


금융생활에 필요한 모든 정보, 인터넷에서 「파인」 두 글자를 쳐보세요

“금융은 튼튼하게, 소비자는 행복하게”

	보 도 자 료		
	보도	2022. 4. 11.(월) 조간	배포 2022. 4. 8.(금)
담당부서	IT검사국	장성옥 국장 (3145-7420), 위충기 팀 장 (3145-7415)	

제 목 : 2022년도 IT리스크 상시감시 및 검사업무 운영방향

◆ 금융감독원은 금융상품의 복잡화·다양화로 인한 전자금융거래의 안전성 확보 및 소비자 피해 예방을 위하여 금융부문 IT업무 전반에 대한 「IT 리스크 상시감시 및 검사업무 운영방향」을 마련하였습니다.

1 추진 배경

- ☐ 금융감독원은 2016년부터 「IT리스크 계량평가 제도」 도입하여 자산규모 2조원 이상인 대형 금융회사에 대하여 IT 인프라 운영상의 주요 리스크를 정기적으로 점검하고 있으나,
 - 최근 중소형 금융회사 및 전자금융업자가 디지털 기반의 금융상품 및 신규서비스 출시를 확대하면서
 - 대형 금융회사에 비해 IT 인프라·정보보호 기반이 열악한 중소형 금융회사 등의 IT 리스크가 증가할 것으로 예상됩니다.
- ☐ 이에 금융감독원은 전자금융업무를 수행하는 모든 금융회사 및 전자금융업자의 IT 리스크에 선제적 대응이 가능하도록 상시감시 및 검사 업무를 운영해 나갈 계획입니다.

2 상시감시 및 검사업무 운영 방향

- ◆ 금융회사 및 전자금융업자의 IT 리스크를 상시 평가하여 도출된 취약점을 자체감사 활동을 통해 자율 시정하도록 유도하고,
 - 금융환경 변화에 따른 IT 리스크에 선제적 대응이 가능하도록 핵심·취약부문에 대한 사전예방적 검사를 강화하겠습니다.

가. IT 리스크에 대한 상시평가 기능 강화

- **(평가대상)** 전자금융업무*를 수행하는 '모든 금융회사 및 전자금융업자'에 대해 IT 리스크 계량평가를 실시할 예정입니다.

* 전자금융거래법상 전자적 장치를 통하여 금융상품 및 서비스를 제공하는 업무

- 자산규모가 2조원 이상이거나 IT 의존도가 높은 금융회사에 대해서는 'IT 리스크 계량평가'를 실시하고,
 - 중소형 금융회사 및 전자금융업자에 대해서는 계량평가 항목을 간소화 한 간이평가를 실시할 예정입니다.

- **(평가방법)** 계량평가 지표는 5개 부문*, 36개 항목에 업권별 특성을 반영, 4~10개 항목(반복지적, 장애 등)을 추가하였고,

* IT감사, IT경영, 시스템 개발·유지보수 등, IT서비스 제공·지원, IT보안·정보보호

- 간이평가 지표는 계량평가 항목 중 IT 인프라 안전성 확보에 필수적인 13~18개 항목을 선정하여 평가할 예정입니다.

[참고] IT리스크 상시평가모형 고도화 추진 방안

- ◇ IT 인프라 운영 및 정보보호 등의 업무를 정량적 지표와 정성적 지표를 활용하여 평가*하고 잠재적 리스크 수준을 판별이 가능한 IT리스크 상시평가 모형 개발 추진

* **(정량평가)** 현행 IT리스크 계량평가 항목을 수정·보완하여 정량평가 지표로 활용
(정성평가) IT인프라 취약점 평가결과, 반복지적사항 등을 토대로 정성평가 지표 개발

나. 자체감사 등을 통한 자율규제 기능 강화

□ **(기본방향)** IT 인프라 운영 및 정보보호 등 IT 업무 전반에 대한 상시평가 과정에서 취약점이 확인되는 경우

- 금융회사 및 전자금융업자에 대해 자체감사를 요구하는 ‘자체감사 요구제도’*(가칭)를 도입·시범 실시할 예정입니다.

* **계획(안)** : 상시평가 및 대상회사 선정 → IT상시협의체* 개최 및 감사요구 배경 및 점검방법 등 설명 → 자체감사 실시 → 감사위원회·금감원 보고 → 적정성 검토

※ IT상시협의체 구성 및 운영 방향

◇ 자체감사 지원 등을 위해 비대면 방식의 IT상시협의체 구성 추진 (☞ 4월중 의견 청취)

- 협의체구성 : (금감원) IT검사국 5개 검사팀 참여, (참여회사) 실무지원반 구성
- 실무지원반 : CISO가 총괄하고, IT운영·정보보호 부문 실무책임자 등으로 구성
- 협의체운영 : (개최주기) 연 1회, 필요시 상시, (운영방식) 참여회사와 1:1 토론 방식

□ **(운영방안)** IT리스크 상시평가 등급이 일정기준 이하인 경우 해당 금융회사 및 전자금융업자의 자체감사 활동을 통해 취약점을 자율시정 하도록 유도*할 예정입니다.

* 금융회사 등의 자체감사 활동을 지원하기 위하여 IT상시협의체를 통하여 각종 노하우 및 체크리스트 등을 제공하는 등 소통을 강화할 예정임

- 금융회사·전자금융업자가 제출한 자체감사 결과는 IT검사국 담당 검사팀에서 ‘적정성 검토(Review)’를 실시하고,
 - 금융회사 등의 자체감사 결과 조치사항이 ‘적정’한 경우에는 금융회사 등의 의견을 원칙적으로 수용하되,
 - 개선 등의 조치가 부실하거나 허위의 사실을 보고하는 등 ‘부적정’한 것으로 판단되는 경우에는 필요시 금융감독원이 직접 검사를 실시할 예정입니다.

다. IT 부문에 대한 사전예방적 검사 강화

□ **(정기검사)** 금융회사의 특성, 규모, IT 의존도 등을 감안하여 2~5년 주기*로 IT부문에 대한 정기검사를 실시하겠습니다.

- IT 업무 전반에 대한 실태평가*와 함께 상시평가 결과 확인된 취약점 및 미흡사항에 대해서도 중점 검사할 예정입니다.

* IT감사 등 5개 부문에 대해 81개 비계량 항목에 대해 정성평가 실시

※ 금융업권의 IT부문 정기검사 운영방안

구 분	주 기	구 분	주 기
은 행	(지주계열 시중은행) 2.5년 (인터넷, 지방은행 등) 3.5 ~ 4.5년	보 험	(대형 생·손보사) 3 ~ 4년 (중형 생·손보사) 5년
금융투자	(종합금융투자사업자) 3년 (대형 증권사) 5년	여신전문	(카드사, 대형 캐피탈) 5년
저축은행	(대형 저축은행) 2년	상호금융	(신협 중앙회) 3년

□ **(수시검사)** IT 사고로 소비자 피해가 발생하였거나, 내부통제가 취약한 금융회사 등을 대상으로 테마검사를 강화할 예정입니다.

- 망분리 규제 준수, 공개용 웹서버 취약점 보정(patch) 등의 보안대책 소홀*에 따른 침해사고**가 발생하거나,

* (예시) 업무용 단말기에 대해 정보보호위원회 승인 없이 망분리 예외를 적용하거나 해킹 공격에 취약한 홈페이지 등 공개용 서버 취약점에 대한 보안 패치 미적용 등

** 전자적 침해행위(DDoS, 해킹 등)로 인해 전자금융기반시설이 교란·마비되는 등의 사고

- 인터넷뱅킹, 모바일 앱 등 대고객 서비스 관련 시스템 자원(서버, 회선, 전산장비 등)에 대한 성능관리 소홀로 장애사고가 발생한 경우 사고원인 규명을 위한 현장검사를 실시할 예정입니다.

- 아울러 IT리스크 상시평가 결과, IT 부문의 내부통제가 취약하여 사고 개연성이 높은 금융회사나 대형 전자금융업자에 대해 내부통제 점검을 위한 현장검사를 실시할 예정입니다.

3 향후 계획

- 금융감독원은 전자적 침해사고 및 장애사고로 인한 소비자 피해를 예방할 수 있도록 금융부문의 IT리스크에 대한 사전예방적 감독·검사를 강화해 나갈 계획입니다.
- 이를 위해 'IT리스크 계량평가 제도'를 보완하여 금융부문의 핵심업무에 대한 IT 리스크 수준을 조기 판별이 가능한 상시평가 모형을 개발하는 한편,
- 금년 4월중 금융업권의 의견을 청취하여 IT상시협의체를 구성하고, 동 협의체를 통해 금융회사 및 전자금융업자와 각종 현안사항 등에 대한 소통을 확대해 나갈 계획입니다.