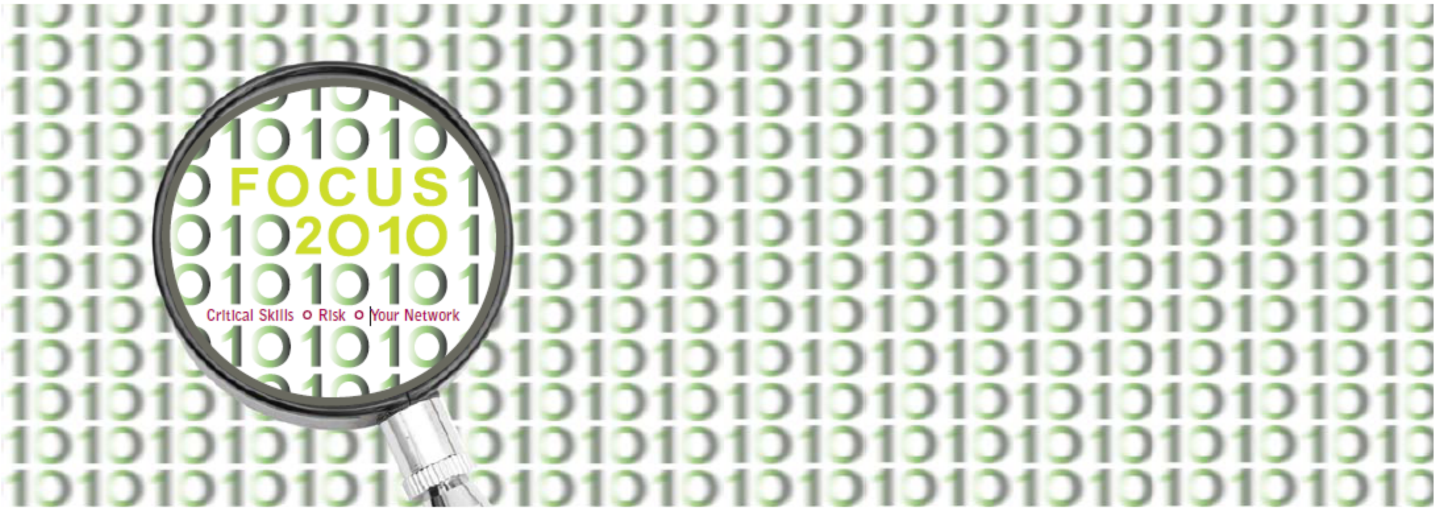
10th Annual SF ISACA Fall Conference

October 4 – 6, 2010



T31: Before, During and After Outsourcing

David Fong, BlackRock

ISACA®

Trust in, and value from, information systems

San Francisco Chapter

ISACA®
Trust in, and value from, information systems
San Francisco Chapter

Before, During and After Outsourcing

David Fong, CISA, CPA

Objective

- Explore reasons why some organizations choose to outsource
- Understanding inherent risks from outsourcing
- Where to do we start?
- Review various audit responses
- Useful references

Why Outsource?

- Leverage efficient operations
  - Gain economies of scales from a ‘producer’ of services
- Leverage vendor expertise
  - Rely on subject-matter expertise in areas where the organization may not have expertise in
- Focus on core competencies
  - Free-up internal resources to focus on mission-critical activities with a higher return

Why Outsource?

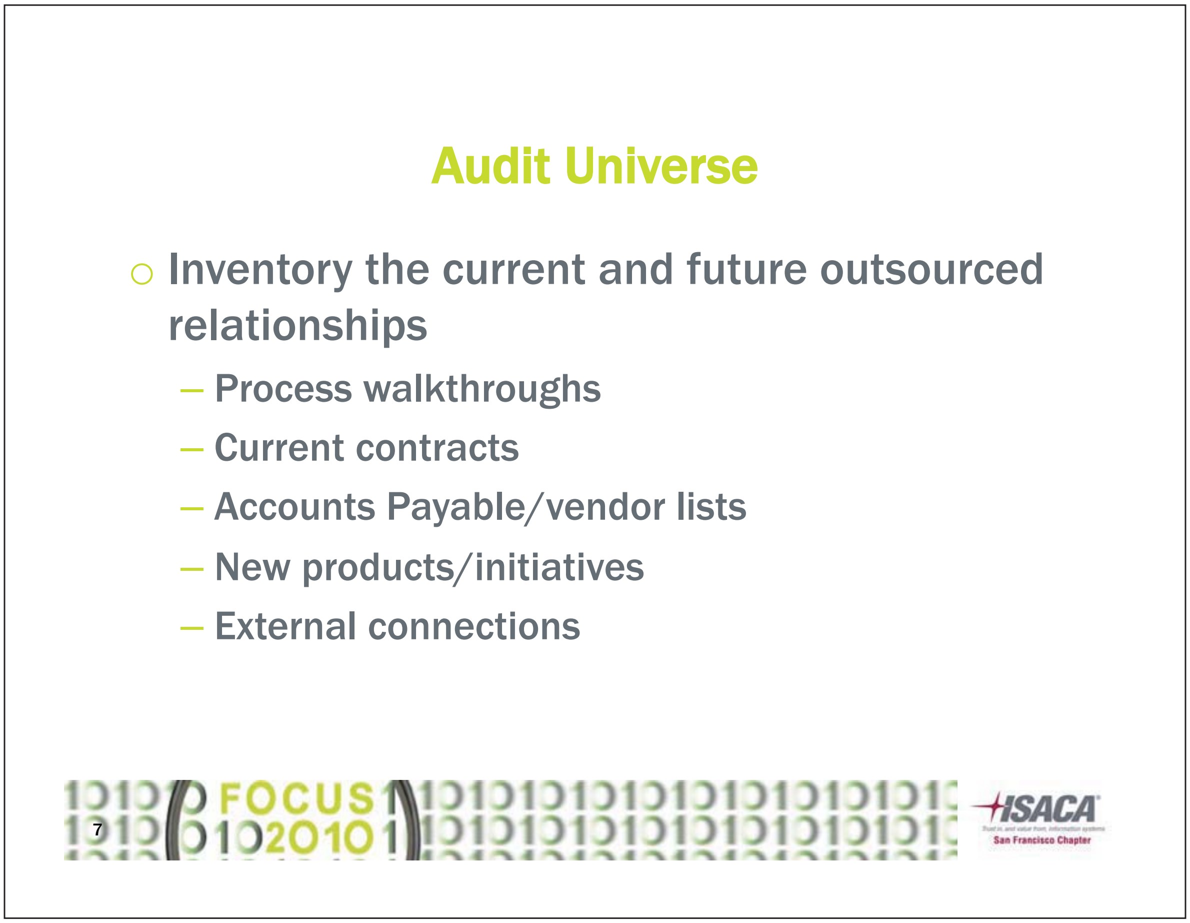
- Cost of labor
  - Lower labor costs
- Speed-to-market
  - Migrate quickly using established vendor processes/infrastructure
- Reduce short-term capital needs
  - Leverage established infrastructure and technologies without needing to the initial capital outlay

Your Outsourcing Experience

- Level of outsourcing
- Types of services being outsourced (technology, customer service, operations)
- Type of vendor management functions (centralized vs. decentralized)
- Aspects of the outsourcing that have been audited

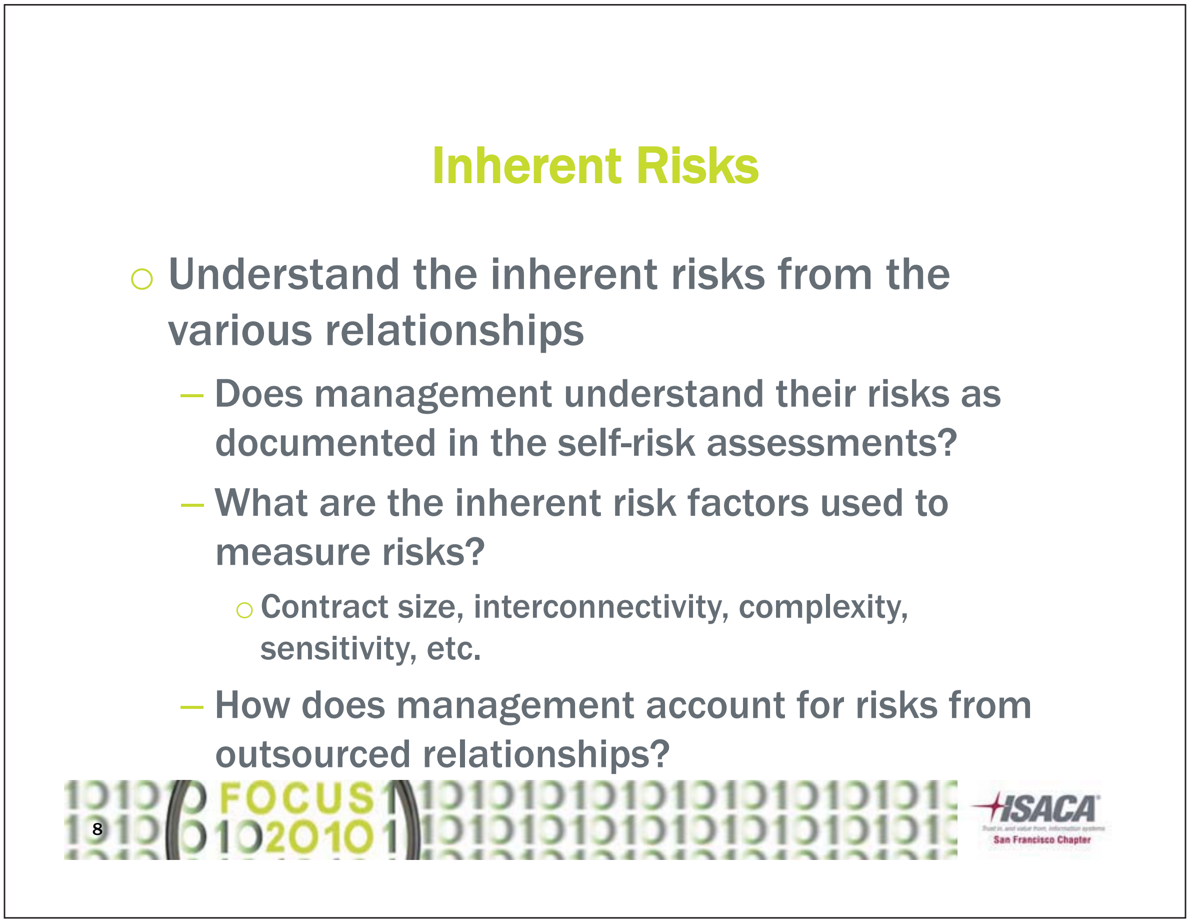
Where to Start

- Inventory the current and future outsourced relationships (audit universe)
- Understand the inherent risks from the various relationships (inherent risks)
- Consider the organizational and department vendor management controls in place (control environment)



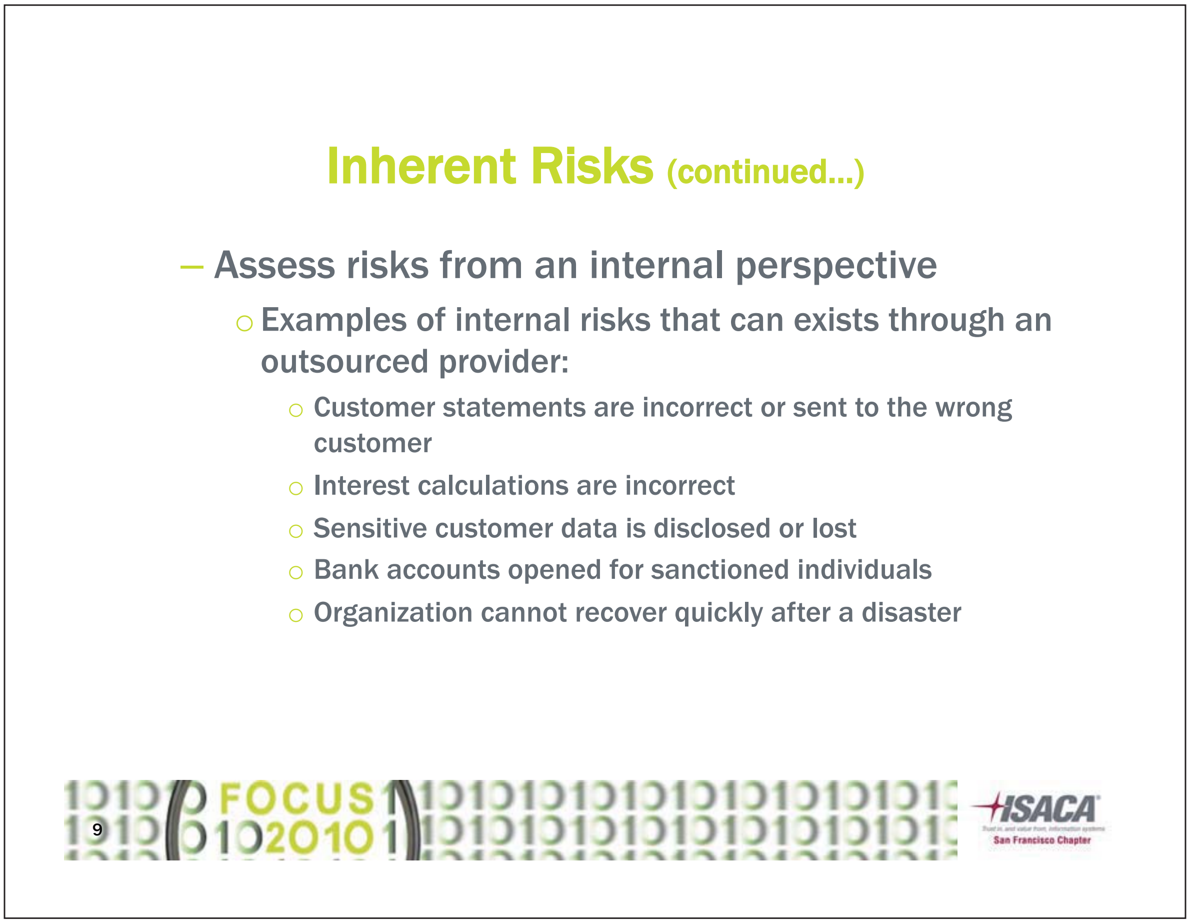
Audit Universe

- Inventory the current and future outsourced relationships
  - Process walkthroughs
  - Current contracts
  - Accounts Payable/vendor lists
  - New products/initiatives
  - External connections



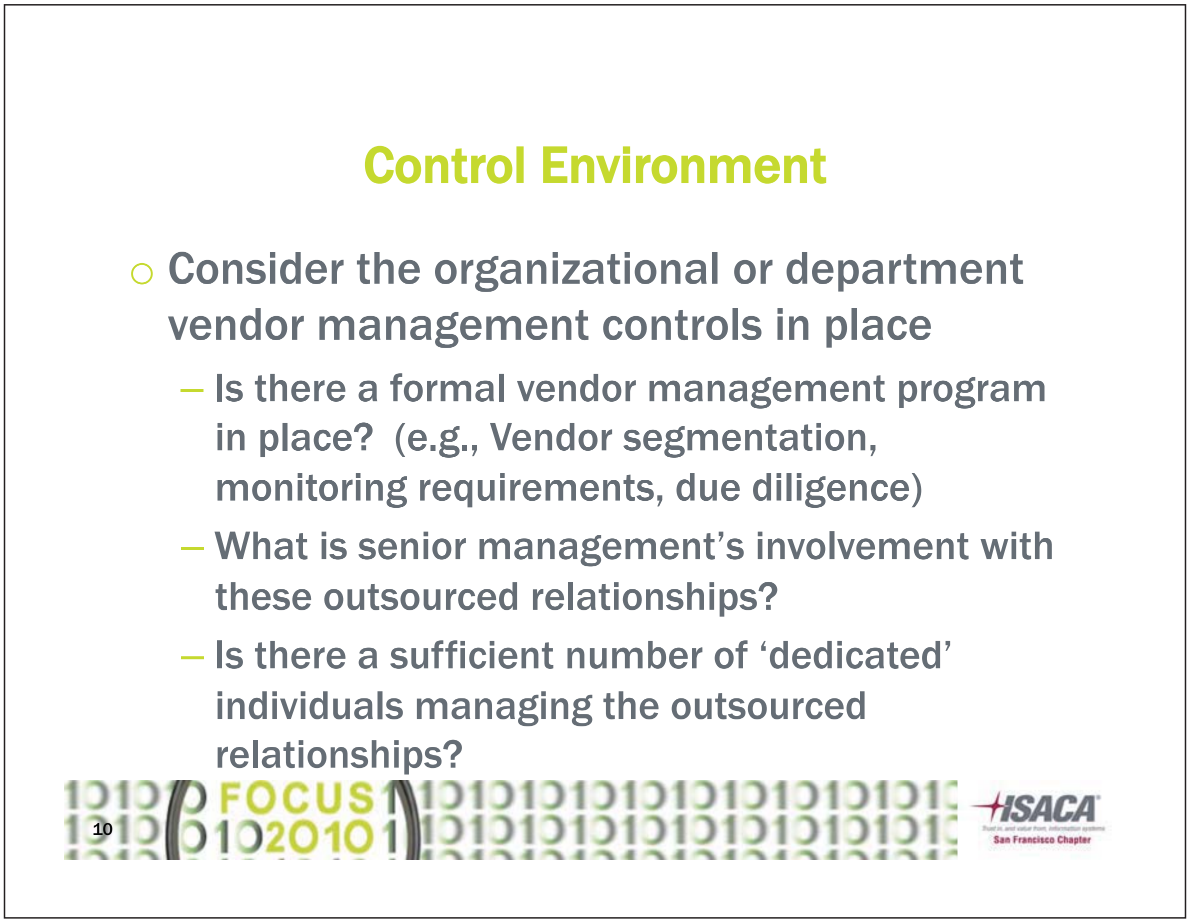
Inherent Risks

- Understand the inherent risks from the various relationships
  - Does management understand their risks as documented in the self-risk assessments?
  - What are the inherent risk factors used to measure risks?
    - Contract size, interconnectivity, complexity, sensitivity, etc.
  - How does management account for risks from outsourced relationships?



Inherent Risks (continued...)

- Assess risks from an internal perspective
  - Examples of internal risks that can exists through an outsourced provider:
    - Customer statements are incorrect or sent to the wrong customer
    - Interest calculations are incorrect
    - Sensitive customer data is disclosed or lost
    - Bank accounts opened for sanctioned individuals
    - Organization cannot recover quickly after a disaster



Control Environment

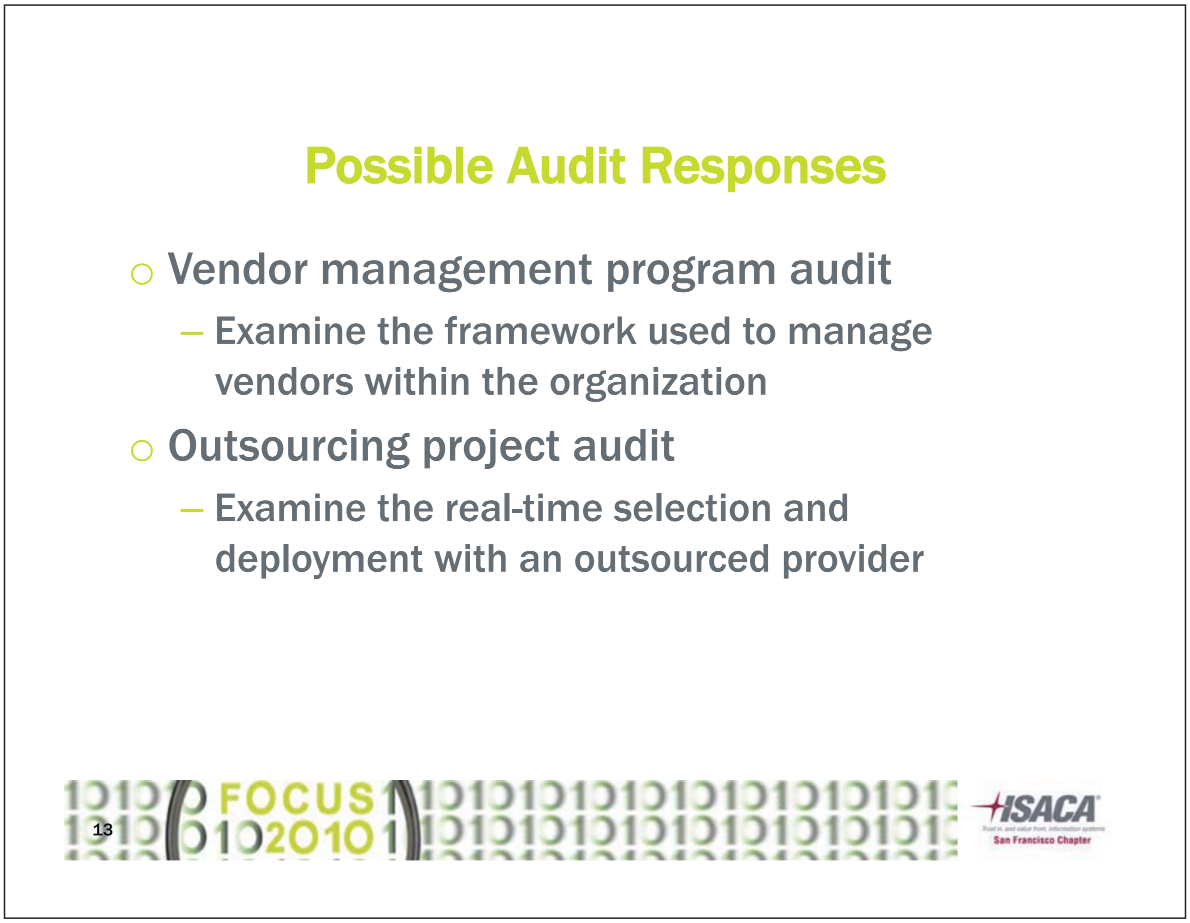
- Consider the organizational or department vendor management controls in place
  - Is there a formal vendor management program in place? (e.g., Vendor segmentation, monitoring requirements, due diligence)
  - What is senior management's involvement with these outsourced relationships?
  - Is there a sufficient number of 'dedicated' individuals managing the outsourced relationships?

Key Risks from Outsourcing

- Anticipated efficiencies and cost savings are not gained
- Vendor is not responsive to problems or changes
- Vendor expertise is limited
- Vendor solution has limited flexibility or does not conform to organization’s requirements

Key Risks from Outsourcing (continued…)

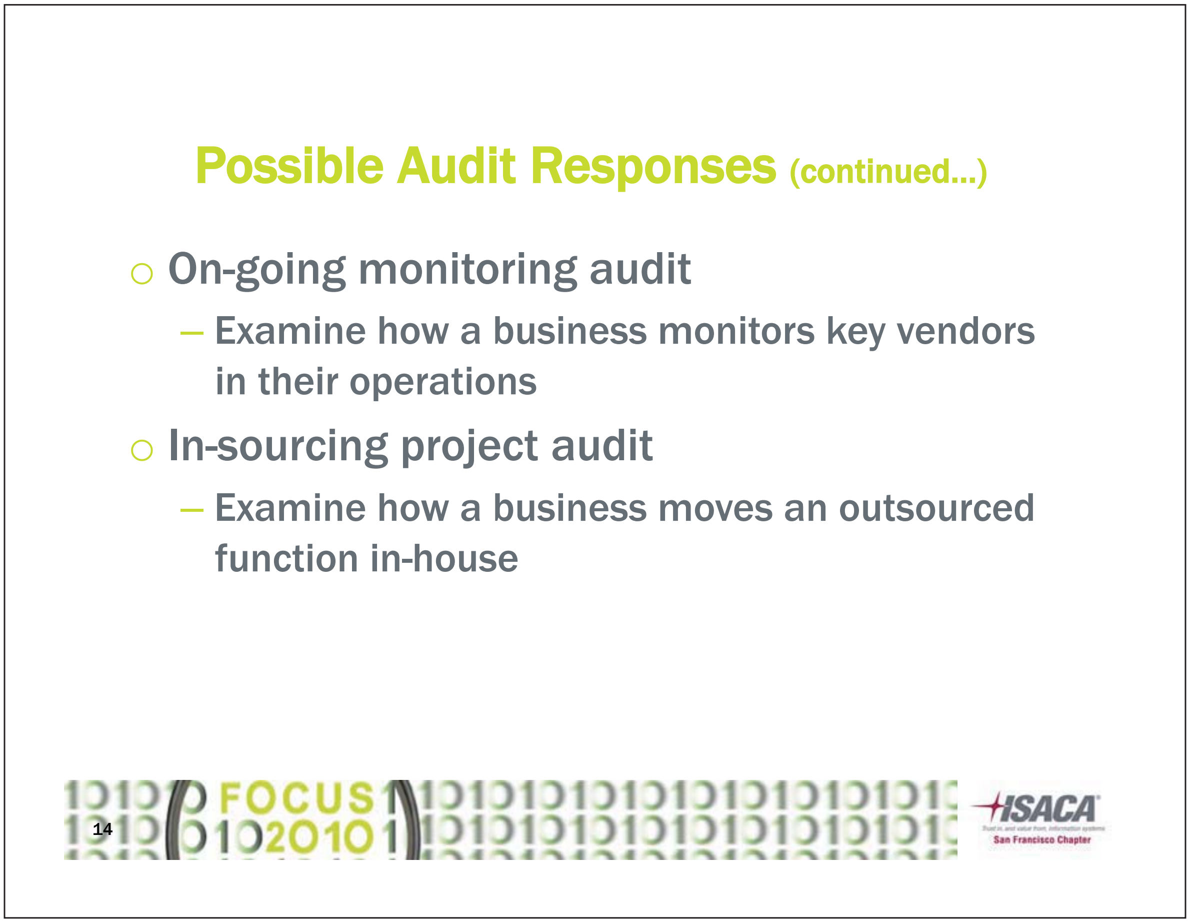
- Insufficient internal expertise or resource to properly oversight vendor
- Internal and external clients are impacted by service gap
- Vendor is acquired or not financially viable
- Inability of the organization to manage service levels from sub-contracted services
- Sensitive data is compromised by vendor



Possible Audit Responses

- Vendor management program audit
  - Examine the framework used to manage vendors within the organization
- Outsourcing project audit
  - Examine the real-time selection and deployment with an outsourced provider

FOCUS
2010
ISACA
San Francisco Chapter



Possible Audit Responses (continued…)

- On-going monitoring audit
  - Examine how a business monitors key vendors in their operations
- In-sourcing project audit
  - Examine how a business moves an outsourced function in-house

FOCUS
2010
ISACA
San Francisco Chapter

Vendor Management Program Review Scope

- Breadth and depth of the vendor management program
- Vendor risk assessments
- Management and operational success indicator reporting
- Training and awareness

Vendor Management Program Key Attributes

- Senior management sponsorship
- Defined roles and responsibilities
- Robust procedures and processes
- Risk-based oversight program
- On-going due diligence
- Monitoring, reporting, and escalation
- Training and awareness

Detailed Risk Assessments

- Fully understand the risk of outsourcing your business operations
  - Risks that the organization assumes from the activity remains with the organization and NOT transferred to the vendor
- Determine the impact and likelihood of a risk materializing
- Implement suitable controls to mitigate a risk within the organization’s risk appetite

Vendor Management Program Review Scope

- Breadth and depth of the vendor management program
  - Which outsourced relationships or business divisions are within scope of the program?
  - Where does the head of the vendor management program report into?
  - Are all vendors managed similarly, or is the approach risk-based?
  - Are there documented vendor monitoring programs for each vendor?

Vendor Management Program Review Scope

- Vendor risk assessments
  - Are there formal risk assessments for each vendor or are the risk assessments embedded within the business?
  - How are vendor risks aggregated if used by more than one business area?
  - Are the risk assessments completed by ‘qualified’ individuals?

Vendor Management Program Review Scope

- Management and operational success indicator reporting
  - How are problems with the vendor collated and reported to the vendor manager?
  - How is performance against the contract and service levels monitored?
  - How are deviations escalated to the vendor and with senior management?

Vendor Management Program
Review Scope

- Training and awareness
  - Are employees aware that there is a vendor management program?
  - Do employees understand what their roles and responsibilities are in managing an outsourced relationship?

Outsourcing Project
Review Scope

- Vendor selection and evaluation process
- Due diligence
- Issues tracking and resolution
- Contract negotiations
- Implementation and training plan
- Exit plan

Outsourcing Project
Key Attributes

- Exhaustive and confidential vendor search process
- Detailed request for proposal based on organization and department requirements
- Risk-based evaluation scorecard
- Focused due diligence
- Contract negotiations
- Implementation/exit plan

Outsourcing Project
Review Scope

- Vendor selection and evaluation process
  - How were prospective vendors identified and selected for a proposal?
  - Were submitted Request-for-Proposal (RFP) evaluated against a risk-based scorecard?
  - Were the due-diligence (DD) activities aligned to the organization's risk assessments?
    - If availability is important, DD activity surrounding vendor recovery is performed

Outsourcing Project Review Scope

- Due Diligence
  - Evaluate vendor ability and experience to perform services based on the organization’s needs and perceived risks
  - Understand vendor processes/controls in place to mitigate inherent risks—validate the effectiveness of these controls
  - Identify the due diligence gaps and consider suitable risk mitigation
  - Business contingency planning

Outsourcing Project Review Scope

- Contract negotiations
  - A well-conceived contract is essential to protecting the interest of the organization
  - Legal counsel is enlisted throughout contract negotiations and reviews
  - Risk acceptance for gaps communicated and approved by senior management
  - Gaps, open issues, and other verbal understandings are incorporated into the contract

Key Contract Terms to Consider

- Limitations of liability
- Define services, SLAs (and measurement specifications), and penalties/rewards
- Confidentiality and records management
- Intellectual property (IP) ownership
- Incident/breach notification
- Costs and fees for start-up and on-going
- Right to audit, even when a SAS 70 exists
- Rights to terminate and transition assistance

On-going Monitoring Review Scope

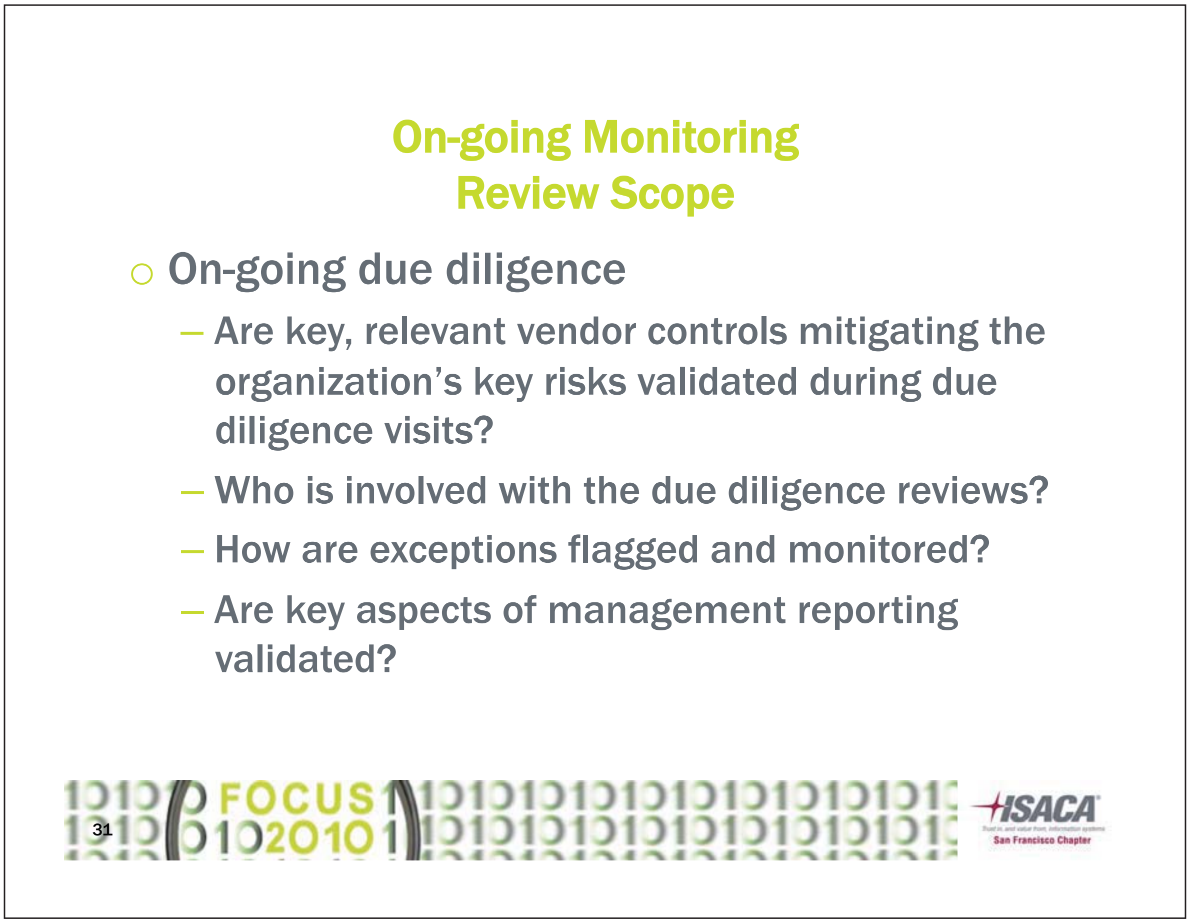
- ○ Key Operational Success Indicators (OSIs)
- ○ On-going due diligence
- ○ Continuous vendor oversight

On-Going Monitoring
Key Attributes

- Regular meetings to review issues logs and service level reporting with the vendor
- Documented vendor management plan
  - Due diligence visits, frequency, and deliverables
  - Review the accuracy of service level reporting
  - Risk-based review of the SAS 70 report
  - Exit plan

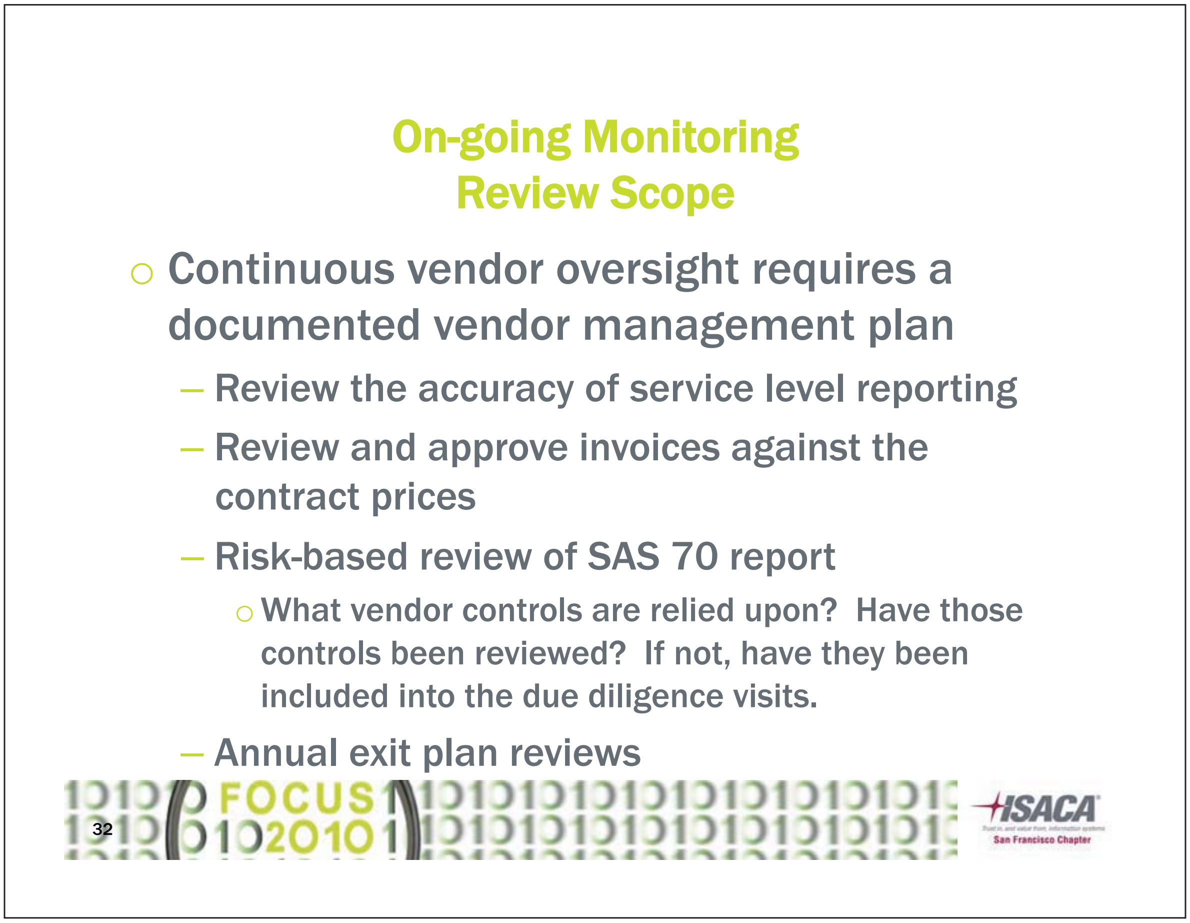
On-going Monitoring
Review Scope

- Key Operational Success Indicators (OSIs)
  - Have OSIs been established for the vendor relationships?
  - What indicators do management use to assess whether the vendor is operating properly?
  - Are these the right indicators produced at the right frequency?
  - How are exceptions flagged and escalated?



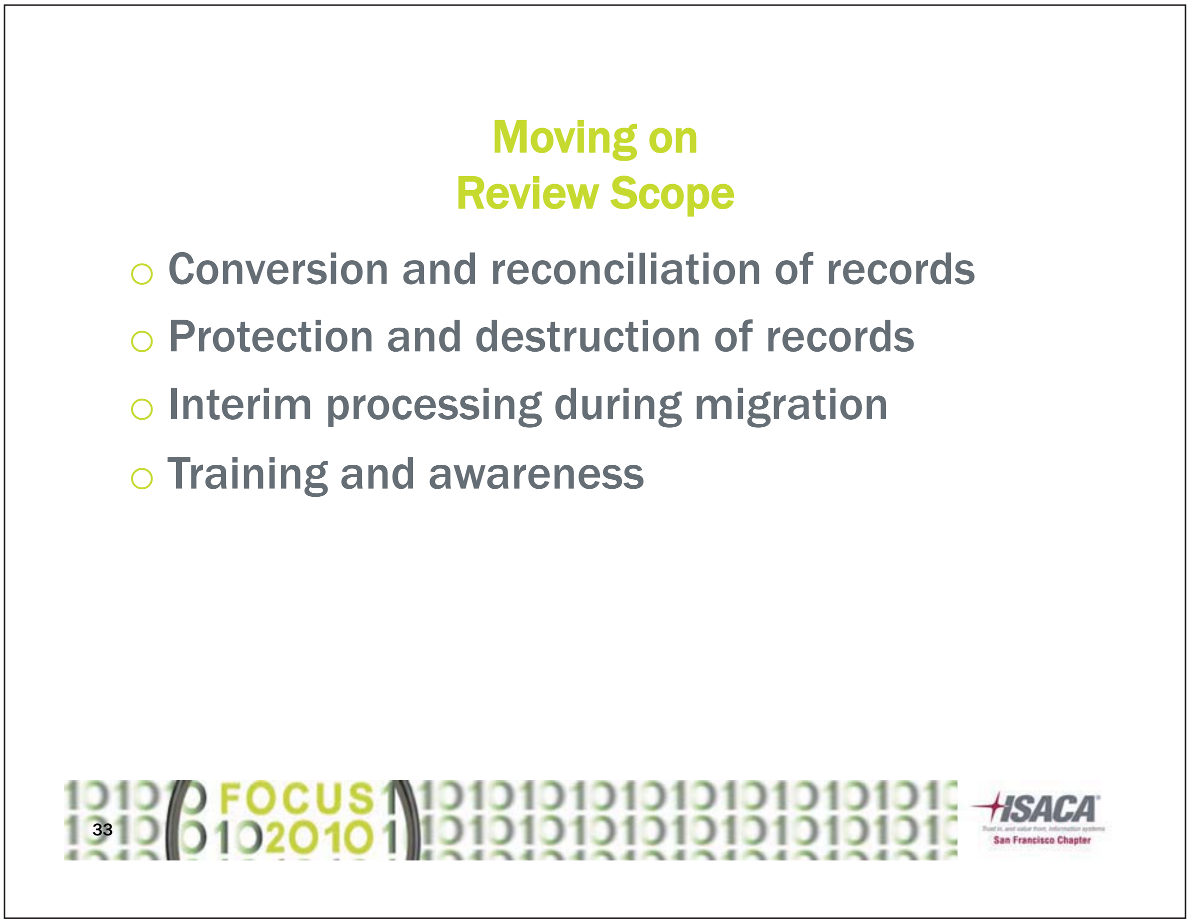
On-going Monitoring Review Scope

- On-going due diligence
  - Are key, relevant vendor controls mitigating the organization’s key risks validated during due diligence visits?
  - Who is involved with the due diligence reviews?
  - How are exceptions flagged and monitored?
  - Are key aspects of management reporting validated?



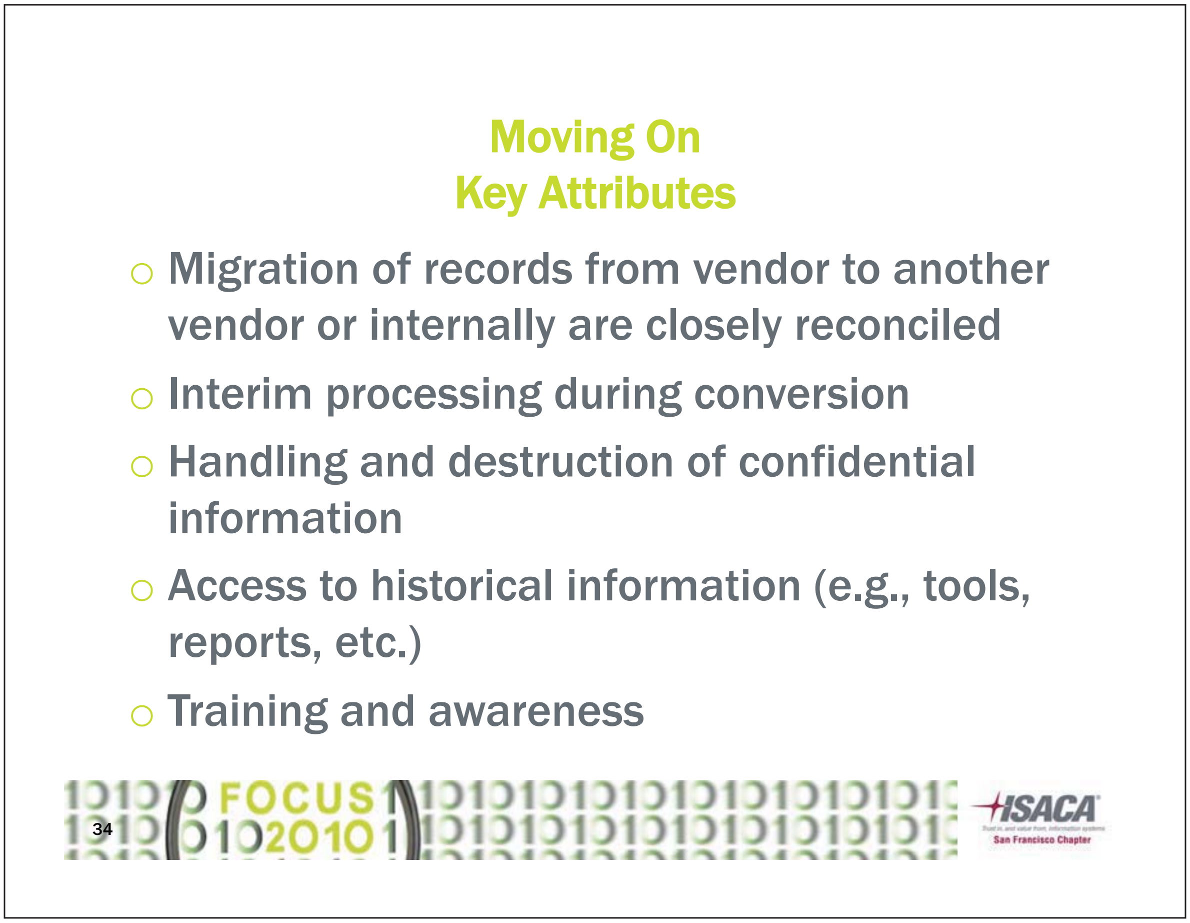
On-going Monitoring Review Scope

- Continuous vendor oversight requires a documented vendor management plan
  - Review the accuracy of service level reporting
  - Review and approve invoices against the contract prices
  - Risk-based review of SAS 70 report
    - What vendor controls are relied upon? Have those controls been reviewed? If not, have they been included into the due diligence visits.
  - Annual exit plan reviews



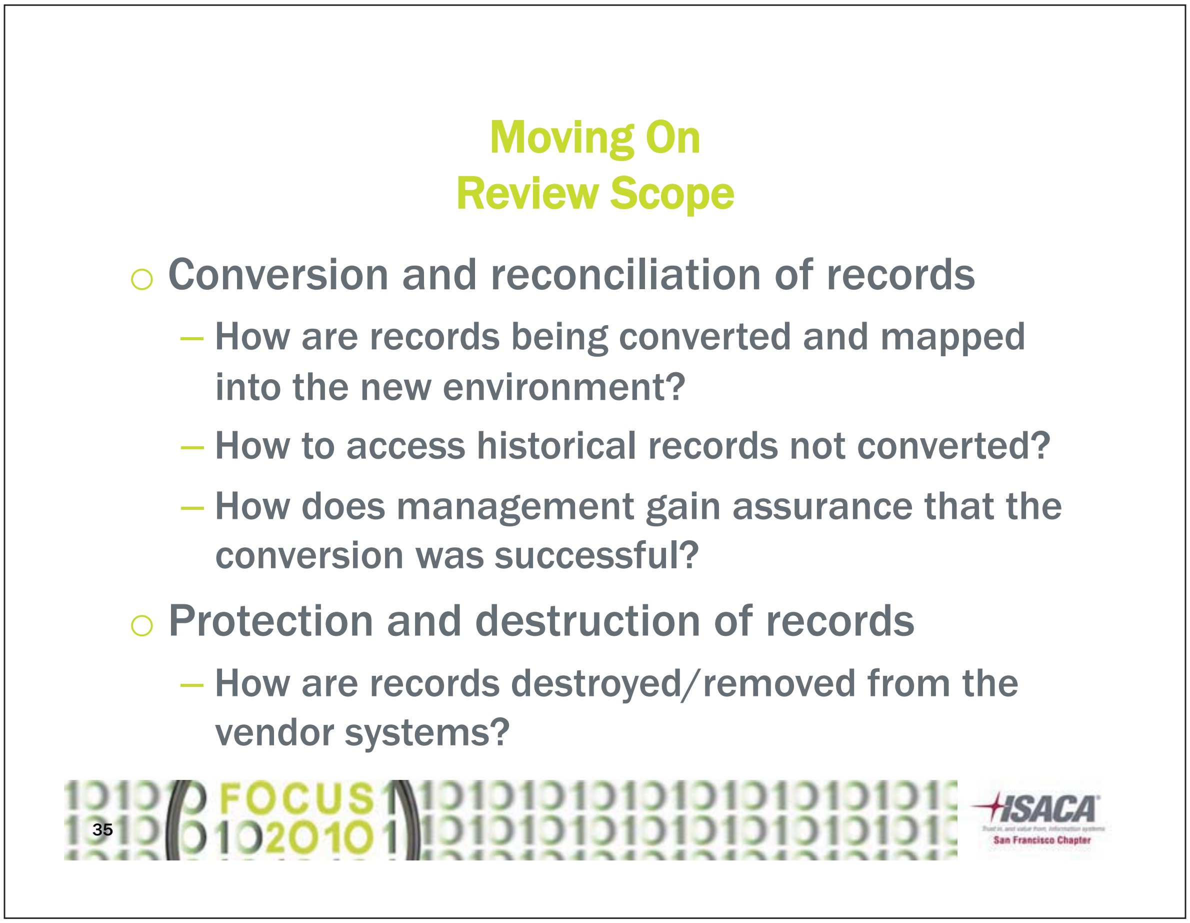
Moving on
Review Scope

- Conversion and reconciliation of records
- Protection and destruction of records
- Interim processing during migration
- Training and awareness



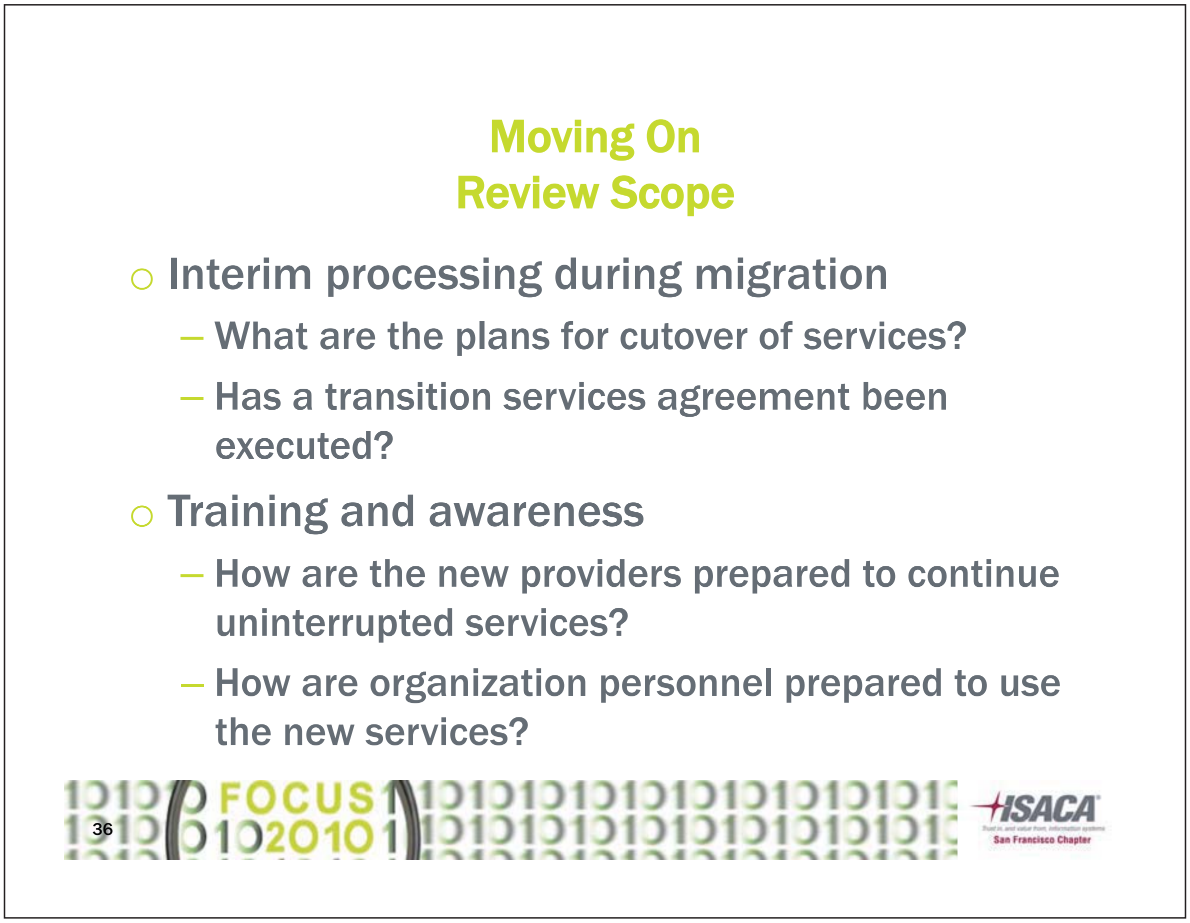
Moving On
Key Attributes

- Migration of records from vendor to another vendor or internally are closely reconciled
- Interim processing during conversion
- Handling and destruction of confidential information
- Access to historical information (e.g., tools, reports, etc.)
- Training and awareness



Moving On
Review Scope

- Conversion and reconciliation of records
  - How are records being converted and mapped into the new environment?
  - How to access historical records not converted?
  - How does management gain assurance that the conversion was successful?
- Protection and destruction of records
  - How are records destroyed/removed from the vendor systems?



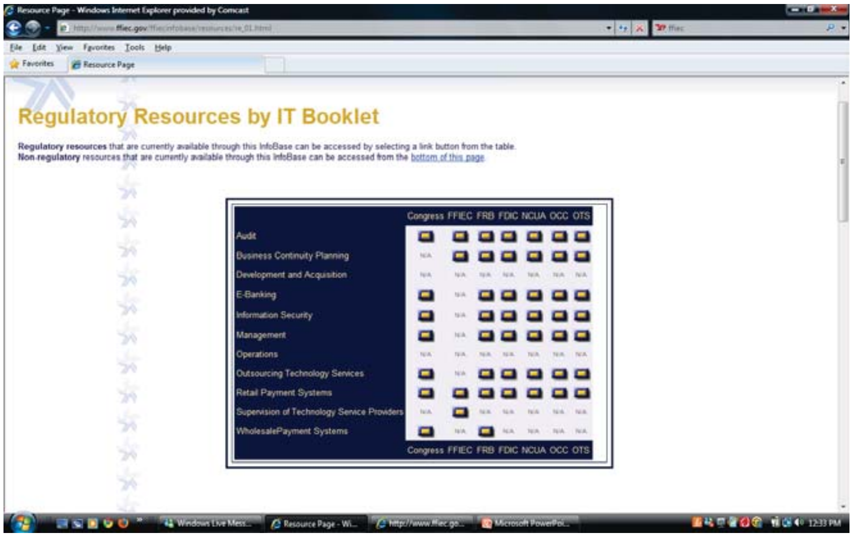
Moving On
Review Scope

- Interim processing during migration
  - What are the plans for cutover of services?
  - Has a transition services agreement been executed?
- Training and awareness
  - How are the new providers prepared to continue uninterrupted services?
  - How are organization personnel prepared to use the new services?

Useful References

- ○ OCC Bulletin 2001-47: Third-Party Relationships
- ○ FDIC FIL-50-2001: Bank Technology Bulletin on Outsourcing

Regulatory Resources


Resource Page - Windows Internet Explorer provided by Comcast
http://www.ffiec.gov/ffiecinfobase/resources/re_01.html
ffiec
File Edit View Favorites Tools Help
Favorites
Resource Page
Windows Live Mess...
Resource Page - Wi...
http://www.ffiec.go...
Microsoft PowerPoi...
12:33 PM

Regulatory Resources by IT Booklet

Regulatory resources that are currently available through this InfoBase can be accessed by selecting a link button from the table.
Non-regulatory resources that are currently available through this InfoBase can be accessed from the bottom of this page.

	Congress	FFIEC	FRB	FDIC	NCUA	OCC	OTS
Audit	■	■	■	■	■	■	■
Business Continuity Planning	N/A	■	■	■	■	■	■
Development and Acquisition	N/A	N/A	N/A	N/A	N/A	N/A	N/A
E-Banking	■	N/A	■	■	■	■	■
Information Security	■	N/A	■	■	■	■	■
Management	■	N/A	■	■	■	■	■
Operations	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Outsourcing Technology Services	■	N/A	■	■	■	■	■
Retail Payment Systems	■	■	■	■	■	■	■
Supervision of Technology Service Providers	N/A	■	N/A	N/A	N/A	N/A	N/A
WholesalePayment Systems	■	N/A	■	N/A	N/A	N/A	N/A
	Congress	FFIEC	FRB	FDIC	NCUA	OCC	OTS