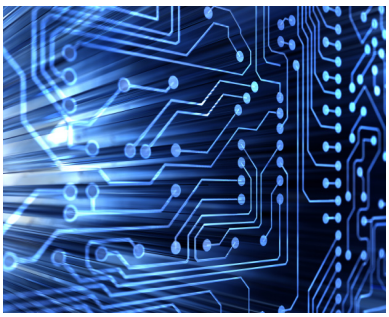
IT Audit Applications for ACL



APPLICATION SHEET

In a data warehousing project involving more than 20 million customer data records, a major power utility cut projected time in half and delivered at a fraction of the anticipated $1 million budget using *ACL* in the extract, transform, and load (ETL) process.

ACL was used in a data quality improvement project to automatically analyze and prepare data from over 40 separate systems for migration to SAP. In the process, *ACL* identified numerous duplications and invalid data entries.

ACL software solutions give organizations confidence in the accuracy and integrity of transactions underlying their key business processes and financial reporting. Within IT Audit, ACL technology is used to focus on the proper implementation, operation, and control of computer resources. IT auditors use ACL software to independently validate and assess controls and security, perform risk assessments and business impact analyses, and improve operational and system performance.

Following are some example usage scenarios:

Active Directory

- Identify active directory entries not assigned to current employees
- Analyze active directory group membership changes
- Identify inactive active directory accounts
- Monitor additions to sensitive active directory groups such as Domain Admin
- Correlate information from HR records to active directory assignments to identify users with similar roles but dissimilar security assignments

Application Security

- Compare employee termination date to last login date for user IDs
- Analyze IDs with last login date over a specified threshold
- Extract IDs where the date of last password change exceeds security standards
- Identify concurrent logins of the same ID
- Join application access records to network logs and IT asset records to identify logins from a computer not assigned to the user
- Analyze patterns of failed access attempts to powerful accounts or key users (CEO, CFO, Payroll manager, etc.)
- Compare vacation records from HR to user access
- Identify suspicious password patterns
  - » Multiple users with the same password or encrypted password
  - » Users who consistently change passwords at the same time
  - » Frequent password resets
- Compare user logins to physical security badge scanning systems and/or remote access logs

Segregation of Duties (SOD)

- Extract security rules and independently verify SOD
- Where potential SOD issues are identified, determine whether rights were exploited
- Independent of security rules, examine the user IDs associated with specific transactions to determine whether SOD violations have occurred (e.g. initiator = approver)
- Identify where users with the same role have different access rights
- Highlight users with powerful profiles / responsibilities
- Identify menus, functions, or transactions assigned to a user profile or responsibility which have never been used
- Identify user profile / responsibility changes made immediate prior to or shortly after an audit

System Security

- Automatically identify inappropriate security settings, or changes to key security parameters
- Correlate distributed security logs and look for suspicious activity (e.g, unusual time, duration, frequency)
- Stratify incoming and outgoing activity by IP address to identify suspicious activity
- Validate system-level controls in databases, operating systems, and applications, including:
  - » validity of user IDs
  - » identification of potential user IDs
  - » identification of "stale", common, or easily broken passwords
- Identify activation of previously-inactive IDs

Help Desk

- Review issues open for an extended period of time
- Stratify average issue resolution by issue type for operational efficiencies
- Highlight potential manipulation of reporting metrics (e.g. close times which do not make sense for the issue type)
- Identify users or departments with frequent or large numbers of issues
- Flag high-risk help desk transactions (e.g. password resets) for further audit
- Stratify problems by hardware, application, severity, etc.

Operations Management

- Independently validate the completeness integrity of selected interfaces
- Analyze job processing logs for frequent abends, terminations, or other system problems
- Benchmark system performance or capacity metrics for improvement opportunities
- Recalculate system usage or other metrics for IT cost allocation

ACL™

Change Control

- Identify program changes occurring after the test signoff date
- Independently test select changes and compare results to actual test results
- Compare key program or file size, timestamps, and other characteristics to a control table to identify instances where a change has occurred
- Extract system problems, occurring shortly after a change, from the help desk log and assess implications on integrity of change control process
- Identify program changes not appearing on change control logs
- Evaluate emergency change frequency by user, application, department, etc.

Application Controls

- Compare application control settings to control tables to identify potential changes
- Evaluate transactional data against control settings identify potential anomalies (e.g., customers with not credit limit, despite credit limit required flag = yes)
- Stratify changes to key parameters by user ID, date/time, etc.
- Identify where custom transactions or programs may be inadvertently bypassing standard system controls
- Validate the completeness and integrity of interfaces and data transfers

Telecommunications

- Report on users with largest cumulated phone minutes, largest average phone duration, most incoming calls, etc.
- Analyze after-hours phone usage by user, phone number, etc.
- Compare phone records to physical access records
- Extract calls to competitors
- Identify extensive calling to employee home numbers
- Compare cell phone outgoing call origination or incoming call destination locations to HR records or travel reports to highlight potential abuse

Data Quality

- Analyze master data for missing information
- Identify inconsistencies in data input
- Detect duplicate records
- Assess data for suspicious or erroneous entries (e.g., description fields with less than 2 characters input)
- Stratify quality metrics by employee to identify training opportunities
- Identify outdated or unused information

System Conversions

- Perform data integrity audits to identify potential data quality issues prior to conversion to a new system
- Convert, cleanse, restructure, harmonize, and consolidate data from legacy or multiple systems before loading into new or common applications
- Compare data from original systems to newly implemented systems for completeness and accuracy
- Validate data converted using mass-move utilities to system control settings
- Identify data changed during the data cleansing process
- Build automated auditing procedures as part of the new system design
- Create system control tables for future comparison with system settings to identify changes

Internet Usage

- Report on most frequently accessed domains and pages, by user, department, location, etc.
- Identify users accumulating the greatest amount of internet usage by day, time, department
- Identify incoming out outgoing traffic to unwanted sites
- Correlate web usage and system performance logs to determine trends

acl.com
info@acl.com

About ACL Services Ltd.

ACL Services Ltd. is the leading global provider of technology for audit and compliance professionals. Combining market-leading audit analytics software and professional services expertise, ACL solutions give auditors confidence in the effectiveness of internal controls and the integrity of the transactions underlying business operations.

Since 1987, ACL has enabled auditors to assure sustainable compliance, reduce risk, detect fraud, enhance profitability, and improve business performance. ACL delivers its solutions to more than 215,000 licensed users in over 150 countries through a global network of ACL offices and channel partners. Our customers include 95 percent of Fortune 100 companies, 85 percent of the Fortune 500 and over two-thirds of the Global 500, as well as hundreds of national, state, and local governments, and the Big Four public accounting firms.