금융보안 선진화
1단계 추진방안

전자금융 감독규정 정비 계획

2024. 2. 1.

금 융 위 원 회
금 융 안 전 과

목 차

Ⅰ. 추진 배경

□ 그간 **몇 차례 보안사고**를 거치면서 시행세칙 등에서 규율하던 **단순·지엽적 사항**을 **감독규정**으로 **상향**함이 누적된 결과,

○ **법률상 1개 항**(전금법 §21.②(안전성 확보의무))에 대응하는 **감독규정상 수범사항**이 **293개**에 달하여 **규제부담이 가중**

□ 감독규정은 금융회사에 **수단선택의 자유**를 주지 않고, **구체적 보안 수단, 방법**을 **열거식**으로 **특정**

○ 이에 따라, **목적 달성**에 보다 **효과적**이나 규정상 열거되지 않은 **대안**(新기술 등)의 **도입 가능성**을 **차단**

○ "**규정만 준수하면 면책**"이라는 인식을 조장하고, 이에 금융회사는 **최소 기준**만 준수할 뿐 **적극적 보안투자**에 소극적

○ 급변하는 IT 환경과 보안리스크에 **유연하게 적응**하기 어려워 **금융회사의 보안역량을 저하**시킬 우려

□ **상기 문제점**을 시정하고자 '**법률개정 → 감독규정 정비**'의 **순차적 보안규제 합리화**를 위해 노력해 왔으나, 『**전자금융법 전면개정안**('21.10월)』의 **국회 논의가 중단***된 상황

* 전면개정안은 금융보안의 개념·행위 등을 체계화하고, 이사회·최고 경영자 등의 책임을 강화하며, 과징금·손해배상 등을 실질화하는 내용을 포함

○ 보안규제 선진화의 **시급한 요구**를 감안하여 **법률개정 없이** 가능한 범위 내에서 **감독규정 개편**을 추진할 필요

○ 이에, 금번에는 "**규칙(Rule) → 원칙(Principle) 중심**"으로 **감독규정을 합리화**하여 **자율보안의 기초 토대**를 마련하고자 함

○ 아울러, 향후 금융보안 분야만의 **별도 법률개정**을 검토하고, 이를 바탕으로 **자율보안체계**로의 **단계적 전환**도 검토

붙 임 **단계별 금융보안 선진화 추진 계획**

금융보안 선진화 추진계획

1단계 감독규정 정비

규칙(Rule) → 원칙(Principle) 중심으로 감독규정 합리화

Before	After
293개 수범사항	**166**개 수범사항
인력·조직·예산(22개)	지나치게 미시적·세부적 사항은 원칙적 삭제(134건)
건물·설비·전산실(15개)	이용자 보호 등은 강화(5건)
정보기술(119개)	금융보안 핵심은 유지(114건)
내부통제(115개)	기타 조정·합리화(45건)
전자금융업무 등(22개)	

급변하는 금융IT 환경·보안 리스크에 유연한 대응 및 금융권의 자율보안 체계 확립 토대 마련

2단계 법률 개정

자율보안 책임성 강화 등을 위한 법률 개정

- 금융보안 거버넌스 강화
- 금융회사 사후책임성 강화 등

3단계 자율보안 체계 전환

자율보안으로 금융보안 패러다임 전환

규정위반 여부 감독 중심 → 자율보안 수립·이행 검증 중심

금융회사 등 ⇄ 금융당국

Ⅱ. 전자금융 감독규정 정비 방안

1 감독규정 정비 계획(총괄)

□ 293개 수범사항(§8~§37) 중 ① 삭제 134건, ② 강화 5건, ③ 현행유지 114건, ④ 조정·합리화 45건 : 293개→ 166개로 축소

① '삭제'는 총 134건으로 29건은 시행세칙에 규정, 그 밖에 규정은 폐지·통합 하거나 해설서로 설명

* 시행세칙은 위임법령과 결합하여 대외적 구속력을 가지나, 해설서는 시행세칙 등의 이해를 위한 설명자료에 해당(미준수시에도 제재 등 X)

- i)내용이 지나치게 지엽적·미시적이거나, ii)유사 입법례 대비 과도한 규정의 경우, iii)금융회사의 자율성이 존중되어야 하는 경우, iv)과거 제재사례가 드문 경우 등은 원칙적으로 삭제

② '규제 강화'는 총 5건으로 재해복구센터 확충, 사고시 이용자 보호체계 강화, 보안거버넌스 개선 등에 중점

* 카카오 데이터센터 화재('22.10월) 등 관련 사이버복원력 및 피해보상 강화 목적

③ '현행 유지'는 총 114건으로, 정보보안·해킹방지 등 금융보안 핵심내용을 유지하고, 운영복원력·제3자 리스크 관리 강화 등 글로벌 추세 등을 감안하여 꼭 필요한 내용만을 존치

* 현행유지 규정의 경우도 세부적·지엽적 내용은 최대한 원칙중심으로 합리화

④ 기타 규정 조정·합리화는 총 45건

< 전자금융 감독규정 정비 검토 결과 >

구분	삭제	유지	조정·합리화	강화	소계 현행	소계 개선
(2절) 인력·조직·예산	5	14	3(신설2)	1	22	19
(3절) 시설	13	0	2	0	15	2
(4절) 정보기술	54	40	25(신설2)	1	119	67
(5절) 내부통제	56	46	13(신설3)	3	115	62
(6절) 전자금융업무	6	14	2	0	22	16
총 계	134	114	45(신설7)	5	293	166

2 주요 삭제 규정

(1) 건물(§9), 설비(§10), 전산실(§11) 관련 지엽적 내용 삭제

□ (주요내용) **건물·설비·전산실** 등 **관리·보호**를 위한 규정

* 예 : 경비원에 의한 통제(건물), 자물쇠 설치(설비), 항온·항습기 구비(전산실)

⇨ **(검토결과)** ① 자율에 맡겨도 충분한 **지엽적·상식적 내용**이 많고, ② 규정위반으로 인한 **제재사례가 거의 없는 점*** 등을 감안,

* 건물(§9), 설비(§10)는 제재사례가 없고, 전산실(§11)은 과거 1건에 불과

→ **감독규정**에는 **원칙**만 남기고 **세부내용(각 호)**은 **삭제**

※ 필수 조항(재해복구센터 국내 설치의무 등)만 남기고 해설서(전산실 출입기록 등)로 전환

[건물에 관한 사항(§9)]
▪ (현행) 출입구 경비원 통제, 비상계단 및 정전대비 유도등 설치, 피뢰설비 등
→(개선) 원칙중심으로 규정화(출입·보안대책 수립·운용), 각 호(1~6호)는 삭제

[전원·공조 등 설비에 관한 사항(§10)]
▪ (현행) 자물쇠 설치, 자가발전 설비, 무정전 전원장치 등
→(개선) 원칙중심으로 규정화(안전성 기준을 수립·준수), 각 호(1~7호)는 삭제

[전산실 등에 관한 사항(§11)]
▪ (현행) CCTV설치, 출입문 이중 안전장치, 이중바닥설치, 항온계·항습계 등
→(개선) 원칙중심으로 규정화하되, 상세 내용은 해설서로 안내

(2) 악성코드(§16) 및 공개형 웹서버 관리대책(§17) 규정 효율화

□ (주요내용) **악성코드 감염방지**를 위한 **진단·치료·복구절차** 및 **공개형 웹서버**(홈페이지 등) **접근·통제** 방안 등을 규정

⇨ **(검토결과)** 다른 규정(제15조 **해킹방지** 등)과 **중복되는 내용**은 **통합**①하고, **유사 입법례**를 참조하여 지나치게 **구체적인 규율**은 **삭제**하고 **원칙중심으로 합리화**②하여 자율보안 시행

[① 중복되는 내용 정비]

▪ (악성코드) 감염시 복구절차(§16.①iii→§15.④로 통합), 감염여부 정기 점검(§16.①iv→§12iii로 통합), 후속조치(§16.②→§15.④로 통합)

▪ (공개형 웹서버) 해킹방지(§17.④→§15.④로 통합), 음란물·도박 차단(§17.⑤→§15.⑦로 이동) 등

[② 원칙중심 합리화(각 호 내용 삭제)]

< 악성코드(§16) >

▪ (현행) 금융회사 또는 전자금융업자는 악성코드 감염을 방지하기 위하여 다음 각 호를 포함한 대책을 수립·운용하여야 한다.

→(개선) 금융회사 또는 전자금융업자는 악성코드 감염 방지, 확산, 피해 최소화 및 복구를 위한 대책을 수립·준수하여야 한다. (각 호 삭제 또는 통합)

❖ (관련 법령) 정보보호 및 개인정보보호 관리체계 인증 등에 관한 고시 별표 7 나. 보호대책 요구사항, 2.10.9 악성코드 통제

바이러스·웜·트로이목마·랜섬웨어 등의 악성코드로부터 개인정보 및 중요정보, 정보시스템 및 업무용 단말기 등을 보호하기 위하여 악성코드 예방·탐지·대응 등의 보호대책을 수립·이행하여야 한다.

< 공개형 웹서버(§17) >

▪ (현행) 금융회사 또는 전자금융업자는 공개용 웹서버에 게재된 내용에 대하여 다음 각 호의 사항을 준수하여야 한다.

→(개선) 금융회사 또는 전자금융업자는 공개용 웹서버에 자료 게시 절차·내용에 관한 내부통제 방안과 개인정보 유출 및 위·변조를 방지하기 위한 보안조치 방안을 수립·운용하여야 한다. (각 호 삭제 또는 통합)

❖ (관련 법령) 정보보호 및 개인정보보호 관리체계 인증 등에 관한 고시 별표 7 나. 보호대책 요구사항, 2.10. 시스템 및 서비스 보안관리, 2.10.3 공개서버 보안

외부 네트워크에 공개되는 서버의 경우 내부 네트워크와 분리하고 취약점 점검, 접근통제, 인증, 정보 수집·저장·공개 절차 등 강화된 보호대책을 수립·이행하여야 한다.

(3) 정보보호 교육 관련 미시적 내용 삭제(§19의2)

□ **(주요내용) 임직원별 정보보안 교육시간** 등을 규정

* 예 : 임원 3시간, 일반직원 6시간, 정보기술 직원 9시간, 정보보호 직원 12시간

⇨ **(검토결과) 교육시간**까지 규율하는 것은 **과도한 측면**이 있어 **삭제**하고, 기타 **중복된 교육관련 사항***은 **타 조항(§8)과 통합**

* 정보보호역량 강화를 위한 교육프로그램 개발 및 교육계획의 수립

(4) 사업추진(§20), 계약(§21), 감리(§22) 관련 세부규정 삭제

□ (주요내용) IT시스템 **사업추진, 계약 및 감리** 관련 **사업 타당성, 계약의 공정성** 등을 확보하기 위한 규정

* 예 : 사업 타당성 및 비용-효과분석, IT계약시 업체선정 기준·절차 및 공정 가격 기준 마련, 감리 기준 등

⇨ (검토결과) ① **자율적 판단**이 특히 요구되는 **경영·운영** 사항으로, ② 정보보안, 해킹방지 등과 달리 **금융보안과 직결되지 않으며**, ③ **추상적·상식적 수준의 내용***인 점 등을 감안하여,

* "충분한 타당성 검토", "공정하고 합리적인 가격 산출", "계약시 귀속관계를 명확히하여 사후분쟁 방지" 등 내용으로 사실상 제재사례 없음

→ **감독규정상 세부내용(각 호) 삭제**(필요시 해설서에 예시로 제공)

(5) 비현실적인 직무분리 세부규정 삭제(§26)

□ (주요내용) **권한·책임을 명확화**하여 **권한 오·남용을 방지**하고 **잠재적인 피해를 예방**하기 위해 **직무간 분리**를 규정

[직무분리 각 호 규정(예시)]
- 프로그래머와 오퍼레이터 간 직무 분리
- 응용프로그래머 ⇔ 시스템프로그래머 간 직무분리
- 시스템보안관리자 ⇔ 시스템프로그래머 간 직무분리
- 전산자료관리자 ⇔ 그 밖의 업무담당자 간 직무분리
- 업무운영자 ⇔ 내부감사자 간 직무분리

⇨ (검토결과) ① **타 입법례*** 대비 규정이 **지나치게 세분화**되어 있고, ② **직무용어**에 대한 **해석상 혼선**이 가능하다는 점 등을 감안하여

→ **내부통제 직무분리 원칙**만 남기고 **각 호는 삭제**

* (정보보호고시 별표 7) 권한 오남용 등으로 인한 잠재적인 피해 예방을 위하여 직무분리기준을 수립하고 적용하여야 한다.

(6) 비밀번호 설정방식 관련 획일적 규율 삭제(§32, §33)

□ (주요내용) **내부 사용자, 이용자** 등의 비밀번호 관리에 있어 **안전성·보안성 유지**를 위한 규정

* 예 : 비밀번호는 아이디, 생년월일, 주민등록번호, 전화번호를 포함하지 않은 숫자와 영문자 및 특수문자 등을 혼합하여 8자리 이상으로 설정

⇨ (검토결과) ① 비밀번호 설정 방식을 **구체적으로 특정**하는 것은 오히려 **보안에 뛰어난 다른 비밀번호 정책 채택을 제한**할 수 있고, ② **타 입법례*** 와 비교하여도 **과도**하며, ③ **생체정보** 등 **신기술을 활용한 인증수단**** 도입에도 장애로 작용

* 정보보호 및 개인정보보호 관리체계 인증 등에 관한 고시, 신용정보업감독규정 등
** 문자·숫자로 표시될 수 없는 지문인증 등 수단에 대한 관리기준이 부재

→ **규정상 원칙만을 존치**하고 **각 호는 삭제**하되, 비밀번호 이외의 수단(지문인증 등) 등이 사용될 수 있는 점을 고려하여 **생체인증 수단** 등 **비밀번호에 준하는 수단**을 포함

▪ (현행) '주민등록번호, 동일숫자, 연속숫자 등 제3자가 쉽게 유추할 수 있는 비밀번호의 등록 불가' 등 세부규칙 존재

→(개선) 제3자가 쉽게 유추할 수 없는 비밀번호 작성규칙 및 등록·변경 절차를 수립·운영할 것

(7) 기타 삭제된 규정

□ (§30 **일괄작업***) 프로그램 통제의 일종으로 §29(프로그램 통제)의 **규제**와 **중복**되고, 지나치게 **미시적·기술적 사항**을 **나열**

→ **각 호**를 **삭제**하고 **오류 최소화 원칙 중심**으로 **수정**

* 일괄작업(Batch) : 다수의 작업을 한 번에 처리하는 명령어 집합

□ (§35 **이용자 유의사항 공지**) 이용자에게 필요한 정보를 금융회사가 **탄력적**으로 **판단**하여 **안전성**을 **확보**할 수 있도록,

→ 세세한 **각 호**는 **삭제**하고 **해설서**로 전환

3 주요 강화 규정

(1) 재해복구센터 설치의무 확대(§23)

□ **(필요성) 카카오 데이터센터 화재** 이후 재해발생시 **재해복구센터**를 이용한 **신속한 업무연속성 회복 필요성**이 확대

○ 현재, 재해복구센터 구축 의무가 없는 **중소 금융회사, 전자금융업자***의 경우 화재 등 **재해발생에 취약**한 측면

* 현재, 중소금융회사 중 카드사, 중앙회 전산을 이용하는 일부 저축은행만이 DR센터 의무구축(그외 여전사·저축은행 및 전금업자는 의무 X)

□ **(주요내용)** 일정 기준*을 충족하는 ① **전금업자**, ② **여전사**(리스·할부금융·신기술) ③ **저축은행**에 대해 **DR센터 구축 의무화**

* (기준안) ①총거래액 2조원 이상(36개사, (28개사 기구축)) ②총자산 2조원 이상(10개사, (6개사 기구축)) ③자체전산 저축은행(12개사, (12개사 기구축))

※ (참고) 기준안을 따를시, **58개社가 의무대상**에 편입되나 이 중 **47개社**가 DR센터를 **이미 구축**하여 규제부담이 크지 않음

(2) 전자금융사고 책임이행보험 한도 상향(§5)

□ **(필요성) 최저보상한도**가 '13년 이후 변경 없이 **낮은 수준***에 머물러 있어 **전자금융거래 확대** 및 **물가상승** 등을 반영하지 못하고 **실질적인 피해보상에 한계**

* 업권별로 최대 20억원(은행), 최소 1억원(보험사, 여전사, 저축은행, 선불업 등)

□ **(주요내용) 거래액 확대, 물가상승 등을 반영**하여 일부 업권 **보상한도를 현실화***하고,

* 선불업·PG 등 : 1억원 → 2억원, 여전사·보험사·저축은행 : 1억원 → 2억원

○ 특히, **최근 3년간 전자금융사고가 자주 발생**한 **자산 2조원 이상 금투업자**에 적용되는 **최저보상한도를 상향**

* (현행) 금투업자 일괄 5억원 → (개선) 자산 2조원 이상 금투업자 10억원

(3) 거버넌스 관련 CISO에 의한 이사회 보고규정 마련(§8의2)

□ **(필요성)** 전 세계적으로 **금융보안 거버넌스**를 강화하는 추세

○ 한국은 **금융보안**에 대한 **이사회, 최고경영진**의 **역할·관심**은 제한적이며, 금융보안을 **CISO 및 정보보호부서**에만 맡겨놓는 경향이 있어 **사고방비의 전사적 대응**에 취약*

* 조직내 고위 의사결정자의 금융보안에 대한 관심이 미흡함에 따라 실제 보안사고가 발생하는 영업·현업부서 등의 보안역량 강화 및 관여 부족

○ **전자금융법 전면개정안**은 **이사회·CEO·현업부서** 등 **다층적 거버넌스 구축 내용**이 있었으나 **법안통과가 지연**되는 상황

□ **(주요내용)** CISO로 하여금 **정보보호위원회 주요 심의·의결사항** 등을 **이사회에 보고하여 처리**하도록 규정

※ (참고) **향후 법 개정**을 통해 **거버넌스 원칙**과 **구성원 책임** 등을 **법률에 규정**하고, **감독규정**에 **세부적 거버넌스**를 설계하여 금융보안에 대한 **전사적 대응체계**를 강화해나갈 계획

4 주요 현행 유지(維持) 규정

※ **현행유지 규정**의 경우도 **세부적·지엽적 내용**은 가능한 범위 내 **원칙중심으로 합리화**하였음(※ 표시)

(1) 정보보안 · 해킹방지 등 금융보안 핵심사항

□ "**전산원장**(§27), **거래**(§28), **프로그램**(§29) **통제**"는 **사고 예방** 및 **감독·검사상 증거 확보** 등을 위해 **현행 유지**

□ "**암호프로그램 및 키 관리 통제**(§31)"는 **최근 코드서명키 유출 사건** 등을 고려하여 **현행 유지**하되, **자구 명확화**

* 규정상 '키'에 코드서명키가 포함되도록 내용을 수정

□ “**자체 보안성심의**(§36)”는 **자율보안의 필수 요소**로 보안이슈를 **금융회사 스스로 인지·관리**하는 효과가 있어 **현행 유지**

※ 단, 사후보고임에도 불구하고 현행 7일내 보고규정은 수범기관이 사실상 사전보고로 느낄 수 있음을 감안하여 30일내 보고로 규제 합리화

□ “**단말기 보호대책**(§12), **해킹 방지**(§15)”는 **악성코드 감염방지, 망분리*** 등과 관련한 **금융보안 핵심내용**으로 **존치**시키되,

☞ (참고) **망분리**의 경우, ’22년 망분리 규제완화 방안 및 ’23년 SaaS에 대한 혁신금융서비스 지정 등의 시장안착 추이를 보아가며 필요시 **추가 개선방안 마련 검토**

(2) 사이버 복원력(Cyber Resilience) 관련 조항

□ “**전산자료 보호대책**(§13), **정보시스템 보호대책**(§14)”은 **카카오 화재**로 촉발된 **자료보호, 백업** 등 **중요성**을 고려하여 **유지**

※ 단, 전산자료 보호대책 분산된 규정은 통합(§13① i , ii , iv → §13① i 로 원칙화)하고, 중복된 기록 보존의무는 §14(정보처리시스템 보호대책)로 일원화

□ “**비상대책 수립·운용**(§23), **비상훈련**(§24)”은 장애·재해시 **신속한 복구시간설정*** 등 **운영복원력 관련 핵심조항**으로 **현행 유지**

※ 단, 지나치게 세부적인 사항(§23.② i ~iv, 비상지원인력 확보·운영 관련 세부사항 등)은 각 호를 삭제하고 해설서로 전환

□ “**해킹 방지**(§15)” 조항에 **사이버 복원력 개념 명시**

* (현행) 피해 발생시 즉시 대처할 수 있도록 적절한 대책을 마련 →
(개선) 피해 최소화 및 신속한 복구를 위한 대책을 수립・운용

(3) 클라우드 아웃소싱 등 제3자 리스크

□ “**클라우드 이용절차**(§14의2)”는 **제3자 리스크 관리** 관련 **중요 규정**으로 **최근에 개정**(’22.12월)되었음을 감안하여 **현행 유지**

※ 단, 보고의무 범위를 명확화(기존 클라우드 계약을 통해 신규업무를 처리하는 경우 등)하고, 양식·서류 등 세부 내용은 삭제 후 세칙에 위임

□ “**외부주문**(outsourcing) **기준**(§60)”은 **외부 주문·계약·위탁 등**과 관련한 타 규정과 **일부 내용이 중복되는 측면**이 있으나,

○ **제3자 리스크 관리 측면**에서 **규정내용을 유지**하되, 향후 **클라우드·망분리** 등과 함께 **규제개선 방안 종합검토**

☞ (참고) **클라우드 이용절차, 외부주문 기준 등**의 경우, 향후 **망분리 규제검토**와 더불어 **규율체계 합리화·효율화** 검토

(4) 전자금융거래 준수사항

□ “**전자금융거래 준수사항**(§34)”은 **암호화 통신, 접근매체 실명발급, 프로그램 위·변조 방지** 등 전자금융거래 **보안의 기본적 사항**을 **규정**하므로 현행 유지

※ 단, 거래인증수단 관련 내용(§34 iv)은 §37과 중복되므로 삭제

5 주요 조정 규정

(1) 사고보고 위반시 과태료 부과(§73) (※ §37의5로 이동)

□ **(필요성)** 보안사고 등에 **조기 대응**을 위해서는 **금융당국**에 대한 **신속한 사고보고** 체계의 정립이 필요하나,

○ **침해사고 등**에 대한 **구체적인 통지 방법**이 없고, **기타 사고보고 미이행**시 **과태료 부과 근거**가 없어 **규범력 확보에 애로**

□ **(주요내용)** 침해사고 등에 관한 **구체적 통지 절차**를 **마련**(§37의4)하고, 보고의무 위반시 **과태료 부과**가 되도록 **조문 이동**(§37의5)*

* 6장 보칙(§73)에 규정된 사고보고 규정을 3장 안전성 확보(§37의5)로 이동할 경우 사고보고 위반시 법률 §21.② 위반에 해당되므로 과태료 부과 가능

Ⅲ. 감독규정 개정 추진 일정

□ **연초 입법예고**(2.1일) → '24.상반기 **감독규정 개정 완료** 추진

※ **재해복구센터 설치의무 확대** 등 규제강화 조항의 경우 업계의견 등을 수렴하여 개정안 시행 후 **최소 6개월 이상의 유예기간**을 부여할 예정

Ⅳ. 향후 금융보안 선진화 추진 계획

□ 금번 **감독규정 정비**를 시작으로 **중장기적**으로 법률개정과 함께 **자율보안으로의 전환을 추진**

○ **(1단계 : 감독규정 정비)** 293개 **수범사항** 중 **지나치게 미시적·세부적인 사항**은 **삭제**하거나 **시행세칙·해설서** 등으로 전환

○ **(2단계 : 법률개정)** 자율보안에 상응하는 **내·외부 책임성을 강화**하고, 위험도에 비례한 금융보안 규제체계 마련

- CEO, **이사회** 등의 금융보안 **관여도·책임도**을 높이고 IT부서 外 **현업부서**의 책임도 강화될 수 있도록 **내부거버넌스 설계**

- 대형사고 등 **사후책임성 강화**를 위한 **과징금 제도 실질화**

* (현행) 5,000만원 → (개선) 해외 입법례를 참고하여, '금융회사 수입의 일정비율' 혹은 '업무정지 기간 이익' 수준의 실질적 과징금 부과 검토

- **위험에 비례한 규제체계 도입**(과태료 차등 등) **기반** 마련

* 예 : 금융보안 개념, 유형을 정의하고 유형별 규제 수준·과태료 등 차등

○ **(3단계 : 자율보안체계 전환)** **금융회사 스스로 수립한** 위험관리 계획을 **당국에 철저히 보고**하고, **당국**은 동 계획의 **적정성을 평가**하고 **이행을 검증**하는 **자율보안체계 확립***

* "규정 위반여부 감독 → 자율보안 수립·이행 검증" 중심으로 패러다임 전환

○ 제도정착을 위해 금융보안원을 통한 **지원·컨설팅 기능**을 강화하고, **중장기적**으로 **민관 협동 금융보안체계*** 도입 검토

* (유럽은행감독청(EBA)) : 제3자(민간 보안기관 등)가 금융회사의 리스크 관리, 자율보안체계 등을 검증하고, 감독당국은 제3자의 자격·활동 적정성을 감독