금융감독원	**보 도 참 고**	금융은 튼튼하게 소비자는 행복하게

보도	2026.7.30.(목) 조간	배포	2026.7.29.(수)

담당부서	금융감독원 디지털금융총괄국	책임자	국 장	이 석	(02-3145-7120)
		담당자	부국장	손인호	(02-3145-7125)
	은행연합회 전략·경영·IT그룹	책임자	상무이사	이인균	(02-3705-5184)
		담당자	부 장	김재근	(02-3705-5331)
	금융투자협회 경영기획본부	책임자	본부장	진양규	(02-2003-9017)
		담당자	부 장	장영훈	(02-2003-9060)
	생명보험협회 경영지원본부	책임자	본부장	최종윤	(02-2262-6614)
		담당자	부 장	여창환	(02-2262-6613)
	손해보험협회 기획관리본부	책임자	본부장	김지훈	(02-3702-8524)
		담당자	부 장	박기준	(02-3702-8548)
	여신금융협회 금융본부	책임자	본부장	이효택	(02-2011-0724)
		담당자	팀 장	이근원	(02-2011-0735)
	저축은행중앙회 IT서비스본부	책임자	본부장	전회준	(02-397-8787)
		담당자	부 장	황두환	(02-397-8801)
	한국핀테크산업협회 사무국	책임자	사무국장	정진국	(02-6949-2675)
		담당자	실 장	신지원	(02-6949-2684)

「금융회사의 제3자 IT 리스크 관리 가이드라인」 마련

◈ **정보처리 업무위탁**에 따른 **IT 리스크**를 **체계적으로 관리**하기 위해 **「이사회·경영진 책임 명확화」**, **「위험평가 체계·방법」**, **「계약 단계 별 위험 식별·대응」** 등 기준 제시

◈ 업권별 **협회·중앙회 모범규준** 제정 등을 통해 **'26.11월 이후 시행**할 계획

Ⅰ. 추진 배경

□ 금융의 **디지털化**가 빠르게 진전되는 가운데 금융회사들이 **클라우드·SaaS**와 같은 **외부 IT 서비스**를 **활용**하거나, **IT 업무**를 **외부 제3자**에 **위탁**하는 사례들이 **보편화**

○ 클라우드·SaaS 서비스에 **장애**가 **발생**하거나, IT 서비스를 제공하는 **수탁회사**에서 **해킹 등 침해사고**나 **정보 유출**이 발생할 경우 **금융회사**는 물론 **금융소비자**까지 **큰 피해**를 초래할 우려

□ 한편, **판매, 결제** 등 일반적인 **업무 위탁**에 수반되는 **제3자 리스크**를 관리하기 위한 **가이드라인 (자율규제)**[*]이 있지만, **사이버 보안, 정보보호** 등이 핵심 요소인 **IT 업무**의 **특성**이 충분히 반영되지 못한 상황[**]

* (은행) 업무 위탁에 따른 은행의 제3자 리스크 관리 모범규준 ('26.4.1. 시행)
(금투) 업무 위탁에 따른 제3자 리스크 관리 가이드라인 ('26.2.18. 시행)
(보험) 보험회사의 제3자 리스크 관리 가이드라인 ('25.12.1. 시행)
(여전) 업무 위탁에 따른 여신전문금융회사의 제3자 리스크 관리 가이드라인 ('25.12.29. 시행)

** 법적 규제의 경우 일반 업무 위탁에 적용하는 「금융기관의 업무 위탁 등에 관한 규정」과 정보처리 업무 위탁에 대한 「금융회사의 정보처리 업무 위탁에 관한 규정」을 각각 제정

○ 이에 금융감독원은 업권별 금융협회·중앙회 (이하 '업권별 협회 등')[*]와 함께 **정보처리 업무 위탁**으로 인한 **제3자 리스크 (제3자 IT 리스크)**를 보다 효과적으로 관리하기 위한 **가이드라인**을 **마련**

* 은행연합회/금융투자협회/생명보험협회/손해보험협회/여신금융협회/저축은행중앙회/한국핀테크산업협회

Ⅱ. 가이드라인 주요 내용

1 이사회 최종 책임 및 경영진 위험 관리 체계 운영 의 역할과 책임 명확화

○ **이사회**가 '제3자 IT 리스크 관리'의 **최종 책임**을 지도록 명시하면서, **위험 관리 정책**과 **감독 관련 주요 사항**을 **심의·의결** 사항으로 규정

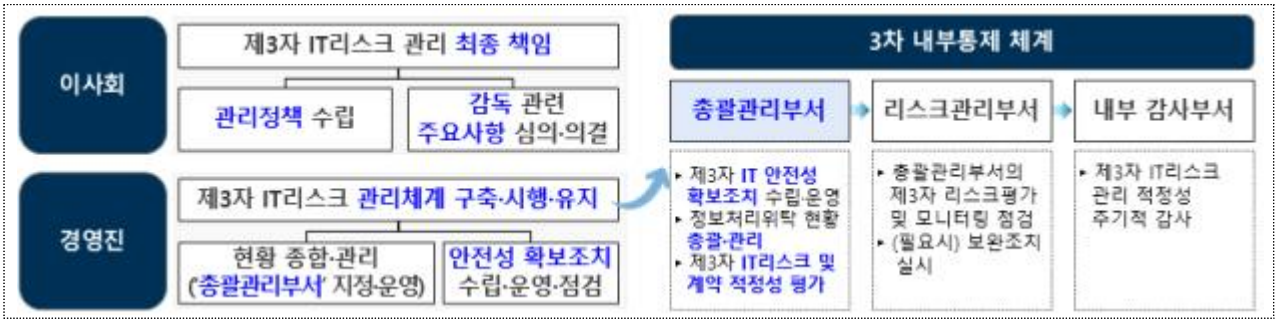
○ **경영진**을 **'제3자 IT 리스크 관리 체계'**를 **구축·시행·유지**할 주체로 정하고, **'총괄관리부서*' 지정·운영**을 통해 ❶ 실효성 높은 **안전성 확보 조치****를 **수립·실행**하는 한편, ❷ 각 사업부서의 **정보처리 업무 위탁 현황**을 총괄하고, ❸ 제3자 **IT 리스크 현황** 및 **위탁 계약**의 **적정성** 등을 **평가**할 책무를 부여

* 이사회·경영진이 마련한 제3자 IT 리스크 관리 정책·체계를 실무적으로 총괄·실행하는 부서

** ① 접근 매체 위·변조, 해킹, 개인정보 유출·오남용 등에 대비한 보안 대책
② 금융회사와 제3자 간의 전용회선 등 안전한 통신 구간 보안 대책
③ 정보처리 시스템 장애 등 서비스 중단에 대비한 비상 대책
④ 업무 지속성 확보를 위한 중요 자료 백업 및 백업 설비 확보 등 백업 대책
⑤ 보안 취약점 최소화 등 보안 유지를 위한 내부통제 체계

○ 이를 바탕으로 **금융회사**는 **제3자 IT 리스크**를 체계적으로 관리할 수 있도록 **'총괄 관리 부서 - 리스크 관리 부서 - 내부 감사 부서'**로 구성되는 **'3단계 통제 체계'**를 **구축·운영**

< 제3자 IT리스크 관리를 위한 금융회사의 거버넌스 >



2 제3자 IT 리스크 식별·평가·관리 구체화

○ 제3자 IT 리스크를 효과적으로 관리하기 위해 **위탁계약**의 **상대방**인 **제3자**의 **재무 건전성**과 **업무 관련 주요 정보** (제공 서비스, 처리 정보 종류·건수, 암호화 및 통신 방식, 사고 대응 체계, 전산 설비 등)를 **식별**하고, **주기적(반기 1회 이상) 점검**을 통해 관련 정보를 **최신화**하여 **유지**

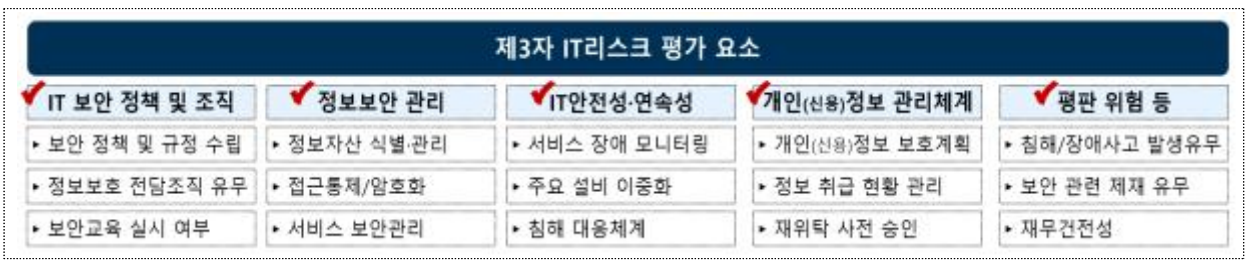
- 특히, **금융회사 업무** 또는 **금융소비자**에 **중대한 영향**을 미치는 **'주요 제3자'**는 별도로 지정하여 **강화된 리스크 관리 적용**

< 제3자 식별·관리 >

○ **제3자 별**로 **IT 리스크**를 **실효성 있게 평가**할 수 있도록 **평가 항목**과 **체크 리스트**를 구체적으로 제시하고,

- 식별된 위험에 대해서는 **보완 조치**를 수행하되, **통제·경감·이전**이 **불가능**할 경우 **계약**을 **중단**하거나, **이사회**가 **유지 여부**를 **결정**

< 제3자 IT리스크 평가 요소 >



3 계약 단계 별 리스크 관리 절차 체계화

○ **계약 검토·체결** 단계부터 **유지·관리** 및 **종료**까지 일련의 **정보 처리 위탁 과정**에서 발생 가능한 제3자 IT 리스크를 **선제적**으로 **식별·대처**할 수 있도록 **단계별 관리 절차**를 체계적으로 제시

- **(계약 前) 현장 실사** 등을 통해 **서비스 역량, 정보보호 관리체계** 등을 **검증**하고, 위·수탁사 간 역할 분담, 사고 발생 시 책임 관계 등의 **필수 사항**을 **계약서**에 **반영**

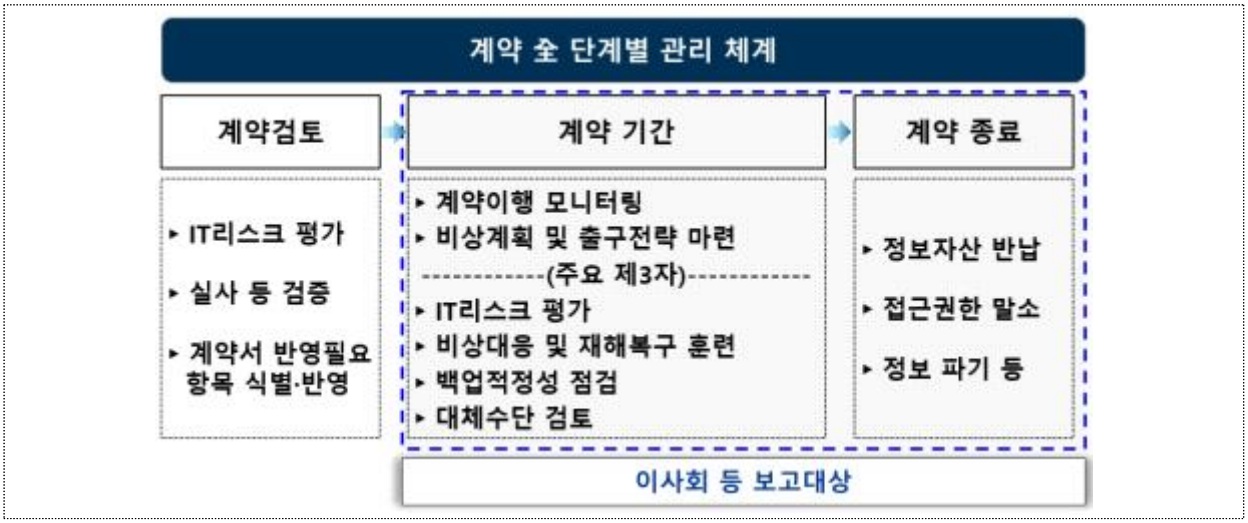
- **(계약 中) 계약 이행 현황**을 정기적으로 **점검** (연 1회 이상) 하고, 시스템 중단 등에 대비한 **비상 대책**, 업무 연속성 유지를 위한 **백업 관리 체계**, 계약 종료에 대비한 **출구 전략** 등을 마련

- **(종료 後) 정보 자산** 반납, **접근권한** 말소, **정보**의 **완전한 파기** 등 수행

※ 주요 제3자에 대해서는 ① IT 리스크 정기 평가 (반기 1회 이상), ② 비상 대응 훈련·재해 복구 훈련 시 포함, ③ 백업 관리 적정성 정기 점검 (연 1회 이상), ④ 대체 가능 수단 사전 검토 및 정기 점검 등을 추가 실시

※ 계약 이행 모니터링, 출구 전략 수립, 계약 종료 후속 조치 등은 이사회 등에 사후 보고

< 계약단계별 제3자 IT리스크 관리 체계 >



4 업무 중요도 및 위험성에 따라 유연한 적용

○ 금번 가이드라인은 제3자 IT 리스크를 **체계적**으로 **관리**하기 위한 **최소한**의 **기준**과 **원칙**을 **Soft Rule 형태**로 제시한 것으로

○ 금융회사들이 위탁한 정보처리 업무의 **중요도**와 **위험성** 등에 따라 **일부 내용**을 **자신에 맞게 강화·완화**하는 등 **유연**하게 **적용 가능**

Ⅲ. 기대 효과

1 이사회 · 경영진의 책임성 강화 및 관심 · 참여 유도

○ **이사회**에 **제3자 IT 리스크 관리**의 **최종 책임**이 있음을 명시하고 **경영진**의 **책무**를 **구체적**으로 **제시**하여 이사회와 경영진의 **책임성**을 **강화**하고 **적극적인 관심·참여 유도**

2 전사적 차원의 제3자 IT 리스크 관리 체계 구축

○ **총괄관리부서**를 중심으로 **제3자 IT 리스크 관리 체계**를 구축하고, 정보처리 위탁 계약 **全 과정**에서 수행해야 할 **리스크 관리 프로세스**를 **구체화**하는 등 **전사적 차원**의 **대응 역량 확립**

Ⅳ. 향후 계획

□ **금융감독원**과 **업권별 협회 등**은 이번에 마련한 '**제3자 IT 리스크 관리 가이드라인**'이 실효성 있게 운영될 수 있도록 적극 지원할 계획

○ **업권별 협회 등**은 동 가이드라인을 기초로 **모범 규준 제정** 등을 통해 **'26.11**월 이후 **시행 계획***

* 단, 업권별 모범규준 제정, 금융회사 내규 반영 및 조직·인력 개편 등 시행 준비 기간을 고려하여 실제 적용시기는 일부 조정 가능

○ **금융감독원**은 **업권별 협회 등**과 함께 가이드라인 **이행 실태**를 **점검·평가**하고, **미비점**을 **개선·보완**하는 등 **지속 고도화**할 예정

□ 이와 더불어 **금융감독원**은 **「사전예방적 디지털 리스크 감독방안」을 지속 추진**함으로써 금융 부문의 **디지털 혁신**이 **철저한 위험관리**를 **기반**으로 **건전**하게 이루어질 수 있도록 **적극 지원**할 계획

※ [참고] EU 「디지털 운영 복원력법」의 제3자 IT리스크 관리

참 고 **EU「디지털 운영 복원력법」의 제3자 IT 리스크 관리 (Chapter V. Managing of ICT third-party risk)**

※ **EU「디지털운영복원력법」(DORA*)** 내용 중 **제3자 ICT위험 관리**(Chapter V) **발췌**

* **(DORA, Digital Operational Resilience Act for financial sector) 금융부문**의 **ICT 위험 관리** 및 **금융시스템**의 **복원력 강화**를 통한 **금융안정성 제고**를 위해 제정('25.1월 시행)

□ **(Article 28 ①)** 서비스 **특성, 규모, 복잡성, 중요도** 및 **계약** 관련 **위험**을 고려하여 **비례성의 원칙**에 따라 **제3자 ICT리스크 관리체계**를 **구축**

□ **(Article 28 ②)** 금융회사는 **제3자 ICT리스크**에 관한 **전략**을 **수립**(정기 점검)하여야 하며, **경영진**은 **주요 ICT 서비스 계약위험 정기 점검**

□ **(Article 28 ③)** 제3자 IT위험관리 체계(framework)로서 **제3자**와의 IT 서비스 이용 계약에 관한 **정보등록부**를 **유지·관리***하여야 함

* 핵심적이거나 중요한 기능을 지원하는 IT서비스 계약과 그렇지 않은 계약을 구별

□ **(Article 28 ④)** **계약 체결 前** **핵심적**이거나 **중요한 기능 여부 평가**, 제3자에 대한 금융회사의 **감독 조건 충족여부** 평가, 계약 관련 **모든 위험**을 **식별·평가**, 제3자에 대한 **실사**(due diligence) 착수 등을 수행

□ **(Article 28 ⑦)** 제3자 서비스 제공자가 법률·규정 위반하는 등의 경우 **금융회사**가 **ICT 서비스 계약**을 **종료**할 수 있도록 **보장**하여야 함

□ **(Article 28 ⑨)** 금융회사는 **핵심적**이거나 **중요한 ICT 서비스**에 대해 **출구 전략**을 **수립***하여야 하며, **계약 종료**시 대고객 **서비스**의 **연속성·품질 저하** 등이 **발생**하지 **않도록** 하여야 함

* 또한 금융기관은 대체수단을 식별하고 전환 계획을 마련하여야 함

□ **(Article 30)** 금융회사와 제3자의 **권리·의무**는 **서면**으로 **기록**되어야 하며, 최소한 **다음**의 **요소**가 **계약적 조치에 포함**되어야 함

○ 제3자 **제공 서비스**에 대한 **명확·완전한 설명**(주요 기능 하청 여부 등), **서비스 제공 위치**(데이터 저장위치 포함), **데이터 가용성·진위성·무결성·기밀성** 등, **감독당국 협조의무**, **계약종료 관련 권한** 등