March
2025

NEWSLETTER

디지털금융팀 | Digital Finance Team

CONTACT

변호사 **이정명**

T: 02.6386.0730
E: chloe.lee
@leeko.com

변호사 **차현정**

T: 02.772.5971
E: hyunjeong.cha
@leeko.com

변호사 **한경원**

T: 02.6386.7924
E: Kyungwon.han
@leeko.com

수석전문위원 **조성인**

T: 02.6386.0739
E: sungin.cho
@leeko.com

전문위원 **정원식**

T: 02.6386.0870
E: ws.jung
@leeko.com

전문위원 **이정훈**

T: 02.6386.1966
E: junghun.lee
@leeko.com

금융권역 「IT감사 가이드라인」 마련

금융감독원이 마련한 「IT감사 가이드라인」이 전 금융권역에 배포되어 최근 시행을 개시하였습니다. 동 가이드라인은 금융감독원을 비롯한 금융협회, 저축은행중앙회, 핀테크산업협회로 구성된 TF에 의해 2025. 2. 13. 자로 완성되었으며, 전 금융권역에서 협회 · 중앙회별 내부 절차를 거쳐 2월말에 배포 및 시행되었습니다.

「IT감사 가이드라인」은 최근 '규칙 → 원칙 중심' 의 규제 패러다임 전환으로 금융회사의 자율성이 확대에 따라 금융회사 및 전자금융업자(이하, **금융회사등**)가 자체 IT리스크에 상응하는 IT내부통제체계 구축의 필요성이 증가하고 있는 상황에서 기준을 제시하기 위하여 마련된 것입니다. ('규칙 → 원칙 중심'의 규제 패러다임 전환과 관련하여서는 본 뉴스레터에 첨부된 저희 법무법인의 지난 뉴스레터를 참고하여 주시기 바랍니다.)

첨부: 디지털금융팀 2월 뉴스레터 '전자금융감독규정 개정 – 자율보안 토대 마련'

「IT감사 가이드라인」은 IT리스크 평가에 기반한 3단계 IT내부통제체계, 사각지대 없는 통제범위 설정, IT감사의 독립성 확보, 표준 IT감사 방법론에 관한 내용을 포함하고 있는데, 이하에서 그 주요 내용에 관하여 살펴보겠습니다.

1. IT리스크 기반 내부통제체계의 수립

금융회사는 자체적으로 IT리스크를 식별 · 분석하고 평가하여 IT내부통제체계를 구성하여야 합니다. 이때 고려하여야 하는 'IT리스크' 는 정보통신기술과 관련한 법규의 위반, ICT 장애 및 기술의 오용, 전산사고 등으로 인한 직접적 손실, 평판 손상, 법적 청구 등 전산시스템 및 전자금융업무 전반에 대한 실제적 · 잠재적 위험으로, 금융회사등은 전사적 리스크관리와 연계하여 IT리스크평가를 수행하여야 합니다.

금융당국이 원칙적으로 예정한 IT내부통제체계는 3단계로 구성되나, IT조직이 소규모인 경우 등에 해당하면 3단계가 반드시 분리되어야 하는 것은 아닌 것으로 이해됩니다. 또한, 「IT감사 가이드라인」에 따르면, IT내부통제를 외부에 위탁하여 IT내부통제체계 수립 · 이행의 적정성을 감사하도록 하는 것도 가능합니다. 즉, 내부인력으로 IT(자체)감사를 수행하게 되는 경우 비용 부담 우려가 있다는 점 등을 고려하여, IT내부통제 업무의 외부위탁(전문업체 등)도 가능하도록 한 것입니다.

3단계 IT내부통제체계의 구체적인 내용은 다음과 같습니다.

1단계 **IT조직의 IT내부통제 방안 수립 및 이행**

IT조직은 IT업무(프로그램, 전산원장 변경 등) 전반에 걸쳐 통제 필요사항에 대하여 법규 등에서 요구되는 IT내부통제 방안을 수립 및 이행하여야 합니다.

2단계 **IT조직 내 IT자체감사인에 의한 IT자체감사**

① **IT자체감사의 내용 : 일상적 내부통제 적정성 감사**

IT자체감사는 IT조직 내에서 기술적 · 실무적 전문성에 기반하여 소관 IT업무의 일상적인 업무영역에서의 IT내부통제 적정성을 자체 점검하는 것입니다. 즉, 금융회사등은 IT조직 및 환경, 규모 등을 고려하여 최고정보책임자(**CIO**: Chief Information Officer), 정보보호최고책임자(**CISO**: Chief Information Security Officer) 등 IT부문 각 조직의 최고책임자 산하에 IT자체감사인을 임명하여 각 조직 소관업무에 대한 IT자체감사를 실시하는 것입니다.

② **IT자체감사인의 지정 및 운용**

IT리스크평가 결과에 따라 필요한 IT조직의 경우 IT자체감사인을 지정·운용하여야 합니다. 이때 유의하여야 할 사항은 다음과 같습니다.

- **(직무분리 완화)** 효과적인 직무수행을 위하여 특정인력이 IT자체감사 직무를 전담하는 것을 권고하나, 주기적으로 IT자체감사인을 순환 지정하는 등 IT조직 내에서 유연한 운용이 가능하도록 하였습니다. 이는 IT자체감사 직무수행 전후로 IT개발 · 운영 업무 수행을 제한할 경우 IT전문성 저하 · 경력 단절 우려에 관한 금융회사의 의견을 반영하여 IT자체감사인의 직무분리 수준을 완화한 것입니다.
- **(독립성 확보)** IT자체감사 직무와 감사대상 업무의 겸직을 금지하고, 본인이 수행한 업무에 대한 감사를 금지하는 등 IT자체감사인의 독립성을 확보하기 위한 조치는 취하여야 합니다. 즉, IT자체감사인도 원칙적으로 피감업무 수행을 제한하여야 하나, 감사자원이 적어 완전한 직무분리가 어려운 경우에는 소속조직 외 타조직(최고책임자 책임 기준) 및 본인 업무에 대한 자체감사를 제한하여 이해 상충을 방지하도록 한 것입니다.
- **(소규모 IT조직의 경우)** IT조직 규모가 작아서 IT자체감사인을 지정하기 곤란한 경우 IT감사가 일상적 내부통제 영역을 포함한 해당 조직의 IT내부통제 적정성 전반을 감사하여야 합니다.

3단계 **감사조직의 IT감사인을 통한 IT감사: 고위험 영역 내부통제 적정성 감사**

내부 IT환경에 대한 모니터링 및 IT리스크평가 결과에 따라 고위험 영역에 대하여 IT내부통제 적정성을 중점감사하여야 합니다(일상적 영역은 IT자체감사에 위임하게 되는 것입니다). 이때 IT감사인은 감사 혹은 감사위원회의 직접 지시를 받아야 하고, 감사업무 수행 직전, 직후 IT현업부서에 대한 인사이동을 제한하여 이해상충을 방지하여야 합니다.

2. 표준 IT감사업무 방법론

「IT감사가이드라인」에서는 그간의 IT검사 지적사례 등을 참고하여 IT감사업무 수행단계에 따라 준수하여야 할 주요 절차 등에 관한 업무기준을 마련하였습니다. 구체적으로, IT감사업무는 ① 자체 IT리스크 평가, ② 감사자원 확보, ③ 감사계획 수립, ④ 감사 실시, ⑤ 결과 보고, ⑥ 검사 결과의 환류의 단계로 구성됩니다. 감사계획의 수립, 감사의 실시 및 보고단계에서 유의하여야 하는 주요사항은 다음과 같습니다.

감사계획 수립	• **(내용)** IT리스크 평가결과에 기반하여 연간 감사계획을 수립 · 보고하고, 중점감사사항을 설정. 이때 IT감사는 사후적 · 징벌적 감사보다는 사전적 위험관리 관점에서 이루어지도록 하여야 함. • **(주체)** IT감사계획은 감사조직에서 마련하여 감사/감사위원회에 보고하여 승인을 득하여야 하고, IT자체감사계획은 필요시 IT조직에서 마련하여 소속 경영진의 승인을 득하여야 함. • **(IT감사업무편람)** IT감사절차 및 항목, 감사요령 등을 수록한 IT감사업무편람을 마련하여야 하는데, 각 금융회사 내부 IT환경에 적합한 감사기법, 가사목적에 따른 주요 점검사항 등 실무적이고 구체적인 내용 위주로 구성하여야 함. 이를 최소 연 1회 이상 검토 및 개정 관리를 수행.

감사의 실시	• **(감사대상의 특성 고려)** 모든 감사대상에 일률적인 기준을 적용하기보다는 내부IT환경 등을 고려하여 합리적으로 감사업무를 수행 • **(감사기법)** 감사대상의 특성에 따라 일률적 체크리스트가 아닌 통계적 표본 추출이나 자동화된 감사도구 등을 활용 • **(문제점에 대한 평가)** 문제점으로 판단한 사항에 대해 조치의 시급성, 발생 가능한 위험 등을 종합적으로 고려하여 자체적으로 중요성을 평가하고, 문제점으로 판단한 이유 및 근거를 문서화하여 감사대상에 공유
감사결과 보고 및 결과의 환류	• **(감사결과보고)** 감사결과 발견된 문제점을 금전적 가치, 법규 위반여부, 발생 가능한 위험 등을 기준으로 중요도와 조치시급성 등을 평가한 결과를 감사결과보고서에 기재 • **(보고대상)** IT(자체)감사인은 감사명령권자(IT자체감사의 경우 CIO, CIS 등, IT감사의 경우 감사/감사위원회)에 보고하여야 하고, 그 전에 이해관계자에 중간 보고하지 않아야 함 • **(결과의 환류)** 조치방안이 이행되었는지 여부를 추적관리하여야 하고, 감사결과는 추후 IT리스크 평가시 반영되는 등 환류가 이루어지도록 할 필요

3. 시사점

금융보안이 자율보안 체계로 전환되는 과정에서 금융회사가 효율적인 IT내부통제체계를 수립·운영하는 것은 매우 중요할 것으로 보입니다. 특히 자율보안 체계로의 전환은 디지털 전환, IT신기술 활용 확대 등의 상황에서 금융회사가 전사적 차원에서 IT리스크를 대응할 수 있도록 하기 위함이라는 점을 고려하면, 그 목적과 취지에 맞게 IT내부통제체계를 수립·운영할 필요가 있을 것입니다.

「IT감사가이드라인」은 행정지도 등 금융규제에 해당하지는 않으나 금융당국은 향후 서면 점검, IT리스크 계량평가 등을 통해 가이드라인 이행 여부를 관리할 예정이며 IT실태평가시 기준으로 활용할 수 있습니다. 또한 이는 결국 전자금융 관련 사고 발생시 금융회사가 관리의무를 다하였는지의 문제로 연결되므로 자체 IT리스크에 맞는 IT내부통제를 운영할 수 있도록 착실히 준비하여야 할 것입니다. 이때 각 금융회사는 협회·중앙회에서 배포하는 「IT감사 가이드라인」 최종안과 함께, 금융감독원이 추후 발표할 예정인 우수사례(Best-Practice) 등을 참고할 필요가 있겠습니다.

특히 각 금융회사마다 요구되는 내부통제의 수준, 방법 등에서 차이가 있을 것이므로 IT내부통제의 취지, 목적, 방법론 등을 기준으로 금융회사의 자체 IT리스크에 적합한 IT내부통제체계를 확립하고 IT운영·통제를 강화하는 것이 중요할 것으로 보입니다.

법무법인(유) 광장의 디지털금융팀은 「전자금융거래법」, 금융보안에 대한 업계 최고의 전문가들로 구성되어 있으며 IT리스크평가 등 계획단계부터 감사실시, 감사결과의 환류까지 다양한 법률적 사항이나 쟁점들에 대하여 폭넓게 경험 및 자문을 해왔습니다. 위 내용과 관련하여 법률전문가의 도움이 필요하신 경우 언제든지 법무법인(유) 광장의 디지털금융팀으로 연락주시기 바랍니다.

Lee & Ko 법무법인(유) 광장
서울 | 판교 | 북경 | 호치민시티 | 하노이
02.772.4000 | mail@leeko.com | www.leeko.com