

Case Study:

Third Party Review (TPR) Audits



CDI helps identify and mitigate risks by assessing security controls through its Service Provider Audit services.

Client Description:

A leading global financial services firm with assets of over \$2 trillion and operations in more than 60 countries. The firm is a leader in investment banking, financial services for consumers, small business and commercial banking, financial transaction processing, asset management and private equity.

Background:

The assurance of service providers protecting personally identifiable, confidential and highly confidential information is paramount for regulated financial institutions. Each line of business in client organizations has an information risk management group whose responsibility is to perform the due diligence on security controls in place with all related third-party organizations.

Business Issue:

Our client required an independent organization to conduct risk assessments of third-party relationships globally, based on the Shared Assessments Program (mapping to COBIT, PCI-DSS and ISO27002 industry security standards) framework yet tailored to internal requirements. This effort would improve cost-effectiveness and quality of assessments provided by the internal investment banking risk management organization.

CDI Solution:

CDI reviewed the business requirements and deliverables and analyzed the existing process, tools and work products for enhancement opportunities. We incorporated quality assurance into the process, implemented a governance model and prioritized the service providers (High, Medium, Low, Nominal/Personally Identifiable Information relationship) utilizing a weighted macro-driven tool which included thresholds for the following components:

1. Critical Service – Is the service being provided critical to organizational operations?
2. Recovery Time Objective (RTO) – What is the RTO classification for the product or service?
3. Personally Identifiable Information (PII) - Does the OSP process, store or transmit PII outside of the organization’s network?
4. Information Classification - Classification based upon the information’s value to the firm, legal and regulatory requirements and the impact to the firm of unauthorized disclosure, modification, or destruction.
5. Externally Facing - The exposure to the firm based on the application or infrastructure provided being accessible by external parties or clients (e.g., is the related application internet facing?).
6. Regulatory Compliance - The product or service activity is subject to a variety of federal, state and local laws, regulations and directives. Failure to follow prescribed directives may result in substantial fines, restrictions in activities and/or major concerns by regulators.
7. Country Risk - Level of risk associated with the country in which the supplier will be performing organizational operations. The Country Risk associated with a supplier in the United States is “Low”.
8. Revenue - The dollar amount of an organization’s annual revenue at risk, associated with products and services.
9. Operations - The product or service involves clearing, settlement and/or other processing activities (i.e.,

deposit or loan processing, shareholder services, etc.). This includes providing fiduciary services to customers. It considers the complexity of the service, including the number of business units serviced, the number of subcontractors used by the supplier and the relative experience of the supplier.

10. Exit Strategy - The availability of alternative providers for the activity and the ease with which services could be transferred in the event of non-performance or business interruptions with consideration for insurance coverage, contract provisions and escrow arrangements.
11. Reputation – Third-party non-performance or substantial non-performance impact on the reputation of the firm. The level of use, sophistication and importance of technology associated with the services provided are considered. The relative experience of the third-party for the services being provided is also evaluated.
12. Concentration - Cumulative business position associated with the product or service activity, expressed as a percentage of the total business function (e.g., payments processed, account portfolio maintained, etc.).
13. Supplier Fees - Level of annual payments to the product or service provider associated with the Supplier activity.
14. TP Strategy - The expected time horizon associated with an organization's relationship with the supplier. Third-parties that are re-engineered or retired are moved to the lowest priority and generally do not require review.

Our Service Provider Audit solution included:

- Leveraging a team of intermixed skills including security and audit professionals
- A decentralized team structure that provided ideal DR/BC
- Supplier Associate agreement with a French firm to aid in providing global coverage (EU, ME-NA and Pacific Rim)
- Multi-stage QA process using interim work products and peer review
- Recommended remediation actions for areas of non-compliance

- Provided an objective independent assessment of each service provider's level of compliance from an IT Risk Management perspective
- Engaged trained yet cost effective resources at various stages of the review process and passed the savings on to the client
- Conducted assessments in accordance with guidelines established by the internal risk management organization and industry standard program, including physical inspection of service providers' production facilities based on the following components:

1. Security policy
2. Change Control
3. Email & IM
4. Encryption
5. Data integrity
6. Logical access control
7. Monitoring
8. Communications & connectivity
9. Physical security
10. Website
11. Incident response
12. DR & BC
13. Backup & offsite storage
14. Media & vital records
15. Outside Service Providers (OSP)
16. Foreign OSPs
17. Regulatory requirements
18. Organization
19. Standard builds
20. Operations
21. Asset management
22. Desktop
23. Application
24. System Development
25. Customer Contact

Results:

The implementation of our solution resulted in improved budgeting for reviews and reduced cost through the use of fixed pricing per assessment, which garnered customer praise. The final products were of highly-professional value

throughout the organization. Once familiar with our client's internal processes, CDI went to the next level by providing and producing standardized templates, streamlining processes and training resources for continual improvement.

CDI's model of engaging thoroughly trained yet cost-effective resources such as security and audit professionals for review analysis including gap identification, risk mitigation and final deliverable review provided a cost savings that was passed along to the client. Since 2006, CDI has completed over 200 security assessments of our client's third party organizations.

Technologies Used:

- Ironkey USB devices – Issued to each team member (with on-board applications) for the processing and storage of sensitive data. Ironkey drives provide hardware based encryption, internet based policy enforcement and device management.
- Macro-enabled tools – For third party risk assessment and prioritization.