IT 감사 및 내부통제 진단 서비스

IT Audit & Internal Control Assessment Service

"IT 통제의 사각지대, 시스템 로그와 운영 데이터로 검증합니다"

HM COMPANY™

1. IT 감사 및 내부통제 진단의 필요성

IT 통제는 더 이상 내부 운영 관리에만 머무르는 이슈가 아닙니다. 강화되는 규제 환경과 감독기관의 검증 요구 속에서 IT 통제 미흡은 과징금·제재·외부감사 지적·경영평가 불이익으로 이어질 수 있는 핵심 리스크가 되고 있습니다.
기업은 시스템 로그와 운영 데이터를 기반으로 IT 통제의 설계·운영 실효성을 점검하고, 운영 리스크를 사전에 식별하여 규제 대응 체계를 갖출 필요가 있습니다.

1,348억원
IT 로그 및 접근통제 미흡으로 인한 대규모 제재 사례
개인정보보호위원회

27.6%
2025년 금융권 IT 실태평가 '미흡' 등급 비율
금융감독원(2025)

18.4%
자산 1,000억 미만 상장사 내부회계관리제도 '비적정' 의견 비율
금융감독원(2024)

강화되는 규제·제도

시행년도	규제·제도	변경 전	변경 후
2022	K-SOX 내부회계관리제도 외부감사	자산 5,000억 이상 상장사 중심 적용	자산 1,000억 이상 상장사로 확대 ITGC 평가 중요성 증가
2023	개인정보보호법	과징금 산정 기준 위반행위 관련 매출액의 3%	과징금 산정 기준 확대 전체 매출액의 3% 적용 가능
2025	전자금융감독규정	정보보호 의사결정 = 실무 부서 중심 운영 재해복구센터 = 대형 금융회사 중심 적용	정보보호 중요사항 이사회 보고 의무화 재해복구센터 구축 대상 확대
2025	금감원 IT 감사	표준화된 IT 감사 기준 미흡 자체감사 중심 운영	금융감독원 「IT 감사 가이드라인」 시행 표준화된 IT 내부통제 점검 체계 요구
2026	개인정보보호법	과징금 한도 = 매출 3% 일반·중대 위반 구분 없이 매출 기준 적용	반복·중대 위반 시 징벌적 과징금 가능성 확대 개인정보 보호 통제의 실효성 요구 강화

출처: 주식회사 등의 외부감사에 관한 법률(법률 제15022호) · 개인정보 보호법(법률 제19234호, 2023.9.15 시행) · 전자금융감독규정 일부개정고시(금융위원회 고시 제2025-4호, 2025.2.5 시행) · 금융감독원 「IT 감사 가이드라인」(2025.2 전 금융권역 시행) · 개인정보 보호법 일부개정법률(2026.9 시행 예정)

© 2026 HM COMPANY™ | ADFS. All Rights Reserved

2. IT 감사 주요 진단 범위

금융감독원, 행정안전부, ITIL, ISO 등 주요 기준을 기반으로 IT 거버넌스부터 응용프로그램 운영, 정보시스템 운영 절차까지 **IT 통제 전반의 설계 적정성과 운영 실효성**을 체계적으로 검증합니다.

1 IT 내부통제 거버넌스 진단

출처: 금융감독원 「IT 감사 가이드라인」 (2025.2)

주요 점검 영역

- IT 내부통제 체계
- IT 리스크 평가
- 자체 IT 감사 체계
- 감사계획 및 후속조치 관리
- 직무분리 및 업무 독립성
- 내부통제 담당 인력 및 교육 체계

핵심 검증 방법

- 권한 매트릭스 기반 교차 분석
- 개선 조치 이행 여부 확인
- 직무분리(SoD) 위반 여부 식별

2 응용프로그램 운영 절차 진단

출처: 행정안전부 「응용프로그램 표준운영절차」, ITIL V4 Change Management

주요 점검 영역

- 변경관리 절차
- 배포관리 절차
- 테스트관리 절차
- 시스템 연계관리
- 형상 및 버전관리
- 운영상태 모니터링

핵심 검증 방법

- 변경 로그 및 승인 이력 분석
- 배포 이력 및 배포 승인 흐름 추적
- 개발·테스트·운영 환경 분리 여부 검증

3 정보시스템 운영 거버넌스 진단

출처: 행정안전부 「정보시스템 표준운영절차」, ITIL V4 Change Management, ISO/IEC 20000·27001

주요 점검 영역

- 요청 및 이벤트 관리
- 장애 및 문제 관리
- 구성정보 관리
- 백업 및 복구 관리
- 서비스수준관리(SLM)
- 접근통제 및 로그 관리

핵심 검증 방법

- 장애 복구 시간(MTTR)과 원인 분석(RCA) 이력 추적
- 백업 복구 목표(RPO/RTO) 충족 여부 검증
- 로그 무결성 및 보관기간 준수 여부 점검

HM COMPANY의 IT 감사 접근 방식

✓ IT 통제의 설계와 실제 운영 상태를 **시스템 로그와 운영 데이터로 실증 검증**

✓ **담당자 인터뷰**를 통해 문서상 통제와 실제 운영 간 차이 확인

✓ **운영 시스템 현장 실사**와 통제 작동 여부 검증 수행

© 2026 HM COMPANY™ | ADFS. All Rights Reserved

3. IT 감사 주요 발견사항 — 권한·접근통제 영역

실제 IT 감사 현장에서 가장 빈번하게 식별되는 결함 유형 중 하나는 **권한 부여·회수·분리에 대한 통제 미흡**입니다.
아래는 권한·접근통제 영역에서 자주 확인되는 주요 결함 유형과 개선 권고 방향입니다.

1 접근권한·계정 관리 미흡

퇴직자·전환배치자 계정이 즉시 회수되지 않거나, 특권 계정(admin/root)이 공유되거나, 권한에 만료기한이 설정되지 않을 경우 비인가 접근·권한 잔존·사후 추적 불가 리스크가 발생합니다. 도용된 계정정보와 자격증명은 침해사고의 주요 진입 경로로 지적되고 있으며, 국내에서도 계정·권한 관리 미흡에 따른 대형 사고가 반복적으로 확인되고 있습니다.

주요 발견사항

- **퇴직 직원의 미회수 인증키로 대규모 개인정보 유출 발생** — 국내 대형 이커머스 기업 사례
- **계정정보 평문 저장 및 보호조치 미흡으로 침해 발생** — 국내 대형 이동통신사 사례
- **권한 만료기한 미설정으로 임시 권한이 장기간 유지되는 사례 발생**

개선 권고 방향

- **계정 생애주기 관리 체계 구축** (입사·전환·퇴사 정보를 인사 시스템과 연계하여 권한 부여·변경·회수 자동화)
- **권한 만료기한 설정 및 정기 재검토** (최소 분기 1회 권한 적정성 점검)
- **계정정보 안전 저장 및 특권 계정 통제** (평문 저장 금지·암호화 적용·개별 계정화·접근 이력 모니터링)

2 직무분리(SoD)·권한 매트릭스 부적정

요청·검토·승인 권한이 동일인에게 집중되거나, 개발-운영-보안 권한이 겸직될 경우 상호견제 통제가 약화되어 비인가 변경과 부정행위 탐지가 어려워질 수 있습니다. **직무분리 통제가 제대로 작동하지 않으면 횡령·비인가 변경·정보유출 등 중대 사고로 이어질 수 있습니다.** SoD 위반은 ITGC 및 내부회계관리제도 평가에서 반복적으로 지적되는 주요 결함 유형입니다.

주요 발견사항

- **변경 요청·검토·승인 권한이 동일인에게 집중되어 상호견제 통제가 약화되는 사례 발생**
- **동일 직원이 장기간 단독으로 주요 업무를 수행하며 부정행위가 발생한 사례**
- **개발자가 운영 시스템 직접 접근 권한을 보유하여 변경 이력의 사후 검증이 어려운 사례**

개선 권고 방향

- **권한 매트릭스 교차 분석을 통한 SoD 위반 및 이해상충 식별** (권한 분배 현황을 정기적으로 진단)
- **단독 수행 업무에 대한 독립적 감시·이중 확인 체계 구축** (장기 단독 수행으로 인한 통제 공백 방지)
- **개발·운영 환경 분리 및 변경관리 워크플로우 자동화** (개발자 운영 권한 제한·변경 이력 자동 추적)

© 2026 HM COMPANY™ | ADFS. All Rights Reserved

4. IT 감사 주요 발견사항 — 외부 연계·이력 관리 영역

외주·협력사 등 외부 접점과 **감사추적·로그 관리**는 IT 운영 통제에서 사각지대가 발생하기 쉬운 영역입니다.
아래는 외부 연계·이력 관리 영역에서 자주 확인되는 주요 결함 유형과 개선 권고 방향입니다.

3 외주·협력사 접근통제 사각지대

외주 인력에 대한 과도한 권한 부여, 작업 종료 후 권한 미회수, 외주 PC·계정 관리 미흡은 비인가 접근과 정보유출의 진입점이 될 수 있습니다. 외주·제3자 접근은 보안 통제의 사각지대가 되기 쉬우며, 국내에서도 외주·협력사를 경유한 우회 침투와 정보유출 사례가 반복적으로 확인되고 있습니다.

주요 발견사항

- **외주·도급업체 인력에 과다 권한이 부여되거나 작업 종료 후에도 권한이 잔존하는 사례**
- **협력 개발자의 인증키 관리 미흡으로 대규모 자산 피해가 발생한 사례**
- **외주 개발자 PC를 통한 고객사 시스템 접속 계정 탈취 및 개인정보 유출 사례**

개선 권고 방향

- **외주 권한 한시 부여 원칙 적용** (작업 단위와 기간을 명시하고 승인 절차에 따라 권한 부여·회수 관리)
- **협력사 인증키·자격증명 안전 관리** (별도 저장소·암호화·정기 교체 체계 운영)
- **외주·유지보수 인력 PC 보안점검 및 접속 통제 강화** (일회성 접속 계정·이중 인증·IP 접근통제·정기 보안교육 운영)

4 감사추적·로그 관리 부실

주요 시스템 이벤트 로그 미보관, 로그 무결성 검증 부재, 변경 전후 데이터 미기록은 사고 발생 시 원인과 영향 범위 재구성을 어렵게 만듭니다. 최근 국내 침해사고에서도 계정·권한·로그·분리 등 기본 운영 통제의 미흡이 주요 원인으로 지적되고 있어, 로그 관리와 감사추적 체계의 중요성이 커지고 있습니다.

주요 발견사항

- **일부 관리서버 로그만 점검하거나 로그 보관기간이 짧아 최초 침해 시점 추적이 어려운 사례**
- **데이터 변경 시 변경 전·후 값이 기록되지 않아 사후 감사 추적이 어려운 사례**
- **접속기록 보관기간 및 정기 점검 기준을 충족하지 못하는 사례**

개선 권고 방향

- **주요 시스템 로그 통합 수집·관리 및 보관기간 준수** (해시값·전자서명 등을 활용한 무결성 검증과 보관기간 관리)
- **변경 전후 데이터 자동 기록** (주요 데이터 변경 이력을 추적 가능하도록 Before/After Image 기록)
- **접속기록 정기 점검 체계 운영** (반기 1회 이상 정기 점검, 임계치 기반 이상 패턴 탐지)

© 2026 HM COMPANY™ | ADFS. All Rights Reserved

5. IT 감사 수행 프로세스 및 산출물

1 IT 환경 파악 및 감사 계획 수립
IT 인프라·시스템 현황 파악
감사 범위·일정·대상 확정

→

2 관련 자료 수집
정책·절차서·로그 등
필요 자료 요청

→

3 통제 테스트 및 시스템 실사
인터뷰·증적 확인 및
시스템 현장 실사

→

4 체크리스트 기반 통제 분석 수행
자료·테스트 결과 및
시스템 실사 결과 종합 분석

→

5 IT 감사 결과 보고서 제공
발견사항·개선 권고
경영진 보고용 산출물

IT 감사 기대효과

1 규제·회계 평가 대응력 확보

- ITGC 결함을 사전에 식별·개선하여 K-SOX 및 내부회계관리제도 평가 대응력 강화
- 내부회계관리제도 적정 의견에 따른 지정감사 리스크 완화
- 금융권 IT 실태평가 미흡 등급 리스크 완화

2 감독·관리 의무 이행 근거 확보

- 감독기관 점검·조사 대응 시 IT 통제 이행에 대한 객관적 증빙으로 활용
- 사고 발생 시 원인·영향 범위·조치 이력의 추적·재구성 가능

3 IT 통제 결함 사전 식별 및 개선

- IT 통제 사각지대를 사전에 식별하여 시스템 운영 안정성과 신뢰성 강화

주요 감사 산출물

1 IT 감사 결과 보고서

발견사항·개선 필요사항·이행 조치 방향을 상세히 기술한 정식 보고서

- 점검 결과 요약 및 위험도 등급 분류
- 주요 발견사항별 원인·영향도 상세 분석
- 경영진 요약 (Executive Summary)

2 IT 감사 조서

체크리스트 기반 점검 결과·증빙자료·테스트 내역을 수록한 감사 조서

- 항목별 점검 내용 및 평가 근거
- 증빙자료와 감사 산출물 매핑
- 인터뷰 및 현장실사 결과

3 개선 로드맵

발견사항별 단기·중장기 개선 과제와 우선순위별 이행 일정을 제시

- 발견사항별 개선 방향
- 이행 우선순위 매트릭스
- 단계별 이행 일정 및 담당 영역

© 2026 HM COMPANY™ | ADFS. All Rights Reserved

6. HM Company 주요 수행 역량 및 실적

HM Company는 2011년 설립 이후 디지털포렌식 전문성을 기반으로 정보유출 조사, 개인정보·정보보호 리스크 진단, IT 감사, 내부감사 등 기업 리스크 대응 서비스를 수행해 왔습니다.

ADFS 본부	RAS 본부	AI MARU 본부
디지털포렌식 서비스	컴플라이언스 리스크 진단	리걸테크: 수사·증거 분석 AI
정보유출 조사 / IT 감사	회계감사 외부전문가 조사	에듀테크: AI 학습 도구
정보보호 리스크 진단	경영진단·내부감사	LLM 오케스트레이션 / RAG
KOLAS 공인시험성적서 발급	직장 내 괴롭힘 조사 / PMA	데이터 어노테이션 플랫폼 LEAP

Why HM COMPANY ADFS

15년+
디지털포렌식 기반
조사·진단 수행 경험

20,397+
누적 디지털포렌식
증거물 처리 경험

KOLAS
민간 최초 디지털포렌식 분야
KOLAS 공인시험기관 인정 보유

NDA
보안서약 체결 및
데이터 안전 폐기 체계 운영

주요 수행 실적

분야	주요 수행 실적
금융	내부감사 자료 검토 및 Co-Sourcing
금융	협력업체 개인정보 및 정보보안 리스크 진단
금융	법인카드 및 골프회원권 사용 적정성 조사
제조	임직원 부정행위 조사 및 사실관계 분석
제조	첨단기술 및 영업비밀 유출 리스크 진단
제조	제품 설계도 등 영업비밀 파일 유출 리스크 진단
제조	회계장부 등 영업비밀 유출 진단
제조	정보유출 및 부정위험 조사·진단
의료·헬스케어	임직원 개인정보 관리실태 진단
의료·헬스케어	임원 부정행위 의혹 조사 및 검토
유통	보유 고객정보 관리실태 진단
유통	협력업체 개인정보 관리실태 진단
법률 사건 지원	디지털 증거 확보, 선별 추출, 전처리, 검색 가능한 검토 환경 구성

© 2026 HM COMPANY™ | ADFS. All Rights Reserved

HM COMPANY™

Contact Us

박 재 현 상무

jaehyun.park@hmcom.co.kr

이 정 훈 수석

jeonghoon.lee@hmcom.co.kr

ADFS본부

02-6237-6213

대표전화

02-6237-6233

본부 소개서

QR코드를 스캔하여
본부 소개서 PDF를 확인하세요.

IT 감사·내부통제 진단 상담을 신청하세요
기업의 규제 환경, 내부회계관리제도, ITGC, 접근권한·
로그 관리 수준을 고려하여
맞춤형 IT 감사 범위와 수행 방안을 안내드립니다.

hmcom.co.kr
hmadfs.com
서울특별시 서초구 효령로70길 36-9, 와이엘타워 2층, 3층

© 2026 HM Company™ | ADFS. All Rights Reserved

IT Audit Service