



## *Shared Assessments Case Study*

### **About DTCC:**

*The Depository Trust & Clearing Corporation (DTCC), through its subsidiaries, provides clearance, settlement and information services for equities, corporate and municipal bonds, government and mortgage-backed securities, money market instruments and over-the-counter derivatives. In addition, DTCC is a leading processor of mutual funds and insurance transactions, linking funds and carriers with financial firms and third parties who market these products. DTCC's depository provides custody and asset servicing for 3.5 million securities issues from the United States and 110 other countries and territories, valued at \$40 trillion. Last year, DTCC settled more than \$1.86 quadrillion in securities transactions. DTCC has operating facilities in multiple locations in the United States and overseas. For more information on DTCC see [www.dtcc.com](http://www.dtcc.com).*

### **Overview:**

This case study describes DTCC's approach to evaluating and implementing a service vendor management program that complies with current FFIEC guidelines and also provides efficient, cost effective risk management capabilities that meet DTCC business resiliency requirements. Program implementation resulted in significant cost savings to DTCC and corroborates the experience of other Financial Institutions (FIs) and Service Providers (SPs) who use the outlined approach. This case study illustrates the benefits to both FIs and SPs.

### **Process:**

DTCC Corporate Information Security (CIS) staff began this project with an inventory of:

- the company's service providers,
- the services provided, and
- the annual service fees paid for each.

CIS staff then completed a risk assessment of the services outsourced. For comparison purposes, DTC also evaluated efforts made by other FIs in gauging the risks inherent in their own vendor provided services. To complete this comparison, DTCC relied on its membership in BITS and through BITS was introduced to the Shared Assessments process.

By reaching out to other FIs, DTCC was able to benchmark its approach to vendor management against those of FIs using the Shared Assessments Program. In so doing, DTCC concluded that the program offers significant process and cost efficiencies. DTCC now relies on the Shared Assessments program as an integral part of its vendor risk evaluation process.



## *Shared Assessments Case Study*

### Research Methodology:

CIS staff divided its list of service providers into three risk-based tiers based as follows:

- Tier 1- service providers that do not require facility or network access to provide services and have no access to Restricted information
- Tier 2- service providers that come on-site to a DTCC facility to provide service requiring badge and network access
- Tier 3- service providers that provide application development services off-site and/or have access at their locations to DTCC restricted information

Requirements for each tier were implemented using existing proprietary tools. Tier 1 vendors were asked to provide information about their information security policy and how the confidentiality requirements were enforced through employee policies. A security questionnaire was implemented for all tier 2 and tier 3 service providers and an on-site security assessment was completed for all tier 3 vendors. The CIS staff added a specific set of security controls for off-site development firms including network connectivity and access control restrictions that applied to only those tier 3 service firms doing off-site application development.

### Findings:

CIS staff analyzed its approach to evaluating service providers and made the following observations:

- The cost of conducting on-site security assessments is escalating rapidly.
- While adequate as a risk assessment tool, the existing proprietary model for conducting on-site assessments is too time-consuming.
- The process of collecting and analyzing information described above requires approximately three times as many person-hours to complete the documentation than the actual on-site inspection. The total time to complete the assessment combined with the travel time made this a very expensive process.
- Vendors resist completing DTCC's vendor questionnaire because it is unique to DTCC and cannot be leveraged for use with additional clients—a key concern that is resolved by implementing the BITS Shared Assessment program
- Using traditional methodology, on-going dialog with each vendor is required to provide the appropriate context for answering the questions.
- The traditional methodology is not scalable and cannot be applied to a growing list of vendors without incurring significant additional costs.

By contrast, The Shared Assessments program allowed for the assumption of a standardized set of artifacts that can be leveraged by the vendor across all of its FI clients. Given cost savings from reduced staff time alone, CIS staff adopted the Shared Assessments tools as part of the DTCC vendor management program. By leveraging an industry standard model for security assessment artifacts, DTCC could reduce the cost and time required for completing security assessments and improve the efficiency of the process for service



## *Shared Assessments Case Study*

providers. The decision was based on DTCC's analysis and on the recommendations of large financial service firms actively engaged with the Shared Assessments Program.

DTCC implemented the Shared Assessments Program primarily to streamline its vendor management program. The program also allows DTCC institutional customers to leverage the Standardized Information Gathering questionnaire (SIG) and Agreed Upon Procedures (AUP) artifacts for their own security assessment requirements. As a result DTCC now has both a more cost-effective vendor management program and an improved risk management capability.

### **Implementation:**

CIS staff prepared responses to the SIG and reviewed the responses with the CIS Leadership Team. The questions were divided into subject matter categories. Staff was then asked to answer questions or to gather answers pertaining to specific controls.

Needs Identified through the program questionnaire- The initial questions reviewed by the CIS Leadership Team generated an unanticipated lesson learned, i.e., that different ways of interpreting each question may arise and a range of possible answers may ensue. In fact, the exercise of reviewing each question, although time-consuming, proved to be quite valuable in identifying all the possible answers and subsequently developing a consensus-based response as to the perceived effectiveness of each control. Despite the time involved in completing the SIG, the process proved beneficial to the CIS staff.

Two outcomes from this experience had equally profound impacts on the DTCC Information Security Program. In completing this process, DTCC realized the need for:

1. A workflow management capability to complete the SIG and share the process with recognized Subject Matter Experts within the institution.
2. An on-going program of testing key security controls and reviewing the results

### **Next Step – An RFP:**

Following its evaluation of the SIG, CIS staff issued a Request for Proposal (RFP) to assessment firms with regard to the AUP requirements. Five consulting firms were contacted, including two that were involved in establishing the Shared Assessments Program. The successful bid was chosen based on the company's experience doing assessments and on pricing considerations.

#### AUP Assessments

The AUP assessment process required three weeks to complete. The scope included all three data centers with on site visits at two. (Note: all of the physical and logical security controls are the same across the centers.) There were no findings of control weaknesses identified relative to the AUP controls, and a summary letter was prepared for DTCC institutional customers.



## *Shared Assessments Case Study*

### **Implementation of the Shared Assessments Program:**

Vendors comprise a key segment of the Shared Assessments population and vendor education and training is critical to the program's success. The CIS staff developed educational material to help vendors understand all aspects of the DTCC vendor management program and held a forum for vendors sponsored in conjunction with DTCC's assessment firm, Churchill & Harriman.

#### Vendor Forum

Seventy attendees participated in-person, ½-day vendor forum and many more took part by phone. The SIG and AUP each were explained in detail. In addition to the program content, Vendors benefited from each others' questions and comments regarding their own approaches to adopting the Shared Assessments Program. Follow-up information was provided to each vendor by mail. CIS staff subsequently scheduled meetings with each tier 3 vendor to agree on adoption dates for the SIG and AUP.

#### **Post Script:**

The release of the SIG version 3.1 enabled DTCC to require just the SIG lite version for Tier 2 service firms. This change made responding to the SIG even simpler and more cost effective for participants

#### **Results:**

In 2007 – the year prior to implementation of the Shared Assessments Program -- total expenses for the DTCC vendor management program security assessment requirements were approximately \$300,000. Year-to-date expenses as of October 30, 2008 were \$1,400 with no further expenses anticipated for the year. In sum, the adoption of the changes to the DTCC Vendor Management Program has improved risk management capability at a substantially lower cost to both DTCC and vendors.

#### **Planned Enhancements:**

DTCC is planning to implement workflow software for the completion of the SIG by both DTCC and its vendors. The software will make it easier to complete questions, review them and track the progress of completing the SIG. Several vendors have workflow software ready for implementation. DTCC is also enhancing its vendor management repository and management tool, provided by Archer technologies, to accept XML output from the SIG workflow tools. This change will make it easier for vendors to both complete the SIG—initially and in annual updates.