



금융감독원

보 도 자 료

금융은 **튼튼**하게 소비자는 **행복**하게

보도	2025.2.13.(목) 14:00	배포	2025.2.13.(목)		
담당부서	금융감독원 IT검사국	책임자	국 장	유희준	(02-3145-7420)
		담당자	팀 장	안태승	(02-3145-7415)
	은행연합회 IT부	책임자	부 장	강동성	(02-3705-5308)
		담당자	팀 장	김재근	(02-3705-5331)
	금융투자협회 IT지원부	책임자	부 장	장영훈	(02-2003-9060)
		담당자	부부장	우승헌	(02-2003-9058)
	생명보험협회 ICT지원부	책임자	부 장	여창환	(02-2262-6613)
		담당자	팀 장	문지환	(02-2262-6686)
	손해보험협회 IT서비스부	책임자	부 장	김병훈	(02-3702-8548)
		담당자	팀 장	정정미	(02-3702-8637)
	여신금융협회 정보시스템부	책임자	부 장	문 혁	(02-2011-0786)
		담당자	팀 장	이근원	(02-2011-0735)
	저축은행중앙회 IT서비스본부	책임자	본부장	전회준	(02-397-8787)
		담당자	팀 장	박인대	(02-397-8806)
	핀테크산업협회 사무국	책임자	국 장	정진국	(02-6949-2683)
		담당자	실 장	임형찬	(02-6949-2623)

금융회사 IT내부통제 강화를 위한 업계 간담회 개최

- 금융회사가 자체 IT리스크를 파악하여 대응하도록 「IT감사 가이드라인」 마련
- AI·클라우드 활용 등 신규 디지털 조직에 대한 내부통제 사각지대 해소 기대

I 간담회 개요

- '25.2.13일(목) 금융감독원은 7개 협회·중앙회와 「IT감사 가이드라인 마련 T/F」 마무리 간담회를 개최하여,
 - 지난 11월부터 T/F를 통해 공동으로 마련한 가이드라인 최종안을 발표하고, 업권별 시행방안 등을 논의하였음

【 IT감사 가이드라인 T/F 마무리 간담회 개요 】

- 일시 / 장소 : 2025.2.13.(목) 14:00 / 금융투자협회(여의도)
- 참석자 : 【금융감독원】 이종오 부원장보(주재), IT검사국장
 【협회·중앙회】 금융협회(은행, 금융투자, 생명보험, 손해보험, 여신) 및 저축은행중앙회, 핀테크산업협회 소속 IT부문 임원

II 간담회 논의 내용

1. 「IT감사 가이드라인」 마련 취지 및 핵심 내용

- 디지털 전환, IT신기술 활용 확대 등에 따른 IT업무 중요성 증가에도 기본적인 IT운영·통제 미흡으로 인한 장애사고가 지속 발생하고 있으며,
 - 최근 “규칙→원칙 중심”의 규제 패러다임 전환으로 금융회사 자율성이 확대되고 있어 자체 IT리스크에 상응하는 IT내부통제 체계의 구축 필요성이 증가
- 이에 금융감독원은 금융업권과 함께 T/F를 구성하여 체계적인 IT내부통제 운영 및 효과적인 IT감사업무 수행을 위한 기준을 가이드라인으로 제시
 - 동 가이드라인은 금융감독원 IT검사 지적사례 및 국제 표준 등을 참고하고 금융업계 의견 수렴을 통해 마련하였으며,
 - ① 자체 IT리스크에 맞는 3단계 IT내부통제 체계 구성, ② 사각지대 없는 통제 범위 설정, ③ IT감사 독립성 확보 및 ④ 표준 IT감사 방법론 등을 권고사항으로 제시

※ 「IT감사 가이드라인」 핵심 내용 (☞ 상세내용 불임1 참고)

- ① (IT내부통제체계) ^[1단계] IT조직의 내부통제 방안 수립·이행 → ^[2단계] IT조직의 자체감사 → ^[3단계] 감사조직의 IT감사로 이어지는 유기적·다층적 통제체계
- ② (IT내부통제 범위) 책무구조를 기준으로 IT내부통제 범위 및 수행주체 명확화
- ③ (IT감사 독립성) IT감사인의 업무 독립성 확보를 위한 직무분리 및 인력 운용 기준
- ④ (IT감사 방법) IT감사계획 수립·실시·보고 단계에 따른 주요 절차 등 업무 기준

2. 주요 당부사항

- 금융감독원 이종오 디지털·IT 부원장보는 “금융회사 IT감사는 단순한 점검이 아닌 혁신의 안전판 역할을 한다.”고 강조하며,
 - 동 가이드라인이 “금융회사의 디지털 경쟁력과 금융IT 안전성을 균형있게 전인하는 든든한 기준점이 되기를 기대한다.”고 언급

- 또한, '25년 2월말까지 전 금융권역에서 협회·중앙회별 내부 절차를 거쳐 가이드라인이 조속히 시행될 수 있도록 차질없이 준비하고,
- 가이드라인 시행 초기에 금융회사가 제정 취지에 맞게 잘 이행할 수 있도록 협회·중앙회에서 적극적인 도움을 줄 것을 요청
- 아울러, 동 가이드라인 시행시 협회·중앙회별로 업권 특성에 맞게 내용을 조정하여 적용이 가능하나 IT내부통제 강화 취지를 벗어나지 않도록 유의할 것을 당부

3. 협회·중앙회 의견 요지

- 금번 가이드라인을 통해 금융회사가 신규 IT업무영역(디지털·AI)을 포함한 IT부문 전반에 대하여 각자 적합한 방식으로 통제체계를 수립·운영할 수 있는 근거를 마련함에 따라
- 내부통제 사각지대가 해소되고 자율적인 통제활동이 활성화되어 전자금융 안전성이 제고될 것으로 기대
- 다만, 금융회사 사정에 따라 동 가이드라인의 이행 시기 및 수준이 상이할 수 있으므로 금융당국과 소통을 통해 유연하게 운영할 필요

III 향후 계획

- 금번 간담회를 통해 발표된 「IT감사 가이드라인」 최종안은 '25년 2월말까지 7개 협회·중앙회별 심의·보고 등 내부 절차를 거쳐 배포·시행될 예정임
- 금융감독원은 앞으로도 금융협회·중앙회 등 금융업계와 지속적인 소통을 통해 가이드라인에 대한 피드백을 반영하고 부족한 부분은 협의하여 개선해 나가도록 하겠음

※ (붙임1) 가이드라인 주요 내용 및 요약
 (붙임2) 가이드라인 관련 질의 및 답변(FAQ)

☞ 본 자료를 인용하여 보도할 경우에는 출처를 표기하여 주시기 바랍니다. (<http://www.fss.or.kr>)

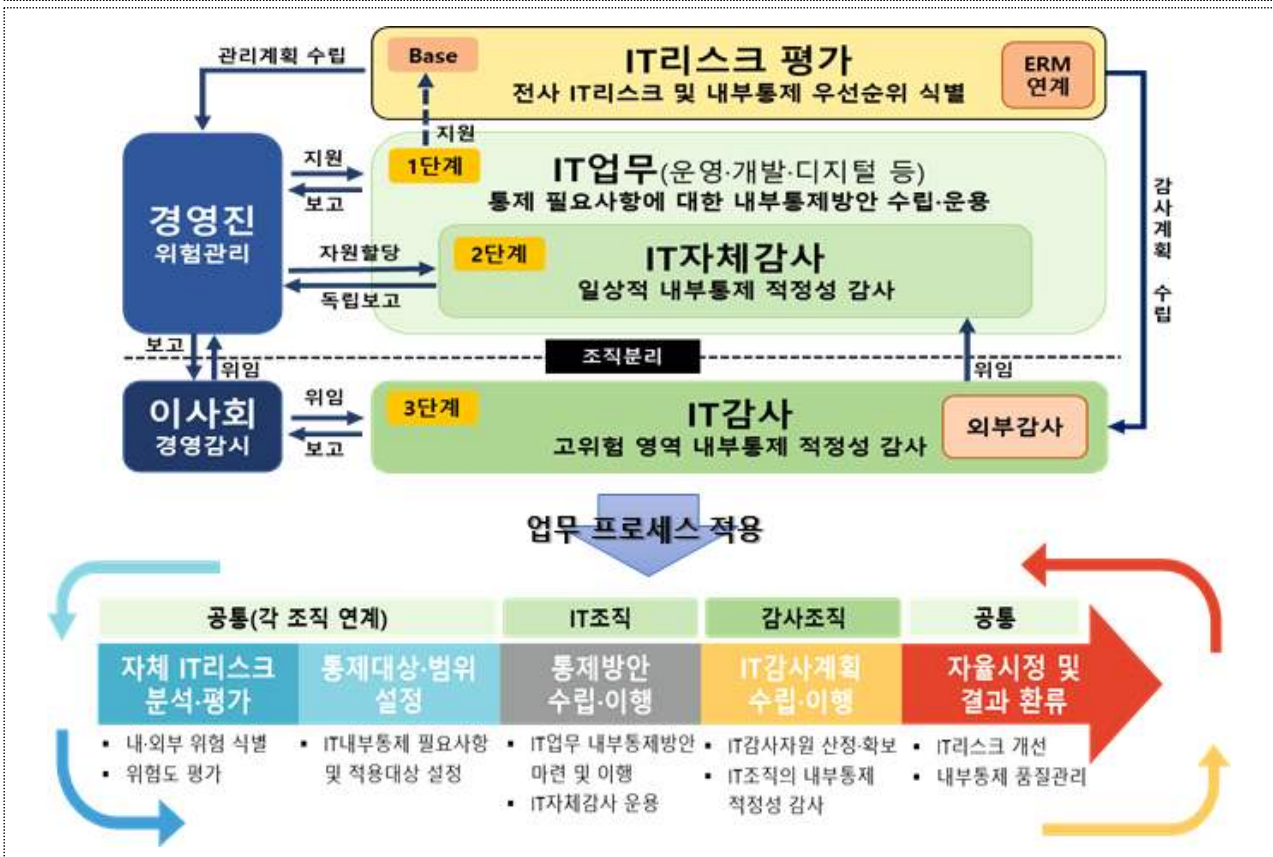
가이드라인 주요 내용

1 금융회사 IT내부통제체계에 대한 청사진을 제시

금융회사가 자체적으로 IT리스크를 식별·분석하고 평가하여 3단계 IT내부통제체계를 구성

3단계 IT내부통제체계

- [1단계] IT조직은 IT업무(프로그램, 전산원장 변경 등) 전반에 걸쳐 법규 등에서 요구되는 IT내부통제 방안을 수립 및 이행
- [2단계] IT조직 내 자체감사인을 통해 일상적 업무영역에서의 IT내부통제 적정성을 자체 점검(CIO, CISO, CDO 등 IT부문 각 최고책임자 소관 IT업무)
- [3단계] 감사조직의 IT감사인을 통해 제3자 관점에서 IT리스크가 높은 영역 등에 대한 IT내부통제 적정성을 감사(IT부문 전반)

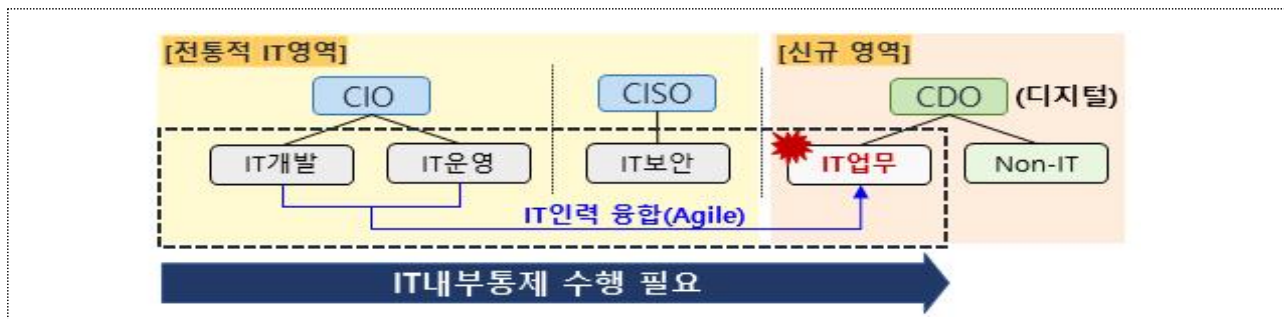


② IT감사 관련 내부통제 범위 및 수행주체를 명확화

최근 IT조직 확장(디지털·AI) 및 유연화(Agile)로 인한 통제 누락사례*를 방지하기 위해 금융회사 책무구조를 기준으로 IT영역별 최고책임자가 소관 IT업무에 대한 내부통제 활동을 수행하도록 IT내부통제 범위 및 수행주체를 명확히 설정

* 디지털최고책임자(CDO) 산하조직에서 수행하는 AI, 데이터 분석 시스템 개발·운영 업무에 대해서는 IT자체감사 및 IT감사를 미수행한 사례를 금융감독원 IT감사에서 지적

IT내부통제 범위의 확장

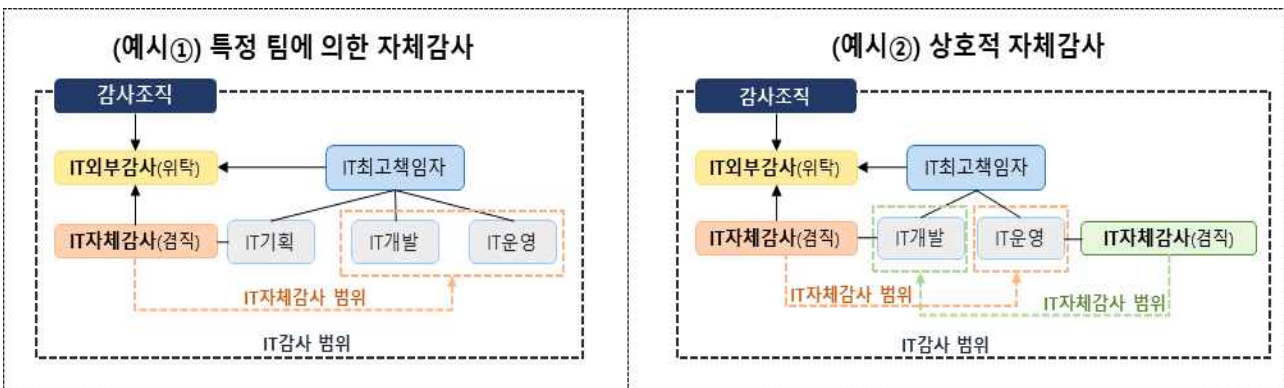


③ IT감사 업무 독립성 등 조직·인력 운용 방향 제시

IT자체감사인 업무 독립성 확보를 위한 직무분리 기준을 마련하고, IT자체감사 전담인력 운용의 어려움에 대한 금융회사 의견*을 반영하여 IT내부통제 업무의 외부위탁(전문업체 등)도 가능하도록 제시

* ①IT자체감사 직무수행 전후로 IT개발·운영 업무 수행을 제한할 경우 IT전문성 저하·경력 단절 등 우려, ②IT자체감사를 내부 인력으로 상시 운영할 경우 비용 부담 우려

IT자체감사인력 운용 예시

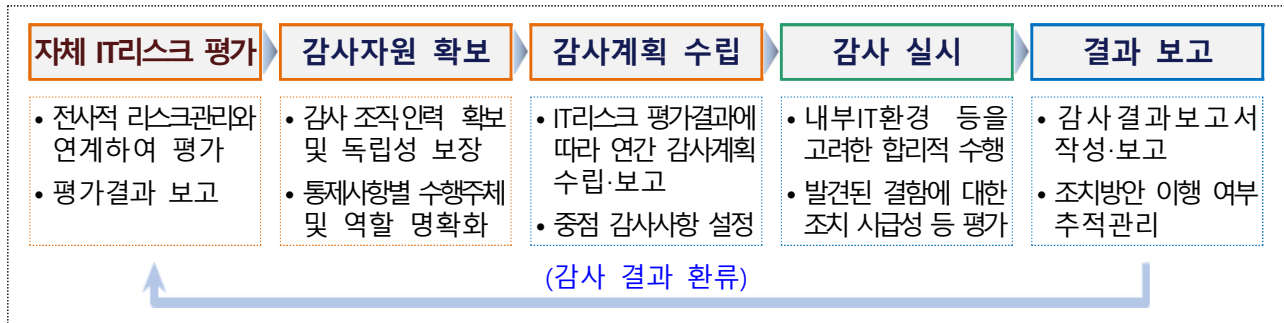


4 IT감사 방법론의 표준을 제시

그간의 IT검사 지적사례* 등을 참고하여 IT감사업무 수행단계에 따라 준수하여야 할 주요 절차 등 업무 기준을 마련

* 감사결과 지연 보고, 후속조치 미이행에 따른 지적사항 반복, 증빙자료 미보관 등

IT감사업무 수행단계(요약)



가이드라인 요약

제1절: IT내부통제 기반사항 주요 내용

가. IT리스크 기반 내부통제체계 수립

- **[기본체계]** 국내외 사례 등을 참고하여 IT리스크 기반의 3단계 IT내부통제체계를 제시하고 단계별 수행 주체 및 역할 정의
- **[IT리스크평가]** 금융회사가 IT리스크를 자체평가한 결과에 따라 내부통제 우선순위 및 필요자원을 산출하여 감사계획 수립·이행·환류
- **[거버넌스]** 경영진(위험관리)과 이사회(경영감시)의 책무에 따라 산하조직인 IT조직(1·2단계)과 감사조직(3단계)의 기능을 구분
 - IT부문 경영진은 소관조직의 내부통제를 이행·점검하고 감사 혹은 감사위원회는 전체 IT부문의 내부통제 적정성을 감사

나. 주요 업무절차 및 조직·인력 운용 원칙 제시

- **[업무절차]** 감사조직이 IT감사를 체계적으로 수행할 수 있도록 주요 업무절차를 정의하고 최소한의 업무 기준 마련

- 연간 IT감사계획의 수립·이행 및 IT감사 결과에 대한 조치 계획 보고·승인 등 기준을 제시하여 IT감사체계 내재화 유도
- **[조직·인력]** IT내부통제업무의 수행을 위한 업무 독립성 확보, 교육 등 IT내부통제조직 및 인력에 대한 운영·관리 원칙 제시
 - IT자체감사인의 직무분리 수준을 IT감사인 대비 **완화**하는 등 금융회사 의견을 적극 반영하여 인력 운용의 유연성 제고

제2절: IT감사업무 수행단계별 준수사항 주요 내용

가. 감사계획 수립 단계

- **[기반 확보]** 내규 등으로 IT내부통제 수행주체 및 역할을 명확히 하여 통제 누락을 방지하고 IT감사에 필요한 자원·권한을 확보
 - 경영진 및 이사회는 IT(자체)감사계획 승인을 통해 IT내부통제인력·예산 및 업무권한 등이 충분히 확보될 수 있도록 지원
- **[예방적 감사]** 감사조직은 사후적·징벌적 감사를 지양하고 사전적 위험관리 관점에서 IT리스크에 따라 감사계획을 수립
 - 내부 IT환경에 대한 모니터링 및 IT리스크평가 결과에 따라 고 위험 영역을 중점감사하고 일상적 영역은 IT자체감사에 위임

나. 감사 실시 단계

- **[거증자료]** 감사결과의 객관성 확보를 위해 거증자료를 확보하고 타인이 생산하거나 제공한 정보는 신뢰성을 검증
- **[감사기법]** 감사대상의 특성에 따라 일률적 체크리스트가 아닌 통계적 표본 추출이나 자동화된 감사도구 등을 활용

다. 감사결과 보고 단계

- **[결과보고]** 감사내역에 대한 자체 평가 등 감사결과보고서에 포함되어야 하는 사항을 제시하여 감사 품질 및 연속성 강화
- **[후속조치]** 발견된 문제점에 대해 중요도 및 조치시급성 등을 평가하고 조치 권고사항 및 조치기한을 감사명령권자에 보고

① 「IT감사 가이드라인」의 법적 성격은?

- 동 가이드라인은 국제 표준 및 IT감사 지적사례 등을 참고하고 각 금융협회·중앙회와 업계 의견을 수렴하여 마련한 것으로
 - 행정지도 등 금융 규제에 해당하지 않음
- 다만, 동 가이드라인은 금융회사가 자체 IT리스크에 적합한 IT내부통제체계를 확립하고 IT운영·통제를 강화하여 전자금융 안전성을 제고하고자 하는 취지로,
 - 향후 서면 점검, IT리스크 계량평가 등을 통해 가이드라인 이행 여부를 관리할 예정이며, IT실태평가지 기준으로 활용할 수 있음

② 업무 전반에 대한 리스크 평가시 IT부문을 포함하여 운영 중인 경우, 이를 동 가이드라인의 IT리스크평가로 같음할 수 있는지?

- IT리스크평가는 금융회사가 각자 적합한 내부통제체계 수립·이행에 필요한 감사자원을 산정하기 위한 수단이자 IT감사 계획의 적정성·당위성을 판단하기 위한 근거로써,
 - 세부적인 평가방법과 운영방식 등은 상기 취지를 고려하여 금융회사가 자율적으로 선택 가능함

③ IT자체감사인은 모든 IT부문 조직에 대하여 각각 지정하고 반드시 IT자체감사 직무를 전담해야 하는지?

- ☐ IT자체감사인은 IT리스크평가 결과에 따라 필요한 IT조직에 지정·운용할 수 있고
 - 효과적인 직무수행을 위하여 특정 인력이 IT자체감사 직무를 전담하는 것을 권고하나, 주기적으로 IT자체감사인을 순환 지정하는 등 IT조직 내에서 유연한 운용이 가능함
 - IT조직 규모가 작아서 IT자체감사인을 지정하기 곤란한 경우 IT감사가 일상적 내부통제 영역을 포함한 해당 조직의 IT 내부통제 적정성 전반을 감사해야함

④ IT내부통제체계와 전사 내부통제(준법감시인 소관)의 관계는?

- ☐ IT내부통제는 CIO, CISO 등 IT부문 담당임원의 책무이고, IT내부통제 적정성에 대한 감사는 감사 혹은 감사위원회의 책무로써
 - 책무구조의 혼선을 방지하기 위하여 준법감시인의 일반적인 내부통제 책무와는 별개의 영역으로 분리되어야 함

⑤ IT리스크평가, IT내부통제 인력 운용 등에 대한 기준은 반드시 전사 차원에서 마련되어야 하는지?

- ☐ 자체 IT리스크에 대한 종합적인 평가 및 그에 따른 자원의 확보라는 취지를 달성하려면 유관조직 간 협의 및 경영진의 의사결정이 필요

- 예를 들어 IT리스크평가 기준에 대해서는 IT조직 및 감사조직 외 리스크관리조직 등이 협업하고
- IT감사인력 운용 기준에 대해서는 조직관리 혹은 인사조직이 협업하는 등 전사적 관점에서의 기준 마련·운영이 필요함

6 IT자체감사인의 업무범위 및 독립성 확보 수준은?

- IT자체감사는 IT부문 임원(최고책임자)이 산하 IT자체감사인을 지정하여 소관업무에 대한 자체적인 감사를 명령하는 것으로,
 - 소관업무 외에 타 IT부문 임원 업무에 대한 ‘자체’감사는 원칙적으로 성립할 수 없으며,
 - ※ 단, 물리적으로 분리된 조직에서 수행하는 IT업무일지라도 회사 책무구조상 해당 IT업무에 대한 내부통제책무가 CIO 등 특정임원에게 부여된 경우 해당 임원산하의 IT자체감사인에 의한 자체감사 수행 가능(최고책임자 책무 기준)
 - 효과적인 직무 수행과 이해상충 방지를 위하여 IT자체감사 직무와 감사대상업무의 겹침 및 본인이 수행한 업무에 대한 감사를 금지하는 등 독립성을 확보하여야 함

7 IT감사계획의 마련 주체는? IT감사계획에 IT자체감사계획을 포함해야 하는지?

- 가이드라인 제1절 제7조에서 규정하는 IT감사계획은 감사조직에서 마련하여 감사 혹은 감사위원회에 보고하여야 하고,
 - IT자체감사계획은 필요시 IT조직에서 마련하여 감사명령권자에 보고하여야 함

⑧ 감독규정상 CISO의 정보보안 점검 의무* 등을 IT자체감사에 갈음할 수 있는지?

* [전자금융감독규정 제8조제1항제4호] 정보보호최고책임자는 임직원이 정보보안 관련법규가 준수되고 있는지 정기적으로 점검하고 그 점검결과를 최고경영자에게 보고할 것

- ☐ IT자체감사의 취지는 소속 조직에 한정하여 일상적 내부통제 적정성을 점검하는 것으로,
 - 점검대상, 범위 등이 감독규정과 차이가 있으므로 갈음할 수 없음

⑨ 동 가이드라인 제정 이후 세부 매뉴얼을 추가 배포할 계획이 있는지?

- ☐ 동 가이드라인은 각 금융회사가 적정한 IT내부통제체계를 수립할 수 있도록 일반적·공통적인 표준을 제시하려는 취지로 제정되었고,
 - 지나치게 개별적·세부적인 기준 제시는 자칫 ‘그림자 규제’로 작용할 소지가 있으므로 세부 매뉴얼 배포 등은 계획되어 있지 않으나
 - 향후 동 가이드라인 운영과정에서 우수사례(Best-Practice)를 발굴하여 금융권에 공유하는 등으로 지원할 예정임