2024년 IT검사 방향

2024.3.11.

금융감독원 IT검사국

목차
table of contents

I

디지털금융 환경 변화와 IT 리스크

디지털금융 환경 변화에 따른 IT리스크

주요 디지털금융 환경 변화(IT리스크 관점)

1. AI 등 IT신기술 기반 금융서비스 증가
2. 클라우드컴퓨팅서비스 등 외부 연계 확대
3. 오픈소스를 활용한 S/W개발의 일상화
4. "규칙(Rule)→원칙(Principle) 중심" 규제 전환

"전산장애 및 보안사고 발생 우려"

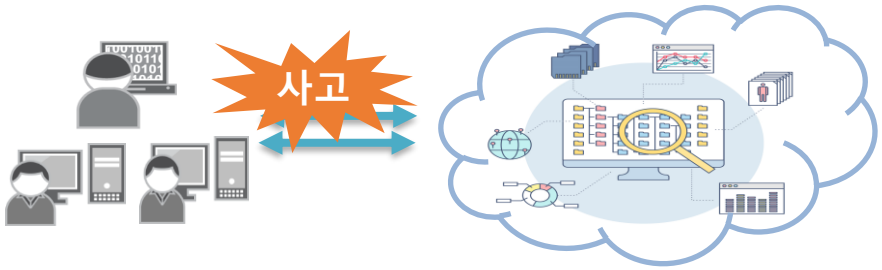
새로운 리스크에 대한 식별 지체

제3자 리스크 증가 　 특정 사업자 종속

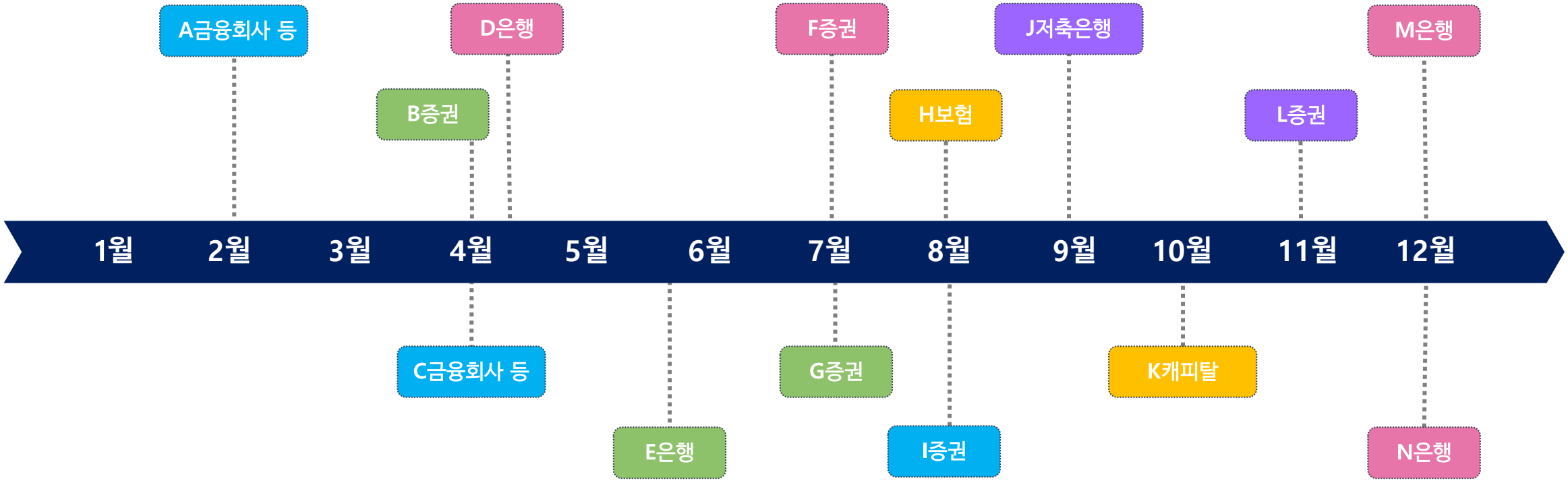
일시적 이용자 급증에 의한 장애

오픈소스 보안 취약점 　 사이버 위협 증가

IT거버넌스 기반 약화 우려



2023년 주요 전자금융사고 현황



- 외부 연계서비스 장애 관리 소홀
- 프로그램 변경 적용 오류로 인한 장애
- 대규모 트래픽 준비 미흡으로 인한 장애
- 클라우드 운영 미흡으로 인한 장애
- 개인(신용)정보 유출 사고

Ⅱ

자율시정체계 구축 및 핀포인트 수시 IT검사 실시

2024년 IT검사 방향

	금융감독원	금융회사
IT감사·거버넌스 강화	• IT감사·거버넌스 체계 확립 요구 - CIO · CISO 간담회 - IT상시협의체 - IT부문 내부감사협의제 • IT감사 가이드라인('24년中 예정)	• 경영진 IT운영 보고 체계 수립 • CIO – CISO 상호 견제 • IT감사(감사조직 등) 및 IT자체감사(IT조직 내) 역량 확충 - 정기적 감사 실시
자율시정체계 구축	① 맞춤형 자가진단 체크리스트 배포 ④ 자율점검 결과 평가 및 高위험사 선정	② IT감사 실시(자율점검 · 시정) ③ 점검 결과(대표이사 확인) 및 건의사항 제출
핀포인트 IT검사 실시	• 핀포인트 수시검사 실시 • 기본사항 위반시 엄중 제재 • 모범 · 취약사례 전파	• IT운영 · 통제 체계 확립 - 기본사항 준수 및 자체점검 실시 • 전자금융사고 억제력 · 복원력 제고

IT검사 업무 운영 방안

핀포인트 수시검사 실시

◦ IT실태평가 위주의 포괄적 검사방식에서 **IT취약부문에 선택·집중**하는 **핀포인트 수시검사 방식**으로 전환

- 평가 항목 효율화 등 **탄력적인 IT실태평가 운영**을 통해 수시검사 **가용인력 확보**
- **긴급 현안** 발생시 **신속·유연**하게 **대응** 가능하도록 팀 구분없는 **애자일* 검사반 운영(검사인력 Pool제)**
- IT검사 **기능별·부문별 전문가**를 **지정(Matrix)·운영**하여 IT검사 품질 제고

*Agile : 부서간 경계를 허물고 필요에 맞게 소규모 팀을 구성해 업무를 수행하는 운영전략

상시감시와 연계한 고위험사 집중 검사

◦ **IT리스크 계량평가** 등 **상시감시**를 **강화**하고, 도출된 **취약요인**을 **검사 착안사항**으로 **연계**

◦ **시급성**을 요하는 **취약요인**이 발견된 경우 **애자일 검사반**을 **구성**하여 **즉시 현장검사** 실시

◦ **취약점**(계량평가 결과)에 대한 **자율개선 요구** 후, **재평가 결과**도 **미흡**한 회사 등은 **현장검사**를 실시하여 **엄정 조치**

선진적·대체적 조치수단을 활용한 제재 수용성 제고

◦ **운영·통제**의 **기본적인 사항 미준수**에 대해 중점 점검하되, **단순·경미**한 위반행위는 **자율시정 유도**(획일적 제재 지양)

기관조치 갈음 MOU

◦ 위규예방, 소비자보호 등 기관제재와 동일한 효과
◦ 제재로 인한 부정적 부수효과는 완화

준법교육조건부 조치면제

◦ 제재수준이 '주의'에 해당하는 경우(상당 포함) 준법교육이수를 조건으로 조치 면제

자율개선이 가능한 경우
현지조치 적극 활용

중점 검사사항 (1)

중점 검사사항

◦ **주요 전자금융사고 발생 원인**인 제3자 리스크 관리, 전산시스템 성능관리, 비상대책 및 프로그램 · 전산원장 통제 관리 등을 중점 점검

- **IT감사 · IT경영** : IT감사 조직 구성, 감사부서의 IT감사 실적 및 정기적인 경영진 보고 여부, 시정처리의 적정성 등
- **전자금융사고 대응 체계** : 사고 보고 및 대응 체계의 적정성, 비상연락체계 관리 등
- **제3자 리스크 관리** : 외부 단일장애지점, IT위탁·연계서비스, SW 공급망 등에 대한 인식(연관관계 명세 등) 및 통제 등
- **전산시스템 성능관리** : IPO, 차세대 등 대형이벤트에 대비한 전산자원별 성능관리 임계치 설정 및 단계별 대책 마련, 모니터링 실시 등
- **프로그램 · 전산원장 통제** : 프로그램 · 전산원장 변경 관리, 제3자 검증 실시, 사전 영향도 분석 및 테스트, 절차 준수 여부 점검 등
- **IT부문 비상대책 수립 · 운용** : 핵심업무 선정 · 관리, 대외기관과의 연계 기능을 포함한 훈련 실시, 전산센터 화재 예방 · 대비 등

신규 IT 트렌드에 대한 선제적 대응

◦ **IT신기술** 도입, **제3자 서비스** 증가 및 **애자일 조직** 확산 등 금융권 동향에 대한 **신규 IT리스크**를 **심층 점검 · 모니터링**하여 전자금융사고 예방

(참고) 주요 금융IT 신기술 활용사례 및 예상 리스크

신기술	활용	주요 예상 리스크
클라우드 (Cloud)	IaaS, PaaS, SaaS	▪ 연구·개발용 망분리 예외 적용 클라우드와 내부망 연결 상 취약점 ▪ 클라우드 제공업체(CSP) 장애시 CSP내 대고객 서비스 중단 가능
데브옵스 (DevOps)	S/W개발	▪ S/W의 개발·운영이 융합되어 각 직무간 경계·통제가 모호 ▪ 자동화로 빠른 개발과 배포를 추구하여 통제 사각 발생
GPT	챗봇고객응대, 투자조언, AI비서	▪ 별도 저장된 학습데이터의 유출·노출·출력 가능 ▪ GPT 사용으로 망분리, 망간연결 문제 등 신규 보안 이슈 발생

중점 검사사항 (2)

합동 재해복구훈련 지속 실시

◦ **대외 기관**과 **연계**한 **재해대응 역량 강화**를 위해 **합동 재해복구훈련**을 **지속 실시**하고, 발견된 **미흡사항 개선**

◦ 금년에는 **지주사 계열 전체** 및 **유관기관**이 참여(1개 지주 선정)하는 합동훈련을 실시할 예정으로,
업무 연속성에 대한 경영진 전체의 관심과 참여 필요

(참고) 재해복구훈련 점검 내용

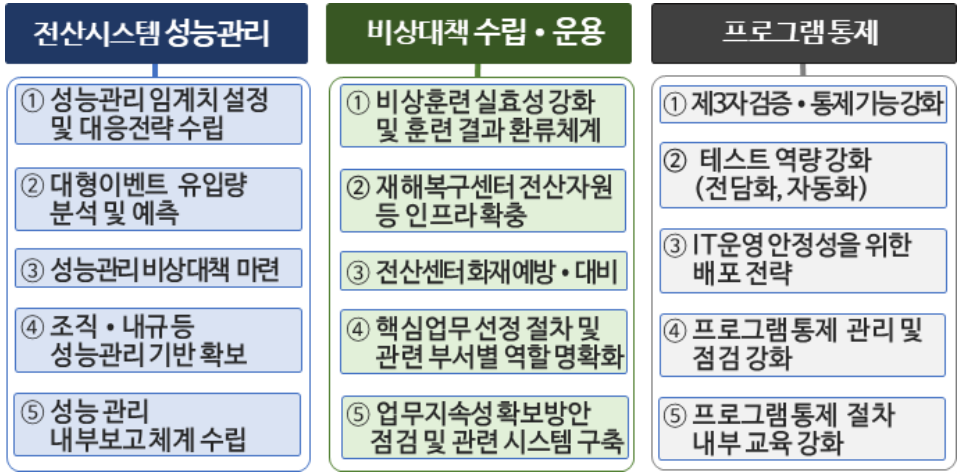
◦ 특정 계열사의 장애가 다른 기관으로 전이되는 리스크 등에 대하여 훈련 시나리오의 적정성, 범위, 사후관리 등을 점검
⇒ 훈련이 실질적으로 비상대응 능력 제고에 기여하는지 확인

<참고> 금융IT 안전성 강화 가이드라인

◦ '23.11월, **IT검사 공통 지적 사항**과 **주요 전산사고** 발생 원인의 **근본적 해소**를 목적으로 **안전성 강화 가이드라인** 마련

◦ IPO 등 대형이벤트 사전 대비, 비상대응 훈련 범위 확대, 프로그램 테스트·검증·배포 통제 강화 등 기준 제시

◦ '24년중 금융회사의 **가이드라인 준수 실태**를 **점검**하여 **실효성 확보**를 위해 지속적으로 노력하고 **원칙중심 자율시정체계 정착** 유도



자율시정체계 적극 지원

IT감사 가이드라인 마련 (추진 중)

◦ IT감사 전문인력·조직 운용, IT감사 주기, 중점 점검항목 등을 포함한 **맞춤형 가이드라인을 마련**하여 **IT부문 감사기능 강화 유도**('24년中 예정)

- 금융회사 **자체 IT감사 조직·인력 구성** 및 **주기적인 감사부서의 IT감사** 실시
- 자체 IT감사 조직·인력을 갖추지 못한 중소형사의 경우 외부용역 등을 활용한 IT내부통제 감사를 실시하도록 권고

◦ **업계참여 T/F** 구성('24.5월 예정), **IT상시협의체 · IT내부감사협의제**를 통해 의견 수렴

소통채널 활성화

◦ **전자금융사고 원인** 등 **주요 IT리스크**, **모범·취약 사례 전파** 및 금융회사 **건의·애로사항 청취** 등 **쌍방향 소통**

[간담회 등] : 경영진
CIO · CISO 간담회 등 현안 발생 시 수시 개최

[IT상시협의체, 세미나 등] : IT실무자
전자금융업 수행 금융회사 대상 분기별 개최
(세미나 : 현안 발생시 수시 개최)

[IT부문 내부감사협의제] : 감사부서
금융회사가 자율시정이 가능한 사항을 찾아 스스로 개선

(참고) 2024년 IT상시협의체 운영방안

◦ 감독규정 개정 내용, 새로운 IT 위협 요인 등 주요 리스크를 공유하고 새로운 유형의 전산사고 및 대처방안 등 신속 전파
◦ 신기술 도입 관련 정보수집, 감독·검사상 애로·쟁점사항 등 다양한 의견을 교환할 수 있는 창구로 활용

Ⅲ

과태료 부과체계 개편 및 사고 대응 체계 강화

과태료 부과체계 개편 주요 내용

전금법 §21②
안전성 확보의무 위반
과태료 산정 "불합리"

⇨ **위반행위별 과태료 부과기준 마련** ('23.12월)

□ **위반행위별 부과원칙**에 따라 **2개 이상**의 질서위반행위가 경합하는 경우에는 **과태료**를 **각각 부과**

◦ ① **시간적·장소적 근접성**, ② **행위의사의 단일성**, ③ **침해 법규정의 동일성**(5개 보호법익)이 모두 인정되면 **하나의 행위**로 **포괄**

(예시)

◦ ⑴전원실에 자물쇠 미설치, ⑵자가발전설비 및 ⑶UPS 설치도 미흡한 경우 질서 위반행위가 여러 개 경합하였으나,

① 시간적으로 근접 및 장소가 동일하고, ② 단일한 과실로 인해 발생하였으며, ③ '인력·조직·예산' 보호법익에 해당하므로 1개의 행위로 포괄하여 과태료 부과

⑴인력·조직·예산, ⑵시설,
⑶정보기술부문 전자적장치 등
⑷정보기술부문 내부통제
⑸전자금융업무

* 감독규정 개정시 변경 가능

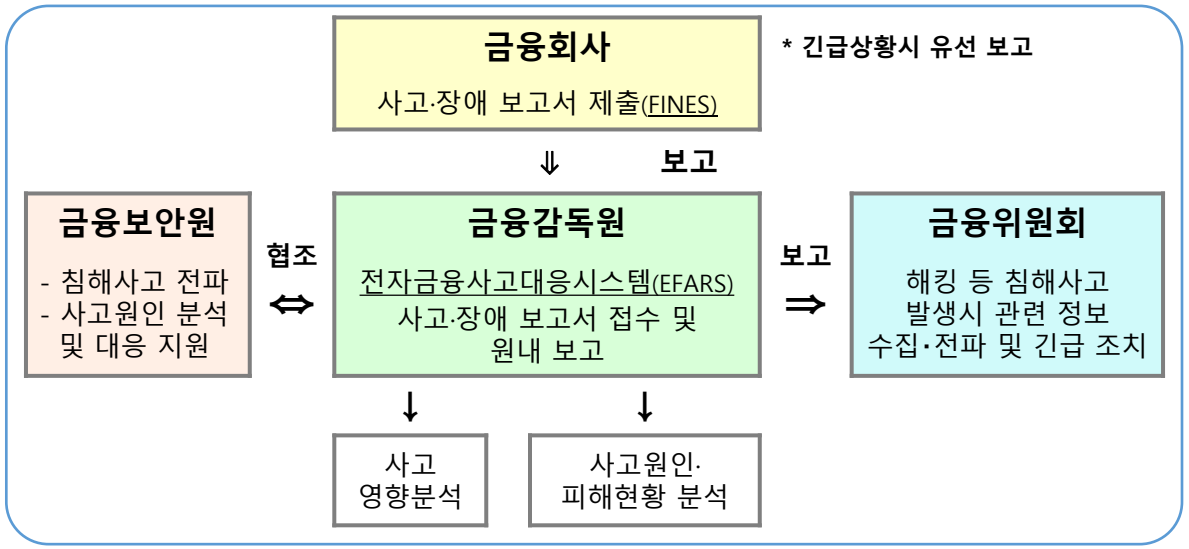
□ **지속·반복적 부작위** 위반은 고의성 등이 없는 경우 **1건**으로 처리

(예시)

◦ 40일간 중요 단말기 악성코드 감염 미점검(§16) ⇒ 1개 행위로 포괄
◦ 다수 일괄작업에 대해 통제절차 미준수(§30) ⇒ 1개 행위로 포괄

전자금융사고 대응 체계 강화

현행 사고 보고 체계



◦ **최초보고** : **사고 인지 후 즉시(24시간 이내)** 실시

- 긴급 상황 시 최초보고 절차를 간소화하는 등 탄력적으로 운영하며, 조치 경과에 따라 최초·중간·종결보고 실시

◦ 사고의 **중대성**에 대한 **기준**이 **모호**하고, **사고보고**가 **누락**되는 문제 등

사고 보고 관련 규정·세칙 개정 (추진 중)

◦ 전자금융사고의 유형, 처리단계, 조치방법, 영향도·심각도 등을 관리하는 **절차**를 **마련**토록 **의무화** <규정>

◦ **사고보고** 기준<시행세칙>을 **명확히**하고 **보고대상**을 **일부 완화** <시행세칙>하는 한편, **미보고**에 대한 **과태료 부과** 근거<규정> 마련

중대사고 분류기준 마련 (추진 중)

◦ **전자금융사고**의 **경·중**에 따라 사고를 명확히 **분류**하고 **대응**을 **차등화** 할 수 있도록 **중대사고 분류기준** 마련

유의사항

◦ 사고 발생 시 **신속 보고**, 중대 사고인 경우 즉시 **담당 RM**에게 연락

◦ **사고 보고 위반시 과태료 부과 유의**(감독규정 개정안 시행 시)

◦ **비상연락체계**(금융회사별 정·부 담당자, CIO, CISO 등) **상시 현행화**

Q&A

감사합니다

금융감독원 IT검사국