

The Depository Trust & Clearing Corporation

BENEFITS OF AUTOMATION

Increasing Data Security and Efficiency with ALERT

Cybersecurity remains a critical issue for the financial services industry, with an expected spend of \$43 billion annually by 2023.* In the settlement space, manual processes such as email are presenting vulnerabilities to SSI data security and quality that can be easily addressed through the use of automated messaging over secure connections and centralized storage of standing settlement instruction (SSI) data. ALERT® is the industry's largest and most compliant platform to maintain and communicate SSI data, and is leading the way to address the issue of keeping your SSI data safe and up to date.

HOW DOES ALERT ENSURE THAT YOUR SSI DATA IS THE MOST UP TO DATE AND ACCURATE “GOLDEN COPY”?

ALERT does this through its many data quality requirements including:

- Allowing users to apply Data Authentication settings to different input types.
- Requiring mandatory Data Authentication for cash-based SSI entries on all new acronyms.
- Providing optional Data Authentication functionality for security-based SSI entries.
- Providing optional third level Data Authentication functionality for all SSI entries.
- ALERT uses Checksum on all SSIs whereby a database code is added to your SSI. This same code is needed to make any changes or updates to data in the ALERT user interface - ensuring that the SSI in the database and in the user interface always match.
- Syntactical Validation ensuring that the format of field values and details such as data type and field length are correct.
- ALERT leverages “golden source data” from monthly BIC code file data feeds, Global Legal Entity Identifier Foundation (GLIEF) master file and DTCC Participant IDs.

WHAT STEPS DOES DTCC TAKE TO ENSURE YOUR ALERT DATA IS SAFE?

DTCC completes a rigorous external audit of controls over business process and information technology on an annual basis as part of the Statement on Standards for Attestation Engagements No. 18 (SSAE 18) examination report. The SSAE 18 report provides coverage over the following key control objectives set forth by the AICPA's Auditing Standard Board.

- Only authorized users and entities can provide data input and utilize system services and resources and that there is a logical separation of data between all parties.
- Transactions received from clients are captured completely and accurately.
- Transactions are matched and enriched, as applicable, completely and accurately.
- Data transmissions between DTCC Institutional Trade Processing (ITP) and its participants are complete and secure.
- Updates to the relevant master data are authorized and processed completely and accurately.
- Logical access to operating system software, application software and client data files, where applicable, is restricted to properly authorized personnel.
- Physical access to the data centers is restricted to authorized personnel.
- New application development, changes to existing applications and data changes are authorized, tested, approved, properly implemented and documented.
- Changes to existing system software infrastructure including operating systems, database management systems and utilities are authorized, tested, approved, properly implemented and documented.
- Processing is scheduled and that deviations from scheduled processing are identified and resolved.
- Data is backed up regularly and is available for restoration in the event of processing errors or unexpected processing interruptions.

In addition to the SSAE18 controls, DTCC adheres to the following:

- Strict physical access control requiring badge checks and turnstile swipes at several points leading to the data center.
- Privileged Access Management system requiring 2 Factor Authentication to check out administrative credentials for both server OS and Database.
- Highly secured Virtual Desktop Infrastructure is required for logical access to the servers in order to perform administrative functions for both server OS and Database.
- Automated security baseline checking and compliance metrics for both server OS and Database.
- Automated security vulnerability checking and metrics for both server OS and Database.
- Operating system security logs are routinely sent to Security Event & Information Management (SEIM).
- Database security monitoring tool installed and sending logs to the SEIM.
- Alert rules in the SEIM for both OS and Database security issues.
- Three-tier architecture that prohibits direct non-privileged user access to any database function.
- Periodic Internal Audit reviews of operating system and database operations and maintenance.
- Ongoing penetration tests to identify vulnerabilities and prioritize them for remediation through an Application Penetration Test.
- Maintaining a robust and comprehensive information security incident response and escalation process that includes procedures for qualifying a security event, assessing the severity of an incident, identifying the root cause of an incident, remediating the cause of an incident, restoring normal operations, and documenting the results. Clients will be promptly notified of any incident impacting the confidentiality, availability, and/or integrity of their data. DTCC's incident response team will work in association with your Relationship Manager to inform the appropriate contact.

ALERT has also achieved Capability Maturity Model Integration (CMMI) Level III, by the CMMI's process level improvement training and appraisal program. This program ensures that an organization's processes are well characterized and understood and are described properly in their standards, procedures, tools and methods.

FOR MORE INFORMATION

Please visit www.dtcc.com/alert

*DTCC Whitepaper, [A Roadmap to SSI Automation: How an SSI Utility Benefits all Participants](#)

© 2019 The Depository Trust & Clearing Corporation. All rights reserved.

The services described above are provided under the "DTCC" brand name by certain affiliates of The Depository Trust & Clearing Corporation ("DTCC"). DTCC itself does not provide such services. Each of these affiliates is a separate legal entity, subject to the laws and regulations of the particular country or countries in which such entity operates. See www.dtcc.com for a detailed description of DTCC, its affiliates and the services they offer.

Certain DTCC ITP LLC services are subject to regulation by the U.S. Securities and Exchange Commission ("SEC") and are offered by DTCC ITP Matching (US) LLC ("DTCC Matching"), which is set out in SEC Release No. 34-44188; File No. 600-32; 66 FR 20494 (April 17, 2001). TradeSuite ID and CTM are services of DTCC Matching and are subject to SEC regulation when used for trades in which either the broker-dealer or its institutional customer is a U.S. entity and the securities in the trade are issued by a U.S. issuer. No other services offered by DTCC ITP LLC are regulated. 25361-PS112019