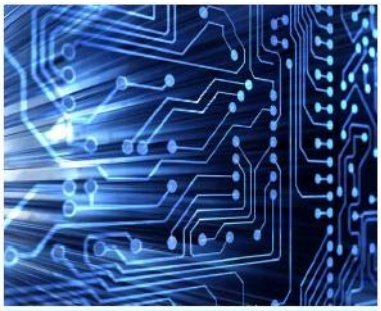
IT Audit Applications for ACL



APPLICATION SHEET

ACL 소프트웨어 솔루션을 통해 기업은 핵심 비즈니스 프로세스 및 재무보고에 있어 처리내역의 정확성 및 무결성에 대한 검증을 할 수 있습니다.

다음은 적용 가능한 시나리오의 예입니다:

Active Directory

- 현재 종업원이 아닌 사람에게 할당된 Active Directory 입력 파악
- Active Directory group membership 변경 분석
- Domain Admin과 같이 민감한 Active Directory group 추가 내역 모니터링
- 유사한 업무를 하지만 다른 보안 수준이 할당된 사용자 파악을 위해 인사 레코드 정보와 Active Directory assignment 연결

Application Security

- 종업원 퇴사일과 마지막 로그인 날짜 비교
- 일정기간 동안 접속하지 않은 ID 분석
- 보안 정책에서 지정한 기한이 초과할 때까지 암호를 변경 하지 않은 ID 추출
- 동일한 ID로 동시에 접속한 ID 파악
- 사용자에게 할당되지 않은 컴퓨터로부터의 로그인 확인을 위해 응용프로그램 접근 레코드와 IT asset 레코드 조인
- 관리자급 사용자 (CEO, CFO, 급여관리자 등)의 접근 시도가 실패된 패턴 분석
- 인사부서의 휴가 레코드와 실제 사용한 휴가 기록 비교
- 의심스러운 암호 패턴 파악:
  - 동일한 패스워드 또는 암호화된 패스워드를 가지고 있는 멀티 유저
  - 지속적으로 동일한 시간에 패스워드 변경하는 사용자
  - 잦은 패스워드 초기화
- 사용자 로그인과 physical security badge scanning system 및 리모트 엑세스 로그와 비교

업무 분장

- 보안 규칙을 추출하고, 업무분장을 독립적으로 확인
- 업무분장 이슈가 된 부분에 대해, 권한이 남용되었는지 확인
- 업무별로 업무분장을 통해 독립성이 유지되어야 하는 부분에 대해 독립성 훼손이 발생된 내역이 있는지 확인 (예: 기안자 = 승인자)
- 동일 업무 수행자들이 다른 접근 권한을 가지고 있는지 확인
- 높은 레벨의 프로파일 / 권한을 가지고 있는 사용자 식별
- 메뉴, 기능 또는 사용자 프로파일에 부여된 처리내역 또는 한번도 사용되지 않은 권한 파악
- 감사 직전 혹은 직후에 변경된 사용자 프로파일 / 권한 파악

시스템 보안

- 부적절한 보안 세팅 또는 핵심 보안 파라미터 변경 파악
- 분산형 데이터 처리 방식의 시큐리티 로그들의 상관관계 입증 및 의심스러운 활동 찾기 (예: 비정상적인 시간, 주기)
- 의심스러운 활동 파악을 위해 IP 주소별로 접속 정보 계층화
  - 사용자 ID 확인
  - 잠재적인 사용자 ID 확인
  - 오랫동안 변경 안되거나, 보편적이거나 또는 쉽게 알아차릴 수 있는 암호 확인
- 이전에 사용 안 하던 ID의 재활성화 된 내역 파악

헬프 데스크

- 오랜 기간 동안 해결되지 않은 이슈 검토
- 운영 효율을 위해 이슈 타입별 처리 시간 층별화
- 잠재적인 보고서 가공 파악 (예: 이슈 타입에 대해 비정상적으로 마감된 내역)
- 잦은 이슈가 발생한 사용자 또는 부서 파악
- 추가 감사를 위해 high-risk 데스크 처리 내역 플래그 (예: 패스워드 초기화)
- 하드웨어별, 응용프로그램별, 중대성별로 층별화

운영 관리

- 선택한 인터페이스의 무결성에 대해 독립적으로 완전성 확인
- 잦은 비정상적인 종료 또는 기타 시스템 문제에 대한 job 프로세싱 로그 분석
- 시스템 성능 또는 처리 능력 벤치마크
- 시스템 사용 또는 다른 IT 비용산정을 위한 기타 metrics 재계산

변경 관리

- 테스트 종료 기간 후에 발생된 프로그램 변경 파악
- 변경 항목을 선택하여, 독립적으로 시스템 결과와 ACL을 통해 나온 결과 비교
- 어디서 변경이 발생되었는지 확인하기 위하여, 핵심 프로그램 또는 파일 사이즈, timestamp, 및 컨트롤 테이블에 있는 기타 특징 비교
- 헬프 데스크 로그를 통해 변경 직후 발생된 시스템 문제 추출 및 변경 관리(control) 프로세스의 무결성 적용 평가
- 변경 관리 로그 (change control log)에 나타나지 않는 프로그램 변경 파악
- 사용자별, 응용프로그램별, 부서별 잦은 긴급 변경 사항 평가

운영 통제

- 잠재적인 변경 파악을 위해, 운영 컨트롤 세팅과 컨트롤 테이블 비교
- 잠재적인 이상치 파악을 위해 컨트롤 세팅과 비교하여 처리내역 데이터 평가 (예: 신용한도 없는 고객, 예금 신용한도 필수 플래그 = yes)
- 사용자 ID별, 날짜/시간별 핵심 파라미터 변경 층별화
- 사용자 필요에 의한 처리 또는 프로그램이 우연하게 표준 시스템 컨트롤을 우회(bypass)하는 곳이 있는지 확인
- 완전성 및 인터페이스 무결성, 그리고 데이터 전송 확인

통신

- 전화 사용량이 제일 많은 사용자, 전화 통화 시간이 제일 많은 사용자, 전화를 많이 받은 사용자 등을 보고
- 사용자별, 전화번호별로 근무시간 이후 통화 사용 분석
- 통화 기록과 실제 청구 내역 비교
- 경쟁사와 통화한 내역 추출
- 종업원 집으로 통화한 내역 파악
- 핸드폰 오남용을 알기 위해, 발신한 위치와 착신한 위치 정보를 인사부서 정보 또는 출장 보고서와 비교

데이터 품질

- 누락된 정보 파악을 위해 마스터 데이터 분석
- 데이터 입력 불일치 파악
- 중복 레코드 검출
- 의심되거나 잘못된 등록 평가 (예: 2개 미만의 문자값을 가지는 설명 필드)
- 교육 시기 파악을 위해 종업원별 품질 metrics 층화
- 오래되거나 사용하지 않는 정보 파악

시스템 이관

- 새로운 시스템으로의 이관 이전에, 잠재적인 데이터 품질 이슈 파악을 위해 데이터 무결성 감사 실행
- 새로운 프로그램에 로딩하기 전에, legacy 또는 멀티 시스템에 있는 데이터를 변환, 제거, 재구성, 조합 및 통합
- 완전성 및 정확성을 위해 오리지널 시스템 데이터와 새로 적용된 시스템의 데이터 비교
- mass-move 유틸리티를 사용하여 된 데이터 확인
- 데이터 클린징 프로세스 동안 변경된 데이터 파악
- 새로운 시스템 디자인의 일부로써 자동 감사 프로시저 구축
- 향후 변경 사항과 시스템 세팅 비교를 위해 시스템 컨트롤 테이블 생성

인터넷 사용

- 사용자별, 부서별, 위치별로 가장 자주 접속하는 도메인 보고
- 일자별, 시간별, 부서별로 가장 많은 인터넷 사용량을 가지고 있는 사용자 파악
- 불필요한 싸이트 접속으로 인한 트래픽 파악
- 트랜드 파악 결정을 위해 웹 사용 및 시스템 성능 로그 상관관계 수립

■ acl.com
aclkorea.co.kr

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.