ISACA®

Trust in, and value from, information systems

San Francisco Chapter

C32 - Introduction to Auditing Outsourced Processes & Services

Nick Harrahill

Inception of an Engagement

- Understanding the relationship
  - What is the external party doing on our behalf?
    - Access to data
    - Access to systems
    - Providing development
    - Collecting data on our behalf
    - Anything that could impact customers, company or brand

Relationships Change- Ensure the business keeps you appraised of changes that impact risk.

Inception of an Engagement

- Relationships Change- Ensure the business keeps you appraised of changes that impact risk.
  - Sensitivity of data processed
  - Change in importance of vendor – are all of our eggs in one basket?
  - A shift towards more dynamic processing – like offline storage of data
  - Incidents at external party
  - Downstream outsourcing – the external party introducing their vendors to our process

Critical Partnerships

- Business Unit Relationship Manager (BURM)
- Procurement
- Legal Team and Privacy
- Information Security, Compliance, and related SME's
- Your counterparts in Information Security and Compliance at the external party

Procurement and Legal are effective traffic cops in ensuring projects get routed for assessment.

Partner with Information Security counterparts at the external party. Help them understand your expectations, learn their processes, and how you will best work together.

Critical Partnerships

- Procurement and Legal as traffic cops
  - “Follow the money”
  - Pursue integrated processes and repositories for all parties supporting the vendor life cycle.
- Partner with Information Security counterparts at external party.
  - Understand where there are gaps and opportunities for compensating controls.
  - Avoid contentious relationships and emphasize our shared interests in compliant processes.

The Legal Agreement

- Ensuring the provisions are outlined and agreed to.
- Understanding additional regional regulatory issues involved to be outlined.
- Support and work through any red-lining or requested changes.

It is not safe to assume that the external party has disseminated the contractual terms to all of their downstream parties.

Ensure that they understand their responsibility-- By way of assessments or on-site audits, these obligations should be validated.

The Legal Agreement

- Ensure responsibilities are understood
  - Escalation processes should an incident occur. Identify POC's and critical support lines.
  - Downstream outsourcing intentions or other external party relationships that impact our process.
  - Audit and/or annual collection of compliance documentation.
  - Changes that impact their localized industry compliance status.
  - Notification of significant changes to security program that impact our process.

Assessing the Risk

- Access to data
- Access to systems
- Providing development
- Collecting data on our behalf
- Anything that could impact customers, company or brand
- Regulatory considerations
- Business continuity

Legal obligations based on residency of data – where the customer resides and where our external partner does.

Customer Privacy agreements should be kept in sync.

What is the impact to our business if services at the vendor are down for hours, days, weeks or longer?

Determine risk thresholds to tier your external partnerships

Assessing the Risk

- Customer Privacy agreements should be kept in sync
  - Does this impact our customer privacy agreement?
  - Global Privacy counterparts should be engaged for review of more sensitive data flows.
- What is the impact to our business if vendor services are down?
  - Does it impact our internal SLA's?
  - Do we have significant redundancy for what the external party provides?

Risk Assessments

- Assess according to vendor risk tier & type

High Risk	• SIG + targeted assessment based on type of vendor • Applicable artifacts – PCI documentation, vulnerability management, SDLC documentation • Vulnerability scanning • On-site audits • Annual reassessment
Medium Risk	• SIG or SIG lite • Vulnerability scanning • Assess as needed or with changes to relationship
Low Risk	• SIG lite • Assess as needed or with changes to relationship

Common Industry Assessment Frameworks

- Standard Information Gathering (SIG) Questionnaire
  - Consistent service provider evaluation process offered by Shared Assessments – www.sharedassessments.org
  - Several sections, including Risk Management, Security Policy, Asset Management, HR, Privacy and
  - Full SIG version and SIG Lite
- SSAE Auditing Standard (formerl
  www.ssae-16.com
  - Done via a third party auditor to de
    controls and safeguards
  - Shared upon execution of NDA's

Ensure your collection of data is consistent with what is required for your own regulatory audits. Artifacts could be subject to audit sampling

One size does not fit all- Utilizing a targeted assessment based on the type of external partner is appropriate as many times you may need information beyond what a standard assessment framework provides. The external partner population can contain Data Centers, Payment Processors, Marketing companies, or small development parties.

High Risk Engagements – The Customer Call Center Use Case

- Maintaining oversight
  - Initial assessment
  - Annual on-site assessments
  - Quarterly self-assessments of ground-level controls
- Annual on-site assessments
  - Provide standards check of controls base that is consistent across external party sites.
  - Test controls you are responsible for, as well as that of the external party .
  - Report to Management, determine appropriate risk mitigation when needed.
- Quarterly self-assessments
  - Light-weight version of audit that can be done by layperson.
  - Deputize coworkers from your company who visit, or assign to external party as self-assessment.
  - Quarterly self-assessment provides good reminder/education for staff that may be new to program.

Setting expectations up front with the external party on audit and assessment obligations is essential to congenial working relationship.

High Risk Engagements – The Customer Call Center Use Case

- Provide concise, meaningful reporting for business stakeholders on individual reviews and performance across the population:

Partner	Physical Security	Logical Security	Administrative Controls	Resiliency & Performance	Average
Partner A	85	88	79	80	83
Partner B	88	90	91	82	87
Partner C	78	85	93	90	86
Partner D	77	80	96	90	85
Partner E	90	90	92	92	91

Other Best Practices and Lessons Learned

- Partner with Business counterparts to build compliance processes into initial RFP flows.
- For large external entities, assess at the project vs entity level to determine specifics of the use case.
- Maintain an accountable process with responsibilities of each party clear (Business Unit – External Party – Legal-etc).
- Review your process on an annual basis – risks evolve, the business changes, and we must adapt with that.
- Evangelize your processes internally – both to demonstrate the requirement and its value proposition.
- Develop a platform repository that supports all ends of the process.

Summary

- Managing effective oversight over outsourced processes and services requires several key points:
  - Understanding the nature of the engagement at its inception
  - Maintaining critical partnerships internally and at the external party
  - Keeping Legal Agreements in sync with your requirements and regulatory obligations
  - Assessing the risk and applying a commensurate auditing structure

Questions