
    - If not in the terms and conditions, a separate mutual NDA might be easier to get in place.

RSM

IT vendor management program

- IT vendor management program
  - SOC reports
    - Typically these are required for only critical- or high-risk vendors but are recommended for other vendors as applicable.
    - SOC 1, SOC 2, and SOC 3 reports

IT vendor management program

- IT vendor management program
  - Third-party security review:
    - Does the vendor have a third-party security review performed?
      - Internal and external network vulnerability and penetration testing preferred
      - Social engineering and application testing strongly recommended
    - The vendor should have a mechanism in place to securely share their report with you.

RSM

IT vendor management program

- IT vendor management program
  - Other vendor documentation/considerations:
    - Insurance coverage—Verify that the vendor has cybersecurity or breach liability insurance in place. Validate the limits and determine if additional insurance is needed to cover the gap.
    - Contractors—Does the vendor utilize contractors or employees to manage their operation/security?

IT vendor management program

- IT vendor management program
  - Other vendor documentation/considerations:
    - Business continuity planning and testing—they should be able to provide business continuity plan and testing evidence.
    - Can their provide copies of their information security policy with particular focus on how they manage sensitive and proprietary information, transmissions of data, and other security measures.

IT vendor management program

- IT vendor management program
  - Other vendor documentation/considerations:
    - Does the vendor monitor their third parties?
    - On-site audits.
    - Automated alerts or tracking of sensitive information.

How to assess vendors for Cybersecurity?

SOC 1 or SOC 2

Users of each report and why

	Who	Why	What
SOC 1	User entity accounting/ finance department and their auditors	Financial Audit	Controls relevant to user financial reporting
SOC 2	User entity departments other than accounting/finance Regulators Others	Governance, risk and compliance (or GRC) programs Oversight Due diligence Cybersecurity	Assurance regarding security, availability, processing integrity, confidentiality, and/or privacy
SOC 3	Any users with need for confidence in service organization's controls	Marketing "Confidence without the detail"	Seal and simplified report on controls

RSM

Trust services principles—updates to privacy

Domain	Principle
Security	The system is protected against unauthorized access (both physical and logical).
Availability	The system is available for operation and use as committed or agreed (includes environmental criteria).
Confidentiality	Information designated as confidential is protected as committed or agreed.
Processing Integrity	System processing is complete, accurate, timely and authorized.
Privacy	Personal information is collected, used, retained, disclosed and destroyed in conformity with the commitments in the entity's privacy notice and with criteria set forth in generally accepted privacy principles (or GAPP) issued by AICPA and Certified Internal Controls Auditor (or CICA).

Trust principles—summary of criteria

Principle	Topic	Criteria
Common Criteria (applicable across all principles and fully inclusive of security) **Total of 28 Shared Criteria**	Organization and Management	4
	Communication	6
	Risk Management	3
	Monitoring of Controls	1
	Logical and Physical Access	8
	System Operations	2
	Change Management	4
Availability	Availability	3
Processing Integrity	Processing Integrity	6
Confidentiality	Confidentiality	6
Privacy	**Privacy**	**73**

RSM

SSAE16s

Vendor Management Myth #1: My Provider is SSAE16 (formerly SAS70) "Certified," so I do not have to worry about my data

- SSAE 16 "Certified" is a misnomer as there is no certification given upon completing an SSAE 16 attestation engagement.
- SSAE16s are a good first step for gaining assurance that the provider has documented control procedures.
- Type I vs. Type II: Type I reports only provide a Service organization's description of controls and an auditors opinion on whether the controls were designed effectively. Type I reports do not include testing of the controls.
- Type II reports also include the results of an independent auditors testing of the controls.
- SAS70s were replaced by SSAE 16 (US standard) and all reports will need to comply with the International Standard – ISAE 3402.
- SOC-1 reporting, which uses the SSAE 16 professional standard, is geared toward reporting on controls relevant to financial reporting.
- SOC-2 and SOC-3 reports are designed for reporting on controls other than those likely to be relevant to user entities' internal controls outside of financial reporting (e.g., security, availability, processing integrity, confidentiality, or privacy). In short, SOC 2 and SOC 3 reports are to be issued under the AT Section 101 attest standard.
- SOC-3 report does not include the detailed description of tests, controls and results that are included in a SOC-2 report.

SSAE16 Reliance & Limitations

- When reviewing SSAE16s, organizations should consider the following:
  - Was it a Type I or a type II?
  - Who performed the SSAE16?
  - Did the entity receive a clean audit opinion?
  - What audit objectives & testing procedures were covered by the SSAE16?
  - Were there any findings and how were they addressed?
  - What Client Control Considerations were included?
  - Is this enough to cover the organizations regulatory requirements (e.g., PCI, SOX, GLBA, Privacy Laws)?
  - Did they cover sub-service organizations?

SSAE16s - The Bottom Line

- Organizations should look for additional assurances besides the SSAE16s, which can include:
  - ISO 27001/27002
  - TRUSTe
  - Verisign
  - Safeharbor
  - SOC2/SOC3 (SysTrust/WebTrust)
- SSAE16s must be reviewed carefully to verify they are still applicable and that all areas that are important to your organization are covered