발 간 번 호
업무참고 2021 - 보안평가 - ① - 21

전자금융기반시설 보안 취약점 평가기준 안내서

(제2022-1호)

금융보안원
FINANCIAL SECURITY INSTITUTE

CONTENTS | 목차

1. 평가 개요 ····· 1

2. 평가 방법 ····· 2

3. 평가 절차 ····· 3

4. 평가기준 구성 ····· 6

5. 평가항목 선정 ····· 12

6. 평가 결과 표현 및 보고 ····· 16

[참고 1] 평가 전담반 구성 기준 및 유의사항 ····· 17

[참고 2] 전자금융기반시설 보안 취약점 평가기준 주요 개정사항(제2022-1호) ····· 21

[참고 3] 전자금융기반시설 보안 취약점 평가기준 (제2022-1호) ····· 55

1. 평가 개요

■ **(개요)** 「보안 취약점 분석·평가」란, 전자금융기반시설의 안전성과 신뢰성을 저해하는 사이버 위협에 대응하기 위해 잠재된 보안 위협을 찾고 이를 개선하기 위한 사전 예방 활동을 의미

■ **(평가대상)** 금융회사 및 전자금융업자(이하 금융회사)는 관계 법령에서 정한 내용에 따라 전자금융 업무를 처리하기 위한 정보처리시스템(전자금융기반시설[1])을 대상으로 취약점을 분석하고 이를 평가

■ **(평가주기)** 공개용 홈페이지 점검은 연 2회 이상, 전자금융기반시설 점검은 연 1회 이상 평가

참고 전자금융기반시설 보안 취약점 분석·평가 관계 법령

[평가대상 및 절차 관련]

- 전자금융거래법 제21조의3 (전자금융기반시설의 취약점 분석·평가)
- 전자금융거래법 시행령 제11조의4 (전자금융기반시설 취약점 분석·평가의 내용), 제11조의5 (전자금융기반시설 취약점 분석·평가의 절차 및 방법 등)

[평가주기 관련]

- 전자금융감독규정 제37조의2(전자금융기반시설의 취약점 분석·평가 주기, 내용 등)
- 전자금융감독규정시행세칙 제7조의2(전자금융기반시설의 취약점 분석·평가의 내용)

※ 자세한 내용은 “국가법령정보센터(http://www.law.go.kr)” 또는 “전자금융감독규정 해설서(2017.5, 금융감독원)” 등을 참고

1) **전자금융기반시설** : 전자금융거래에 이용되는 정보처리시스템 및 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제2조 제1항제1호에 따른 정보통신망을 의미
- **전자금융거래** : 금융회사 또는 전자금융업자가 전자적 장치를 통하여 금융상품 및 서비스를 제공(이하 "전자금융업무"라 한다)하고, 이용자가 금융회사 또는 전자금융업자의 종사자와 직접 대면하거나 의사소통을 하지 아니하고 자동화된 방식으로 이를 이용하는 거래를 말한다.
- **정보통신망** : 「전기통신사업법」 제2조제2호에 따른 전기통신설비를 이용하거나 전기통신설비와 컴퓨터 및 컴퓨터의 이용기술을 활용하여 정보를 수집·가공·저장·검색·송신 또는 수신하는 정보통신체제를 말한다.

2. 평가 방법

본 안내서의 보안 취약점 분석·평가 방법 및 절차는 단순 참고용도로 평가전문기관에서 보유하고 있는 평가 방법 또는 금융회사 내부에서 정한 절차 및 기준을 직접 또는 변형하여 사용해도 무방함

■ **(평가 방법)** 취약점 평가 수행 시 금융회사가 자체전담반을 구성하여 운영하는 방안과 외부 평가전문기관에 위탁하는 방안으로 구분

① 금융회사가 자체전담반을 구성하여 운영하는 방안

- 정보보호최고책임자를 포함한 5인 이상으로 자체전담반을 구성
- 자체전담반 구성 시 구성원 중 100분의 30이상은 「정보보호산업의 진흥에 관한 법률 시행규칙」 제8조의 정보보호 전문서비스 기업 지정기준에서 정한 고급 기술 인력을 갖춘 자로 구성

② 금융회사가 평가전문기관에 위탁하는 방안

- 자체전담반을 구성하지 않을 경우 평가전문기관에 위탁 가능
- 평가전문기관은 「전자금융감독규정」 제37조의3(전자금융기반시설의 취약점 분석·평가전문기관의 지정 등)에서 정의

참고 평가전문기관이란?

[관계 법령]

- 관계 법령에서 정한 평가전문기관으로, 전자금융기반시설에 대해 보안 취약점을 분석·평가할 경우, 정보보호전문서비스기업(약 28개, 2021.12 기준) 또는 침해사고대응기관(금융보안원)에서 수행하도록 규정

- 전자금융감독규정 제37조의2(전자금융기반시설의 취약점 분석·평가 주기, 내용)
  1. 「정보통신기반 보호법」 제16조(정보공유·분석센터)에 따라 금융분야 정보공유·분석센터로 지정된 자
  2. 「정보보호산업의 진흥에 관한 법률」 제23조(정보보호 전문서비스 기업의 지정·관리)에 따라 지정된 정보보호전문서비스기업
  3. 침해사고대응기관

3. 평가 절차

■ **(평가 절차)** 보안 취약점 분석·평가 절차는 5단계로 구성되며, 각 단계별 주요 행위는 다음과 같음

평가 순서	평가 단계	주요 행위
①	사전 분석	평가계획 수립 및 업무현황 파악 등
▼		
②	취약점 분석	자산분석, 취약점 분석 등
▼		
③	취약점 평가	정보보호 분석·평가 지수 산출 등의 종합평가
▼		
④	대책 수립	발견된 취약점에 대한 보안대책 수립 등
▼		
⑤	사후 관리	발견된 취약점에 대한 조치계획 수립 등

① 「사전 분석 단계」에서의 주요 활동

- **(계획 수립)** 취약점 분석·평가를 실시하기 위해 수행 방법, 수행 절차, 소요 예산 등이 포함된 실행 계획을 수립
- **(환경 파악)** 평가대상에 대한 자산 현황, 업무 현황 등 시스템 운영 및 업무환경을 파악[2)]

② 「취약점 분석 단계」에서의 주요 활동

- **(자산 분석)** 자산이 업무 및 서비스에 미치는 영향을 파악하여 자산의 가치(중요도 등)를 산출하는 과정
  - **(자산 분류)** 보유 또는 운영하고 있는 자산의 업무 목적을 파악하여 업무 특성별로 자산을 분류
  - **(자산 평가)** 자산이 가지고 있는 정보의 성격, 자산의 가용성 수준을 복합적으로 평가하여 자산의 중요도를 결정
    - 자산 중요도 : 각 자산에 대한 상대적 중요도를 기준으로 구분

2) **운영 및 업무환경 파악** : 필요에 따라 평가대상 시스템에 대한 보안성 검토 자료 또는 정보보호 정책 및 지침 등을 검토

‖ 자산 중요도 분류 예시 ‖

중요도 \ 역할		점수 (등급)	서버	네트워크장비	정보보호시스템	영향
핵심 설비 (Core)	1 그룹	4	- 중요DB 서버 등	- 인터넷연결구간 네트워크장비 등	- 침입차단시스템 (인터넷 차단) 등	- 금전적 손실 발생 등
	2 그룹	3	- 인터넷뱅킹 서버 등	- 뱅킹서버구간 - 대외구간연결 등	- 침입차단시스템 (뱅킹/대외 등) - 암호화 장비 등	- 정보유출 등
	3 그룹	2	- 메일,DNS 서버 등	- DMZ구간	- 침입탐지시스템	- 손실이 경미한 경우
지원설비 (Peripheral)		1	- 개발서버 타서버	- 내부구간 네트워크장비		- 테스트 용도 등

- 정보 성격 : 위험성이 커지는 정보의 특성과 정보 자체가 가지고 있는 민감성을 고려하여 정보 성격을 구분
- 가용성 수준 : 업무 연속성 측면에서 업무 또는 서비스가 지속적으로 지원되어야 할 성질의 정도를 산정
- **(취약점 분석)** 자산의 중요도 및 업무 목적 등을 고려하여 자산에 내재된 보안 취약점을 분석

③ 「취약점 평가 단계」에서의 주요 활동

- **(취약점 평가)** 식별된 취약점이 금융회사에 미치는 영향을 파악하기 위해 각 취약점에 대한 위험도와 자산의 가치를 고려하여 분야별로 취약 수준을 평가
- **(평가 지수 산출)** 식별된 취약점에 대한 자산 가치, 취약점, 재발생률 등을 종합적으로 분석하여 금융회사의 전반적인 정보보호 관리 상황을 정량적으로 평가

④ 「대책 수립 단계」에서의 주요 활동

- **(우선순위 산정)** 식별된 취약점을 목록화하고 금융회사 업무 및 서비스 환경을 고려하여 조치 우선순위를 산정
- **(보안대책 수립)** 금융회사의 보안정책, 인터뷰 내용, 우선순위 산정 값 등을 활용하여 종합적인 보안대책을 수립

⑤「사후 관리 단계」에서의 주요 활동

- **(이행 계획 수립)** 보안대책 수립 내용을 참고하여 취약점에 대한 조치 이행 계획을 수립하고, 이행 결과를 최고경영자에게 보고
- **(위험 수용)** 보안대책 수립 내용을 참고하여 취약점에 대한 조치 이행 계획을 수립하고, 이행 결과를 최고경영자에게 보고

4. 평가기준 구성

■ **(구성)** 전자금융기반시설 보안 취약점 평가기준은 「금융IT 보안 컴플라이언스 가이드」(2017.10, 금융보안원)를 준용하여 11개 통제분야 및 43개 통제구분으로 분류

‖ 전자금융기반시설 보안 취약점 평가기준 구성 ‖

구분	통제분야 (금융IT 보안컴플라이언스 가이드)	통제구분	평가분야 및 항목
관리적 보안	1. 정보보호 정책	43개 통제구분	10개 평가분야[3)] 669개 평가항목
	2. 정보보호 조직		
	3. 인적 보안		
	8. 업무 지속성 관리		
	10. 외부주문 보안		
기술적 보안	5. 운영 관리		
	6. 접근통제		
	7. IT도입·개발·유지보수 관리		
	9. 전자금융거래 보안		
	11. 보안사고 대응		
물리적 보안	4. 물리적·환경적 보안		

참고 **각 평가항목은 아래 나열된 금융IT 관계법령 및 가이드 등을 참고함**

- 전자금융거래법 (법률 제17354호, 2020. 6. 9.)
- 전자금융거래법 시행령 (대통령령 제32014호, 2021. 9. 24.)
- 전자금융감독규정 (금융위원회고시 제2018-36호, 2018.12.21.)
- 전자금융감독규정시행세칙 (금융감독원세칙, 2021. 2. 25.)
- 주요정보통신기반시설 취약점 분석 평가기준 (과학기술정보통신부고시 제2021-28호, 2021. 3. 29.) 위험도 상/중/하 평가항목

* (유의사항) 「전자금융기반시설 보안 취약점 평가항목」에서 인용되는 각종 법규 내용은 평가항목에 대한 이해 증진을 목적으로 활용된 것으로 이에 관한 해석의 권한은 금융위원회 등 관계 부처에 있음을 밝힘

3) 필수 평가분야 9개(정보보호관리체계, 서버, 데이터베이스 등)와 선택 평가분야 1개(모의해킹)로 구성

■ 통제분야 설명

가. 관리적 보안

- **(1. 정보보호 정책)** 정보보호 및 정보기술 부문 계획 수립 및 관리에 관한 적정성을 평가
  - 통제구분 : 1.1 정보보호 계획
  - 평가분야 : 정보보호관리체계

- **(2. 정보보호 조직)** 정보보호 인력 구성, 예산 및 정보보호최고책임자(CISO) 지정에 관한 적정성을 평가
  - 통제구분 : 2.1 조직 및 인력 구성
    2.2 정보보호 예산
    2.3 정보보호최고책임자(CISO) 지정 및 업무
  - 평가분야 : 정보보호관리체계

- **(3. 인적 보안)** 금융회사 임직원 등에 대한 정보보호 교육 및 훈련에 관한 적정성을 평가
  - 통제구분 : 3.1 정보보호 교육 및 훈련
  - 평가분야 : 정보보호관리체계

- **(8. 업무 지속성 관리)** 업무 지속성 확보 방안, 비상지원 인력 확보 관리 및 위기대응 매뉴얼 수립 등에 관한 적정성을 평가
  - 통제구분 : 8.1 업무지속성 확보방안
    8.2 비상지원인력 확보관리
    8.3 위기대응 행동 매뉴얼 수립
  - 평가분야 : 정보보호관리체계

- **(10. 외부주문 보안)** 외부주문 시 계약 준수 사항, 외부주문 시 보호대책 운영 기준, 업무 위·수탁 운영기준 등에 관한 적정성을 평가
  - 통제구분 : 10.1 외부주문 계약 준수사항
    10.2 외부주문시 보호대책
    10.3 외부주문 등에 대한 기준
  - 평가분야 : 정보보호관리체계

나. 기술적 보안

- **(5. 운영 관리)** 전산자료·정보처리시스템 보호 기술 및 관리에 관한 적정성을 평가

  - 통제구분 : 5.1 단말기 보호대책
    5.2 전산자료 보호대책
    5.3 정보처리시스템 보호대책
      - 5.3.1 보안관리
      - 5.3.2 사용자 인증
      - 5.3.3 패치 관리

    5.4 취약점 분석·평가
    5.5 정보보호시스템 설치 및 운영
      - 5.5.1 보안관리
      - 5.5.2 사용자 인증
      - 5.5.3 패치 관리

    5.6 무선통신망 설치 및 운영
    5.7 악성코드 감염 방지대책
    5.8 공개서버 보안
      - 5.8.1 (전자금융) 거래 인증
      - 5.8.2 (전자금융) 거래정보 검증
      - 5.8.3 (전자금융) 단말 보안
      - 5.8.4 (일반공통) 서비스 보호
      - 5.8.5 (일반공통) 이용자 인증
      - 5.8.6 (일반공통) 단말 보안
      - 5.8.7 (일반공통) 데이터 보호

    5.9 IP주소 관리
    5.10 암호프로그램 및 암호키 관리

  - 평가분야 : 서버, 데이터베이스, 네크워크 인프라, 네트워크 장비, 정보보호시스템 장비, 웹·모바일·HTS 애플리케이션

- **(6. 접근통제)** 전산장비에 대한 사용자 계정 관리를 비롯한 비밀번호 정책 등에 관한 적정성을 평가
  - 통제구분 : 6.1 계정 및 권한 관리
    6.2 정보처리시스템 관리자 통제
    6.3 내부사용자 비밀번호 관리
    6.4 이용자 비밀번호 관리
    6.5 전산원장 통제
    6.6 일괄작업 통제
  - 평가분야 : 정보보호관리체계

- **(7. IT도입·개발·유지보수 관리)** 전자금융과 관련된 시스템 및 서비스 도입에 관한 타당성 검토를 비롯한 통제, 감리 및 보안성 심의 등에 관한 적정성을 평가
  - 통제구분 : 7.1 사업추진 시 준수사항
    7.2 사업계약 관련 준수사항
    7.3 정보처리시스템 감리
    7.4 직무분리
    7.5 프로그램 통제절차 수립
    7.6 자체 보안성심의
  - 평가분야 : 정보보호관리체계

- **(9. 전자금융거래 보안)** 전자금융거래시 준수사항, 전자금융거래 기록·보관 및 이용자 정보보호 등에 관한 적정성을 평가
  - 통제구분 : 9.1 전자금융거래 시 준수사항
    9.2 전자금융거래 기록·보관 (미평가)
    9.3 전자자금이체 한도 (미평가)
    9.4 이용자 정보보호
  - 평가분야 : 정보보호관리체계

- **(11. 보안사고 대응)** 보안사고 발생 시 보고 및 침해사고 대응에 관한 적정성을 평가
  - 통제구분 : 11.1 정보기술부문 및 전자금융 사고보고
    11.2 침해사고 대응
    11.3 손해배상
  - 평가분야 : 정보보호관리체계

다. 물리적 보안

- **(4. 물리적·환경적 보안)** 전산센터 및 전산실에 대한 물리적 환경 보안 사항에 관한 적정성을 평가

  - 통제구분 : 4.1 전산센터 건물
    4.2 전산센터 설비
    4.3 전산실 보안
  - 평가분야 : 정보보호관리체계

■ 평가분야 설명

가. 인프라 영역

- **(정보보호관리체계)** 전자금융거래법, 전자금융감독규정 등을 중심으로 금융회사 내부규정 및 절차의 적정성을 평가
- **(네트워크 인프라)** 네트워크 망분리, 네트워크 접근통제 등 네트워크 구성 및 가용성 확보에 관한 적정성을 관리 중심으로 평가
- **(서버)** 정보처리시스템 운영 시 불필요한 서비스 활성화 등 운영체제 보안설정에 관한 적정성을 기술 중심으로 평가
- **(데이터베이스)** DBA 계정 권한, 비밀번호 등에 관한 보안설정의 적정성을 기술 중심으로 평가
- **(네트워크 장비)** 네트워크 운영 장비에 관한 보안설정 등에 관한 적정성을 기술 중심으로 평가
- **(정보보호시스템 장비)** 보안정책 및 정보보호시스템 보안설정 등에 관한 적정성을 기술 중심으로 평가

나. 서비스 영역

- **(웹 애플리케이션)** 인터넷뱅킹 등 웹 기반 전자금융거래 서비스에 대한 침해 가능성을 기술 중심으로 평가
- **(모바일 애플리케이션)** 모바일뱅킹 등 모바일 기반 전자금융거래 서비스에 대한 보안 침해 가능성을 기술 중심으로 평가
- **(HTS 애플리케이션)** 증권회사에서 제공하는 HTS 애플리케이션에 대한 침해 가능성을 기술 중심으로 평가

■ **(위험도 분류)** 보안 취약점 평가항목에 해당되는 취약점에 대해 위험을 가늠할 수 있도록 위험도의 정도를 5단으로 분류

- 3단 분류 표기법을 이용할 경우 아래 〈표기 방법 적용 예시〉와 같이 상, 중, 하 적용 가능

‖ 위험도 분류에 따른 표기 방법 적용 예시 ‖

위험도 (5단 분류)		위험도 (3단 분류)
높음 (위험도 : 5)	- 시스템 관리자 권한 획득 - 웹 사용자 및 관리자 권한 획득 - 가용성에 직접적인 영향 - 중요 정보 노출 등	**상**
다소 높음 (위험도 : 4)	- 시스템 사용자 권한 획득 - 가용성에 직접적인 영향 - 다른 취약점과 연계될 경우 시스템 관리자 또는 웹 관리자 권한 획득 등	
보통 (위험도 : 3)	- 다른 취약점과 연계될 경우 시스템 사용자 또는 웹 사용자 권한 획득 - 다른 취약점과 연계될 경우 중요 정보 유출 가능성 있음 - 가용성에 간접적인 영향 등	**중**
다소 낮음 (위험도 : 2)	- 추가적인 공격에 활용 가능한 시스템 정보 유출 - 가용성에 간접적인 영향 등	**하**
낮음 (위험도 : 1)	- 공격과 직접적인 연관은 없으나 불필요한 정보 등이 외부에 유출 - 호스트에 관한 일반 정보 유출 등	

5. 평가항목 선정

■ **(공통사항)** 금융회사는 전자금융기반시설에 해당되는 경우 또는 전자금융기반시설과 주요정보통신기반시설을 겸하여 운영되는 경우가 존재하므로, 해당되는 기반시설을 선택하고 평가항목을 최종 결정

■ **기반시설 선택**

|| 해당 기반시설 선택 예시 ||

평가항목	전자금융	주요정보
이용자 비밀번호가 통신용 비밀번호와 계좌원장 비밀번호를 구분하여 사용하고 있는지 여부	o	
정보보안점검의 날 지정 및 운영 여부	o	o

- **(전자금융)** 금융회사가 운영하는 전자금융거래시스템 또는 서비스가 전자금융기반시설인 경우 선택
- **(주요정보)** 금융회사가 운영하는 전자금융거래시스템이 전자금융기반시설과 주요정보통신기반시설을 겸하는 경우 선택

■ **평가항목 선정 방법**

가. 정보보호관리체계, 네트워크 인프라, 정보보호시스템 장비 평가분야

- **(평가항목 선정)** 해당되는 기반시설을 선택하고 평가항목 선정

참고 평가항목 선정 예시

- (예1) 전자금융기반시설에만 해당하는 대상을 평가하는 경우
  ☞ 정보보호관리체계 : 전자금융기반시설 283개 평가항목 선정

- (예2) 전자금융기반시설과 주요정보통신기반시설을 겸하는 대상을 평가하는 경우
  ☞ 정보보호관리체계 : (전자금융 항목 선정) 전자금융기반시설 283개
  (주요정보 항목 선정) 전자금융기반시설 283개 중 주요정보기반시설을 선택하여 해당 평가항목 선정

나. 서버 평가분야

- **(평가항목 선정)** 해당되는 기반시설에서 운영되는 운영체제(OS)를 선택하여 자산별 평가항목을 선정

‖ 평가항목 선정 예시 ‖

평가항목ID	AIX	HP-UX	LINUX	Solaris	Windows
SRV-017	○	○	○	○	
SRV-018					○
SRV-019	○	○	○	○	

☞ (예1) 평가대상이 HP-UX 인 경우 : SRV-017, 019 점검
☞ (예2) 평가대상이 Windows 인 경우 : SRV-018 점검

다. 데이터베이스 평가분야

- **(평가항목 선정)** 해당되는 기반시설에서 운영되는 운영체제(OS)를 선택하여 자산별 평가항목을 선정

‖ 평가항목 선정 예시 ‖

평가항목ID	ORACLE	MSSQL	MYSQL	MariaDB	PostgreSQL	Tibero
DBM-013	○	○	○	○	○	○
DBM-014	○					
DBM-015	○	○				○

☞ (예1) 평가대상이 ORACLE인 경우 : DBM-013, 014, 015 점검
☞ (예2) 평가대상이 Tibero인 경우 : DBM-013, 015 점검

라. 네트워크 장비 평가분야

- **(평가항목 선정)** 해당되는 기반시설에서 평가대상의 그룹 및 장비(스위치, 라우터) 종류를 선택하여 자산별 평가항목을 선정

‖ 평가항목 선정 예시 ‖

평가항목ID	스위치	라우터	A Group (CISCO)	B Group (A10)	C Group (BROCADE, ALTEON, NOTEL,BIGIP, CITRIX,PIOLINK)	D Group (3COM, JUNIPER)
NET-005	○	○	○	○	○	○
NET-006		○	○		○	
NET-007	○	○	○	○	○	○

☞ (예1) 평가대상이 A Group 이고, 스위치인 경우 : NET-005, 007 점검
평가대상이 A Group 이고, 라우터인 경우 : NET-005, 006, 007 점검
☞ (예2) 평가대상이 B Group 이고, 스위치, 라우터인 경우 : NET-005, 007 점검

마. 정보보호시스템 장비 평가분야

- **(평가항목 선정)** 해당되는 기반시설에서 평가대상 장비(방화벽, IDS, DDoS 등)를 선택하여 자산별 평가항목을 선정

‖ 평가항목 선정 예시 ‖

평가항목ID	FW	VPN	IDS	IPS	DDoS	WAF
ISS-011			○	○	○	
ISS-013	○	○				
ISS-014	○	○	○	○	○	○

☞ (예1) 평가대상이 방화벽(FW) 인 경우 : ISS-013, 014 점검
☞ (예2) 평가대상이 웹방화벽(WAF) 인 경우 : ISS-014 점검

바. 웹·모바일·HTS 애플리케이션 평가분야

- **(평가항목 선정)** 해당되는 기반시설에서 평가대상 애플리케이션의 평가분야 및 서비스 유형(금융·비금융)을 선택하여 자산별 평가항목을 선정

‖ 평가항목 선정 예시 ‖

평가항목ID (WEB)	취약점ID (Mobile)	취약점ID (HTS)	Sub NUM
WEB-SER-	MOB-SER-	HTS-SER-	019
	MOB-SER-		020
WEB-SER-			021

☞ (예1) 평가대상이 WEB 인 경우 : WEB-SER-019, WEB-SER-021 점검
☞ (예2) 평가대상이 Mobile 인 경우 : MOB-SER-019, MOB-SER-020 점검
☞ (예3) 평가대상이 HTS 인 경우 : HTS-SER-019 점검

- **(서비스 유형별)** 금융회사에서 제공하는 서비스를 우선 선별 후 선별된 서비스의 유형에 따라 평가항목을 선택하여 평가

‖ 평가항목 선정 예시 ‖

서비스 유형	대상 (예시)	구 분	평가항목 선정결과
전자금융거래 기능이 포함된 경우	- 인터넷뱅킹, 기업뱅킹 등	「전자금융」 평가항목 : 50개」 + 「서비스」 평가항목 : 50개」	100개 항목 적용
전자금융거래 기능이 미포함된 경우	- 단순 홍보성 또는 정보 제공 사이트 등	「전자금융」 평가항목 : NA + 「서비스」 평가항목 : 50개」	50개 항목 적용

■ **(평가항목 예외처리)** 금융회사에서 제공하지 않는 서비스에 관한 평가항목 또는 각종 관계법령에 적용받지 않는 평가항목은 평가 시 예외처리(NA) 가능

참고 **평가항목 예외처리(NA)시 부적절 사례**

☞ **(예1) [평가항목] 전자적 침해행위로 인한 정보처리시스템 사고 보고 여부**
- (적절한 사례) 우리회사는 전자금융감독규정 제00조에서 정한 내용을 준수하지만 최근 발생된 사고가 없어 보고한 사실이 없으므로 → 양호
- (부적절한 사례) 우리회사는 전자금융감독규정 제00조에서 정한 내용을 준수하지만 최근 발생된 사고가 없어 보고한 사실이 없으므로 → NA

☞ **(예2) 불필요한 SMTP 서비스 실행 여부**
- (적절한 사례) 우리회사 서버는 업무와 관계없는 SMTP서비스를 사용하지 않으므로 → 양호
- (부적절한 사례) 우리회사 서버는 업무와 관계없는 SMTP서비스를 사용하지 않으므로 → NA

6. 평가 결과 표현 및 보고

■ **(평가 결과 표현)** 각 평가 결과는 '취약, 양호, 이행, 부분이행' 등 사전에 정한 방법으로 명확하고 일관되게 표기

- 평가 결과 표현을 '권고, 검토, 점검요망' 등 취약 여부를 불명확하게 표기하여 관리 및 보고하는 방법은 권장하지 않음

■ **(취약점 조치)** 평가대상에 실제 적용된 정보를 근거로 취약 여부를 판단하고 발견된 취약점은 시스템 패치, 소스코드 수정, 보안 설정 적용 등의 방법으로 직접 조치

■ **(위험수용)** 취약점 분석·평가에서 도출된 보안 취약점을 제거하기 어렵거나 상응하는 조치가 불가한 경우

- 위험 수용한 취약점은 위험이 제거되지 않은 상태이므로 해당 취약점을 별도로 관리할 것을 권장

■ **(평가 결과 보고)** 금융회사는 내부 정보보호위원회 또는 금융당국 보고 시 발견된 취약점 위주로 보고 및 관리할 것을 권장

참고 **평가 결과 보고시 부적절 사례 예시**

【 가 정 】
- A 금융회사는 금번 평가에서 총 300개의 취약점이 발견됨 (취약그룹 총 20개)
- A 금융회사는 평가기준 중 발견된 취약점 150개를 즉시 조치
- 나머지 150개 취약점 중 130개를 현장에서 위험수용 등 실제 조치 할 잔여 취약점 총 20개

☞ **금융회사 정보보호위원회 내부 보고 및 금융당국 보고시 부적절 사례**
- (예1) 발견된 총 300개 취약점은 보고하지 않고, 취약그룹 20개만 보고
- (예2) 발견된 총 300개 중 잔여 취약점 20개만 보고
- (예3) 130개 위험수용 된 취약점은 조치된 것으로 자체 판단

☞ **금융회사 정보보호위원회 내부 보고 및 금융당국 보고시 적절 사례**

가. 발견된 취약점 총 : 300개
나. 현장조치된 취약점 수 : 150개
다. 잔여취약점 : 20개
라. 위험수용 취약점 : 130개 (정보보호위원회 승인 득함)

[참고 1]

평가 전담반 구성 기준 및 유의사항

[참고 1] 평가 전담반 구성 기준 및 유의사항

아래 내용은 전자금융기반시설 관계 법령 원문을 인용

1 취약점 분석·평가 전담반 구성

- 전자금융감독규정 제37조의2(전자금융기반시설의 취약점 분석·평가 주기, 내용 등) 제2항

② 금융회사 및 전자금융업자는 취약점 분석·평가를 위하여 정보보호최고책임자(정보보호최고책임자가 없는 경우 최고경영자가 지정한다)를 포함하여 5인 이상으로 자체전담반을 구성하여야 하며, 구성원 중 100분의 30 이상은 「정보보호산업의 진흥에 관한 법률 시행규칙」 제8조의 정보보호 전문서비스 기업 지정기준에서 정한 고급 기술인력 이상의 자격을 갖춘 자이어야 한다. 다만, 제37조의3제1항에 따른 평가전문기관에 위탁하는 경우에는 자체전담반을 구성하지 아니할 수 있다.

2 취약점 분석·평가 실시

- 전자금융감독규정 제37조의2(전자금융기반시설의 취약점 분석·평가 주기, 내용 등) 제1항

① 전자금융기반시설의 취약점 분석·평가는 총자산이 2조원 이상이고, 상시 종업원 수(「소득세법」에 따른 원천징수의무자가 근로소득세를 원천징수한 자를 기준으로 한다. 이하 같다) 300명 이상인 금융회사 또는 전자금융업자이거나 「수산업협동조합법」, 「산림조합법」, 「신용협동조합법」, 「상호저축은행법」 및 「새마을금고법」에 따른 중앙회의 경우 연 1회 이상(홈페이지에 대해서는 6개월에 1회 이상) 실시하여야 한다.

3 취약점 분석·평가 결과 제출

- 전자금융거래법 제21조의3(전자금융기반시설 취약점 분석·평가)

① 금융회사 및 전자금융업자는 전자금융거래의 안전성과 신뢰성을 확보하기 위하여 전자금융기반시설에 대한 다음 각 호의 사항을 분석·평가하고 그결과(「정보통신기반 보호법」제9조에 따른 취약점 분석·평가를 한 경우에는 그 결과를 말한다)를 금융위원회에 보고하여야 한다.

1. 정보기술부문의 조직, 시설 및 내부통제에 관한 사항
2. 정보기술부문의 전자적 장치 및 접근매체에 관한 사항
3. 전자금융거래의 유지를 위한 침해사고 대응조치에 관한 사항
4. 그 밖에 대통령령으로 정하는 사항

- 전자금융거래법시행령 제11조의5(전자금융기반시설 취약점 분석·평가의 절차 및 방법 등) 제3항

③ 금융회사 및 전자금융업자는 법 제21조의3제1항에 따라 전자금융기반시설의 취약점 분석·평가를 하였을 때에는 다음 각 호의 사항이 포함된 결과보고 및 보완조치 이행계획서를 그 취약점 분석·평가 종료 후 30일 이내에 금융위원회에 제출하여야 한다.

1. 취약점 분석·평가의 사유, 대상, 기간 등 실시개요
2. 취약점 분석·평가의 세부 수행방법
3. 취약점 분석·평가 결과
4. 취약점 분석·평가 결과에 따른 필요한 보완조치의 이행계획
5. 그 밖에 취약점 분석·평가의 적정성을 확보하기 위하여 필요한 사항으로서 금융위원회가 정하여 고시하는 사항

- 전자금융거래법시행령 제30조(권한의 위탁)제1항, 제2항

① 금융위원회는 법 제48조에 따라 다음 각 호의 업무를 금융감독원장에게 위탁한다.
(1의3) 법 제21조의3제1항에 따른 취약점 분석·평가 결과의 접수

② 금융감독원장은 제1항에 따라 위탁받은 업무의 처리결과를 금융위원회가 정하여 고시하는 바에 따라 금융위원회에 보고하여야 한다.

4 취약점 분석·평가 의무위반에 관한 관련제재

- 전자금융거래법 제51조(과태료) 제2항, 제3항

② 다음 각 호의 어느 하나에 해당하는 자에게는 2천만원 이하의 과태료를 부과한다. 〈개정 2014.10.15., 2017.4.18.〉

4. 제21조의3제1항을 위반하여 전자금융기반시설의 취약점을 분석·평가하지 아니한 자
5. 제21조의3제2항을 위반하여 보완조치의 이행계획을 수립·시행하지 아니한 자

③ 다음 각 호의 어느 하나에 해당하는 자(제1호, 제6호부터 제8호까지 및 제10호의 경우에는 제28조제4항에 따라 해당 규정을 준용하는 선불전자지급수단을 발행하는 자를 포함한다)에게는 1천만원 이하의 과태료를 부과한다. 〈개정 2017.4.18.〉

5. 제21조의3제1항을 위반하여 전자금융기반시설의 취약점 분석·평가의 결과를 보고하지 아니한 자

[참고 2]

전자금융기반시설 보안 취약점 평가기준 주요 개정사항

(제2022-1호)

전자금융기반시설 보안 취약점 평가기준 개정사항

■ **개정 결과(요약)**

● 전체 661개 항목 중 **119개 항목 개정**

【 (현행) 제2021-1호 】			【 (개정) 제2022-1호 】				
평가분야		제2021-1호	제2022-1호	신규	통합	삭제	개선
인프라 영역 (필수)	정보보호관리체계	279	280	2	1	-	25
	서버	117	117	-	-	-	6
	데이터베이스	30	27	-	2	1	27
	네트워크 인프라	19	19	-	-	-	-
	네트워크 장비	44	43	-	-	1	3
	정보보호시스템 장비	41	41	-	-	-	-
서비스 영역 (필수)	웹	51	50	2	3	-	8
	모바일	48	48	3	3	-	8
	HTS	32	44	15	3	-	6
공통 (선택)	모의해킹[4]	시나리오 기반	-	-	-	-	-
합계		661	669	22	12	2	83

4) 선택 평가분야로 금융회사 담당자와 협의하여 1개 이상 모의해킹 시나리오를 정하고 이를 평가
(예1) 외주 직원망에서 내부 운영망으로의 불법 접속 가능성
(예2) DMZ망에서 내부 운영시스템으로의 불법 접속 가능성 등

■ **정보보호 관리체계 분야 개정사항**

● 전체 280개 항목 중 **28개 항목 개정**

【 (현행) 제2021-1호 】				【 (개정) 제2022-1호 】		
구분	평가항목ID	평가항목	개정사항	평가항목ID	평가항목	주요 개정사항
1	FISM-005	IT 아웃소싱(이하 'IT자회사'포함) 통제/관리 조직(인력포함) 운영 여부	**개선**	-	-	• **관련 근거 변경** - (기존) 감독규정 제8조제1항제1호 ➜ (변경) 감독규정 제8조제1항제2호
2	FISM-016	정보보안점검의 날 지정 및 운영 여부	**개선**	FISM-016	정보보안점검의 날 지정 여부	• **평가항목명 변경**
3	FISM-034	무정전전원장치 설치 여부	**개선**	-	-	• **관련 근거 변경** - (기존) 감독규정 제10조제3호 ➜ (변경) 감독규정 제10조제4호
4	FISM-059	정보처리시스템 접속에 관한 사용자 인증여부 및 사후 확인할 수 있는 기록물 저장 여부	**개선**	FISM-059	정보처리시스템 접속에 관한 사용자인가의 여부를 확인할 수 있는 기록 유지 여부	• **평가항목명 변경**
5	FISM-088	정보처리시스템의 운영체제(Operating System) 계정으로 로그인(Log in)할 경우 계정 및 비밀번호 이외에 별도의 추가인증 적용 여부	**개선**	-	-	• **관련 근거 변경** - (기존) 감독규정 제14조제8호 ➜ (변경) 감독규정 제14조제9호

【 (현행) 제2021-1호 】				【 (개정) 제2022-1호 】		
구분	평가항목ID	평가항목	개정사항	평가항목ID	평가항목	주요 개정사항
6	FISM-089	정보처리시스템 운영체제(Operating System) 계정에 대한 사용권한, 접근 기록, 작업 내역 등에 대한 상시 모니터링 체계 수립 여부 및 이상 징후 발생 시 필요한 통제 조치 시행 여부	**개선**	-	-	• **관련 근거 변경** - (기존) 감독규정 제14조제8호 ➜ (변경) 감독규정 제14조제10호
7	FISM-092	전자금융기반시설의 취약점 분석·평가는 연 1회 이상(홈페이지에 대해서는 6개월에 1회 이상) 실시 여부	**개선**	-	-	• **관련 근거 변경** - (기존) 감독규정 제37조의2 제1항,제3항,제4항,제6항 ➜ (변경) 감독규정 제37조의2제1항
8	FISM-099	내부통신망에서의 파일 배포기능 이용 시 파일 무결성 검증 수행 여부	**개선**	-	-	• **관련 근거 변경** - (기존) 감독규정 시행세칙 제2조의2 삭제
9	FISM-100	전산실 내에 위치한 정보처리시스템과 해당 정보처리시스템의 운영, 개발, 보안 목적으로 직접 접속하는 단말기가 인터넷 등 외부통신망으로부터 물리적으로 분리 여부	**개선**	-	-	• **관련 근거 변경** - (기존) 감독규정 시행세칙 제2조의2 ➜ (변경) 제2조의2제2항제4호
10	FISM-109	무선통신망 이용 업무의 소관부서장 승인 및 사전 지정	**개선**	FISM-109	무선통신망 이용 업무의 정보보호최고책임자 승인 및 사전 지정 여부	• **평가항목명 변경**

【 (현행) 제2021-1호 】				【 (개정) 제2022-1호 】		
구분	평가항목ID	평가항목	개정사항	평가항목ID	평가항목	주요 개정사항
11	FISM-151	내부사용자 비밀번호 설정 시, 비밀번호에 생년월일, 주민등록번호, 전화번호 포함 금지 여부	**개선**	FISM-151	내부사용자 비밀번호 설정 시, 이용자 식별부호(아이디), 생년월일, 주민등록번호, 전화번호 포함 금지 여부	• **평가항목명 변경**
12	FISM-166	이용자 비밀번호 입력 시 핀패드 등의 보안장치 이용 여부	**통합**	FISM-168	비밀번호를 등록·사용하는 경우 핀패드 등 보안장치를 이용 또는 사후에 전자적 장치를 이용하여 직접 입력 여부	• **평가항목 통합**
	FISM-168	비밀번호를 등록·사용하는 경우 핀패드 등 보안장치를 이용 또는 사후에 전자적 장치를 이용하여 직접 입력 여부				
13	FISM-219	정보기술부문 및 전자금융업무에 대한 자체 보안성 검토 및 정기 보안점검 실시 여부	**개선**	-	-	• **관련 근거 추가** - 감독규정 제36조제1항
14	FISM-220	정보통신망을 이용하여 이용자를 대상으로 신규 전자금융업무를 수행하거나 복수의 금융회사 또는 전자금융업자가 공동으로 전자금융거래 관련 표준을 제정하는 경우 자체 보안성심의 여부	**개선**	-	-	• **관련 근거 추가** - (추가) 감독규정 제36조제1항제1호, 제36조제1항제2호

【 (현행) 제2021-1호 】				【 (개정) 제2022-1호 】		
구분	평가항목ID	평가항목	개정사항	평가항목ID	평가항목	주요 개정사항
15	FISM-230	주전산센터와 일정거리 이상 떨어진 안전장소에 재해복구센터 구축 및 운영 여부	**개선**	-	-	• **관련 근거 변경** - (기존) 감독규정 제23조제8항, 제23조제9항 ➜ (변경) 감독규정 제23조제8항
16	FISM-241	연 1회 해킹, 디도스공격 등 침해사고 대응 및 복구훈련 실시와 침해사고대응기관에 제출 여부	**개선**	-	-	• **관련 근거 변경** - (기존) 감독규정 제37조의4 ➜ (변경) 감독규정 제37조의4제5항
17	FISM-256	IT외부주문 업무에 대한 업무적정성 검토 여부	**개선**	-	-	• **관련 근거 추가** - 감독규정 제8조제1항제2호
18	FISM-257	IT외부주문 계약 체결시 계약내용의 적정성 검토 여부	**개선**	-	-	• **관련 근거 추가** - 감독규정 제8조제1항제2호
19	FISM-271	외부주문 사항에 대해 위탁된 금융거래 정보가 위탁회사의 안전한 장소(전산실 등)에서 관리 및 주기적인 확인여부	**개선**	FISM-271	외부주문 사항에 대해 위탁된 금융거래정보가 위탁회사의 전산실 내 관리 및 보관 여부	• **평가항목명 변경**
20	FISM-274	정보처리시스템 또는 통신회선 등의 장애로 10분 이상 전산업무가 중단 또는 지연 사고에 대한 금융감독원장 보고 여부	**개선**	-	-	• **관련 근거 변경** - (기존) 전자금융거래법 제21조의6 ➜ (변경) 제21조의5 - (기존) 전자금융거래법 시행령 제11조의6 ➜ (변경) 제11조의2

【 (현행) 제2021-1호 】				【 (개정) 제2022-1호 】		
구분	평가항목ID	평가항목	개정사항	평가항목ID	평가항목	주요 개정사항
21	FISM-275	전산자료 또는 프로그램의 조작과 관련 금융사고 보고에 대한 금융감독원장 보고 여부	**개선**	-	-	• **관련 근거 변경** - (기존) 전자금융거래법 제21조의6 ➜ (변경) 제21조의5 - (기존) 전자금융거래법 시행령 제11조의6 ➜ (변경) 제11조의2
22	FISM-276	전자적 침해행위로 인한 정보처리시스템 사고에 대한 금융감독원장 보고 여부	**개선**	-	-	• **관련 근거 변경** - (기존) 전자금융거래법 제21조의6 ➜ (변경) 제21조의5 - (기존) 전자금융거래법 시행령 제11조의6 ➜ (변경) 제11조의2
23	FISM-277	이용자가 전자적 침해행위로 인해 금전적 피해를 입었다고 통지한 사고에 대한 금융감독원장 보고 여부	**개선**	-	-	• **관련 근거 변경** - (기존) 전자금융거래법 제21조의6 ➜ (변경) 제21조의5 - (기존) 전자금융거래법 시행령 제11조의6 ➜ (변경) 제11조의2
24	FISM-278	접근매체의 위조나 변조로 발생한 사고에 대한 금융감독원장 보고 여부	**개선**	-	-	• **관련 근거 변경** - (기존) 전자금융거래법 제21조의6 ➜ (변경) 제9조제1항제1호 - (기존) 전자금융거래법 시행령 제11조의6 ➜ (삭제)
25	FISM-279	계약체결 또는 거래지시의 전자적 전송이나 처리과정에서 발생한 사고에 대한 금융감독원장 보고 여부	**개선**	-	-	• **관련 근거 변경** - (기존) 전자금융거래법 제21조의6 ➜ (변경) 제9조제1항제2호 - (기존) 전자금융거래법 시행령 제11조의6 ➜ (삭제)

【 (현행) 제2021-1호 】				【 (개정) 제2022-1호 】		
구분	평가항목ID	평가항목	개정사항	평가항목ID	평가항목	주요 개정사항
26	FISM-280	사고보고의 고의 지연 및 숨긴 자에 대한 징계절차 수립 여부	**개선**	-	-	• **관련 근거 변경** - (기존) 전자금융거래법 제21조의6 ➜ (변경) 제21조의5 - (기존) 전자금융거래법 시행령 제11조의6 ➜ (변경) 제11조의2
27	-	-	**신규**	FISM-286	전자금융거래를 위한 전자적 장치 또는 정보통신망에 침입하여 부정한 방법으로 획득한 접근매체의 이용으로 발생한 사고에 대한 금융감독원장 보고 여부	• **신규 평가항목**
28	-	-	**신규**	FISM-287	오픈뱅킹 운영기관 등에서 정한 기준에 따라 보안 점검을 실시*하고, 결과에 따른 미흡사항의 제거 또는 그에 상응하는 조치 시행 여부 * 오픈뱅킹 서비스 개시 1년 이상 경과한 금융회사 등에 해당	• **신규 평가항목**

■ **서버 분야 개정사항**

● 전체 117개 항목 중 **6개 항목 개정**

【 (현행) 제2021-1호 】				【 (개정) 제2022-1호 】		
구분	평가항목ID	평가항목	개정사항	평가항목ID	평가항목	주요 개정사항
1	SRV-035	취약한 서비스 활성화	**개선**	-	-	• **판단기준 변경** - 취약한 서비스(r계열 서비스) 목록에서 rsync 삭제
2	SRV-037	불필요한 FTP 서비스 실행	**개선**	SRV-037	취약한 FTP 서비스 실행	• **평가항목명 변경** • **판단기준 개선** - 판단기준에 도움이 되는 설명* 추가 * 업무상 필요하여 FTPS를 활용하는 등 통신 암호화를 위한 별도의 보안 수단이 적용된 경우는 양호
3	SRV-095	존재하지 않는 소유자 및 그룹 권한을 가진 파일 또는 디렉터리 존재	**개선**	-	-	• **판단방법 변경** - 소유자(user)와 그룹(group) 조회 조건 변경 * (기존) 소유자와 그룹 조회 시 and 조건 검색 ➜ (변경) 소유자와 그룹 조회 시 or 조건 검색

【 (현행) 제2021-1호 】				【 (개정) 제2022-1호 】		
구분	평가항목ID	평가항목	개정사항	평가항목ID	평가항목	주요 개정사항
4	SRV-108	로그에 대한 접근통제 및 관리 미흡	**개선**	-	-	• **판단기준 변경** - LINUX, SOLARIS에 특정 로그파일*의 경우 디렉터리 내 로그 파일들의 권한 변경이 불가하여 예외 사항 명시 * /var/log/btmp, /var/log/wtmp
5	SRV-127	계정 잠금 임계값 설정 미비	**개선**	-	-	• **판단방법 변경** - 평가방법 추가(LINUX) * (기존) pam_faillock.so 설정 점검 ➜ (변경) pam_faillock.so, pam_tally2.so, pam_tally.so 설정 점검
6	SRV-135	TCP 보안 설정 미비	**개선**	-	-	• **판단기준 변경** - Windows 버전별 확인해야 할 레지스트리 값 명시 * (기존) 모든 Windows 버전의 DoS 방어 레지스트리 확인 값 동일 ➜ (변경) Windows 2008 이상 버전과 미만 버전에 따라 DoS 방어 레지스트리 값 확인

■ **데이터베이스 분야 개정사항**

● 전체 30개 항목 중 **30개 항목 개정**

【 (현행) 제2021-1호 】				【 (개정) 제2022-1호 】		
구분	평가항목ID	평가항목	개정사항	평가항목ID	평가항목	주요 개정사항
1	DBM-001	유추가능한 비밀번호 설정 여부(DB계정)	**개선**	DBM-001	취약하게 설정된 비밀번호 존재	• **평가항목 개선** - 유추 가능한 비밀번호, 비밀번호 복잡도 설정 만족 여부 등에 대해 점검 가능 하도록 개선 • **평가항목 통합** • **평가대상 확대** - Tibero 추가 • **판단기준, 판단방법 양식 변경** - (기존) 모든 평가대상의 판단기준, 판단방법 동일 ➜ (변경) 평가대상별로 각각 판단기준, 판단방법 분리
2	DBM-002	기본 계정 및 패스워드 변경 (디폴트 ID 및 패스워드 변경 및 잠금)	**통합**	DBM-001	취약하게 설정된 비밀번호 존재	• **평가항목 통합(삭제)** - DBM-001 항목으로 통합

【 (현행) 제2021-1호 】				【 (개정) 제2022-1호 】		
구분	평가항목ID	평가항목	개정사항	평가항목ID	평가항목	주요 개정사항
3	DBM-003	비인가자의 접근 차단을 위한 사용자 계정 관리	**개선**	DBM-003	업무상 불필요한 계정 존재	• **평가항목명 변경** • **평가대상 확대** - Tibero 추가 • **판단기준, 판단방법 양식 변경** - (기존) 모든 평가대상의 판단기준, 판단방법 동일 ➜ (변경) 평가대상별로 각각 판단기준, 판단방법 분리
4	DBM-004	DBA 계정 권한 관리	**개선**	DBM-004	업무상 불필요하게 관리자 권한이 부여된 계정 존재	• **평가항목명 변경** • **평가대상 확대** - Tibero 추가 • **판단기준, 판단방법 양식 변경** - (기존) 모든 평가대상의 판단기준, 판단방법 동일 ➜ (변경) 평가대상별로 각각 판단기준, 판단방법 분리

【 (현행) 제2021-1호 】				【 (개정) 제2022-1호 】		
구분	평가항목ID	평가항목	개정사항	평가항목ID	평가항목	주요 개정사항
5	DBM-005	DB서버 중요정보 암호화 적용 여부	**개선**	DBM-005	데이터베이스 내 중요정보 암호화 미적용	• **평가항목명 변경** • **평가대상 확대** - Tibero 추가 • **판단기준, 판단방법 양식 변경** - (기존) 모든 평가대상의 판단기준, 판단방법 동일 ➜ (변경) 평가대상별로 각각 판단기준, 판단방법 분리
6	DBM-006	로그인 실패 횟수에 따른 잠금시간 등 계정 잠금 정책 설정	**개선**	DBM-006	로그인 실패 횟수에 따른 접속 제한 설정 미흡	• **평가항목명 변경** • **평가대상 확대** - MSSQL, MySQL, PostgreSQL, Tibero 추가 • **판단기준, 판단방법 양식 변경** - (기존) 모든 평가대상의 판단기준, 판단방법 동일 ➜ (변경) 평가대상별로 각각 판단기준, 판단방법 분리

【 (현행) 제2021-1호 】				【 (개정) 제2022-1호 】		
구분	평가항목ID	평가항목	개정사항	평가항목ID	평가항목	주요 개정사항
7	DBM-007	비밀번호 복잡도 설정	**개선**	DBM-007	비밀번호의 복잡도 정책 설정 미흡	• **평가항목명 변경** • **평가대상 확대** - Tibero 추가 • **판단기준, 판단방법 양식 변경** - (기존) 모든 평가대상의 판단기준, 판단방법 동일 ➜ (변경) 평가대상별로 각각 판단기준, 판단방법 분리
8	DBM-008	비밀번호의 주기적인 변경	**개선**	DBM-008	주기적인 비밀번호 변경 미흡	• **평가항목명 변경** • **평가대상 확대** - Tibero 추가 • **판단기준, 판단방법 양식 변경** - (기존) 모든 평가대상의 판단기준, 판단방법 동일 ➜ (변경) 평가대상별로 각각 판단기준, 판단방법 분리

【 (현행) 제2021-1호 】				【 (개정) 제2022-1호 】		
구분	평가항목ID	평가항목	개정사항	평가항목ID	평가항목	주요 개정사항
9	DBM-009	세션 Idle timeout 설정	**개선**	DBM-009	사용되지 않는 세션 종료 미흡	• **평가항목명 변경** • **평가대상 확대** - Tibero 추가 • **판단기준, 판단방법 양식 변경** - (기존) 모든 평가대상의 판단기준, 판단방법 동일 ➜ (변경) 평가대상별로 각각 판단기준, 판단방법 분리
10	DBM-010	관리자계정 로그인 제한 설정	**삭제**	-	-	• **평가항목 삭제** - 관리자계정 로그인 제한에 대한 방안으로 비밀번호 인증 방식만이 DB접속 제한에 대한 보안성을 강화하는 방안은 아니므로 해당 항목 삭제 ※ '[SRV-027] 서비스 접근 IP 및 포트 제한 미비' 항목에서 DB 서버에 대한 접근 통제 강화

【 (현행) 제2021-1호 】				【 (개정) 제2022-1호 】		
구분	평가항목ID	평가항목	개정사항	평가항목ID	평가항목	주요 개정사항
11	DBM-011	감사 기능 설정 점검	**개선**	DBM-011	감사 로그 수집 및 백업 미흡	• **평가항목명 변경** • **평가대상 확대** - Tibero 추가 • **판단기준, 판단방법 양식 변경** - (기존) 모든 평가대상의 판단기준, 판단방법 동일 ➜ (변경) 평가대상별로 각각 판단기준, 판단방법 분리
12	DBM-012	listener 비밀번호 설정 및 디폴트 포트 변경	**개선**	DBM-012	Listener Control Utility(lsnrnctl) 보안 설정 미흡	• **평가항목명 변경** • **판단기준 변경** - 디폴트 포트(1521)로 설정 유무 확인 내용 삭제
13	DBM-022	데이터베이스의 주요 설정파일, 패스워드 파일 등 주요 파일들의 접근 권한 적절성 여부	**개선**	DBM-022	설정 파일 및 중요정보가 포함된 파일의 접근 권한 설정 미흡	• **평가항목명 변경** • **평가대상 확대** - MSSQL, MySQL, MaridaDB, PostgreSQL, Tibero 추가 • **판단기준, 판단방법 양식 변경** - (기존) 모든 평가대상의 판단기준, 판단방법 동일 ➜ (변경) 평가대상별로 각각 판단기준, 판단방법 분리

【 (현행) 제2021-1호 】				【 (개정) 제2022-1호 】		
구분	평가항목ID	평가항목	개정사항	평가항목ID	평가항목	주요 개정사항
14	DBM-027	오라클 리스너 로그 및 trace 파일에 대한 파일권한 적절성 여부	**통합**	DBM-012	Listener Control Utility(lsnrnctl) 보안 설정 미흡	• **평가항목 통합(삭제)** - [DBM-027]에서 오라클 리스너 파라미터의 변경이 관리자만 가능한지 점검*하였던 내용을 [DBM-012]로 통합 * listenr.ora파일에서 ADMIN_RESTRICTIONS_LISTENER=ON 필드가 존재하는지 확인 - [DBM-027]에서 주요 파일(listener.ora) 및 로그 파일에 대한 파일권한을 확인했던 내용을 [DBM-022]로 통합
				DBM-022	설정 파일 및 중요정보가 포함된 파일의 접근 권한 설정 미흡	
15	DBM-013	원격에서 DB로의 접속 제한	**개선**	DBM-013	원격 접속에 대한 접근 제어 미흡	• **평가항목명 변경** • **평가대상 확대** - Tibero 추가 • **판단기준, 판단방법 양식 변경** - (기존) 모든 평가대상의 판단기준, 판단방법 동일 ➜ (변경) 평가대상별로 각각 판단기준, 판단방법 분리

【 (현행) 제2021-1호 】				【 (개정) 제2022-1호 】		
구분	평가항목ID	평가항목	개정사항	평가항목ID	평가항목	주요 개정사항
16	DBM-014	OS_ROLES, REMOTE_OS_ROLES 설정	**개선**	DBM-014	취약한 운영체제 역할 인증 기능(OS_ROLES, REMOTE_OS _ROLES) 사용	• **평가항목명 변경** • **판단기준, 판단방법 양식 변경** - (기존) 모든 평가대상의 판단기준, 판단방법 동일 ➜ (변경) 평가대상별로 각각 판단기준, 판단방법 분리
17	DBM-015	Public Role에 불필요한 권한 존재 여부	**개선**	-	-	• **평가대상 확대** - PostgreSQL, Tibero 추가 • **판단기준 변경** - (기존) Public role에 DBA 계정의 role이 Public으로 설정된 경우에 취약 ➜ (변경) Public role에 DBA 계정의 role 외에 불필요한 권한 및 역할이 부여된 경우도 취약으로 판단 • **판단기준, 판단방법 양식 변경** - (기존) 모든 평가대상의 판단기준, 판단방법 동일 ➜ (변경) 평가대상별로 각각 판단기준, 판단방법 분리

【 (현행) 제2021-1호 】				【 (개정) 제2022-1호 】		
구분	평가항목ID	평가항목	개정사항	평가항목ID	평가항목	주요 개정사항
18	DBM-016	DBMS 최신 보안패치와 밴더 권고사항 적용	**개선**	DBM-016	최신 보안패치와 벤더 권고 사항 미적용	• **평가항목명 변경** • **평가대상 확대** - Tibero 추가 • **판단기준, 판단방법 양식 변경** - (기존) 모든 평가대상의 판단기준, 판단방법 동일 ➜ (변경) 평가대상별로 각각 판단기준, 판단방법 분리
19	DBM-017	DBA이외의 인가되지 않은 사용자가 시스템 테이블에 접근할 수 없도록 설정	**개선**	DBM-017	업무상 불필요한 시스템 테이블 접근 권한 존재	• **평가항목명 변경** • **평가대상 확대** - Tibero 추가 • **판단기준 변경** - (기존) DBA만 접근 가능한 테이블에 일반 사용자 접근이 가능한 경우 취약 ➜ (변경) 업무상 불필요하게 시스템 접근 권한이 존재할 경우 취약 • **판단기준, 판단방법 양식 변경** - (기존) 모든 평가대상의 판단기준, 판단방법 동일 ➜ (변경) 평가대상별로 각각 판단기준, 판단방법 분리

【 (현행) 제2021-1호 】				【 (개정) 제2022-1호 】		
구분	평가항목ID	평가항목	개정사항	평가항목ID	평가항목	주요 개정사항
20	DBM-019	패스워드 재사용 방지 설정 여부	**개선**	DBM-019	비밀번호 재사용 방지 설정 미흡	• **평가항목명 변경** • **평가대상 확대** - MSSQL, MySQL, MaridaDB, PostgreSQL, Tibero 추가 • **판단기준, 판단방법 양식 변경** - (기존) 모든 평가대상의 판단기준, 판단방법 동일 ➜ (변경) 평가대상별로 각각 판단기준, 판단방법 분리
21	DBM-020	DB 사용자 계정을 개별적으로 부여	**개선**	DBM-020	사용자별 계정 분리 미흡	• **평가항목명 변경** • **평가대상 확대** - Tibero 추가 • **판단기준 변경** - 계정을 공유해서 사용하는 경우, 서드파트솔루션등을 통해 접속자 별 감사로그 식별이 가능한 경우는 양호로 판단하도록 예외 사항 추가 • **판단기준, 판단방법 양식 변경** - (기존) 모든 평가대상의 판단기준, 판단방법 동일 ➜ (변경) 평가대상별로 각각 판단기준, 판단방법 분리

【 (현행) 제2021-1호 】				【 (개정) 제2022-1호 】		
구분	평가항목ID	평가항목	개정사항	평가항목ID	평가항목	주요 개정사항
22	DBM-021	불필요한 ODBC/OLE-DB 데이터 소스와 드라이브 제거	**개선**	DBM-021	업무상 불필요한 ODBC/OLE-DB 데이터 소스 및 드라이버 존재	• **평가항목명 변경** • **판단기준, 판단방법 양식 변경** - (기존) 모든 평가대상의 판단기준, 판단방법 동일 ➜ (변경) 평가대상별로 각각 판단기준, 판단방법 분리
23	DBM-024	Role에 의한 grant option 설정 여부	**개선**	DBM-024	불필요하게 WITH GRANT OPTION 옵션이 설정된 권한 존재	• **평가항목명 변경** • **평가대상 확대** - MSSQL, MySQL, MaridaDB, PostgreSQL, Tibero 추가 • **판단기준, 판단방법 양식 변경** - (기존) 모든 평가대상의 판단기준, 판단방법 동일 ➜ (변경) 평가대상별로 각각 판단기준, 판단방법 분리
24	DBM-025	서비스 지원이 종료된(EOS) DBMS 사용 여부	**개선**	DBM-025	서비스 지원이 종료된(EoS) 데이터베이스 사용	• **평가항목명 변경** • **평가대상 확대** - Tibero 추가 • **판단기준, 판단방법 양식 변경** - (기존) 모든 평가대상의 판단기준, 판단방법 동일 ➜ (변경) 평가대상별로 각각 판단기준, 판단방법 분리

【 (현행) 제2021-1호 】				【 (개정) 제2022-1호 】		
구분	평가항목ID	평가항목	개정사항	평가항목ID	평가항목	주요 개정사항
25	DBM-026	데이터베이스의 주요 파일 보호 등을 위한 DB 계정의 umask 설정	**개선**	DBM-026	데이터베이스 구동 계정의 umask 설정 미흡	• **평가항목명 변경** • **평가대상 확대** – Tibero 추가 • **판단기준, 판단방법 양식 변경** – (기존) 모든 평가대상의 판단기준, 판단방법 동일 ➜ (변경) 평가대상별로 각각 판단기준, 판단방법 분리
26	DBM-028	인가되지 않은 Object Owner가 존재 여부	**개선**	DBM-028	업무상 불필요한 데이터베이스 Object 존재	• **평가항목명 변경** • **평가대상 확대** – Tibero 추가 • **판단기준, 판단방법 양식 변경** – (기존) 모든 평가대상의 판단기준, 판단방법 동일 ➜ (변경) 평가대상별로 각각 판단기준, 판단방법 분리
27	DBM-029	데이터베이스의 자원 제한 기능 설정 여부	**개선**	DBM-029	데이터베이스의 자원 사용 제한 설정 미흡	• **평가항목명 변경** • **판단기준, 판단방법 양식 변경** – (기존) 모든 평가대상의 판단기준, 판단방법 동일 ➜ (변경) 평가대상별로 각각 판단기준, 판단방법 분리

【 (현행) 제2021-1호 】				【 (개정) 제2022-1호 】		
구분	평가항목ID	평가항목	개정사항	평가항목ID	평가항목	주요 개정사항
28	DBM-030	데이터베이스 관리자 계정에 Audit Table이 속해 있는 여부	**개선**	DBM-030	Audit Table에 대한 접근 제어 미흡	• **평가항목명 변경** • **평가대상 확대** - Tibero 추가 • **판단기준, 판단방법 양식 변경** - (기존) 모든 평가대상의 판단기준, 판단방법 동일 ➜ (변경) 평가대상별로 각각 판단기준, 판단방법 분리
29	DBM-031	Windows 인증 모드 사용	**개선**	DBM-031	SA 계정에 대한 보안설정 미흡	• **평가항목명 변경** • **판단기준 변경** - (기존) 혼합인증 모드를 사용하고, 'sa' 계정에 대한 유추 가능한 비밀번호를 설정한 경우 취약 ➜ (변경) 'sa' 계정이 활성화되어 있고 보안 설정이 적절하게 이루어지지 않았을 경우 취약 • **판단기준, 판단방법 양식 변경** - (기존) 모든 평가대상의 판단기준, 판단방법 동일 ➜ (변경) 평가대상별로 각각 판단기준, 판단방법 분리

【 (현행) 제2021-1호 】				【 (개정) 제2022-1호 】		
구분	평가항목ID	평가항목	개정사항	평가항목ID	평가항목	주요 개정사항
30	DBM-032	로그인 시 암호화통신 적용 여부	**개선**	DBM-032	데이터베이스 접속 시 통신 구간에 비밀번호 평문 노출	• **평가항목명 변경** • **판단기준, 판단방법 양식 변경** - (기존) 모든 평가대상의 판단기준, 판단방법 동일 ➜ (변경) 평가대상별로 각각 판단기준, 판단방법 분리

■ **네트워크 장비 분야 개정사항**

● 전체 44개 항목 중 **4개 항목 개정**

【 (현행) 제2021-1호 】				【 (개정) 제2022-1호 】		
구분	평가항목ID	평가항목	개정사항	평가항목ID	평가항목	주요 개정사항
1	NET-001	네트워크 장비 설정 백업 여부	**개선**	-	-	• **판단기준 변경** - (기존) 네트워크 운영체제 및 설정내용 등을 정기적으로 백업하고 있지 않을 경우 취약 ➜ (변경) 네트워크 장비의 설정을 정기적으로 백업하고 있지 않을 경우 취약
2	NET-032	로깅 Timezone 설정 여부	**삭제**	-	-	• **평가항목 삭제** - 타 점검항목에서 NTP 서버 동기화 설정에 대한 점검을 하고 있고, 로그에 기록되는 시간을 한국표준시(KST)로 강제하는 것은 현 운영환경과 맞지 않는 것으로 판단되어 평가항목 삭제
3	NET-040	스푸핑방지 필터 설정	**개선**	-	-	• **판단기준 변경** - 네트워크 장비 상단에 보안장비를 설치하여 스푸핑방지 필터를 적용하고 있는 경우 양호로 판단하도록 예외 사항 추가
4	NET-047	서비스 거부 공격(DDoS) 공격 차단 필터링 설정	**개선**	NET-047	서비스 거부 공격(DDoS) 차단 필터링 설정	• **판단항목명 변경** • **판단기준 문구 개선** - 네트워크 장비 상단에 DDoS 대응장비가 운영되어 공격이 차단되는 경우에 대한 예외 사항 문구 개선

■ 웹 애플리케이션 분야 개정사항

- 전체 51개 항목 중 **13개 항목 개정**

【 (현행) 제2021-1호 】				【 (개정) 제2022-1호 】		
구분	평가항목ID	평가항목	개정사항	평가항목ID	평가항목	주요 개정사항
1	WEB-FIN-001	[전자금융] 거래 인증수단 검증 오류 (지식기반)	**개선**	WEB-FIN-001	[전자금융] 거래 인증수단 검증 오류	• **평가항목명 변경** • **상세설명 변경**
2	WEB-FIN-002	[전자금융] 거래 인증수단 검증 오류 (소지기반)	**통합**	WEB-FIN-001	[전자금융] 거래 인증수단 검증 오류	• **평가항목명 통합(삭제)**
3	WEB-FIN-024	[전자금융] 거래 인증수단 검증 오류 (생체기반)	**통합**	WEB-FIN-001	[전자금융] 거래 인증수단 검증 오류	• **평가항목명 통합(삭제)**
4	WEB-FIN-004	[전자금융] 거래정보 무결성 검증	**개선**	-	-	• **상세설명 변경**
5	WEB-FIN-008	[전자금융] 거래시 비밀번호 오류횟수 제한기능 제공 여부	**통합**	WEB-SER-032	인증 오류 횟수 제한기능 제공 여부	• **평가항목명 통합(삭제)**
6	WEB-SER-032	비밀번호 오류횟수 제한기능 제공 여부	**개선**	WEB-SER-032	인증 오류 횟수 제한기능 제공 여부	• **평가항목명 변경** • **상세설명 변경**

【 (현행) 제2021-1호 】				【 (개정) 제2022-1호 】		
구분	평가항목ID	평가항목	개정사항	평가항목ID	평가항목	주요 개정사항
7	WEB-SER-004	이용자 인증정보 재사용	**개선**	-	-	• **상세설명 변경**
8	WEB-SER-006	유추가능한 인증정보 이용(비밀번호)	**개선**	WEB-SER-006	유추가능한 인증정보 이용	• **평가항목명 변경** • **상세설명 변경**
9	WEB-SER-021	자동화공격	**개선**	-	-	• **상세설명 변경**
10	WEB-SER-035	취약한 HTTPS 암호 알고리즘 이용	**개선**	-	-	• **상세설명 변경**
11	WEB-SER-048	세션정보 재사용	**개선**	-	-	• **상세설명 변경**
12	-	-	**신규**	WEB-FIN-027	[전자금융] 접근매체 발급 시 실명확인 수행 여부	• **신규 평가항목**
13	-	-	**신규**	WEB-SER-049	인증수단 소유자 검증 여부	• **신규 평가항목**

■ **모바일 애플리케이션 분야 개정사항**

● 전체 48개 항목 중 **14개 항목 개정**

【 (현행) 제2021-1호 】				【 (개정) 제2022-1호 】		
구분	평가항목ID	평가항목	개정사항	평가항목ID	평가항목	주요 개정사항
1	MOB-FIN-001	[전자금융] 거래 인증수단 검증 오류 (지식기반)	**개선**	MOB-FIN-001	[전자금융] 거래 인증수단 검증 오류	• **평가항목명 변경** • **상세설명 변경**
2	MOB-FIN-002	[전자금융] 거래 인증수단 검증 오류 (소지기반)	**통합**	MOB-FIN-001	[전자금융] 거래 인증수단 검증 오류	• **평가항목 통합(삭제)**
3	MOB-FIN-024	[전자금융] 거래 인증수단 검증 오류 (생체기반)	**통합**	MOB-FIN-001	[전자금융] 거래 인증수단 검증 오류	• **평가항목 통합(삭제)**
4	MOB-FIN-004	[전자금융] 거래정보 무결성 검증	**개선**	-	-	• **상세설명 변경**
5	MOB-FIN-008	[전자금융] 거래시 비밀번호 오류횟수 제한기능 제공 여부	**통합**	MOB-SER-032	인증 오류 횟수 제한기능 제공 여부	• **평가항목 통합(삭제)**
6	MOB-SER-032	비밀번호 오류횟수 제한기능 제공 여부	**개선**	MOB-SER-032	인증 오류 횟수 제한기능 제공 여부	• **평가항목명 변경** • **상세설명 변경**
7	MOB-SER-004	이용자 인증정보 재사용	**개선**	-	-	• **상세설명 변경**
8	MOB-SER-006	유추가능한 인증정보 이용(비밀번호)	**개선**	MOB-SER-006	유추가능한 인증정보 이용	• **평가항목명 변경** • **상세설명 변경**

【 (현행) 제2021-1호 】				【 (개정) 제2022-1호 】		
구분	평가항목ID	평가항목	개정사항	평가항목ID	평가항목	주요 개정사항
9	MOB-SER-048	세션정보 재사용	**개선**	-	-	• **상세설명 변경**
10	MOB-FIN-020	[전자금융] 소스코드 난독화 적용 여부	**개선**	-	-	• **상세설명 변경**
11	MOB-FIN-021	[전자금융] 디버깅 탐지기능 적용 여부	**개선**	-	-	• **상세설명 변경**
12	-	-	**신규**	MOB-SER-021	자동화공격	• **신규 평가항목**
13	-	-	**신규**	MOB-FIN-027	[전자금융] 접근매체 발급 시 실명확인 수행 여부	• **신규 평가항목**
14	-	-	**신규**	MOB-SER-049	인증수단 소유자 검증 여부	• **신규 평가항목**

■ HTS 애플리케이션 분야 개정사항

● 전체 32개 항목 중 **24개 항목 개정**

【 (현행) 제2021-1호 】				【 (개정) 제2022-1호 】		
구분	평가항목ID	평가항목	개정사항	평가항목ID	평가항목	주요 개정사항
1	HTS-FIN-001	[전자금융] 거래 인증수단 검증 오류 (지식기반)	**개선**	HTS-FIN-001	[전자금융] 거래 인증수단 검증 오류	• **평가항목명 변경** • **상세설명 변경**
2	HTS-FIN-002	[전자금융] 거래 인증수단 검증 오류 (소지기반)	**통합**	HTS-FIN-001	[전자금융] 거래 인증수단 검증 오류	• **평가항목 통합(삭제)**
3	HTS-FIN-004	[전자금융] 거래정보 무결성 검증	**개선**	-	-	• **상세설명 변경**
4	HTS-FIN-023	[전자금융] 중요파일 실행파일 보호(Packing) 기술 적용 여부	**통합**	HTS-FIN-020	[전자금융] 소스코드 난독화 적용 여부	• **평가항목 통합(삭제)** - 기존에 실행파일보호(Packing) 적용 여부만 점검하였던 것을, 좀 더 강화된 애플리케이션 보호 수단(난독화, 디버깅 탐지기능)을 적용하도록 개선 * [HTS-FIN-023]에서 코드분석 방지 기능을 [HTS-FIN-020]로 통합 * [HTS-FIN-023]에서 동적분석 방지 기능을 [HTS-FIN-021]로 통합
5	HTS-FIN-021	[전자금융] 디버깅 탐지기능 적용 여부				

【 (현행) 제2021-1호 】				【 (개정) 제2022-1호 】		
구분	평가항목ID	평가항목	개정사항	평가항목ID	평가항목	주요 개정사항
6	-	-	**신규**	HTS-FIN-020	[전자금융] 소스코드 난독화 적용 여부	• **신규 평가항목**
7	-	-	**신규**	HTS-FIN-021	[전자금융] 디버깅 탐지 기능 적용 여부	• **신규 평가항목**
8	-	-	**신규**	HTS-FIN-027	[전자금융] 접근매체 발급 시 실명확인 수행 여부	• **신규 평가항목**
9	-	-	**신규**	HTS-SER-001	SQL Injection	• **신규 평가항목**
10	-	-	**신규**	HTS-SER-002	악성파일 업로드	• **신규 평가항목**
11	HTS-SER-004	이용자 인증정보 재사용	**개선**	-	-	• **상세설명 변경**
12	-	-	**신규**	HTS-SER-005	고정된 인증정보 이용	• **신규 평가항목**
13	HTS-SER-006	유추가능한 인증정보 이용 (비밀번호)	**개선**	HTS-SER-006	유추가능한 인증정보 이용	• **평가항목명 변경** • **상세설명 변경**

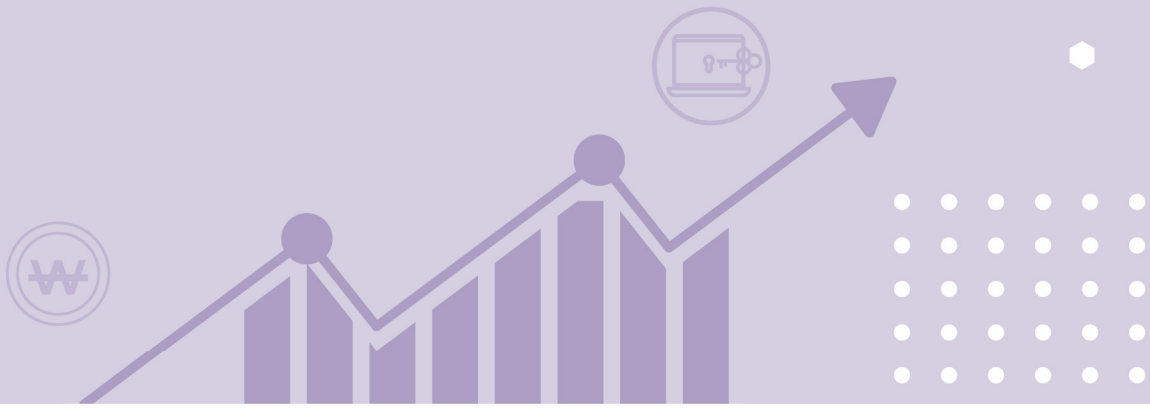
【 (현행) 제2021-1호 】				【 (개정) 제2022-1호 】		
구분	평가항목ID	평가항목	개정사항	평가항목ID	평가항목	주요 개정사항
14	-	-	**신규**	HTS-SER-010	파일 다운로드	• **신규 평가항목**
15	-	-	**신규**	HTS-SER-011	외부사이트에 의한 시스템 운영정보 노출 여부	• **신규 평가항목**
16	-	-	**신규**	HTS-SER-014	운영체제 명령실행	• **신규 평가항목**
17	-	-	**신규**	HTS-SER-015	XML 외부객체 공격 (XXE)	• **신규 평가항목**
18	-	-	**신규**	HTS-SER-020	화면 내 중요정보 평문노출 여부	• **신규 평가항목**
19	-	-	**신규**	HTS-SER-021	자동화공격	• **신규 평가항목**
20	-	-	**신규**	HTS-SER-022	버퍼오버플로우(Buffer Over flow Attack)	• **신규 평가항목**
21	-	-	**신규**	HTS-SER-023	포맷스트링 (Format String Attack)	• **신규 평가항목**
22	HTS-FIN-008	[전자금융] 거래시 비밀번호 오류횟수 제한기능 제공 여부	**통합**	HTS-SER-032	인증 오류 횟수 제한기능 제공 여부	• **평가항목 통합(삭제)**

【 (현행) 제2021-1호 】				【 (개정) 제2022-1호 】		
구분	평가항목ID	평가항목	개정사항	평가항목ID	평가항목	주요 개정사항
23	HTS-SER-032	비밀번호 오류횟수 제한기능 제공 여부	**개선**	HTS-SER-032	인증 오류 횟수 제한기능 제공 여부	• **평가항목명 변경** • **상세설명 변경**
24	HTS-SER-048	세션정보 재사용	**개선**	-	-	• **상세설명 변경**

[참고 3]

전자금융기반시설 보안 취약점 평가기준

(제2022-1호)



【정보보호관리체계】

■ **평가기준**

평가 항목ID	통제구분	평가항목	위험도	[근거조항] 전자금융감독규정 (금융위원회고시 제2018-36호, 2018. 12. 21) 전자금융감독규정시행세칙 (금융감독원세칙, 2021. 2. 25)
FISM-001	1.1 정보보호 계획	정보보안 관련법규 위반에 관한 제재기준 및 절차수립 및 운영 여부	5	○ **(전자금융감독규정)** - 제8조(인력, 조직 및 예산)제1항제5호 ① 금융회사 또는 전자금융업자는 인력 및 조직의 운용에 관하여 다음 각 호의 사항을 준수하여야 한다. 〈개정 2013. 12. 3.〉 5. 최고경영자는 임직원이 정보보안 관련법규를 위반할 경우 그 제재에 관한 세부기준 및 절차를 마련하여 운영할 것 〈신설 2013. 12. 3.〉
FISM-002	1.1 정보보호 계획	정보기술(IT)부문계획 매년 수립 및 운용 여부	5	○ **(전자금융감독규정)** - 제19조(정보기술부문 계획서 제출 절차 등)제19조제1항 ① 시행령 제11조의2에 따라 금융위원회에 정보기술부문 계획서를 제출해야 하는 금융회사 또는 전자금융업자는 현실적이고 실현 가능한 장·단기 정보기술부문 계획을 매년 수립·운용하여야 한다. 〈개정 2013. 12. 3.〉
FISM-003	2.1 조직 및 인력 구성	정보처리시스템 관련 전담조직 운영 여부	5	○ **(전자금융감독규정)** - 제8조(인력, 조직 및 예산)제1항제1호 ① 금융회사 또는 전자금융업자는 인력 및 조직의 운용에 관하여 다음 각 호의 사항을 준수하여야 한다. 〈개정 2013. 12. 3.〉 1. 정보처리시스템 및 전자금융업무 관련 전담 조직을 확보할 것

평가 항목ID	통제구분	평가항목	위험도	[근거조항] 전자금융감독규정 (금융위원회고시 제2018-36호, 2018. 12. 21) 전자금융감독규정시행세칙 (금융감독원세칙, 2021. 2. 25)
FISM-004	2.1 조직 및 인력 구성	전자금융업무 관련 전담조직 운영 여부	5	○ **(전자금융감독규정)** - 제8조(인력, 조직 및 예산)제1항제1호 ① 금융회사 또는 전자금융업자는 인력 및 조직의 운용에 관하여 다음 각 호의 사항을 준수하여야 한다. 〈개정 2013. 12. 3.〉 1. 정보처리시스템 및 전자금융업무 관련 전담 조직을 확보할 것
FISM-005	2.1 조직 및 인력 구성	IT 아웃소싱(이하 'IT자회사'포함) 통제/관리 조직(인력포함) 운영 여부	5	○ **(전자금융감독규정)** - 제8조(인력, 조직 및 예산)제1항제2호 ① 금융회사 또는 전자금융업자는 인력 및 조직의 운용에 관하여 다음 각 호의 사항을 준수하여야 한다.〈개정 2013. 12. 3.〉 2. 외부주문등에 관한 계약을 체결하는 때에는 계약내용의 적정성을 검토하고 자체적으로 통제가 가능하도록 회사내부에 조직과 인력을 갖출 것
FISM-010	2.3 정보보호최고 책임자 지정 및 업무	정보보호최고책임자(CISO) 지정 여부	5	○ **(전자금융감독규정)** - 제6조의2(정보보호최고책임자의 지정대상)제1항,제2항 ① 시행령 제11조의3제1항 후단에서 "금융위원회가 정하여 고시하는 상시 종업원 수의 산정방식"이란 「소득세법」에 따른 원천징수의무자가 근로소득세를 원천징수한 자를 말한다. ② 시행령 〈별표 1〉의제3호나목 단서에서 "금융위원회가 정하여 고시하는 산정방식"이란 「소득세법」에 따른 원천징수의무자가 근로소득세를 원천징수한 자를 말한다.
FISM-011	2.3 정보보호최고 책임자 지정 및 업무	정기적으로 수행되는 임직원 정보보안 관련법규 준수여부 점검결과에 대한 임원(정보보호최고 책임자, 최고경영자) 보고 여부	5	○ **(전자금융감독규정)** - 제8조(인력, 조직 및 예산)제1항제4호 ① 금융회사 또는 전자금융업자는 인력 및 조직의 운용에 관하여 다음 각 호의 사항을 준수하여야 한다. 〈개정 2013. 12. 3.〉

평가 항목ID	통제구분	평가항목	위험도	[근거조항] 전자금융감독규정 (금융위원회고시 제2018-36호, 2018. 12. 21) 전자금융감독규정시행세칙 (금융감독원세칙, 2021. 2. 25)
				4. 정보보호최고책임자는 임직원이 정보보안 관련법규가 준수되고 있는지 정기적으로 점검하고 그 점검결과를 최고경영자에게 보고할 것 〈신설 2013. 12. 3.〉
FISM-012	2.3 정보보호최고책임자 지정 및 업무	정보보호 관련 사항을 심의·의결하는 정보보호 위원회 설치 및 운영 여부	5	○ **(전자금융감독규정)** - 제8조의2(정보보호위원회 운영)제1항 ① 금융회사 또는 전자금융업자는 중요 정보보호에 관한 사항을 심의·의결하는 정보보호위원회를 설치 운영하여야 한다.
FISM-013	2.3 정보보호최고책임자 지정 및 업무	정보보보호위원회 구성의 적정성	5	○ **(전자금융감독규정)** - 제8조의2(정보보호위원회 운영)제2항 ② 정보보호위원회의 장은 정보보호최고책임자로 하며, 위원은 정보보호업무 관련 부서장, 전산운영 및 개발 관련 부서장, 준법업무 관련 부서의 장 등으로 구성한다.
FISM-014	2.3 정보보호최고책임자 지정 및 업무	정보보호위원회 심의·의결 사항에 관한 적정성	5	○ **(전자금융감독규정)** - 제8조의2(정보보호위원회 운영)제3항 ③ 정보보호위원회는 다음 각 호의 사항을 심의·의결한다. 1. 법 제21조제4항에 따른 정보기술부문 계획서에 관한 사항 2. 법 제21조의2제4항제1호에 관한 사항 〈개정 2015. 6. 24.〉 3. 법 제21조의3에서 정한 취약점 분석·평가 결과 및 보완조치의 이행계획에 관한 사항 4. 전산보안사고 및 전산보안관련 규정 위반자의 처리에 관한 사항 5. 기타 정보보호위원회의 장이 정보보안업무 수행에 필요하다고 정한 사항

평가 항목ID	통제구분	평가항목	위험도	[근거조항] 전자금융감독규정 (금융위원회고시 제2018-36호, 2018. 12. 21) 전자금융감독규정시행세칙 (금융감독원세칙, 2021. 2. 25)
FISM-015	2.3 정보보호최고책임자 지정 및 업무	정보보호위원회 심의·의결 사항에 관한 임원(정보보호최고책임자, 최고경영자) 보고 여부	5	○ **(전자금융감독규정)** - 제8조의2(정보보호위원회 운영)제4항 ④ 정보보호최고책임자는 정보보호위원회 심의·의결사항을 최고경영자에게 보고하여야 한다.
FISM-016	2.3 정보보호최고책임자 지정 및 업무	정보보안점검의 날 지정 여부	5	○ **(전자금융감독규정)** - 제37조의5(정보보호최고책임자의 업무) 정보보호최고책임자는 정보보안점검의 날을 지정하고, 임직원이 금융감독원장이 정하는 정보보안 점검항목을 준수했는지 여부를 매월 점검하고, 그 점검 결과 및 보완 계획을 최고경영자에게 보고하여야 한다. ○ **(전자금융감독규정시행세칙)** - 제12조(정보기술부문 사고보고)제1항,제2항,제3항,제4항 ① 금융회사 및 전자금융업자는 규정 제73조에 따른 정보기술부문 및 전자금융사고가 발생한 경우 별지 제2호서식 별첨1에 따라 즉시 보고하여야 한다. 다만, 규정 제73조제1항제4호의 사고 중 사고금액이 3억원 미만인 사고의 경우 매월 발생한 사고를 익월 15일까지 별지 제2호서식 별첨2에 따라 일괄 보고할 수 있다. ② 제1항에 따른 사고보고는 최초보고, 중간보고 및 종결보고로 구분한다. 1. 최초보고 : 사고를 인지 또는 발견한 즉시 감독원의 전자금융사고 대응시스템(Electronic Financial Accident Response System : EFARS), 서면, 팩시밀리 또는 전화로 보고하되, 전화로 보고한 경우에는 즉시 전자금융사고 대응시스템, 서면 또는 팩시밀리로 보고한다. 2. 중간보고 : 제1호의 즉시보고 후 사고내용 보완할 필요가 있는 경우에는 즉시 중간보고를 하여야 하며, 제3호의 조치완료 시까지 2월 이상 소요될 경우에는

평가 항목ID	통제구분	평가항목	위험도	[근거조항] 전자금융감독규정 (금융위원회고시 제2018-36호, 2018. 12. 21) 전자금융감독규정시행세칙 (금융감독원세칙, 2021. 2. 25)
				인지·발견일로부터 2월 이내 및 종결 시까지 매 6월마다 제1호의 방법에 따라 보고한다. 다만, 즉시보고 후 조치완료 시까지 2월 미만이 소요될 경우에는 중간 보고를 생략할 수 있다. 3. 종결보고 : 사고금액에 대한 배상조치가 완료되거나 사고조치 등이 완료되어 정상적인 업무를 수행하게 된 때 제1호의 방법에 따라 보고한다. 다만, 최초보고 시 조치가 이미 완료된 경우에는 종결보고를 생략할 수 있다. ③ 감독원장은 금융회사 및 전자금융업자 정보기술부문의 사고보고 등을 전담할 비상연락 담당자를 회사별로 지정할 수 있다. ④ 금융회사 및 전자금융업자는 비상연락 담당자가 제3항에 따라 지정되거나 변경된 경우에는 제2항제1호에서 정한 보고방법에 따라 감독원장에게 즉시 보고하여야 한다.
FISM-017	2.3 정보보호최고책임자 지정 및 업무	정보보안 점검의 날 금융감독원장이 정한 정보보호 점검항목에 대한 점검 이행(매월) 여부	5	○ **(전자금융감독규정)** - 제37조의5(정보보호최고책임자의 업무) 정보보호최고책임자는 정보보안점검의 날을 지정하고, 임직원이 금융감독원장이 정하는 정보보안 점검항목을 준수했는지 여부를 매월 점검하고, 그 점검 결과 및 보완 계획을 최고경영자에게 보고하여야 한다. ○ **(전자금융감독규정시행세칙)** - 제7조의3(정보보호최고책임자의 업무) 규정 제37조의5에 따라 감독원장이 정하는 정보보안 점검항목은 별표 3-2와 같다.
FISM-018	2.3 정보보호최고책임자 지정 및 업무	정보보안 점검의 날 점검결과에 관한 최고경영자에게 보고 여부	5	○ **(전자금융감독규정)** - 제37조의5(정보보호최고책임자의 업무) 정보보호최고책임자는 정보보안점검의 날을 지정하고, 임직원이 금융감독원장이 정하는 정보보안 점검항목을 준수했는지 여부를 매월 점검하고, 그 점검 결과

평가 항목ID	통제구분	평가항목	위험도	[근거조항] 전자금융감독규정 (금융위원회고시 제2018-36호, 2018. 12. 21) 전자금융감독규정시행세칙 (금융감독원세칙, 2021. 2. 25)
				및 보완 계획을 최고경영자에게 보고하여야 한다. ○ **(전자금융감독규정시행세칙)** - 제7조의3(정보보호최고책임자의 업무) 규정 제37조의5에 따라 감독원장이 정하는 정보보안 점검항목은 별표 3-2와 같다.
FISM-019	3.1 정보보호 교육 및 훈련	IT인력 및 정보보호인력에 대한 연수 프로그램 운영 여부	5	○ **(전자금융감독규정)** - 제8조(인력, 조직 및 예산)제1항제3호 ① 금융회사 또는 전자금융업자는 인력 및 조직의 운용에 관하여 다음 각 호의 사항을 준수하여야 한다. 〈개정 2013. 12. 3.〉 3. 전산인력의 자질향상 및 예비요원 양성을 위한 교육 및 연수프로그램을 운영할 것
FISM-020	3.1 정보보호 교육 및 훈련	정보보호최고책임자는 임직원의 정보보호역량 강화를 위하여 필요한 교육프로그램을 개발하고, 전자금융감독규정에서 정한 기준에 따른 주기(매년)적 교육 시행 여부	5	○ **(전자금융감독규정)** - 제19조의2(정보보호 교육계획의 수립 시행)제19조의2제1항 ① 정보보호최고책임자는 임직원의 정보보호역량 강화를 위하여 필요한 교육프로그램을 개발하고, 다음 각 호의 기준에 따라 매년 교육계획을 수립·시행하여야 한다. 1. 임원 : 3시간 이상(단, 정보보호최고책임자는 6시간 이상) 2. 일반직원 : 6시간 이상 3. 정보기술부문업무 담당 직원 : 9시간 이상 4. 정보보호업무 담당 직원 : 12시간 이상

평가 항목ID	통제구분	평가항목	위험도	[근거조항] 전자금융감독규정 (금융위원회고시 제2018-36호, 2018. 12. 21) 전자금융감독규정시행세칙 (금융감독원세칙, 2021. 2. 25)
FISM-021	3.1 정보보호 교육 및 훈련	정보보호 교육 실시 이후, 대상 임직원에 대한 평가 수행 여부	5	○ **(전자금융감독규정)** - 제19조의2(정보보호 교육계획의 수립 시행)제2항 ② 최고경영자는 정보보호교육을 실시한 이후 대상 임직원에 대해 평가를 실시하여야 한다.
FISM-022	4.1 전산센터 건물	건물 출입통제보안대책의 수립/운용 여부	5	○ **(전자금융감독규정)** - 제9조(건물에 관한 사항)제1호 금융회사 또는 전자금융업자는 전산실이 위치한 건물에 관하여 다음 각 호의 사항을 준수하여야 한다. 〈개정 2013. 12. 3.〉 1. 건물 출입구는 경비원에 의하여 통제하고 출입통제 보안대책을 수립·운용할 것
FISM-023	4.1 전산센터 건물	건물 출입구의 경비원 통제 여부	5	○ **(전자금융감독규정)** - 제9조(건물에 관한 사항)제1호 금융회사 또는 전자금융업자는 전산실이 위치한 건물에 관하여 다음 각 호의 사항을 준수하여야 한다. 〈개정 2013. 12. 3.〉 1. 건물 출입구는 경비원에 의하여 통제하고 출입통제 보안대책을 수립·운용할 것
FISM-024	4.1 전산센터 건물	비상시 대피를 위한 비상계단 설치 여부	5	○ **(전자금융감독규정)** - 제9조(건물에 관한 사항)제2호 금융회사 또는 전자금융업자는 전산실이 위치한 건물에 관하여 다음 각 호의 사항을 준수하여야 한다. 〈개정 2013. 12. 3.〉 2. 비상시 대피를 위한 비상계단 및 정전대비 유도등을 설치할 것 〈개정 2013. 12. 3.〉

평가 항목ID	통제구분	평가항목	위험도	[근거조항] 전자금융감독규정 (금융위원회고시 제2018-36호, 2018. 12. 21) 전자금융감독규정시행세칙 (금융감독원세칙, 2021. 2. 25)
FISM-025	4.1 전산센터 건물	정전대비 유도등 설치 여부	5	○ **(전자금융감독규정)** - 제9조(건물에 관한 사항)제2호 금융회사 또는 전자금융업자는 전산실이 위치한 건물에 관하여 다음 각 호의 사항을 준수하여야 한다. 〈개정 2013. 12. 3.〉 2. 비상시 대피를 위한 비상계단 및 정전대비 유도등을 설치할 것 〈개정 2013. 12. 3.〉
FISM-026	4.1 전산센터 건물	피뢰설비 설치 여부	5	○ **(전자금융감독규정)** - 제9조(건물에 관한 사항)제3호 금융회사 또는 전자금융업자는 전산실이 위치한 건물에 관하여 다음 각 호의 사항을 준수하여야 한다. 〈개정 2013. 12. 3.〉 3. 번개, 과전류 등 고전압으로 인한 전산장비 및 통신장비 등의 피해 예방을 위하여 피뢰설비를 갖출 것
FISM-027	4.1 전산센터 건물	적재하중 안전대책 수립 및 운용 여부	5	○ **(전자금융감독규정)** - 제9조(건물에 관한 사항)제4호 금융회사 또는 전자금융업자는 전산실이 위치한 건물에 관하여 다음 각 호의 사항을 준수하여야 한다. 〈개정 2013. 12. 3.〉 4. 서버, 스토리지(Storage) 등 전산장비 및 통신장비 등의 중량을 감안한 적재하중 안전대책을 수립·운용할 것
FISM-028	4.1 전산센터 건물	소화기 및 자동소화설비 등 설치 여부	5	○ **(전자금융감독규정)** - 제9조(건물에 관한 사항)제5호 금융회사 또는 전자금융업자는 전산실이 위치한 건물에 관하여 다음 각 호의 사항을

평가 항목ID	통제구분	평가항목	위험도	[근거조항] 전자금융감독규정 (금융위원회고시 제2018-36호, 2018. 12. 21) 전자금융감독규정시행세칙 (금융감독원세칙, 2021. 2. 25)
				준수하여야 한다. 〈개정 2013. 12. 3.〉 5. 화재발생 시 조기진압을 위한 소화기 및 자동소화설비 등을 갖추고, 화재전파 방지를 위한 배연설비설치 등 화재예방 안전대책을 수립·운용할 것
FISM-029	4.1 전산센터 건물	배연설비 설치 등 화재예방 안전대책 수립 및 운용 여부	5	○ **(전자금융감독규정)** - 제9조(건물에 관한 사항)제5호 금융회사 또는 전자금융업자는 전산실이 위치한 건물에 관하여 다음 각 호의 사항을 준수하여야 한다. 〈개정 2013. 12. 3.〉 5. 화재발생 시 조기진압을 위한 소화기 및 자동소화설비 등을 갖추고, 화재전파 방지를 위한 배연설비설치 등 화재예방 안전대책을 수립·운용할 것
FISM-030	4.2 전산센터 설비	전산센터가 위치한 건물에 대해 화재 발생, 상습침수 및 진동피해발생 등 물리적, 환경적 위험지역 제외 및 건물 구조의 안정성 확보 여부	5	○ **(전자금융감독규정)** - 제9조(건물에 관한 사항)제6호 금융회사 또는 전자금융업자는 전산실이 위치한 건물에 관하여 다음 각 호의 사항을 준수하여야 한다. 〈개정 2013. 12. 3.〉 6. 화재발생 위험이 높은 지역, 상습 침수지역 및 진동피해 발생지역 등 외부환경에 의하여 전산장비 등이 영향을 받을 수 있는 지역은 제외할 것
FISM-031	4.2 전산센터 설비	주요설비시설 출입통제장치 설치 여부	5	○ **(전자금융감독규정)** - 제10조(전원, 공조 등 설비에 관한 사항)제1호 금융회사 또는 전자금융업자는 전산실이 위치한 건물의 전원, 공조 등 설비에 관하여 다음 각 호의 사항을 준수하여야 한다. 〈개정 2013. 12. 3.〉 1. 전원실, 공조실 등 주요 설비시설에 자물쇠 등 출입통제장치를 설치할 것

평가 항목ID	통제구분	평가항목	위험도	[근거조항] 전자금융감독규정 (금융위원회고시 제2018-36호, 2018. 12. 21) 전자금융감독규정시행세칙 (금융감독원세칙, 2021. 2. 25)
FISM-032	4.2 전산센터 설비	전원, 공조, 방재, 방범 설비에 대한 감시제어 시스템 설치 여부	5	○ **(전자금융감독규정)** - 제10조(전원, 공조 등 설비에 관한 사항)제2호 금융회사 또는 전자금융업자는 전산실이 위치한 건물의 전원, 공조 등 설비에 관하여 다음 각 호의 사항을 준수하여야 한다. 〈개정 2013. 12. 3.〉 2. 전원, 공조, 방재 및 방범 설비에 대한 적절한 감시제어시스템을 갖출 것
FISM-033	4.2 전산센터 설비	자가발전설비 설치 여부	5	○ **(전자금융감독규정)** - 제10조(전원, 공조 등 설비에 관한 사항)제3호 금융회사 또는 전자금융업자는 전산실이 위치한 건물의 전원, 공조 등 설비에 관하여 다음 각 호의 사항을 준수하여야 한다. 〈개정 2013. 12. 3.〉 3. 전산실의 전력공급 중단에 대비하여 자가발전설비를 갖출 것
FISM-034	4.2 전산센터 설비	무정전전원장치 설치 여부	5	○ **(전자금융감독규정)** - 제10조(전원, 공조 등 설비에 관한 사항)제4호 금융회사 또는 전자금융업자는 전산실이 위치한 건물의 전원, 공조 등 설비에 관하여 다음 각 호의 사항을 준수하여야 한다.〈개정 2013. 12. 3.〉 4. 전력공급 장애 시 전력선 대체가 가능하도록 복수회선을 설치하고 전력공급의 연속성 유지를 위한 무정전전원장치(Uninterruptible Power Supply : UPS)를 갖출 것
FISM-035	4.2 전산센터 설비	전력선 대체를 위한 복수회선 설치 여부	5	○ **(전자금융감독규정)** - 제10조(전원, 공조 등 설비에 관한 사항)제4호 금융회사 또는 전자금융업자는 전산실이 위치한 건물의 전원, 공조 등 설비에 관하여 다음 각 호의 사항을 준수하여야 한다.〈개정 2013. 12. 3.〉

평가 항목ID	통제구분	평가항목	위험도	[근거조항] 전자금융감독규정 (금융위원회고시 제2018-36호, 2018. 12. 21) 전자금융감독규정시행세칙 (금융감독원세칙, 2021. 2. 25)
				4. 전력공급 장애 시 전력선 대체가 가능하도록 복수회선을 설치하고 전력공급의 연속성 유지를 위한 무정전전원장치(Uninterruptible Power Supply : UPS)를 갖출 것 〈개정 2013. 12. 3.〉
FISM-036	4.2 전산센터 설비	과전류차단기, 누전경보기 등 설치 여부	5	○ **(전자금융감독규정)** - 제10조(전원, 공조 등 설비에 관한 사항)제5호 금융회사 또는 전자금융업자는 전산실이 위치한 건물의 전원, 공조 등 설비에 관하여 다음 각 호의 사항을 준수하여야 한다. 〈개정 2013. 12. 3.〉 5. 과전류, 누전에 의한 장애 방지를 위하여 과전류차단기, 누전경보기 등을 설치하고 일정한 전압 및 주파수 유지를 위한 정전압정주파수장치(Constant Voltage Constant Frequency : CVCF)를 갖출 것
FISM-037	4.2 전산센터 설비	정전압정주파수장치 설치 여부	5	○ **(전자금융감독규정)** - 제10조(전원, 공조 등 설비에 관한 사항)제5호 금융회사 또는 전자금융업자는 전산실이 위치한 건물의 전원, 공조 등 설비에 관하여 다음 각 호의 사항을 준수하여야 한다. 〈개정 2013. 12. 3.〉 5. 과전류, 누전에 의한 장애 방지를 위하여 과전류차단기, 누전경보기 등을 설치하고 일정한 전압 및 주파수 유지를 위한 정전압정주파수장치(Constant Voltage Constant Frequency : CVCF)를 갖출 것
FISM-038	4.2 전산센터 설비	전원 및 공조설비는 부하가 큰 설비 부분과 분리 설치 여부	5	○ **(전자금융감독규정)** - 제10조(전원, 공조 등 설비에 관한 사항)제6호 금융회사 또는 전자금융업자는 전산실이 위치한 건물의 전원, 공조 등 설비에 관하여 다음 각 호의 사항을 준수하여야 한다. 〈개정 2013. 12. 3.〉

평가 항목ID	통제구분	평가항목	위험도	[근거조항] 전자금융감독규정 (금융위원회고시 제2018-36호, 2018. 12. 21) 전자금융감독규정시행세칙 (금융감독원세칙, 2021. 2. 25)
				6. 전산실에 공급되는 전원 및 공조 설비는 부하가 큰 설비부분과 분리하여 설치하고 공조 설비 상태 점검을 위한 압력계, 온도계 등을 갖출 것
FISM-039	4.2 전산센터 설비	공조설비 상태 점검을 위한 압력계, 온도계 등 설치	5	○ **(전자금융감독규정)** - 제10조(전원, 공조 등 설비에 관한 사항)제6호 금융회사 또는 전자금융업자는 전산실이 위치한 건물의 전원, 공조 등 설비에 관하여 다음 각 호의 사항을 준수하여야 한다. 〈개정 2013. 12. 3.〉 6. 전산실에 공급되는 전원 및 공조 설비는 부하가 큰 설비부분과 분리하여 설치하고 공조 설비 상태 점검을 위한 압력계, 온도계 등을 갖출 것
FISM-040	4.2 전산센터 설비	전산실내 자동제어 항온/항습기 설치 여부	5	○ **(전자금융감독규정)** - 제10조(전원, 공조 등 설비에 관한 사항)제7호 금융회사 또는 전자금융업자는 전산실이 위치한 건물의 전원, 공조 등 설비에 관하여 다음 각 호의 사항을 준수하여야 한다. 〈개정 2013. 12. 3.〉 7. 전산실에 24시간 동안 적정한 온도 및 습도를 유지하기 위해서 자동제어 항온·항습기를 갖출 것
FISM-041	4.3 전산실 보안	화재감지센서와 연동된 경보장치 설치 여부	5	○ **(전자금융감독규정)** - 제11조(전산실 등에 관한 사항)제1호 금융회사 또는 전자금융업자는 전산실에 관하여 다음 각 호의 사항을 준수하여야 한다. 〈개정 2013. 12. 3.〉 1. 화재·수해 등의 재해 및 외부 위해(危害) 방지대책을 수립·운용할 것

평가 항목ID	통제구분	평가항목	위험도	[근거조항] 전자금융감독규정 (금융위원회고시 제2018-36호, 2018. 12. 21) 전자금융감독규정시행세칙 (금융감독원세칙, 2021. 2. 25)
FISM-042	4.3 전산실 보안	재해 및 외부 위해방지대책 수립/운용 여부	5	○ **(전자금융감독규정)** - 제11조(전산실 등에 관한 사항)제1호 금융회사 또는 전자금융업자는 전산실에 관하여 다음 각 호의 사항을 준수하여야 한다. 〈개정 2013. 12. 3.〉 1. 화재·수해 등의 재해 및 외부 위해(危害) 방지대책을 수립·운용할 것
FISM-043	4.3 전산실 보안	상시출입문은 한 곳으로 설치 여부	5	○ **(전자금융감독규정)** - 제11조(전산실 등에 관한 사항)제2호 금융회사 또는 전자금융업자는 전산실에 관하여 다음 각 호의 사항을 준수하여야 한다. 〈개정 2013. 12. 3.〉 2. 상시 출입문은 한 곳으로 정하며 상시 출입은 업무와 직접 관련이 있는 사전 등록자에 한하여 허용하고, 그 밖의 출입자에 대하여는 책임자의 승인을 받아 출입하도록 하며 출입자 관리기록부를 기록·보관할 것
FISM-044	4.3 전산실 보안	상시출입자의 사전 등록 여부	5	○ **(전자금융감독규정)** - 제11조(전산실 등에 관한 사항)제2호 금융회사 또는 전자금융업자는 전산실에 관하여 다음 각 호의 사항을 준수하여야 한다. 〈개정 2013. 12. 3.〉 2. 상시 출입문은 한 곳으로 정하며 상시 출입은 업무와 직접 관련이 있는 사전 등록자에 한하여 허용하고, 그 밖의 출입자에 대하여는 책임자의 승인을 받아 출입하도록 하며 출입자 관리기록부를 기록·보관할 것

평가 항목ID	통제구분	평가항목	위험도	[근거조항] 전자금융감독규정 (금융위원회고시 제2018-36호, 2018. 12. 21) 전자금융감독규정시행세칙 (금융감독원세칙, 2021. 2. 25)
FISM-045	4.3 전산실 보안	상시출입자외 책임자 승인 및 출입자 관리기록부 기록 및 보관 여부	5	○ **(전자금융감독규정)** - 제11조(전산실 등에 관한 사항)제2호 금융회사 또는 전자금융업자는 전산실에 관하여 다음 각 호의 사항을 준수하여야 한다. 〈개정 2013. 12. 3.〉 2. 상시 출입문은 한 곳으로 정하며 상시 출입은 업무와 직접 관련이 있는 사전 등록자에 한하여 허용하고, 그 밖의 출입자에 대하여는 책임자의 승인을 받아 출입하도록 하며 출입자 관리기록부를 기록·보관할 것
FISM-046	4.3 전산실 보안	상시출입자외 출입사항 사후 확인을 위한 무인감시카메라 또는 출입자 동기록시스템설치 등 조치 및 사후 확인 가능 여부	5	○ **(전자금융감독규정)** - 제11조(전산실 등에 관한 사항)제3호 금융회사 또는 전자금융업자는 전산실에 관하여 다음 각 호의 사항을 준수하여야 한다. 〈개정 2013. 12. 3.〉 3. 상시 출입이 허용된 자 이외의 출입자의 출입사항에 대하여는 전산실의 규모 및 설치장소 등을 감안하여 무인감시카메라 또는 출입자동기록시스템 설치 등 적절한 조치를 취하여 사후 확인이 가능하도록 할 것
FISM-047	4.3 전산실 보안	출입문은 이중안전장치로 보호 여부	5	○ **(전자금융감독규정)** - 제11조(전산실 등에 관한 사항)제4호 금융회사 또는 전자금융업자는 전산실에 관하여 다음 각 호의 사항을 준수하여야 한다. 〈개정 2013. 12. 3.〉 4. 출입문은 이중 안전장치로 보호하며 외벽이 유리인 경우 유리창문을 통하여 접근할 수 없도록 조치할 것

평가 항목ID	통제구분	평가항목	위험도	[근거조항] 전자금융감독규정 (금융위원회고시 제2018-36호, 2018. 12. 21) 전자금융감독규정시행세칙 (금융감독원세칙, 2021. 2. 25)
FISM-048	4.3 전산실 보안	외벽 유리 창문을 통한 접근차단조치 여부	5	○ **(전자금융감독규정)** - 제11조(전산실 등에 관한 사항)제4호 금융회사 또는 전자금융업자는 전산실에 관하여 다음 각 호의 사항을 준수하여야 한다. 〈개정 2013. 12. 3.〉 4. 출입문은 이중 안전장치로 보호하며 외벽이 유리인 경우 유리창문을 통하여 접근할 수 없도록 조치할 것
FISM-049	4.3 전산실 보안	외벽과 전산장비간 충분한 거리 유지 여부	5	○ **(전자금융감독규정)** - 제11조(전산실 등에 관한 사항)제5호 금융회사 또는 전자금융업자는 전산실에 관하여 다음 각 호의 사항을 준수하여야 한다. 〈개정 2013. 12. 3.〉 5. 천정·바닥·벽의 침수로 인한 정보처리시스템의 장애가 발생하지 않도록 외벽과 전산장비와의 거리를 충분히 유지하고 이중바닥설치 등 방안을 강구할 것
FISM-050	4.3 전산실 보안	이중바닥설치 등 침수 대비 방안 강구 여부	5	○ **(전자금융감독규정)** - 제11조(전산실 등에 관한 사항)제5호 금융회사 또는 전자금융업자는 전산실에 관하여 다음 각 호의 사항을 준수하여야 한다. 〈개정 2013. 12. 3.〉 5. 천정·바닥·벽의 침수로 인한 정보처리시스템의 장애가 발생하지 않도록 외벽과 전산장비와의 거리를 충분히 유지하고 이중바닥설치 등 방안을 강구할 것

평가 항목ID	통제구분	평가항목	위험도	[근거조항] 전자금융감독규정 (금융위원회고시 제2018-36호, 2018. 12. 21) 전자금융감독규정시행세칙 (금융감독원세칙, 2021. 2. 25)
FISM-051	4.3 전산실 보안	온도/습도자료 자동기록장치 및 경보장치 설치 등 조치 여부	5	○ **(전자금융감독규정)** - 제11조(전산실 등에 관한 사항)제6호 금융회사 또는 전자금융업자는 전산실에 관하여 다음 각 호의 사항을 준수하여야 한다. 〈개정 2013. 12. 3.〉 6. 적정수준의 온도·습도를 유지하기 위하여 온도·습도 자료 자동기록장치 및 경보장치 설치 등 적절한 조치를 취할 것
FISM-052	4.3 전산실 보안	전용 통로관 설치 등 케이블보호조치 강구 여부	5	○ **(전자금융감독규정)** - 제11조(전산실 등에 관한 사항)제7호 금융회사 또는 전자금융업자는 전산실에 관하여 다음 각 호의 사항을 준수하여야 한다. 〈개정 2013. 12. 3.〉 7. 케이블이 안전하게 유지되도록 전용 통로관 설치 등 적절한 보호조치를 강구할 것
FISM-053	4.3 전산실 보안	조명설비 및 휴대용손전등 비치 여부	5	○ **(전자금융감독규정)** - 제11조(전산실 등에 관한 사항)제8호 금융회사 또는 전자금융업자는 전산실에 관하여 다음 각 호의 사항을 준수하여야 한다. 〈개정 2013. 12. 3.〉 8. 정전에 대비하여 조명설비 및 휴대용손전등을 비치할 것
FISM-054	4.3 전산실 보안	IDC 등 다수기관 공동이용장소에 정보처리시스템 설치 시 미승인자 접근 차단에 필요한 접근 통제대책 수립 및 운용 여부	5	○ **(전자금융감독규정)** - 제11조(전산실 등에 관한 사항) 금융회사 또는 전자금융업자는 전산실에 관하여 다음 각 호의 사항을 준수하여야 한다. 〈개정 2013. 12. 3.〉

평가 항목ID	통제구분	평가항목	위험도	[근거조항] 전자금융감독규정 (금융위원회고시 제2018-36호, 2018. 12. 21) 전자금융감독규정시행세칙 (금융감독원세칙, 2021. 2. 25)
				9. 집적정보통신시설(Internet Data Center : IDC) 등과 같이 다수의 기관이 공동으로 이용하는 장소에 정보처리시스템을 설치하는 경우에는 미승인자가 접근하지 못하도록 적절한 접근통제 대책을 마련할 것
FISM-055	4.3 전산실 보안	전산센터, 재해복구센터, 전산자료 보관실, 정보보호시스템 설치장소 등 중요시설 및 지역의 보호구역 설정 및 관리 여부	5	○ **(전자금융감독규정)** - 제11조(전산실 등에 관한 사항)제10호 금융회사 또는 전자금융업자는 전산실에 관하여 다음 각 호의 사항을 준수하여야 한다. 〈개정 2013. 12. 3.〉 10. 다음 각 목의 중요 시설 및 지역을 보호구역으로 설정 관리할 것 가. 전산센터 및 재해복구센터 나. 전산자료 보관실 다. 정보보호시스템 설치장소 라. 그 밖에 보안관리가 필요하다고 인정되는 정보처리시스템 설치장소
FISM-056	4.3 전산실 보안	국내 본점을 둔 금융기관의 전산실 및 재해복구센터의 국내 설치 여부	5	○ **(전자금융감독규정)** - 제11조(전산실 등에 관한 사항)제11호 금융회사 또는 전자금융업자는 전산실에 관하여 다음 각 호의 사항을 준수하여야 한다. 〈개정 2013. 12. 3.〉 11. 국내에 본점을 둔 금융회사의 전산실 및 재해복구센터는 국내에 설치할 것 〈개정 2016. 6. 30.〉
FISM-057	4.3 전산실 보안	전산실내 무선통신망 설치 및 운용 금지 여부	5	○ **(전자금융감독규정)** - 제11조(전산실 등에 관한 사항)제12호 금융회사 또는 전자금융업자는 전산실에 관하여 다음 각 호의 사항을 준수하여야 한다. 〈개정 2013. 12. 3.〉 12. 무선통신망을 설치하지 아니할 것

평가 항목ID	통제구분	평가항목	위험도	[근거조항] 전자금융감독규정 (금융위원회고시 제2018-36호, 2018. 12. 21) 전자금융감독규정시행세칙 (금융감독원세칙, 2021. 2. 25)
FISM-058	5.1 단말기 보호대책	업무(관련)담당자 이외 사용자에 대한 단말기 무단조작 방지조치 적용 여부	5	○ **(전자금융감독규정)** - 제12조(단말기 보호대책) 금융회사 또는 전자금융업자는 단말기 보호를 위하여 다음 각 호의 사항을 준수하여야 한다. 〈개정 2013. 12. 3.〉 1. 업무담당자 이외의 사람이 단말기를 무단으로 조작하지 못하도록 조치할 것 〈개정 2015. 2. 3.〉
FISM-059	5.1 단말기 보호대책	정보처리시스템 접속에 관한 사용자 인가의 여부를 확인할 수 있는 기록 유지 여부	5	○ **(전자금융감독규정)** - 제12조(단말기 보호대책)제2호 금융회사 또는 전자금융업자는 단말기 보호를 위하여 다음 각 호의 사항을 준수하여야 한다. 〈개정 2013. 12. 3.〉 2. 정보처리시스템에 접속하는 단말기에 대해 정당한 사용자인가의 여부를 확인할 수 있는 기록을 유지할 것 〈개정 2015. 2. 3.〉
FISM-060	5.1 단말기 보호대책	외부 반출, 인터넷 접속, 그룹웨어 접속의 금지 등 강화된 보호대책이 적용되는 중요 단말기 지정 여부	5	○ **(전자금융감독규정)** - 제12조(단말기 보호대책)제3호 금융회사 또는 전자금융업자는 단말기 보호를 위하여 다음 각 호의 사항을 준수하여야 한다. 〈개정 2013. 12. 3.〉 3. 외부 반출, 인터넷 접속, 그룹웨어 접속의 금지 등 강화된 보호대책이 적용되는 중요단말기를 지정할 것 〈개정 2013. 12. 3., 2015. 2. 3.〉
FISM-061	5.1 단말기 보호대책	사용자 단말기에서 보조기억매체 및 휴대용 전산장비에 관한 접근통제 (정보유출, 악성코드 감염방지 등) 여부	5	○ **(전자금융감독규정)** - 제12조(단말기 보호대책)제4호 금융회사 또는 전자금융업자는 단말기 보호를 위하여 다음 각 호의 사항을 준수하여야 한다. 〈개정 2013. 12. 3.〉

평가 항목ID	통제구분	평가항목	위험도	[근거조항] 전자금융감독규정 (금융위원회고시 제2018-36호, 2018. 12. 21) 전자금융감독규정시행세칙 (금융감독원세칙, 2021. 2. 25)
				4. 정보유출, 악성코드 감염 등을 방지할 수 있도록 단말기에서 보조기억매체 및 휴대용 전산장비에 접근하는 것을 통제할 것 〈개정 2015. 2. 3.〉
FISM-062	5.2 전산자료 보호대책	전산자료 보유현황 관리 여부	5	○ **(전자금융감독규정)** - 제13조(전산자료 보호대책)제1항제3호 ① 금융회사 또는 전자금융업자는 전산자료의 유출, 파괴 등을 방지하기 위하여 다음 각 호를 포함한 전산자료 보호대책을 수립·운용하여야 한다. 〈개정 2013. 12. 3.〉 3. 전산자료의 보유현황을 관리하고 책임자를 지정·운영할 것
FISM-063	5.2 전산자료 보호대책	전산자료 책임자 지정 여부	5	○ **(전자금융감독규정)** - 제13조(전산자료 보호대책)제1항제3호 ① 금융회사 또는 전자금융업자는 전산자료의 유출, 파괴 등을 방지하기 위하여 다음 각 호를 포함한 전산자료 보호대책을 수립·운용하여야 한다. 〈개정 2013. 12. 3.〉 3. 전산자료의 보유현황을 관리하고 책임자를 지정·운영할 것
FISM-064	5.2 전산자료 보호대책	전산자료 및 전산장비의 반출/반입 통제 여부	5	○ **(전자금융감독규정)** - 제13조(전산자료 보호대책)제1항제5호 ① 금융회사 또는 전자금융업자는 전산자료의 유출, 파괴 등을 방지하기 위하여 다음 각 호를 포함한 전산자료 보호대책을 수립·운용하여야 한다. 〈개정 2013. 12. 3.〉 5. 전산자료 및 전산장비의 반출·반입을 통제할 것

평가 항목ID	통제구분	평가항목	위험도	[근거조항] 전자금융감독규정 (금융위원회고시 제2018-36호, 2018. 12. 21) 전자금융감독규정시행세칙 (금융감독원세칙, 2021. 2. 25)
FISM-065	5.2 전산자료 보호대책	보조기억매체 등 전산자료에 대한 안전지출 및 파기계획 수립 및 운용 여부	5	○ **(전자금융감독규정)** - 제13조(전산자료 보호대책)제1항제6호 ① 금융회사 또는 전자금융업자는 전산자료의 유출, 파괴 등을 방지하기 위하여 다음 각 호를 포함한 전산자료 보호대책을 수립·운용하여야 한다. 〈개정 2013. 12. 3.〉 6. 비상시에 대비하여 보조기억매체 등 전산자료에 대한 안전지출 및 긴급파기 계획을 수립·운용할 것 〈개정 2013. 12. 3.〉
FISM-066	5.2 전산자료 보호대책	보조기억매체 보유현황 및 관리실태에 관한 정기점검 및 책임자 확인 여부	5	○ **(전자금융감독규정)** - 제13조(전산자료 보호대책)제1항제7호 ① 금융회사 또는 전자금융업자는 전산자료의 유출, 파괴 등을 방지하기 위하여 다음 각 호를 포함한 전산자료 보호대책을 수립·운용하여야 한다. 〈개정 2013. 12. 3.〉 7. 정기적으로 보조기억매체의 보유 현황 및 관리실태를 점검하고 책임자의 확인을 받을 것
FISM-067	5.2 전산자료 보호대책	전산자료의 정기백업/소산 등 백업 내역에 관한 기록 및 관리 여부	5	○ **(전자금융감독규정)** - 제13조(전산자료 보호대책)제1항제8호 ① 금융회사 또는 전자금융업자는 전산자료의 유출, 파괴 등을 방지하기 위하여 다음 각 호를 포함한 전산자료 보호대책을 수립·운용하여야 한다. 〈개정 2013. 12. 3.〉 8. 중요도에 따라 전산자료를 정기적으로 백업하여 원격 안전지역에 소산하고 백업내역을 기록·관리할 것

평가 항목ID	통제구분	평가항목	위험도	[근거조항] 전자금융감독규정 (금융위원회고시 제2018-36호, 2018. 12. 21) 전자금융감독규정시행세칙 (금융감독원세칙, 2021. 2. 25)
FISM-068	5.2 전산자료 보호대책	전산자료 중요도 분류기준 수립 여부	5	○ **(전자금융감독규정)** - 제13조(전산자료 보호대책)제1항제8호 ① 금융회사 또는 전자금융업자는 전산자료의 유출, 파괴 등을 방지하기 위하여 다음 각 호를 포함한 전산자료 보호대책을 수립·운용하여야 한다. 〈개정 2013. 12. 3.〉 8. 중요도에 따라 전산자료를 정기적으로 백업하여 원격 안전지역에 소산하고 백업내역을 기록·관리할 것
FISM-069	5.2 전산자료 보호대책	주요 백업 전산자료에 대한 정기 검증 여부	5	○ **(전자금융감독규정)** - 제13조(전산자료 보호대책)제1항제9호 ① 금융회사 또는 전자금융업자는 전산자료의 유출, 파괴 등을 방지하기 위하여 다음 각 호를 포함한 전산자료 보호대책을 수립·운용하여야 한다. 〈개정 2013. 12. 3.〉 9. 주요 백업 전산자료에 대하여 정기적으로 검증할 것
FISM-070	5.2 전산자료 보호대책	이용자 정보 조회 및 출력에 대한 통제 여부	5	○ **(전자금융감독규정)** - 제13조(전산자료 보호대책)제1항제10호 ① 금융회사 또는 전자금융업자는 전산자료의 유출, 파괴 등을 방지하기 위하여 다음 각 호를 포함한 전산자료 보호대책을 수립·운용하여야 한다. 〈개정 2013. 12. 3.〉 10. 이용자 정보의 조회·출력에 대한 통제를 하고 테스트 시 이용자 정보 사용 금지(다만, 법인인 이용자 정보는 금융감독원장이 정하는 바에 따라 이용자의 동의를 얻은 경우 테스트 시 사용 가능하며, 그 외 부하 테스트 등 이용자 정보의 사용이 불가피한 경우 이용자 정보를 변환하여 사용하고 테스트 종료 즉시 삭제하여야 한다) 〈개정 2013. 12. 3., 2016. 10. 5.〉

평가 항목ID	통제구분	평가항목	위험도	[근거조항] 전자금융감독규정 (금융위원회고시 제2018-36호, 2018. 12. 21) 전자금융감독규정시행세칙 (금융감독원세칙, 2021. 2. 25)
				○ **(전자금융감독규정시행세칙)** - 제2조의4 (법인 이용자 정보의 사용에 대한 동의) 규정 제13조 제1항 제10호에 따라 동의를 얻는 경우 다음 각 호의 사항을 정보주체에게 사전에 알려야 한다. 1. 테스트의 목적 및 기간 2. 사용되는 이용자 정보의 항목 3. 테스트 기간 중 정보유출 방지를 위한 통제 계획 4. 테스트 종료 후 테스트에 사용된 이용자 정보의 파기 계획
FISM-071	5.2 전산자료 보호대책	테스트 시 이용자 정보 사용금지 (부하테스트 등의 불가피한 경우 이용자정보 변환 사용 및 테스트 종료즉시 삭제) 여부	5	○ **(전자금융감독규정)** - 제13조(전산자료 보호대책) ① 금융회사 또는 전자금융업자는 전산자료의 유출, 파괴 등을 방지하기 위하여 다음 각 호를 포함한 전산자료 보호대책을 수립·운용하여야 한다. 〈개정 2013. 12. 3.〉 10. 이용자 정보의 조회·출력에 대한 통제를 하고 테스트 시 이용자 정보 사용 금지(다만, 법인인 이용자 정보는 금융감독원장이 정하는 바에 따라 이용자의 동의를 얻은 경우 테스트 시 사용 가능하며, 그 외 부하 테스트 등 이용자 정보의 사용이 불가피한 경우 이용자 정보를 변환하여 사용하고 테스트 종료 즉시 삭제하여야 한다) 〈개정 2013. 12. 3., 2016. 10. 5.〉 ○ **(전자금융감독규정시행세칙)** - 제2조의4 (법인 이용자 정보의 사용에 대한 동의) 규정 제13조 제1항 제10호에 따라 동의를 얻는 경우 다음 각 호의 사항을 정보

평가 항목ID	통제구분	평가항목	위험도	[근거조항] 전자금융감독규정 (금융위원회고시 제2018-36호, 2018. 12. 21) 전자금융감독규정시행세칙 (금융감독원세칙, 2021. 2. 25)
				주체에게 사전에 알려야 한다. 1. 테스트의 목적 및 기간 2. 사용되는 이용자 정보의 항목 3. 테스트 기간 중 정보유출 방지를 위한 통제 계획 4. 테스트 종료 후 테스트에 사용된 이용자 정보의 파기 계획
FISM-072	5.2 전산자료 보호대책	정보처리시스템 가동기록(정보처리시스템 접속기록, 전산자료 사용기록, 전산자료 처리기록) 1년 이상 보존 여부	5	○ **(전자금융감독규정)** - 제13조(전산자료 보호대책)제1항제11호,제4항 ① 금융회사 또는 전자금융업자는 전산자료의 유출, 파괴 등을 방지하기 위하여 다음 각 호를 포함한 전산자료 보호대책을 수립·운용하여야 한다. 〈개정 2013. 12. 3.〉 11. 정보처리시스템의 가동기록은 1년 이상 보존할 것 ④ 제1항제11호의 정보처리시스템 가동기록의 경우 다음 각 호의 사항이 접속의 성공여부와 상관없이 자동적으로 기록·유지되어야 한다. 1. 정보처리시스템에 접속한 일시, 접속자 및 접근을 확인할 수 있는 접근기록 2. 전산자료를 사용한 일시, 사용자 및 자료의 내용을 확인할 수 있는 접근기록 3. 정보처리시스템내 전산자료의 처리 내용을 확인할 수 있는 사용자 로그인, 액세스 로그 등 접근기록
FISM-073	5.2 전산자료 보호대책	정보처리시스템 접속 오류(최대 5회) 시 사용 제한 여부	5	○ **(전자금융감독규정)** - 제13조(전산자료 보호대책)제1항제12호 ① 금융회사 또는 전자금융업자는 전산자료의 유출, 파괴 등을 방지하기 위하여 다음 각 호를 포함한 전산자료 보호대책을 수립·운용하여야 한다. 〈개정 2013. 12. 3.〉 12. 정보처리시스템 접속 시 5회 이내의 범위에서 미리 정한 횟수 이상의 접속 오류가 발생하는 경우 정보처리시스템의 사용을 제한할 것

평가 항목ID	통제구분	평가항목	위험도	[근거조항] 전자금융감독규정 (금융위원회고시 제2018-36호, 2018. 12. 21) 전자금융감독규정시행세칙 (금융감독원세칙, 2021. 2. 25)
FISM-074	5.2 전산자료 보호대책	단말기에 이용자 정보 등 주요정보 보관 금지 여부	5	○ **(전자금융감독규정)** - 제13조(전산자료 보호대책)제1항제13호 ① 금융회사 또는 전자금융업자는 전산자료의 유출, 파괴 등을 방지하기 위하여 다음 각 호를 포함한 전산자료 보호대책을 수립·운용하여야 한다. 〈개정 2013. 12. 3.〉 13. 단말기에 이용자 정보 등 주요정보를 보관하지 아니하고, 단말기를 공유하지 아니할 것(다만, 불가피하게 단말기에 보관할 필요가 있는 경우 보관사유, 보관기간 및 관리 비밀번호 등을 정하여 책임자의 승인을 받아야 한다)
FISM-075	5.2 전산자료 보호대책	단말기 공유 금지 여부	5	○ **(전자금융감독규정)** - 제13조(전산자료 보호대책)제1항제13호 ① 금융회사 또는 전자금융업자는 전산자료의 유출, 파괴 등을 방지하기 위하여 다음 각 호를 포함한 전산자료 보호대책을 수립·운용하여야 한다. 13. 단말기에 이용자 정보 등 주요정보를 보관하지 아니하고, 단말기를 공유하지 아니할 것(다만, 불가피하게 단말기에 보관할 필요가 있는 경우 보관사유, 보관기간 및 관리 비밀번호 등을 정하여 책임자의 승인을 받아야 한다)
FISM-076	5.2 전산자료 보호대책	단말기 내 주요정보 보관 필요시, 관련 절차 수립 여부	5	○ **(전자금융감독규정)** - 제13조(전산자료 보호대책)제1항제13호 ① 금융회사 또는 전자금융업자는 전산자료의 유출, 파괴 등을 방지하기 위하여 다음 각 호를 포함한 전산자료 보호대책을 수립·운용하여야 한다. 13. 단말기에 이용자 정보 등 주요정보를 보관하지 아니하고, 단말기를 공유하지 아니할 것(다만, 불가피하게 단말기에 보관할 필요가 있는 경우 보관사유, 보관기간 및 관리 비밀번호 등을 정하여 책임자의 승인을 받아야 한다)

평가 항목ID	통제구분	평가항목	위험도	[근거조항] 전자금융감독규정 (금융위원회고시 제2018-36호, 2018. 12. 21) 전자금융감독규정시행세칙 (금융감독원세칙, 2021. 2. 25)
FISM-077	5.2 전산자료 보호대책	정보처리시스템 접근기록(접속일시, 접속자, 전산자료 사용일시, 사용자, 자료내용, 사용자 로그인, 액세스 로그 등)에 대한 자동 기록 및 보관 여부	5	○ **(전자금융감독규정)** - 제13조(전산자료 보호대책)제1항제11호,제4항 ① 금융회사 또는 전자금융업자는 전산자료의 유출, 파괴 등을 방지하기 위하여 다음 각 호를 포함한 전산자료 보호대책을 수립·운용하여야 한다. 11. 정보처리시스템의 가동기록은 1년 이상 보존할 것 ④ 제1항제11호의 정보처리시스템 가동기록의 경우 다음 각 호의 사항이 접속의 성공여부와 상관없이 자동적으로 기록·유지되어야 한다. 1. 정보처리시스템에 접속한 일시, 접속자 및 접근을 확인할 수 있는 접근기록 2. 전산자료를 사용한 일시, 사용자 및 자료의 내용을 확인할 수 있는 접근기록 3. 정보처리시스템내 전산자료의 처리 내용을 확인할 수 있는 사용자 로그인, 액세스 로그 등 접근기록
FISM-078	5.3 정보처리 시스템 보호대책	주요 정보처리시스템에 대한 시스템 운영 매뉴얼 작성 여부	5	○ **(전자금융감독규정)** - 제14조(정보처리시스템 보호대책)제1호 금융회사 또는 전자금융업자는 정보처리시스템의 안전한 운영을 위하여 다음 각 호를 포함한 보호대책을 수립·운용하여야 한다. 〈개정 2013. 12. 3.〉 1. 주요 정보처리시스템에 대한 구동, 조작방법, 명령어 사용법, 운용순서, 장애조치 및 연락처 등 시스템 운영매뉴얼을 작성할 것
FISM-079	5.3 정보처리 시스템 보호대책	주요 정보처리시스템에 대한 시스템 운영 매뉴얼에 구동, 조작방법, 명령어사용법, 운용순서, 장애조치 및 연락처 등 포함 여부	5	○ **(전자금융감독규정)** - 제14조(정보처리시스템 보호대책)제1호 금융회사 또는 전자금융업자는 정보처리시스템의 안전한 운영을 위하여 다음 각 호를 포함한 보호대책을 수립·운용하여야 한다. 〈개정 2013. 12. 3.〉 1. 주요 정보처리시스템에 대한 구동, 조작방법, 명령어 사용법, 운용순서, 장애조치 및 연락처 등 시스템 운영매뉴얼을 작성할 것

평가 항목ID	통제구분	평가항목	위험도	[근거조항] 전자금융감독규정 (금융위원회고시 제2018-36호, 2018. 12. 21) 전자금융감독규정시행세칙 (금융감독원세칙, 2021. 2. 25)
FISM-080	5.3 정보처리 시스템 보호대책	주요 프로그램에 대한 유지보수 관리대장에 작업일, 작업내용, 작업결과 등을 작성 및 보관 여부	5	○ **(전자금융감독규정)** - 제14조(정보처리시스템 보호대책)제2호 금융회사 또는 전자금융업자는 정보처리시스템의 안전한 운영을 위하여 다음 각 호를 포함한 보호대책을 수립·운용하여야 한다. 〈개정 2013. 12. 3.〉 2. 데이터베이스관리시스템(Database Management System : DBMS)·운영체제·웹프로그램 등 주요 프로그램에 대하여 정기적으로 유지보수를 실시하고, 작업일, 작업내용, 작업결과 등을 기록한 유지보수관리대장을 작성·보관할 것
FISM-081	5.3 정보처리 시스템 보호대책	데이터베이스관리시스템(Database Management System : DBMS), 운영체제(Operating System), 웹프로그램에 대한 주기적 유지보수 여부	5	○ **(전자금융감독규정)** - 제14조(정보처리시스템 보호대책)제2호 금융회사 또는 전자금융업자는 정보처리시스템의 안전한 운영을 위하여 다음 각 호를 포함한 보호대책을 수립·운용하여야 한다. 〈개정 2013. 12. 3.〉 2. 데이터베이스관리시스템(Database Management System : DBMS)·운영체제·웹프로그램 등 주요 프로그램에 대하여 정기적으로 유지보수를 실시하고, 작업일, 작업내용, 작업결과 등을 기록한 유지보수관리대장을 작성·보관할 것
FISM-082	5.3 정보처리 시스템 보호대책	정보처리시스템 장애 발생시 장애상황기록부에 장애일시, 장애내용, 조치사항 등을 작성 및 보관 여부	5	○ **(전자금융감독규정)** - 제14조(정보처리시스템 보호대책)제3호 금융회사 또는 전자금융업자는 정보처리시스템의 안전한 운영을 위하여 다음 각 호를 포함한 보호대책을 수립·운용하여야 한다. 〈개정 2013. 12. 3.〉 3. 정보처리시스템의 장애발생 시 장애일시, 장애내용 및 조치사항 등을 기록한 장애상황기록부를 상세하게 작성·보관할 것

평가 항목ID	통제구분	평가항목	위험도	[근거조항] 전자금융감독규정 (금융위원회고시 제2018-36호, 2018. 12. 21) 전자금융감독규정시행세칙 (금융감독원세칙, 2021. 2. 25)
FISM-083	5.3 정보처리 시스템 보호대책	정상작동여부 확인을 위한 정보처리시스템 자원 상태의 감시, 경고 및 제어가 가능한 모니터링 시스템 설치 및 운영 여부	5	○ **(전자금융감독규정)** - 제14조(정보처리시스템 보호대책)제4호 금융회사 또는 전자금융업자는 정보처리시스템의 안전한 운영을 위하여 다음 각 호를 포함한 보호대책을 수립·운용하여야 한다. 〈개정 2013. 12. 3.〉 4. 정보처리시스템의 정상작동여부 확인을 위하여 시스템 자원 상태의 감시, 경고 및 제어가 가능한 모니터링시스템을 갖출 것
FISM-084	5.3 정보처리 시스템 보호대책	시스템 통합, 전환 및 재개발시 정보처리시스템의 운영에 지장을 초래하지 않도록 통제절차 마련 여부	5	○ **(전자금융감독규정)** - 제14조(정보처리시스템 보호대책)제5호 금융회사 또는 전자금융업자는 정보처리시스템의 안전한 운영을 위하여 다음 각 호를 포함한 보호대책을 수립·운용하여야 한다. 〈개정 2013. 12. 3.〉 5. 시스템 통합, 전환 및 재개발 시 장애 등으로 인하여 정보처리시스템의 운영에 지장이 초래되지 않도록 통제 절차를 마련하여 준수할 것
FISM-085	5.3 정보처리 시스템 보호대책	정보처리시스템 책임자 지정 및 운영 여부	5	○ **(전자금융감독규정)** - 제14조(정보처리시스템 보호대책)제6호 금융회사 또는 전자금융업자는 정보처리시스템의 안전한 운영을 위하여 다음 각 호를 포함한 보호대책을 수립·운용하여야 한다. 〈개정 2013. 12. 3.〉 6. 정보처리시스템의 책임자를 지정·운영할 것
FISM-086	5.3 정보처리 시스템 보호대책	운영체계, 시스템 유틸리티 등의 긴급하고 중요한 보정(patch)사항에 대하여는 즉시 보정 여부	5	○ **(전자금융감독규정)** - 제14조(정보처리시스템 보호대책)제7호 금융회사 또는 전자금융업자는 정보처리시스템의 안전한 운영을 위하여 다음 각 호를 포함한 보호대책을 수립·운용하여야 한다. 〈개정 2013. 12. 3.〉 7. 정보처리시스템의 운영체계, 시스템 유틸리티 등의 긴급하고 중요한 보정

평가 항목ID	통제구분	평가항목	위험도	[근거조항] 전자금융감독규정 (금융위원회고시 제2018-36호, 2018. 12. 21) 전자금융감독규정시행세칙 (금융감독원세칙, 2021. 2. 25)
				(patch)사항에 대하여는 즉시 보정 작업을 할 것 - 제15조(해킹 등 방지대책)제1항제2호 ① 금융회사 또는 전자금융업자는 정보처리시스템 및 정보통신망을 해킹 등 전자적 침해행위로부터 방지하기 위하여 다음 각 호의 대책을 수립·운용하여야 한다. 2. 해킹 등 전자적 침해행위에 대비한 시스템프로그램 등의 긴급하고 중요한 보정(patch)사항에 대하여 즉시 보정작업 실시
FISM-087	5.3 정보처리 시스템 보호대책	중요도에 따른 운영체제(Operating System) 및 설정내용 등의 정기 백업, 원격안전지역 소산 및 백업 자료 1년 이상 기록/관리 여부	5	○ **(전자금융감독규정)** - 제14조(정보처리시스템 보호대책)제8호 금융회사 또는 전자금융업자는 정보처리시스템의 안전한 운영을 위하여 다음 각 호를 포함한 보호대책을 수립·운용하여야 한다. 〈개정 2013. 12. 3.〉 8. 중요도에 따라 정보처리시스템의 운영체제 및 설정내용 등을 정기 백업 및 원격 안전지역에 소산하고 백업자료는 1년 이상 기록·관리할 것
FISM-088	5.3 정보처리 시스템 보호대책	정보처리시스템의 운영체제(Operating System) 계정으로 로그인(Log in)할 경우 계정 및 비밀번호 이외에 별도의 추가인증 적용 여부	5	○ **(전자금융감독규정)** - 제14조(정보처리시스템 보호대책)제9호 금융회사 또는 전자금융업자는 정보처리시스템의 안전한 운영을 위하여 다음 각 호를 포함한 보호대책을 수립·운용하여야 한다. 〈개정 2013. 12. 3.〉 9. 정보처리시스템의 운영체제(Operating System) 계정으로 로그인(Login)할 경우 계정 및 비밀번호 이외에 별도의 추가인증 절차를 의무적으로 시행할 것
FISM-089	5.3 정보처리 시스템 보호대책	정보처리시스템 운영체제(Operating System) 계정에 대한 사용권한, 접근기록, 작업 내역 등에 대한 상시 모니터링 체계 수립 여부 및 이상 징후 발생 시 필요한 통제 조치 시행	5	○ **(전자금융감독규정)** - 제14조(정보처리시스템 보호대책)제10호 금융회사 또는 전자금융업자는 정보처리시스템의 안전한 운영을 위하여 다음 각 호를 포함한 보호대책을 수립·운용하여야 한다. 〈개정 2013. 12. 3.〉

평가 항목ID	통제구분	평가항목	위험도	[근거조항] 전자금융감독규정 (금융위원회고시 제2018-36호, 2018. 12. 21) 전자금융감독규정시행세칙 (금융감독원세칙, 2021. 2. 25)
		여부		10. 정보처리시스템 운영체제(Operating System) 계정에 대한 사용권한, 접근 기록, 작업 내역 등에 대한 상시 모니터링체계를 수립하고, 이상 징후 발생 시 필요한 통제 조치를 즉시 시행할 것
FISM-091	5.3 정보처리 시스템 보호대책	정보처리시스템 사용 현황 및 추이 분석 등 정기적 실시 여부	5	○ **(전자금융감독규정)** - 제25조(정보처리시스템의 성능관리) 금융회사 또는 전자금융업자는 정보처리시스템의 장애예방 및 성능의 최적화를 위하여 정보처리시스템의 사용 현황 및 추이 분석 등을 정기적으로 실시하여야 한다. 〈개정 2013. 12. 3.〉
FISM-092	5.4 취약점 분석·평가	전자금융기반시설의 취약점 분석·평가는 연 1회 이상(홈페이지에 대해서는 6개월에 1회 이상) 실시 여부	5	○ **(전자금융감독규정)** - 제37조의2(전자금융기반시설의 취약점 분석·평가 주기, 내용 등)제1항 ① 전자금융기반시설의 취약점 분석·평가는 총자산이 2조원 이상이고, 상시 종업원수(「소득세법」에 따른 원천징수의무자가 근로소득세를 원천징수한 자를 기준으로 한다. 이하 같다) 300명 이상인 금융회사 또는 전자금융업자이거나 「수산업 협동조합법」, 「산림조합법」, 「신용협동조합법」, 「상호저축은행법」 및 「새마을금고법」에 따른 중앙회의 경우 연 1회 이상(홈페이지에 대해서는 6개월에 1회 이상) 실시하여야 한다. ○ **(전자금융감독규정시행세칙)** - 제7조의2(전자금융기반시설의 취약점 분석·평가의 내용) 규정 제37조의2제3항에 따라 감독원장이 정하는 취약점 분석·평가의 내용은 별표 3과 같다.

평가 항목ID	통제구분	평가항목	위험도	[근거조항] 전자금융감독규정 (금융위원회고시 제2018-36호, 2018. 12. 21) 전자금융감독규정시행세칙 (금융감독원세칙, 2021. 2. 25)
FISM-093	5.4 취약점 분석·평가	취약점 분석·평가결과에 따른 취약점 제거 또는 이에 상응하는 조치 시행 여부	5	○ **(전자금융감독규정)** - 제37조의2(전자금융기반시설의 취약점 분석·평가 주기, 내용 등)제5항제1호 ⑤ 금융회사 또는 전자금융업자는 취약점 분석·평가에 따라 이행계획을 수립·시행하여야 하며 다음 각 호의 사항을 준수하여야 한다. 1. 취약점 분석·평가 결과에 따른 취약점의 제거 또는 이에 상응하는 조치의 시행
FISM-094	5.4 취약점 분석·평가	취약점 제거 또는 이에 상응하는 조치가 불가한 경우 최고경영자 승인 취득 여부	5	○ **(전자금융감독규정)** - 제37조의2(전자금융기반시설의 취약점 분석·평가 주기, 내용 등)제5항제2호 ⑤ 금융회사 또는 전자금융업자는 취약점 분석·평가에 따라 이행계획을 수립·시행하여야 하며 다음 각 호의 사항을 준수하여야 한다. 2. 취약점의 제거 또는 이에 상응하는 조치가 불가한 경우에는 최고경영자 승인을 득할 것
FISM-095	5.4 취약점 분석·평가	취약점 분석·평가결과에 대한 이행계획 수립 여부 및 최고경영자 보고 여부	5	○ **(전자금융감독규정)** - 제37조의2(전자금융기반시설의 취약점 분석·평가 주기, 내용 등)제5항 ⑤ 금융회사 또는 전자금융업자는 취약점 분석·평가에 따라 이행계획을 수립·시행하여야 하며 다음 각 호의 사항을 준수하여야 한다. 1. 취약점 분석·평가 결과에 따른 취약점의 제거 또는 이에 상응하는 조치의 시행 2. 취약점의 제거 또는 이에 상응하는 조치가 불가한 경우에는 최고경영자 승인을 득할 것 3. 이행계획의 시행 결과는 최고경영자에게 보고할 것

평가 항목ID	통제구분	평가항목	위험도	[근거조항] 전자금융감독규정 (금융위원회고시 제2018-36호, 2018. 12. 21) 전자금융감독규정시행세칙 (금융감독원세칙, 2021. 2. 25)
FISM-096	5.5 정보보호 시스템 설치 및 운영	해킹 등을 방지하기 위한 정보보호시스템 설치 및 운영 여부	5	○ **(전자금융감독규정)** - 제15조(해킹 등 방지대책)제1항제1호 ① 금융회사 또는 전자금융업자는 정보처리시스템 및 정보통신망을 해킹 등 전자적 침해행위로부터 방지하기 위하여 다음 각 호의 대책을 수립·운용하여야 한다. 1. 해킹 등 전자적 침해행위로 인한 사고를 방지하기 위한 정보보호시스템 설치 및 운영
FISM-097	5.5 정보보호 시스템 설치 및 운영	내부 단말기의 정보보호시스템을 우회한 인터넷 등 외부 통신망(무선통신망 포함) 접속 차단 여부	5	○ **(전자금융감독규정)** - 제15조(해킹 등 방지대책)제1항제3호 ① 금융회사 또는 전자금융업자는 정보처리시스템 및 정보통신망을 해킹 등 전자적 침해행위로부터 방지하기 위하여 다음 각 호의 대책을 수립·운용하여야 한다. 3. 내부통신망과 연결된 내부 업무용시스템은 인터넷(무선통신망 포함) 등 외부통신망과 분리·차단 및 접속 금지(단, 업무상 불가피하여 금융감독원장의 확인을 받은 경우에는 그러하지 아니하다) 〈개정 2013. 12. 3.〉
FISM-098	5.5 정보보호 시스템 설치 및 운영	내부통신망과 연결된 내부 업무용시스템이 인터넷(무선통신망 포함) 등 외부통신망과 분리·차단 및 접속 금지 여부	5	○ **(전자금융감독규정)** - 제15조(해킹 등 방지대책)제1항제3호 ① 금융회사 또는 전자금융업자는 정보처리시스템 및 정보통신망을 해킹 등 전자적 침해행위로부터 방지하기 위하여 다음 각 호의 대책을 수립·운용하여야 한다. 3. 내부통신망과 연결된 내부 업무용시스템은 인터넷(무선통신망 포함) 등 외부통신망과 분리·차단 및 접속 금지(단, 업무상 불가피하여 금융감독원장의 확인을 받은 경우에는 그러하지 아니하다) 〈개정 2013. 12. 3.〉

평가 항목ID	통제구분	평가항목	위험도	[근거조항] 전자금융감독규정 (금융위원회고시 제2018-36호, 2018. 12. 21) 전자금융감독규정시행세칙 (금융감독원세칙, 2021. 2. 25)
				○ **(전자금융감독규정시행세칙)** - 제2조의2 (망분리 적용 예외) ① 규정 제15조제1항제3호에서 금융감독원장의 확인을 받은 경우란 다음 각 호의 어느 하나와 같다. 1. 내부 통신망에 연결된 단말기가 업무상 필수적으로 외부기관과 연결해야 하는 경우 (다만, 이 경우 필요한 서비스번호(port)에 한하여 특정 외부기관과 연결할 수 있다). 2. 규정 제12조의 보안대책을 적용한 단말기에서 전용회선과 동등한 보안수준을 갖춘 통신망을 이용하여 외부망으로부터 내부 업무용시스템으로 원격접속 하는 경우 ③ 제1항 및 제2항의 규정은 금융회사 또는 전자금융업자가 자체 위험성 평가를 실시한 후 〈별표 7〉에서 정한 망분리 대체 정보보호통제를 적용하고 정보보호위원회가 승인한 경우에 한하여 적용한다.
FISM-099	5.5 정보보호 시스템 설치 및 운영	내부통신망에서의 파일 배포기능 이용 시 파일 무결성 검증 수행 여부	5	○ **(전자금융감독규정)** - 제15조(해킹 등 방지대책)제1항제4호 ① 금융회사 또는 전자금융업자는 정보처리시스템 및 정보통신망을 해킹 등 전자적 침해행위로부터 방지하기 위하여 다음 각 호의 대책을 수립·운용 하여야 한다. 4. 내부통신망에서의 파일 배포기능은 통합 및 최소화하여 운영하고, 이를 배포할 경우에는 무결성 검증을 수행할 것〈신설 2013. 12. 3.〉
FISM-100	5.5 정보보호 시스템 설치 및 운영	전산실 내에 위치한 정보처리시스템과 해당 정보처리시스템의 운영, 개발, 보안 목적으로 직접 접속하는 단말기가 인터넷 등 외부통신망으로부터 물리적으로 분리 여부	5	○ **(전자금융감독규정)** - 제15조(해킹 등 방지대책)제1항제5호 ① 금융회사 또는 전자금융업자는 정보처리시스템 및 정보통신망을 해킹 등 전자적 침해행위로부터 방지하기 위하여 다음 각 호의 대책을 수립·운용 하여야 한다. 5. 전산실 내에 위치한 정보처리시스템과 해당 정보처리시스템의 운영, 개발,

평가 항목ID	통제구분	평가항목	위험도	[근거조항] 전자금융감독규정 (금융위원회고시 제2018-36호, 2018. 12. 21) 전자금융감독규정시행세칙 (금융감독원세칙, 2021. 2. 25)
				보안 목적으로 직접 접속하는 단말기에 대해서는 인터넷 등 외부통신망으로부터 물리적으로 분리할 것(단, 업무 특성상 분리하기 어렵다고 금융감독원장이 인정하는 경우에는 분리하지 아니하여도 된다.) 〈신설 2013. 12. 3., 개정 2015. 2. 3.〉 ○ **(전자금융감독규정시행세칙)** - 제2조의2 (망분리 적용 예외)제2항제4호 ② 규정 제15조제1항제5호에서 금융감독원장이 인정하는 경우란 다음 각 호와 같다. 4. 전산실 내에 위치한 정보처리시스템의 운영, 개발, 보안 목적으로 직접 접속하는 단말기와 외부통신망과의 연결 구간, 규정 제15조제1항제3호의 내부 업무용 시스템과의 연결 구간을 각각 차단한 경우
FISM-101	5.5 정보보호 시스템 설치 및 운영	정보보호시스템에 최소한의 서비스 번호와 기능 적용 여부	5	○ **(전자금융감독규정)** - 제15조(해킹 등 방지대책)제2항제2호 ② 제1항제1호의 규정에 따른 정보보호시스템을 설치·운영하는 경우에는 다음 각 호의 사항을 준수하여야 한다. 2. 최소한의 서비스번호(port)와 기능만을 적용하고 업무목적 이외의 기능 및 프로그램을 제거할 것
FISM-102	5.5 정보보호 시스템 설치 및 운영	정보보호시스템의 업무목적 이외 기능 및 프로그램 제거 여부	5	○ **(전자금융감독규정)** - 제15조(해킹 등 방지대책)제2항제2호 ② 제1항제1호의 규정에 따른 정보보호시스템을 설치·운영하는 경우에는 다음 각 호의 사항을 준수하여야 한다. 2. 최소한의 서비스번호(port)와 기능만을 적용하고 업무목적 이외의 기능 및 프로그램을 제거할 것

평가 항목ID	통제구분	평가항목	위험도	[근거조항] 전자금융감독규정 (금융위원회고시 제2018-36호, 2018. 12. 21) 전자금융감독규정시행세칙 (금융감독원세칙, 2021. 2. 25)
FISM-103	5.5 정보보호 시스템 설치 및 운영	정보보안 정책 승인 및 적용 시, 정책 등록, 변경, 삭제 내용에 대한 보관 여부	5	○ **(전자금융감독규정)** - 제15조(해킹 등 방지대책)제2항제3호,제3항 ② 제1항제1호의 규정에 따른 정보보호시스템을 설치·운영하는 경우에는 다음 각 호의 사항을 준수하여야 한다. 3. 보안정책의 승인·적용 및 보안정책의 등록, 변경 및 삭제에 대한 이력을 기록·보관할 것 ③ 제1항 각 호의 정보보호시스템에 대하여 책임자를 지정·운영하여야 하며, 운영 결과는 1년 이상 보존하여야 한다.
FISM-104	5.5 정보보호 시스템 설치 및 운영	정보보호시스템 원격관리 차단 여부	5	○ **(전자금융감독규정)** - 제15조(해킹 등 방지대책)제2항제4호 ② 제1항제1호의 규정에 따른 정보보호시스템을 설치·운영하는 경우에는 다음 각 호의 사항을 준수하여야 한다. 4. 정보보호시스템 원격관리를 금지할 것. 다만, 원격관리가 불가피한 경우 전용회선(전용회선과 동등한 보안수준을 갖춘 가상의 전용회선을 포함한다) 사용, 접근통제 등을 포함한 원격 접속 보안 대책을 수립·운영할 것 〈개정 2016. 10. 5.〉
FISM-105	5.5 정보보호 시스템 설치 및 운영	정보보호시스템 원격관리 이용 시, 원격 접속에 관한 보안대책 수립 여부	5	○ **(전자금융감독규정)** - 제15조(해킹 등 방지대책)제2항제4호 ② 제1항제1호의 규정에 따른 정보보호시스템을 설치·운영하는 경우에는 다음 각 호의 사항을 준수하여야 한다. 4. 정보보호시스템 원격관리를 금지할 것. 다만, 원격관리가 불가피한 경우 전용

평가 항목ID	통제구분	평가항목	위험도	[근거조항] 전자금융감독규정 (금융위원회고시 제2018-36호, 2018. 12. 21) 전자금융감독규정시행세칙 (금융감독원세칙, 2021. 2. 25)
				회선(전용회선과 동등한 보안수준을 갖춘 가상의 전용회선을 포함한다) 사용, 접근통제 등을 포함한 원격 접속 보안 대책을 수립·운영할 것 〈개정 2016. 10. 5.〉
FISM-106	5.5 정보보호 시스템 설치 및 운영	정보보호시스템 작동상태 모니터링 여부	5	○ **(전자금융감독규정)** - 제15조(해킹 등 방지대책)제2항제5호 ② 제1항제1호의 규정에 따른 정보보호시스템을 설치·운영하는 경우에는 다음 각 호의 사항을 준수하여야 한다. 5. 정보보호시스템의 작동 상태를 주기적으로 점검할 것 〈신설 2016. 10. 5〉
FISM-107	5.5 정보보호 시스템 설치 및 운영	정보보호시스템에 대한 백업 및 복구절차 수립 및 시행 여부	5	○ **(전자금융감독규정)** - 제15조(해킹 등 방지대책) ② 제1항제1호의 규정에 따른 정보보호시스템을 설치·운영하는 경우에는 다음 각 호의 사항을 준수하여야 한다. 6. 시스템 장애, 가동중지 등 긴급사태에 대비하여 백업 및 복구 절차 등을 수립·시행할 것 〈종전의 제5호에서 이동〉
FISM-108	5.5 정보보호 시스템 설치 및 운영	정보보호시스템 책임자 지정/운영 및 운영결과 1년 이상 보존 여부	5	○ **(전자금융감독규정)** - 제15조(해킹 등 방지대책)제3항 ③ 제1항 각 호의 정보보호시스템에 대하여 책임자를 지정·운영하여야 하며, 운영결과는 1년 이상 보존하여야 한다.
FISM-109	5.6 무선통신망 설치 및 운영	무선통신망 이용 업무의 정보보호 최고책임자 승인 및 사전 지정 여부	5	○ **(전자금융감독규정)** - 제15조(해킹 등 방지대책)제6항제1조 ⑥ 금융회사 또는 전자금융업자는 무선통신망을 설치·운용할 때에는 다음 각 호의

평가 항목ID	통제구분	평가항목	위험도	[근거조항] 전자금융감독규정 (금융위원회고시 제2018-36호, 2018. 12. 21) 전자금융감독규정시행세칙 (금융감독원세칙, 2021. 2. 25)
				사항을 준수하여야 한다. 〈개정 2013. 12. 3.〉 1. 무선통신망 이용 업무는 최소한으로 국한하고 법 제21조의2에 따른 정보보호 최고책임자의 승인을 받아 사전에 지정할 것
FISM-110	5.6 무선통신망 설치 및 운영	사용자인증, 암호화 등 무선통신망 보안대책 수립	5	○ **(전자금융감독규정)** - 제15조(해킹 등 방지대책)제6항제2조 ⑥ 금융회사 또는 전자금융업자는 무선통신망을 설치·운용할 때에는 다음 각 호의 사항을 준수하여야 한다. 〈개정 2013. 12. 3.〉 2. 무선통신망을 통한 불법 접속을 방지하기 위한 사용자인증, 암호화 등 보안 대책을 수립할 것
FISM-111	5.6 무선통신망 설치 및 운영	금융회사 내부망에 연결된 정보처리 시스템이 지정 된 업무 용도와 사용 지역(zone) 이외의 무선통신망에 접속하는 것을 차단하기 위한 차단 시스템 구축 여부	5	○ **(전자금융감독규정)** - 제15조(해킹 등 방지대책)제6항제3조 ⑥ 금융회사 또는 전자금융업자는 무선통신망을 설치·운용할 때에는 다음 각 호의 사항을 준수하여야 한다. 〈개정 2013. 12. 3.〉 3. 금융회사 내부망에 연결된 정보처리 시스템이 지정된 업무 용도와 사용 지역(zone) 이외의 무선통신망에 접속하는 것을 차단하기 위한 차단시스템을 구축하고 실시간 모니터링체계를 운영할 것 〈개정 2015. 2. 3.〉
FISM-112	5.6 무선통신망 설치 및 운영	무선통신망 실시간 모니터링체계 운영 여부	5	○ **(전자금융감독규정)** - 제15조(해킹 등 방지대책)제6항제3조 ⑥ 금융회사 또는 전자금융업자는 무선통신망을 설치·운용할 때에는 다음 각 호의 사항을 준수하여야 한다. 〈개정 2013. 12. 3.〉 3. 금융회사 내부망에 연결된 정보처리 시스템이 지정된 업무 용도와 사용 지역

평가 항목ID	통제구분	평가항목	위험도	[근거조항] 전자금융감독규정 (금융위원회고시 제2018-36호, 2018. 12. 21) 전자금융감독규정시행세칙 (금융감독원세칙, 2021. 2. 25)
				(zone) 이외의 무선통신망에 접속하는 것을 차단하기 위한 차단시스템을 구축하고 실시간 모니터링체계를 운영할 것 〈개정 2015. 2. 3.〉
FISM-113	5.6 무선통신망 설치 및 운영	비인가 무선접속장비 설치/접속여부 및 중요정보노출 여부에 대한 주기적 점검 여부	5	○ **(전자금융감독규정)** - 제15조(해킹 등 방지대책)제6항제4조 ⑥ 금융회사 또는 전자금융업자는 무선통신망을 설치·운용할 때에는 다음 각 호의 사항을 준수하여야 한다. 〈개정 2013. 12. 3.〉 4. 비인가 무선접속장비(Access Point : AP) 설치·접속여부, 중요 정보 노출 여부를 주기적으로 점검할 것
FISM-114	5.7 악성코드 감염 방지대책	응용프로그램에 대한 악성코드검색 프로그램 진단/치료 후 사용 여부	5	○ **(전자금융감독규정)** - 제16조(악성코드 감염 방지대책)제1항제1호 ① 금융회사 또는 전자금융업자는 악성코드 감염을 방지하기 위하여 다음 각 호를 포함한 대책을 수립·운용하여야 한다. 〈개정 2013. 12. 3.〉 1. 응용프로그램을 사용할 때에는 악성코드 검색프로그램 등으로 진단 및 치료 후 사용할 것
FISM-115	5.7 악성코드 감염 방지대책	악성코드 검색 및 치료프로그램의 최신상태 유지 여부	5	○ **(전자금융감독규정)** - 제16조(악성코드 감염 방지대책)제1항제2호 ① 금융회사 또는 전자금융업자는 악성코드 감염을 방지하기 위하여 다음 각 호를 포함한 대책을 수립·운용하여야 한다. 〈개정 2013. 12. 3.〉 2. 악성코드 검색 및 치료프로그램은 최신상태로 유지할 것

평가 항목ID	통제구분	평가항목	위험도	[근거조항] 전자금융감독규정 (금융위원회고시 제2018-36호, 2018. 12. 21) 전자금융감독규정시행세칙 (금융감독원세칙, 2021. 2. 25)
FISM-116	5.7 악성코드 감염 방지대책	악성코드 감염대비 복구절차 마련 여부	5	○ **(전자금융감독규정)** - 제16조(악성코드 감염 방지대책)제1항제3호 ① 금융회사 또는 전자금융업자는 악성코드 감염을 방지하기 위하여 다음 각 호를 포함한 대책을 수립·운용하여야 한다. 〈개정 2013. 12. 3.〉 3. 악성코드 감염에 대비하여 복구 절차를 마련할 것
FISM-117	5.7 악성코드 감염 방지대책	중요 단말기의 악성코드 감염 여부 매일 점검 여부	5	○ **(전자금융감독규정)** - 제12조(단말기 보호대책)제3호 금융회사 또는 전자금융업자는 단말기 보호를 위하여 다음 각 호의 사항을 준수하여야 한다. 〈개정 2013. 12. 3.〉 3. 외부 반출, 인터넷 접속, 그룹웨어 접속의 금지 등 강화된 보호대책이 적용되는 중요단말기를 지정할 것 〈개정 2013. 12. 3., 2015. 2. 3.〉 - 제16조(악성코드 감염 방지대책)제1항제4호 ① 금융회사 또는 전자금융업자는 악성코드 감염을 방지하기 위하여 다음 각 호를 포함한 대책을 수립·운용하여야 한다. 〈개정 2013. 12. 3.〉 4. 제12조제3호에 따른 중요 단말기는 악성코드 감염여부를 매일 점검할 것 〈개정 2015. 2. 3.〉
FISM-118	5.7 악성코드 감염 방지대책	악성코드 감염 발견시 악성코드 확산 및 피해 최소화를 위한 필요 조치 마련 및 시행 여부	5	○ **(전자금융감독규정)** - 제16조(악성코드 감염 방지대책) ② 금융회사 또는 전자금융업자는 악성코드 감염이 발견된 경우 악성코드 확산 및 피해를 최소화하기 위하여 필요한 조치를 신속하게 취하여야 한다. 〈개정 2013. 12. 3.〉

평가 항목ID	통제구분	평가항목	위험도	[근거조항] 전자금융감독규정 (금융위원회고시 제2018-36호, 2018. 12. 21) 전자금융감독규정시행세칙 (금융감독원세칙, 2021. 2. 25)
FISM-119	5.8 공개 서버 보안	공개용 웹서버의 DMZ구간내 설치 여부	5	○ **(전자금융감독규정)** - 제17조(홈페이지 등 공개용 웹서버 관리대책) ① 금융회사 또는 전자금융업자는 공개용 웹서버의 안전한 관리를 위하여 다음 각 호를 포함한 적절한 대책을 수립·운용하여야 한다. 〈개정 2013. 12. 3.〉 1. 공개용 웹서버를 내부통신망과 분리하여 내부통신망과 외부통신망사이의 독립된 통신망(이하 "DMZ구간"이라 한다)에 설치하고 네트워크 및 웹 접근 제어 수단으로 보호할 것
FISM-120	5.8 공개 서버 보안	공개용 웹서버의 네트워크 및 웹 접근 제어 수단으로 보호 여부	5	○ **(전자금융감독규정)** - 제17조(홈페이지 등 공개용 웹서버 관리대책)제1항제1호 ① 금융회사 또는 전자금융업자는 공개용 웹서버의 안전한 관리를 위하여 다음 각 호를 포함한 적절한 대책을 수립·운용하여야 한다. 〈개정 2013. 12. 3.〉 1. 공개용 웹서버를 내부통신망과 분리하여 내부통신망과 외부통신망사이의 독립된 통신망(이하 "DMZ구간"이라 한다)에 설치하고 네트워크 및 웹 접근 제어 수단으로 보호할 것
FISM-121	5.8 공개 서버 보안	공개용 웹서버 접근 사용자계정을 업무관련자로 제한 여부	5	○ **(전자금융감독규정)** - 제17조(홈페이지 등 공개용 웹서버 관리대책)제1항제2호 ① 금융회사 또는 전자금융업자는 공개용 웹서버의 안전한 관리를 위하여 다음 각 호를 포함한 적절한 대책을 수립·운용하여야 한다. 〈개정 2013. 12. 3.〉 2. 공개용 웹서버에 접근할 수 있는 사용자계정은 업무관련자만 접속할 수 있도록 제한하고 아이디·비밀번호 이외에 추가 인증수단을 적용할 것 〈개정 2015. 2. 3.〉

평가 항목ID	통제구분	평가항목	위험도	[근거조항] 전자금융감독규정 (금융위원회고시 제2018-36호, 2018. 12. 21) 전자금융감독규정시행세칙 (금융감독원세칙, 2021. 2. 25)
FISM-122	5.8 공개 서버 보안	공개용 웹서버에 접근할 수 있는 사용자계정은 아이디 비밀번호 이외에 추가인증수단 적용 여부	5	○ **(전자금융감독규정)** - 제17조(홈페이지 등 공개용 웹서버 관리대책)제1항제2호 ① 금융회사 또는 전자금융업자는 공개용 웹서버의 안전한 관리를 위하여 다음 각 호를 포함한 적절한 대책을 수립·운용하여야 한다. 〈개정 2013. 12. 3.〉 2. 공개용 웹서버에 접근할 수 있는 사용자계정은 업무관련자만 접속할 수 있도록 제한하고 아이디·비밀번호 이외에 추가 인증수단을 적용할 것 〈개정 2015. 2. 3.〉
FISM-123	5.8 공개 서버 보안	공개용 웹서버 제공이외 다른 서비스 및 시험/개발도구 등의 사용 제한 여부	5	○ **(전자금융감독규정)** - 제17조(홈페이지 등 공개용 웹서버 관리대책)제17조제1항제3호 ① 금융회사 또는 전자금융업자는 공개용 웹서버의 안전한 관리를 위하여 다음 각 호를 포함한 적절한 대책을 수립·운용하여야 한다. 〈개정 2013. 12. 3.〉 3. 공개용 웹서버에서 제공하는 서비스를 제외한 다른 서비스 및 시험·개발 도구 등의 사용을 제한할 것
FISM-124	5.8 공개 서버 보안	DMZ구간내 이용자 정보 등 주요정보 저장 및 관리 금지 여부	5	○ **(전자금융감독규정)** - 제17조(홈페이지 등 공개용 웹서버 관리대책)제1항제4호 ① 금융회사 또는 전자금융업자는 공개용 웹서버의 안전한 관리를 위하여 다음 각 호를 포함한 적절한 대책을 수립·운용하여야 한다. 〈개정 2013. 12. 3.〉 4. DMZ구간 내에 이용자 정보 등 주요 정보를 저장 및 관리하지 아니할 것 (다만, 거래로그를 관리하기 위한 경우에는 예외로 하되 이 경우 반드시 암호화하여 저장·관리하여야 한다)

평가 항목ID	통제구분	평가항목	위험도	[근거조항] 전자금융감독규정 (금융위원회고시 제2018-36호, 2018. 12. 21) 전자금융감독규정시행세칙 (금융감독원세칙, 2021. 2. 25)
FISM-125	5.8 공개 서버 보안	공개용 웹서버 거래로그의 암호화하여 저장/관리 여부	5	○ **(전자금융감독규정)** - 제17조(홈페이지 등 공개용 웹서버 관리대책)제1항제4호 ① 금융회사 또는 전자금융업자는 공개용 웹서버의 안전한 관리를 위하여 다음 각 호를 포함한 적절한 대책을 수립·운용하여야 한다. 〈개정 2013. 12. 3.〉 4. DMZ구간 내에 이용자 정보 등 주요 정보를 저장 및 관리하지 아니할 것(다만, 거래로그를 관리하기 위한 경우에는 예외로 하되 이 경우 반드시 암호화하여 저장·관리하여야 한다)
FISM-126	5.8 공개 서버 보안	공개용 웹서버 게시자료에 대한 사전 관리 실시 여부	5	○ **(전자금융감독규정)** - 제17조(홈페이지 등 공개용 웹서버 관리대책)제2항제1호 ② 금융회사 또는 전자금융업자는 공개용 웹서버에 게재된 내용에 대하여 다음 각 호의 사항을 준수하여야 한다. 〈개정 2013. 12. 3.〉 1. 게시자료에 대한 사전 내부통제 실시
FISM-127	5.8 공개 서버 보안	공개용 웹서버에 무기명 또는 가명에 의한 게시 금지 여부	5	○ **(전자금융감독규정)** - 제17조(홈페이지 등 공개용 웹서버 관리대책)제2항제2호 ② 금융회사 또는 전자금융업자는 공개용 웹서버에 게재된 내용에 대하여 다음 각 호의 사항을 준수하여야 한다. 〈개정 2013. 12. 3.〉 2. 무기명 또는 가명에 의한 게시 금지

평가 항목ID	통제구분	평가항목	위험도	[근거조항] 전자금융감독규정 (금융위원회고시 제2018-36호, 2018. 12. 21) 전자금융감독규정시행세칙 (금융감독원세칙, 2021. 2. 25)
FISM-128	5.8 공개 서버 보안	홈페이지에 자료를 게시하는 담당자의 지정/운용 여부	5	○ **(전자금융감독규정)** - 제17조(홈페이지 등 공개용 웹서버 관리대책)제2항제3호 ② 금융회사 또는 전자금융업자는 공개용 웹서버에 게재된 내용에 대하여 다음 각 호의 사항을 준수하여야 한다. 〈개정 2013. 12. 3.〉 3. 홈페이지에 자료를 게시하는 담당자의 지정·운용
FISM-129	5.8 공개 서버 보안	개인정보의 유출 및 위/변조를 방지하기 위한 보안조치 여부	5	○ **(전자금융감독규정)** - 제17조(홈페이지 등 공개용 웹서버 관리대책)제2항제4호 ② 금융회사 또는 전자금융업자는 공개용 웹서버에 게재된 내용에 대하여 다음 각 호의 사항을 준수하여야 한다. 〈개정 2013. 12. 3.〉 4. 개인정보의 유출 및 위·변조를 방지하기 위한 보안조치
FISM-130	5.8 공개 서버 보안	공개용 웹서버가 해킹공격에 노출되지 않도록 대응 조치 여부	5	○ **(전자금융감독규정)** - 제17조(홈페이지 등 공개용 웹서버 관리대책)제4항 ④ 금융회사 또는 전자금융업자는 공개용 웹서버가 해킹공격에 노출되지 않도록 대응 조치하여야 한다. 〈개정 2013. 12. 3., 2015. 2. 3.〉
FISM-131	5.8 공개 서버 보안	단말기에서 음란, 도박 등 업무와 무관한 프로그램 및 인터넷사이트에 대한 접근 통제 여부	5	○ **(전자금융감독규정)** - 제17조(홈페이지 등 공개용 웹서버 관리대책)제5항 ⑤ 금융회사 또는 전자금융업자는 단말기에서 음란, 도박 등 업무와 무관한 프로그램 또는 인터넷 사이트에 접근하는 것에 대한 통제대책을 마련하여야 한다. 〈개정 2013. 12. 3.〉

평가 항목ID	통제구분	평가항목	위험도	[근거조항] 전자금융감독규정 (금융위원회고시 제2018-36호, 2018. 12. 21) 전자금융감독규정시행세칙 (금융감독원세칙, 2021. 2. 25)
FISM-132	5.9 IP주소 관리	내부통신망 IP에 대한 사설IP 주소 사용 여부	5	○ **(전자금융감독규정)** - 제18조(IP주소 관리대책)제1호 금융회사 또는 전자금융업자는 정보제공자 주소(이하 "IP주소"라 한다)의 안전한 사용을 위하여 다음 각 호를 포함하여 적절한 대책을 수립·운용하여야 한다. 〈개정 2013. 12. 3.〉 1. 내부통신망에서 사용하는 IP주소의 경우 사설 IP주소 사용 등으로 보안을 강화하며 내부 IP주소체계의 외부유출을 금지할 것
FISM-133	5.9 IP주소 관리	IP주소 체계 외부유출 금지 여부	5	○ **(전자금융감독규정)** - 제18조(IP주소 관리대책)제1호 금융회사 또는 전자금융업자는 정보제공자 주소(이하 "IP주소"라 한다)의 안전한 사용을 위하여 다음 각 호를 포함하여 적절한 대책을 수립·운용하여야 한다. 〈개정 2013. 12. 3.〉 1. 내부통신망에서 사용하는 IP주소의 경우 사설 IP주소 사용 등으로 보안을 강화하며 내부 IP주소체계의 외부유출을 금지할 것
FISM-134	5.9 IP주소 관리	개인별로 내부 IP주소를 부여 및 유지/관리 여부	5	○ **(전자금융감독규정)** - 제18조(IP주소 관리대책)제2호 금융회사 또는 전자금융업자는 정보제공자 주소(이하 "IP주소"라 한다)의 안전한 사용을 위하여 다음 각 호를 포함하여 적절한 대책을 수립·운용하여야 한다. 〈개정 2013. 12. 3.〉 2. 개인별로 내부 IP주소를 부여하여 유지·관리할 것

평가 항목ID	통제구분	평가항목	위험도	[근거조항] 전자금융감독규정 (금융위원회고시 제2018-36호, 2018. 12. 21) 전자금융감독규정시행세칙 (금융감독원세칙, 2021. 2. 25)
FISM-135	5.9 IP주소 관리	내/외부 IP주소의 인터넷 접속내용 1년이상 별도 기록/보관 여부	5	○ **(전자금융감독규정)** - 제18조(IP주소 관리대책)제3호 금융회사 또는 전자금융업자는 정보제공자 주소(이하 "IP주소"라 한다)의 안전한 사용을 위하여 다음 각 호를 포함하여 적절한 대책을 수립·운용하여야 한다. 〈개정 2013. 12. 3.〉 3. 내부 IP주소 및 외부 IP주소의 인터넷 접속내용을 1년 이상 별도로 기록·보관할 것
FISM-136	5.9 IP주소 관리	운영, 개발, 외주 등 업무특성별로 네트워크 분리 및 IP주소 사용 여부	5	○ **(전자금융감독규정)** - 제18조(IP주소 관리대책)제4호 금융회사 또는 전자금융업자는 정보제공자 주소(이하 "IP주소"라 한다)의 안전한 사용을 위하여 다음 각 호를 포함하여 적절한 대책을 수립·운용하여야 한다. 〈개정 2013. 12. 3.〉 4. 정보처리시스템의 운영담당, 개발담당 및 외부직원 등 업무 특성별로 네트워크를 적절하게 분리하여 IP주소를 사용할 것. 다만, 외부직원 등과의 공동작업 수행 등 네트워크의 분리가 어렵다고 금융감독원장이 정하는 경우에는 업무특성별로 접근권한을 분리하여 IP주소를 사용할 수 있다. 〈개정 2015. 6. 24.〉
FISM-137	5.9 IP주소 관리	내부통신망의 다른 기관 내부 통신망과 분리 사용 여부	5	○ **(전자금융감독규정)** - 제18조(IP주소 관리대책)제5호 금융회사 또는 전자금융업자는 정보제공자 주소(이하 "IP주소"라 한다)의 안전한 사용을 위하여 다음 각 호를 포함하여 적절한 대책을 수립·운용하여야 한다. 〈개정 2013. 12. 3.〉 5. 내부통신망은 다른 기관 내부통신망과 분리하여 사용할 것

평가 항목ID	통제구분	평가항목	위험도	[근거조항] 전자금융감독규정 (금융위원회고시 제2018-36호, 2018. 12. 21) 전자금융감독규정시행세칙 (금융감독원세칙, 2021. 2. 25)
FISM-138	5.10 암호프로그램 및 암호키 관리	암호프로그램 담당자 지정 여부	5	○ **(전자금융감독규정)** - 제31조(암호프로그램 및 키 관리 통제)제1항 ① 금융회사 또는 전자금융업자는 암호프로그램에 대하여 담당자 지정, 담당자 이외의 이용 통제 및 원시프로그램(source program) 별도 보관 등을 준수하여 유포 및 부당 이용이 발생하지 않도록 하여야 한다. 〈개정 2013. 12. 3.〉
FISM-139	5.10 암호프로그램 및 암호키 관리	암호프로그램의 비담당자 이용에 관한 통제 여부	5	○ **(전자금융감독규정)** - 제31조(암호프로그램 및 키 관리 통제)제1항 ① 금융회사 또는 전자금융업자는 암호프로그램에 대하여 담당자 지정, 담당자 이외의 이용 통제 및 원시프로그램(source program) 별도 보관 등을 준수하여 유포 및 부당 이용이 발생하지 않도록 하여야 한다. 〈개정 2013. 12. 3.〉
FISM-140	5.10 암호프로그램 및 암호키 관리	암호프로그램에 대한 원시프로그램 별도 보관 여부	5	○ **(전자금융감독규정)** - 제31조(암호프로그램 및 키 관리 통제)제1항 ① 금융회사 또는 전자금융업자는 암호프로그램에 대하여 담당자 지정, 담당자 이외의 이용 통제 및 원시프로그램(source program) 별도 보관 등을 준수하여 유포 및 부당 이용이 발생하지 않도록 하여야 한다. 〈개정 2013. 12. 3.〉
FISM-141	5.10 암호프로그램 및 암호키 관리	암호 및 인증시스템에 적용되는 키에 대하여 주입/운용/갱신/폐기에 대한 절차 및 방법 마련 여부	5	○ **(전자금융감독규정)** - 제31조(암호프로그램 및 키 관리 통제)제2항 ② 금융회사 또는 전자금융업자는 암호 및 인증시스템에 적용되는 키에 대하여 주입·운용·갱신·폐기에 대한 절차 및 방법을 마련하여 안전하게 관리하여야 한다. 〈개정 2013. 12. 3.〉

평가 항목ID	통제구분	평가항목	위험도	[근거조항] 전자금융감독규정 (금융위원회고시 제2018-36호, 2018. 12. 21) 전자금융감독규정시행세칙 (금융감독원세칙, 2021. 2. 25)
FISM-142	6.1 계정 및 권한 관리	사용자계정에 대한 비밀번호 등록/변경/폐기 체계 및 절차 마련 여부	5	○ **(전자금융감독규정)** - 제13조(전산자료 보호대책)제1항제1호 ① 금융회사 또는 전자금융업자는 전산자료의 유출, 파괴 등을 방지하기 위하여 다음 각 호를 포함한 전산자료 보호대책을 수립·운용하여야 한다. 〈개정 2013. 12. 3.〉 1. 사용자계정과 비밀번호를 개인별로 부여하고 등록·변경·폐기를 체계적으로 관리할 것
FISM-143	6.1 계정 및 권한 관리	개인별 사용자계정 및 비밀번호 부여 여부	5	○ **(전자금융감독규정)** - 제13조(전산자료 보호대책)제1항제1호 ① 금융회사 또는 전자금융업자는 전산자료의 유출, 파괴 등을 방지하기 위하여 다음 각 호를 포함한 전산자료 보호대책을 수립·운용하여야 한다. 〈개정 2013. 12. 3.〉 1. 사용자계정과 비밀번호를 개인별로 부여하고 등록·변경·폐기를 체계적으로 관리할 것
FISM-144	6.1 계정 및 권한 관리	외부사용자에 대한 최소 작업권한 할당 및 통제장치 설치 여부	5	○ **(전자금융감독규정)** - 제13조(전산자료 보호대책)제1항제2호 ① 금융회사 또는 전자금융업자는 전산자료의 유출, 파괴 등을 방지하기 위하여 다음 각 호를 포함한 전산자료 보호대책을 수립·운용하여야 한다. 〈개정 2013. 12. 3.〉 2. 외부사용자에게 사용자계정을 부여하는 경우 최소한의 작업권한만 할당하고 적절한 통제장치를 갖출 것

평가 항목ID	통제구분	평가항목	위험도	[근거조항] 전자금융감독규정 (금융위원회고시 제2018-36호, 2018. 12. 21) 전자금융감독규정시행세칙 (금융감독원세칙, 2021. 2. 25)
FISM-145	6.1 계정 및 권한 관리	전산자료 입력/출력/열람 시 사용자 업무별 접근권한 통제 여부	5	○ **(전자금융감독규정)** - 제13조(전산자료 보호대책) ① 금융회사 또는 전자금융업자는 전산자료의 유출, 파괴 등을 방지하기 위하여 다음 각 호를 포함한 전산자료 보호대책을 수립·운용하여야 한다. 〈개정 2013. 12. 3.〉 4. 전산자료의 입력·출력·열람을 함에 있어 사용자의 업무별로 접근권한을 통제할 것
FISM-146	6.1 계정 및 권한 관리	사용자 인사조치 시 지체없이 해당 사용자 계정 삭제, 사용 중지, 공동사용 계정 변경 등 정보처리시스템 접근 통제 여부	5	○ **(전자금융감독규정)** - 제13조(전산자료 보호대책)제1항제14호 ① 금융회사 또는 전자금융업자는 전산자료의 유출, 파괴 등을 방지하기 위하여 다음 각 호를 포함한 전산자료 보호대책을 수립·운용하여야 한다. 〈개정 2013. 12. 3.〉 14. 사용자가 전출·퇴직 등 인사조치가 있을 때에는 지체 없이 해당 사용자 계정 삭제, 계정 사용 중지, 공동 사용 계정 변경 등 정보처리시스템에 대한 접근을 통제할 것 〈개정 2013. 12. 3.〉
FISM-147	6.1 계정 및 권한 관리	사용자 계정 공동사용 시 개인별 사용내역에 대한 기록저장 및 관리 여부	5	○ **(전자금융감독규정)** - 제13조(전산자료 보호대책)제1항제1호,제2항 ① 금융회사 또는 전자금융업자는 전산자료의 유출, 파괴 등을 방지하기 위하여 다음 각 호를 포함한 전산자료 보호대책을 수립·운용하여야 한다. 〈개정 2013. 12. 3.〉 1. 사용자계정과 비밀번호를 개인별로 부여하고 등록·변경·폐기를 체계적으로 관리할 것 ② 제1항제1호의 사용자계정의 공동 사용이 불가피한 경우에는 개인별 사용내역을 기록·관리하여야 한다.

평가 항목ID	통제구분	평가항목	위험도	[근거조항] 전자금융감독규정 (금융위원회고시 제2018-36호, 2018. 12. 21) 전자금융감독규정시행세칙 (금융감독원세칙, 2021. 2. 25)
FISM-148	6.2 정보처리 시스템 관리자 통제	정보처리시스템 관리자에 대한 적절한 통제장치 마련 및 운용 여부	5	○ **(전자금융감독규정)** - 제13조(전산자료 보호대책)제5항 ⑤ 금융회사 또는 전자금융업자는 단말기와 전산자료의 접근권한이 부여되는 정보처리시스템 관리자에 대하여 적절한 통제장치를 마련·운용하여야 한다. 다만, 정보처리시스템 관리자의 주요 업무 관련 행위는 책임자가 제28조제2항에 따라 이중확인 및 모니터링을 하여야 한다. 〈개정 2013. 12. 3.〉
FISM-149	6.2 정보처리 시스템 관리자 통제	정보처리시스템 관리자 주요업무 관련행위의 책임자 이중 확인 및 모니터링 여부	5	○ **(전자금융감독규정)** - 제13조(전산자료 보호대책)제5항 ⑤ 금융회사 또는 전자금융업자는 단말기와 전산자료의 접근권한이 부여되는 정보처리시스템 관리자에 대하여 적절한 통제장치를 마련·운용하여야 한다. 다만, 정보처리시스템 관리자의 주요 업무 관련 행위는 책임자가 제28조제2항에 따라 이중확인 및 모니터링을 하여야 한다. 〈개정 2013. 12. 3.〉
FISM-150	6.3 내부사용자 비밀번호 관리	내부사용자에 대한 비밀번호 설정 및 운영 여부	5	○ **(전자금융감독규정)** - 제32조(내부사용자 비밀번호 관리)제1호 금융회사 또는 전자금융업자는 내부사용자의 비밀번호 유출을 방지하지 위하여 다음 각 호의 사항을 정보처리시스템에 반영하여야 한다. 〈개정 2013. 12. 3.〉 1. 담당업무 외에는 열람 및 출력을 제한할 수 있는 접근자의 비밀번호를 설정하여 운영할 것
FISM-151	6.3 내부사용자 비밀번호 관리	내부사용자 비밀번호 설정 시, 이용자 식별부호(아이디), 생년월일, 주민등록번호, 전화번호 포함 금지 여부	5	○ **(전자금융감독규정)** - 제32조(내부사용자 비밀번호 관리)제2호가목 금융회사 또는 전자금융업자는 내부사용자의 비밀번호 유출을 방지하기 위하여 다음

평가 항목ID	통제구분	평가항목	위험도	[근거조항] 전자금융감독규정 (금융위원회고시 제2018-36호, 2018. 12. 21) 전자금융감독규정시행세칙 (금융감독원세칙, 2021. 2. 25)
				각 호의 사항을 정보처리시스템에 반영하여야 한다. 〈개정 2013. 12. 3.〉 2. 비밀번호는 다음 각 목의 사항을 준수할 것 가. 비밀번호는 이용자 식별부호(아이디), 생년월일, 주민등록번호, 전화번호를 포함하지 않은 숫자와 영문자 및 특수문자 등을 혼합하여 8자리 이상으로 설정하고 분기별 1회 이상 변경
FISM-152	6.3 내부사용자 비밀번호 관리	비밀번호는 숫자, 영문자 및 특수문자 등 혼합 8자리이상 설정 여부	5	○ **(전자금융감독규정)** - 제32조(내부사용자 비밀번호 관리)제2호가목 금융회사 또는 전자금융업자는 내부사용자의 비밀번호 유출을 방지하지 위하여 다음 각 호의 사항을 정보처리시스템에 반영하여야 한다. 〈개정 2013. 12. 3.〉 2. 비밀번호는 다음 각 목의 사항을 준수할 것 가. 비밀번호는 이용자 식별부호(아이디), 생년월일, 주민등록번호, 전화번호를 포함하지 않은 숫자와 영문자 및 특수문자 등을 혼합하여 8자리 이상으로 설정하고 분기별 1회 이상 변경
FISM-153	6.3 내부사용자 비밀번호 관리	내부사용자 비밀번호에 관한 주기적(분기별 1회 이상) 변경 여부	5	○ **(전자금융감독규정)** - 제32조(내부사용자 비밀번호 관리)제2호가목 금융회사 또는 전자금융업자는 내부사용자의 비밀번호 유출을 방지하지 위하여 다음 각 호의 사항을 정보처리시스템에 반영하여야 한다. 〈개정 2013. 12. 3.〉 2. 비밀번호는 다음 각 목의 사항을 준수할 것 가. 비밀번호는 이용자 식별부호(아이디), 생년월일, 주민등록번호, 전화번호를 포함하지 않은 숫자와 영문자 및 특수문자 등을 혼합하여 8자리 이상으로 설정하고 분기별 1회 이상 변경

평가 항목ID	통제구분	평가항목	위험도	[근거조항] 전자금융감독규정 (금융위원회고시 제2018-36호, 2018. 12. 21) 전자금융감독규정시행세칙 (금융감독원세칙, 2021. 2. 25)
FISM-154	6.3 내부사용자 비밀번호 관리	내부사용자 비밀번호 보관시 암호화 여부	5	○ **(전자금융감독규정)** - 제32조(내부사용자 비밀번호 관리)제2호나목 금융회사 또는 전자금융업자는 내부사용자의 비밀번호 유출을 방지하지 위하여 다음 각 호의 사항을 정보처리시스템에 반영하여야 한다. 〈개정 2013. 12. 3.〉 2. 비밀번호는 다음 각 목의 사항을 준수할 것 나. 비밀번호 보관 시 암호화
FISM-155	6.3 내부사용자 비밀번호 관리	정보처리시스템마다 각기 다른 관리자 비밀번호 적용 여부	5	○ **(전자금융감독규정)** - 제32조(내부사용자 비밀번호 관리)제2호다목 금융회사 또는 전자금융업자는 내부사용자의 비밀번호 유출을 방지하지 위하여 다음 각 호의 사항을 정보처리시스템에 반영하여야 한다. 〈개정 2013. 12. 3.〉 2. 비밀번호는 다음 각 목의 사항을 준수할 것 다. 시스템마다 관리자 비밀번호를 다르게 부여
FISM-156	6.3 내부사용자 비밀번호 관리	내부사용자 비밀번호 연속 입력 오류(최대5회)시 즉시 접속 차단 여부	5	○ **(전자금융감독규정)** - 제32조(내부사용자 비밀번호 관리) 금융회사 또는 전자금융업자는 내부사용자의 비밀번호 유출을 방지하지 위하여 다음 각 호의 사항을 정보처리시스템에 반영하여야 한다. 〈개정 2013. 12. 3.〉 3. 비밀번호 입력 시 5회 이내의 범위에서 미리 정한 횟수 이상의 입력오류가 연속하여 발생한 경우 즉시 해당 비밀번호를 이용하는 접속을 차단하고 본인 확인절차를 거쳐 비밀번호를 재부여하거나 초기화 할 것

평가 항목ID	통제구분	평가항목	위험도	[근거조항] 전자금융감독규정 (금융위원회고시 제2018-36호, 2018. 12. 21) 전자금융감독규정시행세칙 (금융감독원세칙, 2021. 2. 25)
FISM-157	6.3 내부사용자 비밀번호 관리	차단된 내부사용자 비밀번호 변경 시 본인확인 절차 적용 여부	5	○ **(전자금융감독규정)** - 제32조(내부사용자 비밀번호 관리)제3호 금융회사 또는 전자금융업자는 내부사용자의 비밀번호 유출을 방지하지 위하여 다음 각 호의 사항을 정보처리시스템에 반영하여야 한다. 〈개정 2013. 12. 3.〉 3. 비밀번호 입력 시 5회 이내의 범위에서 미리 정한 횟수 이상의 입력오류가 연속하여 발생한 경우 즉시 해당 비밀번호를 이용하는 접속을 차단하고 본인 확인절차를 거쳐 비밀번호를 재부여하거나 초기화 할 것
FISM-158	6.4 이용자 비밀번호 관리	정보처리시스템 및 전산자료에 보관하고 있는 이용자 비밀번호 암호화 보관 여부	5	○ **(전자금융감독규정)** - 제33조(이용자 비밀번호 관리)제1항 ① 금융회사 또는 전자금융업자는 정보처리시스템 및 전산자료에 보관하고 있는 이용자의 비밀번호를 암호화하여 보관하며 동 비밀번호를 조회할 수 없도록 하여야 한다. 다만, 비밀번호의 조회가 불가피하다고 인정되는 경우에는 그 조회사유·내용 등을 기록·관리하여야 한다. 〈개정 2013. 12. 3.〉
FISM-159	6.4 이용자 비밀번호 관리	이용자 비밀번호 조회 금지 및 불가피한 경우 조회사유 및 내용 기록 관리 여부	5	○ **(전자금융감독규정)** - 제33조(이용자 비밀번호 관리)제1항 ① 금융회사 또는 전자금융업자는 정보처리시스템 및 전산자료에 보관하고 있는 이용자의 비밀번호를 암호화하여 보관하며 동 비밀번호를 조회할 수 없도록 하여야 한다. 다만, 비밀번호의 조회가 불가피하다고 인정되는 경우에는 그 조회사유·내용 등을 기록·관리하여야 한다. 〈개정 2013. 12. 3.〉

평가 항목ID	통제구분	평가항목	위험도	[근거조항] 전자금융감독규정 (금융위원회고시 제2018-36호, 2018. 12. 21) 전자금융감독규정시행세칙 (금융감독원세칙, 2021. 2. 25)
FISM-160	6.4 이용자 비밀번호 관리	이용자 비밀번호 등록 시, 주민등록번호/동일숫자/연속숫자 등 제3자가 쉽게 유추할 수 있는 비밀번호의 등록 금지 여부	5	○ **(전자금융감독규정)** - 제33조(이용자 비밀번호 관리)제2항제1호 ② 금융회사 또는 전자금융업자는 이용자의 비밀번호 유출을 방지하기 위하여 다음 각 호의 사항을 정보처리시스템에 반영하여야 한다. 〈개정 2013. 12. 3.〉 1. 주민등록번호, 동일숫자, 연속숫자 등 제3자가 쉽게 유추할 수 있는 비밀번호의 등록 불가
FISM-161	6.4 이용자 비밀번호 관리	이용자 비밀번호가 통신용 비밀번호와 계좌원장 비밀번호 구분하여 사용하고 있는지 여부	5	○ **(전자금융감독규정)** - 제33조(이용자 비밀번호 관리)제2항제2호 ② 금융회사 또는 전자금융업자는 이용자의 비밀번호 유출을 방지하기 위하여 다음 각 호의 사항을 정보처리시스템에 반영하여야 한다. 〈개정 2013. 12. 3.〉 2. 통신용 비밀번호와 계좌원장 비밀번호를 구분해서 사용
FISM-162	6.4 이용자 비밀번호 관리	이용자 비밀번호가 일정횟수(최대5회) 입력오류 시 해당비밀번호 이용 거래에 대한 즉시 중지 여부	5	○ **(전자금융감독규정)** - 제33조(이용자 비밀번호 관리)제2항제3호 ② 금융회사 또는 전자금융업자는 이용자의 비밀번호 유출을 방지하기 위하여 다음 각 호의 사항을 정보처리시스템에 반영하여야 한다. 〈개정 2013. 12. 3.〉 3. 5회 이내의 범위에서 미리 정한 횟수 이상의 비밀번호 입력 오류가 발생한 경우 즉시 해당 비밀번호를 이용하는 거래를 중지시키고 본인 확인절차를 거친 후 비밀번호 재부여 및 거래 재개(이체 비밀번호 등 동일한 비밀번호가 다양한 형태의 전자금융거래에 공통으로 이용되는 경우, 입력오류 횟수는 이용되는 모든 전자금융거래에 대하여 통산한다)

평가 항목ID	통제구분	평가항목	위험도	[근거조항] 전자금융감독규정 (금융위원회고시 제2018-36호, 2018. 12. 21) 전자금융감독규정시행세칙 (금융감독원세칙, 2021. 2. 25)
FISM-163	6.4 이용자 비밀번호 관리	이체비밀번호 등 동일한 비밀번호가 다양한 형태의 전자금융거래에 공통으로 이용되는 경우 입력오류 횟수는 이용되는 모든 전자금융거래에 통산 여부	5	○ **(전자금융감독규정)** - 제33조(이용자 비밀번호 관리)제2항제3호 ② 금융회사 또는 전자금융업자는 이용자의 비밀번호 유출을 방지하기 위하여 다음 각 호의 사항을 정보처리시스템에 반영하여야 한다. 〈개정 2013. 12. 3.〉 3. 5회 이내의 범위에서 미리 정한 횟수 이상의 비밀번호 입력 오류가 발생한 경우 즉시 해당 비밀번호를 이용하는 거래를 중지시키고 본인 확인절차를 거친 후 비밀번호 재부여 및 거래 재개(이체 비밀번호 등 동일한 비밀번호가 다양한 형태의 전자금융거래에 공통으로 이용되는 경우, 입력오류 횟수는 이용되는 모든 전자금융거래에 대하여 통산한다)
FISM-164	6.4 이용자 비밀번호 관리	이용 중지된 이용자 비밀번호의 재부여 또는 거래재개 시 본인확인 절차 적용 여부	5	○ **(전자금융감독규정)** - 제33조(이용자 비밀번호 관리)제2항제3호 ② 금융회사 또는 전자금융업자는 이용자의 비밀번호 유출을 방지하기 위하여 다음 각 호의 사항을 정보처리시스템에 반영하여야 한다. 〈개정 2013. 12. 3.〉 3. 5회 이내의 범위에서 미리 정한 횟수 이상의 비밀번호 입력 오류가 발생한 경우 즉시 해당 비밀번호를 이용하는 거래를 중지시키고 본인 확인절차를 거친 후 비밀번호 재부여 및 거래 재개(이체 비밀번호 등 동일한 비밀번호가 다양한 형태의 전자금융거래에 공통으로 이용되는 경우, 입력오류 횟수는 이용되는 모든 전자금융거래에 대하여 통산한다)
FISM-165	6.4 이용자 비밀번호 관리	거래전표, 계좌개설신청서 등에 이용자 비밀번호 기재 금지 여부	5	○ **(전자금융감독규정)** - 제33조(이용자 비밀번호 관리)제2항제4호 ② 금융회사 또는 전자금융업자는 이용자의 비밀번호 유출을 방지하기 위하여 다음 각 호의 사항을 정보처리시스템에 반영하여야 한다. 〈개정 2013. 12. 3.〉

평가 항목ID	통제구분	평가항목	위험도	[근거조항] 전자금융감독규정 (금융위원회고시 제2018-36호, 2018. 12. 21) 전자금융감독규정시행세칙 (금융감독원세칙, 2021. 2. 25)
				4. 금융회사가 이용자로부터 받은 비밀번호는 거래전표, 계좌개설신청서 등에 기재하지 말고 핀패드(PIN pad) 등 보안장치를 이용하여 입력 받을 것 〈개정 2013. 12. 3.〉
FISM-167	6.4 이용자 비밀번호 관리	신규거래, 비밀번호 변경, 이체 신청 등 비밀번호를 등록/사용하는 경우 사전에 신청서등에 기재 금지 여부	5	○ **(전자금융감독규정)** - 제33조(이용자 비밀번호 관리)제2항제5호 ② 금융회사 또는 전자금융업자는 이용자의 비밀번호 유출을 방지하기 위하여 다음 각 호의 사항을 정보처리시스템에 반영하여야 한다. 〈개정 2013. 12. 3.〉 5. 신규 거래, 비밀번호 변경, 이체 신청과 같이 비밀번호를 등록·사용하는 경우 사전에 신청서 등에 기입하지 않고, 핀패드 등 보안장치를 이용하거나 이용자가 사후에 전자적 장치를 이용하여 직접 입력하는 방식으로 운영할 것
FISM-168	6.4 이용자 비밀번호 관리	비밀번호 등록·사용하는 경우 핀패드 등 보안장치 이용 또는 사후 전자적 장치를 이용하여 직접 입력 여부	5	○ **(전자금융감독규정)** - 제33조(이용자 비밀번호 관리)제2항제5호 ② 금융회사 또는 전자금융업자는 이용자의 비밀번호 유출을 방지하기 위하여 다음 각 호의 사항을 정보처리시스템에 반영하여야 한다. 〈개정 2013. 12. 3.〉 5. 신규 거래, 비밀번호 변경, 이체 신청과 같이 비밀번호를 등록·사용하는 경우 사전에 신청서 등에 기입하지 않고, 핀패드 등 보안장치를 이용하거나 이용자가 사후에 전자적 장치를 이용하여 직접 입력하는 방식으로 운영할 것
FISM-169	6.5 전산원장 통제	전산원장 변경을 위한 변경절차 수립 및 운용 여부	5	○ **(전자금융감독규정)** - 제27조(전산원장 통제)제1항 ① 금융기관 또는 전자금융업자는 장애 또는 오류 등에 의한 전산원장의 변경을 위하여 별도의 변경절차를 수립·운용하여야 한다.

평가 항목ID	통제구분	평가항목	위험도	[근거조항] 전자금융감독규정 (금융위원회고시 제2018-36호, 2018. 12. 21) 전자금융감독규정시행세칙 (금융감독원세칙, 2021. 2. 25)
FISM-170	6.5 전산원장 통제	전산원장 변경절차에 변경 대상 및 방법 포함 여부	5	○ **(전자금융감독규정)** - 제27조(전산원장 통제)제2항 ② 제1항의 절차에는 변경 대상 및 방법, 변경 권한자 지정, 변경 전후내용 자동기록 및 보존, 변경내용의 정당여부에 대한 제3자 확인 등이 포함되어야 한다.
FISM-171	6.5 전산원장 통제	전산원장 변경절차에 변경 권한자 지정 포함 여부	5	○ **(전자금융감독규정)** - 제27조(전산원장 통제)제2항 ② 제1항의 절차에는 변경 대상 및 방법, 변경 권한자 지정, 변경 전후내용 자동기록 및 보존, 변경내용의 정당여부에 대한 제3자 확인 등이 포함되어야 한다.
FISM-172	6.5 전산원장 통제	전산원장 변경 절차에 변경 전후 내용 자동기록 및 보존 포함 여부	5	○ **(전자금융감독규정)** - 제27조(전산원장 통제) ② 제1항의 절차에는 변경 대상 및 방법, 변경 권한자 지정, 변경 전후 내용 자동기록 및 보존, 변경내용의 정당여부에 대한 제3자 확인 등이 포함되어야 한다.
FISM-173	6.5 전산원장 통제	전산원장 변경절차에 변경내용의 정당여부에 대한 제3자 확인 포함 여부	5	○ **(전자금융감독규정)** - 제27조(전산원장 통제) ② 제1항의 절차에는 변경 대상 및 방법, 변경 권한자 지정, 변경 전후내용 자동기록 및 보존, 변경내용의 정당여부에 대한 제3자 확인 등이 포함되어야 한다.
FISM-174	6.5 전산원장 통제	대차대조표 등 중요자료 계상액과 각종 보조부/거래기록/전산원장 파일의 계상액에 대한 상호일치 여부에 대한 전산시스템을 통한 주기적인 확인 여부	5	○ **(전자금융감독규정)** - 제27조(전산원장 통제)제3항 ③ 금융회사 또는 전자금융업자는 대차대조표 등 중요 자료의 계상액과 각종 보조부·거래기록·전산원장파일의 계상액에 대한 상호일치 여부를 전산시스템을 통하여 주기적으로 확인하여야 한다. 〈개정 2013. 12. 3.〉

평가 항목ID	통제구분	평가항목	위험도	[근거조항] 전자금융감독규정 (금융위원회고시 제2018-36호, 2018. 12. 21) 전자금융감독규정시행세칙 (금융감독원세칙, 2021. 2. 25)
FISM-175	6.5 전산원장 통제	전산원장 불일치 원인과 조치 내용을 전산자료 형태로 5년간 보존 여부	5	○ **(전자금융감독규정)** - 제27조(전산원장 통제)제4항 ④ 금융회사 또는 전자금융업자는 제3항에 따른 확인 결과 불일치가 발견된 때에는 그 원인 및 조치 내용을 전산자료의 형태로 5년간 보존하여야 한다. 〈개정 2013. 12. 3.〉
FISM-176	6.5 전산원장 통제	중요원장의 조회, 수정, 삭제, 삽입한 작업자와 작업내용 기록 및 5년간 보존 여부	5	○ **(전자금융감독규정)** - 제27조(전산원장 통제)제5항 ⑤ 금융회사 또는 전자금융업자는 이용자 중요원장에 직접 접근하여 중요원장을 조회·수정·삭제·삽입하는 경우에는 작업자 및 작업내용 등을 기록하여 5년간 보존하여야 한다. 〈개정 2013. 12. 3.〉
FISM-177	6.5 전산원장 통제	사고위험도가 높은 거래에 대한 전산시스템 기반의 책임자 이중확인 절차 적용 여부	5	○ **(전자금융감독규정)** - 제28조(거래통제 등)제1항 ① 금융회사 또는 전자금융업자는 사고위험도가 높은 거래에 대하여는 책임자 승인 거래로 처리토록 하는 등 전산시스템에 의한 이중확인이 가능하도록 하여야 한다. 〈개정 2013. 12. 3.〉
FISM-178	6.5 전산원장 통제	전산원장, 주요정보, 이용자정보 등이 저장된 정보처리시스템 중요 작업에 대한 책임자 이중 확인 여부	5	○ **(전자금융감독규정)** - 제13조(전산자료 보호대책)제5항 ⑤ 금융회사 또는 전자금융업자는 단말기와 전산자료의 접근권한이 부여되는 정보처리시스템 관리자에 대하여 적절한 통제장치를 마련·운용하여야 한다. 다만, 정보처리시스템 관리자의 주요 업무 관련 행위는 책임자가 제28조제2항에 따라 이중확인 및 모니터링을 하여야 한다. 〈개정 2013. 12. 3.〉

평가 항목ID	통제구분	평가항목	위험도	[근거조항] 전자금융감독규정 (금융위원회고시 제2018-36호, 2018. 12. 21) 전자금융감독규정시행세칙 (금융감독원세칙, 2021. 2. 25)
				- 제28조(거래통제 등)제2항 ② 금융회사 또는 전자금융업자는 전산원장, 주요정보 또는 이용자 정보 등이 저장된 정보처리시스템에 대한 중요작업 수행 시 책임자가 이중확인을 해야 한다. 〈개정 2013. 12. 3.〉
FISM-179	6.6 일괄작업 통제	일괄작업 요청 시 작업요청서의 책임자 승인 여부	5	○ **(전자금융감독규정)** - 제30조(일괄작업에 대한 통제)제1호 금융회사 또는 전자금융업자는 안전하고 체계적인 일괄작업(batch)의 수행을 위하여 다음 각 호의 사항을 준수하여야 한다. 〈개정 2013. 12. 3.〉 1. 일괄작업은 작업요청서에 의한 책임자의 승인을 받은 후 수행할 것
FISM-180	6.6 일괄작업 통제	일괄작업 자동화 및 오류 최소화 방안 적용 여부	5	○ **(전자금융감독규정)** - 제30조(일괄작업에 대한 통제)제2호 금융회사 또는 전자금융업자는 안전하고 체계적인 일괄작업(batch)의 수행을 위하여 다음 각 호의 사항을 준수하여야 한다. 〈개정 2013. 12. 3.〉 2. 일괄작업은 최대한 자동화하여 오류를 최소화할 것
FISM-181	6.6 일괄작업 통제	일괄작업 오류 발생시 책임자 확인 여부	5	○ **(전자금융감독규정)** - 제30조(일괄작업에 대한 통제)제3호 금융회사 또는 전자금융업자는 안전하고 체계적인 일괄작업(batch)의 수행을 위하여 다음 각 호의 사항을 준수하여야 한다. 〈개정 2013. 12. 3.〉 3. 일괄작업 수행 과정에서 오류가 발생하였을 경우 반드시 책임자의 확인을 받을 것

평가 항목ID	통제구분	평가항목	위험도	[근거조항] 전자금융감독규정 (금융위원회고시 제2018-36호, 2018. 12. 21) 전자금융감독규정시행세칙 (금융감독원세칙, 2021. 2. 25)
FISM-182	6.6 일괄작업 통제	모든 일괄작업 내용 기록 및 관리 여부	5	○ **(전자금융감독규정)** - 제30조(일괄작업에 대한 통제) 금융회사 또는 전자금융업자는 안전하고 체계적인 일괄작업(batch)의 수행을 위하여 다음 각 호의 사항을 준수하여야 한다. 〈개정 2013. 12. 3.〉 4. 모든 일괄작업의 작업내용을 기록·관리할 것
FISM-183	6.6 일괄작업 통제	일괄작업 수행자 주요업무관련 행위에 관한 책임자 모니터링 여부	5	○ **(전자금융감독규정)** - 제30조(일괄작업에 대한 통제)제5호 금융회사 또는 전자금융업자는 안전하고 체계적인 일괄작업(batch)의 수행을 위하여 다음 각 호의 사항을 준수하여야 한다. 〈개정 2013. 12. 3.〉 5. 책임자는 일괄작업 수행자의 주요업무 관련 행위를 모니터링할 것
FISM-184	7.1 사업추진 시 준수사항	부서장 전결 금액 이상 사업에 대한 사전 타당성 검토 여부	5	○ **(전자금융감독규정)** - 제20조(정보처리시스템 구축 및 전자금융거래 관련 사업 추진)제1호 금융회사 또는 전자금융업자는 정보처리시스템 및 전자금융거래와 관련된 사업을 추진하는 경우에 다음 각 호의 사항을 준수하여야 한다. 〈개정 2013. 12. 3.〉 1. 조직에 미치는 영향이 크거나 내부직무전결기준에 따라 부서장 전결 금액 이상의 사업 추진 시에는 사전에 충분한 타당성 검토를 실시할 것
FISM-185	7.1 사업추진 시 준수사항	사업 신규/통합/전환/재개발 등 주요 추진사업에 대한 효과분석 실시 여부	5	○ **(전자금융감독규정)** - 제20조(정보처리시스템 구축 및 전자금융거래 관련 사업 추진)제2호 금융회사 또는 전자금융업자는 정보처리시스템 및 전자금융거래와 관련된 사업을 추진하는 경우에 다음 각 호의 사항을 준수하여야 한다. 〈개정 2013. 12. 3.〉 2. 정보처리시스템의 신규 사업 및 통합·전환·재개발 등과 같은 주요 추진사업에 대하여 비용 대비 효과분석을 실시할 것

평가 항목ID	통제구분	평가항목	위험도	[근거조항] 전자금융감독규정 (금융위원회고시 제2018-36호, 2018. 12. 21) 전자금융감독규정시행세칙 (금융감독원세칙, 2021. 2. 25)
FISM-186	7.1 사업추진 시 준수사항	타당성 검토와 비용대비 효과분석 결과에 대한 전산운영위원회 등 승인 여부	5	○ **(전자금융감독규정)** - 제20조(정보처리시스템 구축 및 전자금융거래 관련 사업 추진)제3호 금융회사 또는 전자금융업자는 정보처리시스템 및 전자금융거래와 관련된 사업을 추진하는 경우에 다음 각 호의 사항을 준수하여야 한다. 〈개정 2013. 12. 3.〉 3. 타당성 검토와 비용 대비 효과분석 결과는 전산운영위원회 등 독립적인 조직의 승인을 받을 것
FISM-187	7.1 사업추진 시 준수사항	정보처리시스템의 분석/설계 단계부터 보안대책 마련 여부	5	○ **(전자금융감독규정)** - 제20조(정보처리시스템 구축 및 전자금융거래 관련 사업 추진)제4호 금융회사 또는 전자금융업자는 정보처리시스템 및 전자금융거래와 관련된 사업을 추진하는 경우에 다음 각 호의 사항을 준수하여야 한다. 〈개정 2013. 12. 3.〉 4. 정보처리시스템의 안전성과 신뢰성을 확보하기 위하여 분석·설계 단계부터 보안대책을 강구할 것
FISM-188	7.2 사업계약 관련 준수사항	객관적인 업체 선정 기준 및 절차 마련 및 운용 여부	5	○ **(전자금융감독규정)** - 제21조(정보처리시스템 구축 및 전자금융거래 관련 계약)제1호 금융회사 또는 전자금융업자는 정보처리시스템 구축 및 전자금융거래와 관련된 계약 체결 시에 다음 각 호의 사항을 준수하여야 한다. 〈개정 2013. 12. 3.〉 1. 적합한 업체를 공정하게 선정하기 위하여 객관적인 업체 선정 기준 및 절차를 마련·운용할 것

평가 항목ID	통제구분	평가항목	위험도	[근거조항] 전자금융감독규정 (금융위원회고시 제2018-36호, 2018. 12. 21) 전자금융감독규정시행세칙 (금융감독원세칙, 2021. 2. 25)
FISM-189	7.2 사업계약 관련 준수사항	업체 선정 기준 및 절차에 정보보안 관련사항 포함 여부	5	○ **(전자금융감독규정)** - 제21조(정보처리시스템 구축 및 전자금융거래 관련 계약)제2호 금융회사 또는 전자금융업자는 정보처리시스템 구축 및 전자금융거래와 관련된 계약 체결 시에 다음 각 호의 사항을 준수하여야 한다. 〈개정 2013. 12. 3.〉 2. 정보처리시스템의 안전성과 신뢰성을 확보하기 위하여 제1호에 따른 기준 및 절차의 내용에는 정보보안 관련 사항을 포함할 것
FISM-190	7.2 사업계약 관련 준수사항	공정하고 합리적인 예정가격 산출 기준 수립 및 적용 여부	5	○ **(전자금융감독규정)** - 제21조(정보처리시스템 구축 및 전자금융거래 관련 계약)제3호 금융회사 또는 전자금융업자는 정보처리시스템 구축 및 전자금융거래와 관련된 계약 체결 시에 다음 각 호의 사항을 준수하여야 한다. 〈개정 2013. 12. 3.〉 3. 공정하고 합리적인 예정가격 산출 기준을 수립·적용할 것
FISM-191	7.2 사업계약 관련 준수사항	계약이행에 필요한 내용을 포함한 계약서 작성기준 수립 및 운용 여부	5	○ **(전자금융감독규정)** - 제21조(정보처리시스템 구축 및 전자금융거래 관련 계약)제4호 금융회사 또는 전자금융업자는 정보처리시스템 구축 및 전자금융거래와 관련된 계약 체결 시에 다음 각 호의 사항을 준수하여야 한다. 〈개정 2013. 12. 3.〉 4. 계약금액, 구축완료일자, 납품방법 및 대금지급방법 등 계약이행에 필요한 내용을 포함한 계약서 작성 기준을 수립·운용할 것
FISM-192	7.2 사업계약 관련 준수사항	소유권, 저작권, 지적재산권 등의 귀속관계 명확화 및 사후 분쟁 방지 대책 마련 여부	5	○ **(전자금융감독규정)** - 제21조(정보처리시스템 구축 및 전자금융거래 관련 계약)제5호 금융회사 또는 전자금융업자는 정보처리시스템 구축 및 전자금융거래와 관련된 계약 체결 시에 다음 각 호의 사항을 준수하여야 한다. 〈개정 2013. 12. 3.〉 5. 구매 또는 개발한 제품의 소유권, 저작권 및 지적재산권 등의 귀속관계를 명확히 하여 사후 분쟁이 발생하지 않도록 할 것

평가 항목ID	통제구분	평가항목	위험도	[근거조항] 전자금융감독규정 (금융위원회고시 제2018-36호, 2018. 12. 21) 전자금융감독규정시행세칙 (금융감독원세칙, 2021. 2. 25)
FISM-193	7.2 사업계약 관련 준수사항	공급업체 파산 등 비상사태 대비 대책 마련 및 운용 여부	5	○ **(전자금융감독규정)** - 제21조(정보처리시스템 구축 및 전자금융거래 관련 계약)제6호 금융회사 또는 전자금융업자는 정보처리시스템 구축 및 전자금융거래와 관련된 계약 체결 시에 다음 각 호의 사항을 준수하여야 한다. 〈개정 2013. 12. 3.〉 6. 납품 또는 개발이 완료된 소프트웨어 등에 대하여 공급업체 파산 등 비상사태에 대비한 대책을 마련·운용할 것
FISM-194	7.2 사업계약 관련 준수사항	검수의 계약자, 개발자 등 이해당사자 배제 및 공정한 검수 실시 여부	5	○ **(전자금융감독규정)** - 제21조(정보처리시스템 구축 및 전자금융거래 관련 계약)제7호 금융회사 또는 전자금융업자는 정보처리시스템 구축 및 전자금융거래와 관련된 계약 체결 시에 다음 각 호의 사항을 준수하여야 한다. 〈개정 2013. 12. 3.〉 7. 검수는 개발자, 계약자 등 이해당사자를 배제하여 공정하게 실시할 것
FISM-195	7.2 사업계약 관련 준수사항	계약조항 미이행 또는 계약조항 변경에 대한 검사부서 승인 여부	5	○ **(전자금융감독규정)** - 제21조(정보처리시스템 구축 및 전자금융거래 관련 계약)제8호 금융회사 또는 전자금융업자는 정보처리시스템 구축 및 전자금융거래와 관련된 계약 체결 시에 다음 각 호의 사항을 준수하여야 한다. 〈개정 2013. 12. 3.〉 8. 계약조항을 이행하지 못하는 사유가 발생하였거나 계약조항을 변경할 경우에는 검사부서의 승인을 받을 것
FISM-196	7.2 사업계약 관련 준수사항	감사가 정한 금액이상 계약에 대한 자체감사 또는 검사부서 승인 여부	5	○ **(전자금융감독규정)** - 제21조(정보처리시스템 구축 및 전자금융거래 관련 계약)제9호 금융회사 또는 전자금융업자는 정보처리시스템 구축 및 전자금융거래와 관련된 계약 체결 시에 다음 각 호의 사항을 준수하여야 한다. 〈개정 2013. 12. 3.〉 9. 내부감사규정에 따라 감사가 정한 금액 이상의 계약에 대하여는 자체 감사를 실시하거나 검사부서의 승인을 받을 것

평가 항목ID	통제구분	평가항목	위험도	[근거조항] 전자금융감독규정 (금융위원회고시 제2018-36호, 2018. 12. 21) 전자금융감독규정시행세칙 (금융감독원세칙, 2021. 2. 25)
FISM-197	7.3 정보처리 시스템 감리	정보처리시스템 감리 지침에 감리 목적, 대상, 감리인, 감리시기, 계획 등 일반기준 포함 여부	5	○ **(전자금융감독규정)** - 제22조(정보처리시스템 감리)제1호 금융회사 또는 전자금융업자는 정보처리시스템의 안전성 및 효율성 확보를 위하여 다음 각 호의 사항을 포함한 정보처리시스템 감리 지침을 작성·운용하여야 한다. 〈개정 2013. 12. 3.〉 1. 목적 및 대상, 시스템 감리인, 감리시기 및 계획 등 일반기준
FISM-198	7.3 정보처리 시스템 감리	정보처리시스템 감리 지침에 기획, 개발 및 운영의 감리 실시 기준 포함 여부	5	○ **(전자금융감독규정)** - 제22조(정보처리시스템 감리)제2호 금융회사 또는 전자금융업자는 정보처리시스템의 안전성 및 효율성 확보를 위하여 다음 각 호의 사항을 포함한 정보처리시스템 감리 지침을 작성·운용하여야 한다. 〈개정 2013. 12. 3.〉 2. 기획, 개발 및 운용의 감리 실시 기준
FISM-199	7.3 정보처리 시스템 감리	정보처리시스템 감리 지침에 지적사항 및 개선사항 등 감리 후 보고 기준 포함 여부	5	○ **(전자금융감독규정)** - 제22조(정보처리시스템 감리)제3호 금융회사 또는 전자금융업자는 정보처리시스템의 안전성 및 효율성 확보를 위하여 다음 각 호의 사항을 포함한 정보처리시스템 감리 지침을 작성·운용하여야 한다. 〈개정 2013. 12. 3.〉 3. 지적사항 및 개선사항 등 감리 후 보고 기준
FISM-200	7.3 정보처리 시스템 감리	정보처리시스템 감리 지침에 전자금융업무와 관련된 외부주문 등의 감리기준 포함 여부	5	○ **(전자금융감독규정)** - 제22조(정보처리시스템 감리)제4호 금융회사 또는 전자금융업자는 정보처리시스템의 안전성 및 효율성 확보를 위하여

평가 항목ID	통제구분	평가항목	위험도	[근거조항] 전자금융감독규정 (금융위원회고시 제2018-36호, 2018. 12. 21) 전자금융감독규정시행세칙 (금융감독원세칙, 2021. 2. 25)
				다음 각 호의 사항을 포함한 정보처리시스템 감리 지침을 작성·운용하여야 한다. 〈개정 2013. 12. 3.〉 4. 전자금융업무와 관련된 외부주문등에 대한 감리 기준
FISM-201	7.4 직무분리	프로그래머와 오퍼레이터의 직무 분리 여부	5	○ **(전자금융감독규정)** - 제26조(직무의 분리)제1호 금융회사 또는 전자금융업자는 다음 각 호의 업무에 대하여 직무를 분리·운영하여야 한다. 〈개정 2013. 12. 3.〉 1. 프로그래머와 오퍼레이터
FISM-202	7.4 직무분리	응용프로그래머와 시스템프로그래머의 직무 분리 여부	5	○ **(전자금융감독규정)** - 제26조(직무의 분리)제2호 금융회사 또는 전자금융업자는 다음 각 호의 업무에 대하여 직무를 분리·운영하여야 한다. 〈개정 2013. 12. 3.〉 2. 응용프로그래머와 시스템프로그래머
FISM-203	7.4 직무분리	시스템보안관리자와 시스템프로그래머의 직무 분리 여부	5	○ **(전자금융감독규정)** - 제26조(직무의 분리)제3호 금융회사 또는 전자금융업자는 다음 각 호의 업무에 대하여 직무를 분리·운영하여야 한다. 〈개정 2013. 12. 3.〉 3. 시스템보안관리자와 시스템프로그래머
FISM-204	7.4 직무분리	전산자료관리와 그 밖의 업무 담당자의 직무 분리 여부	5	○ **(전자금융감독규정)** - 제26조(직무의 분리)제4호 금융회사 또는 전자금융업자는 다음 각 호의 업무에 대하여 직무를 분리·운영하여야 한다. 〈개정 2013. 12. 3.〉 4. 전산자료관리자(librarian)와 그 밖의 업무 담당자

평가 항목ID	통제구분	평가항목	위험도	[근거조항] 전자금융감독규정 (금융위원회고시 제2018-36호, 2018. 12. 21) 전자금융감독규정시행세칙 (금융감독원세칙, 2021. 2. 25)
FISM-205	7.4 직무분리	업무운영자와 내부감사자의 직무 분리 여부	5	○ **(전자금융감독규정)** - 제26조(직무의 분리)제5호 금융회사 또는 전자금융업자는 다음 각 호의 업무에 대하여 직무를 분리·운영하여야 한다. 〈개정 2013. 12. 3.〉 5. 업무운영자와 내부감사자
FISM-206	7.4 직무분리	내부인력과 전자금융보조업자 및 유지보수업자 등을 포함한 외부인력의 직무 분리 여부	5	○ **(전자금융감독규정)** - 제26조(직무의 분리)제6호 금융회사 또는 전자금융업자는 다음 각 호의 업무에 대하여 직무를 분리·운영하여야 한다. 〈개정 2013. 12. 3.〉 6. 내부인력과 전자금융보조업자 및 유지보수업자 등을 포함한 외부인력
FISM-207	7.4 직무분리	정보기술부문인력과 정보보호인력의 직무 분리 여부	5	○ **(전자금융감독규정)** - 제26조(직무의 분리)제7호 금융회사 또는 전자금융업자는 다음 각 호의 업무에 대하여 직무를 분리·운영하여야 한다. 〈개정 2013. 12. 3.〉 7. 정보기술부문인력과 정보보호인력
FISM-208	7.4 직무분리	내부통제와 관련한 직무 분리 여부	5	○ **(전자금융감독규정)** - 제26조(직무의 분리)제8호 금융회사 또는 전자금융업자는 다음 각 호의 업무에 대하여 직무를 분리·운영하여야 한다. 〈개정 2013. 12. 3.〉 8. 그 밖에 내부통제와 관련하여 직무의 분리가 요구되는 경우

평가 항목ID	통제구분	평가항목	위험도	[근거조항] 전자금융감독규정 (금융위원회고시 제2018-36호, 2018. 12. 21) 전자금융감독규정시행세칙 (금융감독원세칙, 2021. 2. 25)
FISM-209	7.5 프로그램 통제절차 수립	적용대상 프로그램 종류 및 등록/변경/폐기 방법에 관한 절차 수립 및 운영 여부	5	○ **(전자금융감독규정)** - 제29조(프로그램 통제)제1호 금융회사 또는 전자금융업자는 다음 각 호의 사항을 포함한 프로그램 등록·변경·폐기 절차를 수립·운용하여야 한다. 〈개정 2013. 12. 3.〉 1. 적용대상 프로그램 종류 및 등록·변경·폐기 방법을 마련할 것
FISM-210	7.5 프로그램 통제절차 수립	프로그램 변경 전후내용 기록 여부	5	○ **(전자금융감독규정)** - 제29조(프로그램 통제)제2호 금융회사 또는 전자금융업자는 다음 각 호의 사항을 포함한 프로그램 등록·변경·폐기 절차를 수립·운용하여야 한다. 〈개정 2013. 12. 3.〉 2. 프로그램 변경 전후 내용을 기록·관리할 것
FISM-211	7.5 프로그램 통제절차 수립	프로그램 등록/변경/폐기 내용의 정당성에 대한 제3자 검증 여부	5	○ **(전자금융감독규정)** - 제29조(프로그램 통제)제3호 금융회사 또는 전자금융업자는 다음 각 호의 사항을 포함한 프로그램 등록·변경·폐기 절차를 수립·운용하여야 한다. 〈개정 2013. 12. 3.〉 3. 프로그램 등록·변경·폐기내용의 정당성에 대해 제3자의 검증을 받을 것
FISM-212	7.5 프로그램 통제절차 수립	개발 또는 테스트 시스템으로 복사 후 프로그램 수정 여부	5	○ **(전자금융감독규정)** - 제29조(프로그램 통제)제4호 금융회사 또는 전자금융업자는 다음 각 호의 사항을 포함한 프로그램 등록·변경·폐기 절차를 수립·운용하여야 한다. 〈개정 2013. 12. 3.〉 4. 변경 필요시 해당 프로그램을 개발 또는 테스트 시스템으로 복사 후 수정할 것 〈개정 2013. 12. 3.〉

평가 항목ID	통제구분	평가항목	위험도	[근거조항] 전자금융감독규정 (금융위원회고시 제2018-36호, 2018. 12. 21) 전자금융감독규정시행세칙 (금융감독원세칙, 2021. 2. 25)
FISM-213	7.5 프로그램 통제절차 수립	업무담당자에 한정하여 프로그램 접근 여부	5	○ **(전자금융감독규정)** - 제29조(프로그램 통제)제5호 금융회사 또는 전자금융업자는 다음 각 호의 사항을 포함한 프로그램 등록·변경·폐기 절차를 수립·운용하여야 한다. 〈개정 2013. 12. 3.〉 5. 프로그램에 대한 접근은 업무담당자에 한정할 것
FISM-214	7.5 프로그램 통제절차 수립	정보의 기밀성/무결성/가용성을 고려하여 충분한 테스트 및 관련 책임자 승인 후 운영 시스템에 적용 여부	5	○ **(전자금융감독규정)** - 제29조(프로그램 통제)제6호 금융회사 또는 전자금융업자는 다음 각 호의 사항을 포함한 프로그램 등록·변경·폐기 절차를 수립·운용하여야 한다. 〈개정 2013. 12. 3.〉 6. 운영시스템 적용은 처리하는 정보의 기밀성·무결성·가용성을 고려하여 충분한 테스트 및 관련 책임자 승인 후 실시할 것
FISM-215	7.5 프로그램 통제절차 수립	프로그램 반출, 실행프로그램 생성 및 운영시스템 등록은 전산자료 관리자 등 해당프로그램 담당자 이외자의 수행 여부	5	○ **(전자금융감독규정)** - 제29조(프로그램 통제)제7호 금융회사 또는 전자금융업자는 다음 각 호의 사항을 포함한 프로그램 등록·변경·폐기 절차를 수립·운용하여야 한다. 〈개정 2013. 12. 3.〉 7. 프로그램 반출, 실행프로그램의 생성 및 운영시스템 등록은 전산자료 관리자 등 해당프로그램 담당자 이외의 자가 수행할 것
FISM-216	7.5 프로그램 통제절차 수립	데이터베이스관리시스템(Database Management System : DBMS), 운영체제(Operating System) 등 시스템프로그램의 응용프로그램과 동일 수준 관리	5	○ **(전자금융감독규정)** - 제29조(프로그램 통제)제8호 금융회사 또는 전자금융업자는 다음 각 호의 사항을 포함한 프로그램 등록·변경·폐기 절차를 수립·운용하여야 한다. 〈개정 2013. 12. 3.〉 8. 운영체제, 데이터베이스관리프로그램 등의 시스템 프로그램도 응용프로그램과 동일한 수준으로 관리할 것

평가 항목ID	통제구분	평가항목	위험도	[근거조항] 전자금융감독규정 (금융위원회고시 제2018-36호, 2018. 12. 21) 전자금융감독규정시행세칙 (금융감독원세칙, 2021. 2. 25)
FISM-217	7.5 프로그램 통제절차 수립	프로그램 설명서, 입/출력레코드 설명서, 프로그램 목록, 사용자 지침서, 운영자지침서 등 프로그램 유지보수 문서 작성 및 관리 여부	5	○ **(전자금융감독규정)** - 제29조(프로그램 통제)제9호 금융회사 또는 전자금융업자는 다음 각 호의 사항을 포함한 프로그램 등록·변경·폐기 절차를 수립·운용하여야 한다. 〈개정 2013. 12. 3.〉 9. 프로그램 설명서, 입·출력 레코드 설명서, 프로그램 목록 및 사용자·운영자 지침서 등 프로그램 유지보수에 필요한 문서를 작성·관리할 것
FISM-218	7.5 프로그램 통제절차 수립	전자금융거래용 전산프로그램에 대한 사전 보안성 검증 여부	5	○ **(전자금융감독규정)** - 제29조(프로그램 통제)제10호 금융회사 또는 전자금융업자는 다음 각 호의 사항을 포함한 프로그램 등록·변경·폐기 절차를 수립·운용하여야 한다. 〈개정 2013. 12. 3.〉 10. 전자 금융거래에 사용되는 전산프로그램은 실제 업무를 처리하는 정보처리 시스템에 설치하기 전에 자체 보안성 검증을 실시할 것
FISM-219	7.6 자체 보안성심의	정보기술부문 및 전자금융업무에 대한 자체 보안성 검토 및 정기 보안점검 실시 여부	5	○ **(전자금융감독규정)** - 제36조(자체 보안성심의) ① 금융회사 또는 전자금융업자는 다음 각 호의 행위를 하고자 하는 경우 금융감독원장이 정하는 기준과 절차에 따라 보안성심의를 실시하여야 한다. 〈개정 2016. 6. 30.〉 1. 정보통신망을 이용하여 이용자를 대상으로 신규 전자금융업무를 수행 2. 복수의 금융회사 또는 전자금융업자가 공동으로 전자금융거래 관련 표준을 제정

평가 항목ID	통제구분	평가항목	위험도	[근거조항] 전자금융감독규정 (금융위원회고시 제2018-36호, 2018. 12. 21) 전자금융감독규정시행세칙 (금융감독원세칙, 2021. 2. 25)
				○ **(전자금융감독규정시행세칙)** - 제3조(자체 보안성심의 기준 등) ① 규정 제36조제1항에 따른 금융감독원장이 정하는 기준과 절차란 다음 각 호를 말한다. 1. 정보통신망을 이용하여 신규전자금융업무를 수행하는 경우 〈별표 1〉의 기준에 따라 보안성심의를 실시한 후 정보보호최고책임자의 승인을 받을 것 2. 공동으로 전자금융거래 관련 표준을 제정하는 경우 〈별표 1의2〉의 기준에 따라 보안성심의를 실시할 것(다만, 이 경우 특정 금융회사 또는 전자금융업자가 다른 금융회사등을 대표하여 규정 제36조제2항에 따른 자체 보안성심의 결과보고서를 제출할 수 있음)
FISM-220	7.6 자체 보안성심의	정보통신망을 이용하여 이용자를 대상으로 신규 전자금융업무를 수행하거나 복수의 금융회사 또는 전자금융업자가 공동으로 전자금융거래 관련 표준을 제정하는 경우 자체 보안성심의 여부	5	○ **(전자금융감독규정)** - 제36조(자체 보안성심의) ① 금융회사 또는 전자금융업자는 다음 각 호의 행위를 하고자 하는 경우 금융감독원장이 정하는 기준과 절차에 따라 보안성심의를 실시하여야 한다. 〈개정 2016. 6. 30.〉 1. 정보통신망을 이용하여 이용자를 대상으로 신규 전자금융업무를 수행 2. 복수의 금융회사 또는 전자금융업자가 공동으로 전자금융거래 관련 표준을 제정 ○ **(전자금융감독규정시행세칙)** - 제3조(자체 보안성심의 기준 등) ① 규정 제36조제1항에 따른 금융감독원장이 정하는 기준과 절차란 다음 각 호를 말한다. 1. 정보통신망을 이용하여 신규전자금융업무를 수행하는 경우 〈별표 1〉의 기준에 따라 보안성심의를 실시한 후 정보보호최고책임자의 승인을 받을 것

평가 항목ID	통제구분	평가항목	위험도	[근거조항] 전자금융감독규정 (금융위원회고시 제2018-36호, 2018. 12. 21) 전자금융감독규정시행세칙 (금융감독원세칙, 2021. 2. 25)
				2. 공동으로 전자금융거래 관련 표준을 제정하는 경우 〈별표 1의2〉의 기준에 따라 보안성심의를 실시할 것(다만, 이 경우 특정 금융회사 또는 전자금융업자가 다른 금융회사등을 대표하여 규정 제36조제2항에 따른 자체 보안성심의 결과보고서를 제출할 수 있음)
FISM-221	8.1 업무 지속성 확보방안	업무지속성 확보방안에 상황별 대응 절차 포함 여부	5	○ **(전자금융감독규정)** - 제23조(비상대책 등의 수립·운용)제1항제1호 ① 금융회사 또는 전자금융업자는 장애·재해·파업·테러 등 긴급한 상황이 발생하더라도 업무가 중단되지 않도록 다음 각 호의 내용을 포함한 업무지속성 확보 방안을 수립·준수하여야 한다. 〈개정 2013. 12. 3., 2016. 10. 5.〉 1. 상황별 대응절차
FISM-222	8.1 업무 지속성 확보방안	업무지속성 확보방안에 백업 또는 재해복구센터를 활용한 재해복구 계획 포함 여부	5	○ **(전자금융감독규정)** - 제23조(비상대책 등의 수립·운용)제1항제2호 ① 금융회사 또는 전자금융업자는 장애·재해·파업·테러 등 긴급한 상황이 발생하더라도 업무가 중단되지 않도록 다음 각 호의 내용을 포함한 업무지속성 확보 방안을 수립·준수하여야 한다. 〈개정 2013. 12. 3., 2016. 10. 5.〉 2. 백업 또는 재해복구센터를 활용한 재해복구계획
FISM-223	8.1 업무 지속성 확보방안	업무지속성 확보방안에 비상대응 조직의 구성 및 운용 포함	5	○ **(전자금융감독규정)** - 제23조(비상대책 등의 수립·운용)제1항제3호 ① 금융회사 또는 전자금융업자는 장애·재해·파업·테러 등 긴급한 상황이 발생하더라도 업무가 중단되지 않도록 다음 각 호의 내용을 포함한 업무지속성 확보 방안을 수립·준수하여야 한다. 〈개정 2013. 12. 3., 2016. 10. 5.〉 3. 비상대응조직의 구성 및 운용

평가 항목ID	통제구분	평가항목	위험도	[근거조항] 전자금융감독규정 (금융위원회고시 제2018-36호, 2018. 12. 21) 전자금융감독규정시행세칙 (금융감독원세칙, 2021. 2. 25)
FISM-224	8.1 업무 지속성 확보방안	업무지속성 확보방안에 입력대행, 수작업 등의 조건 및 절차 포함 여부	5	○ **(전자금융감독규정)** - 제23조(비상대책 등의 수립·운용)제1항제4호 ① 금융회사 또는 전자금융업자는 장애·재해·파업·테러 등 긴급한 상황이 발생하더라도 업무가 중단되지 않도록 다음 각 호의 내용을 포함한 업무지속성 확보 방안을 수립·준수하여야 한다. 〈개정 2013. 12. 3., 2016. 10. 5.〉 4. 입력대행, 수작업 등의 조건 및 절차
FISM-225	8.1 업무 지속성 확보방안	업무지속성 확보방안에 모의 훈련의 실시 포함 여부	5	○ **(전자금융감독규정)** - 제23조(비상대책 등의 수립·운용)제1항제5호 ① 금융회사 또는 전자금융업자는 장애·재해·파업·테러 등 긴급한 상황이 발생하더라도 업무가 중단되지 않도록 다음 각 호의 내용을 포함한 업무지속성 확보 방안을 수립·준수하여야 한다. 〈개정 2013. 12. 3., 2016. 10. 5.〉 5. 모의훈련의 실시
FISM-226	8.1 업무 지속성 확보방안	업무지속성 확보방안에 유관기관 및 관련업체와의 비상연락체계 포함 여부	5	○ **(전자금융감독규정)** - 제23조(비상대책 등의 수립·운용)제1항제6호 ① 금융회사 또는 전자금융업자는 장애·재해·파업·테러 등 긴급한 상황이 발생하더라도 업무가 중단되지 않도록 다음 각 호의 내용을 포함한 업무지속성 확보 방안을 수립·준수하여야 한다. 〈개정 2013. 12. 3., 2016. 10. 5.〉 6. 유관기관 및 관련업체와의 비상연락체제 구축
FISM-227	8.1 업무 지속성 확보방안	업무지속성 확보방안에 보고 및 대외 통보의 범위와 절차 포함 여부	5	○ **(전자금융감독규정)** - 제23조(비상대책 등의 수립·운용)제1항제7호 ① 금융회사 또는 전자금융업자는 장애·재해·파업·테러 등 긴급한 상황이 발생하더라도 업무가 중단되지 않도록 다음 각 호의 내용을 포함한 업무지속성 확보

평가 항목ID	통제구분	평가항목	위험도	[근거조항] 전자금융감독규정 (금융위원회고시 제2018-36호, 2018. 12. 21) 전자금융감독규정시행세칙 (금융감독원세칙, 2021. 2. 25)
				방안을 수립·준수하여야 한다. 〈개정 2013. 12. 3., 2016. 10. 5.〉 7. 보고 및 대외통보의 범위와 절차 등
FISM-228	8.1 업무 지속성 확보방안	업무지속성 확보대책을 매년 1회 이상 점검 및 최신상태 유지 및 관리 여부	5	○ **(전자금융감독규정)** - 제23조(비상대책 등의 수립·운용)제3항 ③ 금융회사 또는 전자금융업자는 제1항의 규정에 따른 업무지속성 확보대책의 실효성·적정성 등을 매년 1회 이상 점검하여 최신상태로 유지하고 관리하여야 한다. 〈개정 2013. 12. 3.〉
FISM-229	8.1 업무 지속성 확보방안	정보처리시스템 및 데이터저장장치 등 주요 전산장비의 이중화 구축 또는 예비장치 확보 여부	5	○ **(전자금융감독규정)** - 제23조(비상대책 등의 수립·운용)제7항 ⑦ 금융회사 또는 전자금융업자는 중앙처리장치, 데이터저장장치 등 주요 전산장비에 대하여 이중화 또는 예비장치를 확보하여야 한다. 〈개정 2013. 12. 3.〉
FISM-230	8.1 업무 지속성 확보방안	주전산센터와 일정거리 이상 떨어진 안전장소에 재해복구센터 구축 및 운영 여부	5	○ **(전자금융감독규정)** - 제23조(비상대책 등의 수립·운용)제8항,제9항 ⑧ 다음 각 호의 금융회사는 시스템 오류, 자연재해 등으로 인한 전산센터 마비에 대비하여 업무지속성을 확보할 수 있도록 적정 규모·인력을 구비한 재해복구센터를 주전산센터와 일정거리 이상 떨어진 안전한 장소에 구축·운용하여야 한다. 〈개정 2013. 12. 3., 2015. 6. 24.〉 1. 「은행법」에 의해 인가를 받아 설립된 은행(다만, 「은행법」 제58조에 의해 인가를 받은 외국금융회사의 국내지점은 제외한다)〈개정 2013. 12. 3.〉 2. 「한국산업은행법」에 의한 한국산업은행, 「중소기업은행법」에 의한 중소기업은행, 「농업협동조합법」에 의한 농협은행, 「수산업협동조합법」에 의한 수산업협동조합중앙회의 신용사업부문 〈개정 2013. 12. 3.〉 3. 「자본시장과 금융투자업에 관한 법률」에 의한 투자매매업자·투자중개업자(다만,

평가 항목ID	통제구분	평가항목	위험도	[근거조항] 전자금융감독규정 (금융위원회고시 제2018-36호, 2018. 12. 21) 전자금융감독규정시행세칙 (금융감독원세칙, 2021. 2. 25)
				「자본시장과 금융투자업에 관한 법률」 제12조에 의해 인가를 받은 외국 투자매매업자·투자중개업자의 지점 등은 제외한다) 4. 「자본시장과 금융투자업에 관한 법률」에 의한 증권금융회사 및 한국예탁결제원 5. 「자본시장과 금융투자업에 관한 법률」에 의한 거래소 〈개정 2013. 12. 3.〉 6. 「여신전문금융업법」에 의한 신용카드업자(다만, 법인신용카드 회원에 한하여 신용카드업을 영위하는 자는 제외한다) 7. 「보험업법」에 의한 보험요율산출기관 8. 「상호저축은행법」에 의한 상호저축은행중앙회 9. 「신용협동조합법」에 의한 신용협동조합중앙회 10. 「보험업법」에 의한 보험회사
FISM-231	8.1 업무 지속성 확보방안	적정한 규모와 인력을 구비한 재해복구센터 구축 및 운영 여부	5	○ **(전자금융감독규정)** - 제23조(비상대책 등의 수립·운용)제8항 ⑧ 다음 각 호의 금융회사는 시스템 오류, 자연재해 등으로 인한 전산센터 마비에 대비하여 업무지속성을 확보할 수 있도록 적정 규모·인력을 구비한 재해복구센터를 주전산센터와 일정거리 이상 떨어진 안전한 장소에 구축·운용하여야 한다. 〈개정 2013. 12. 3., 2015. 6. 24.〉 1. 「은행법」에 의해 인가를 받아 설립된 은행(다만,「은행법」제58조에 의해 인가를 받은 외국금융회사의 국내지점은 제외한다) 〈개정 2013. 12. 3.〉 2. 「한국산업은행법」에 의한 한국산업은행, 「중소기업은행법」에 의한 중소기업은행, 「농업협동조합법」에 의한 농협은행, 「수산업협동조합법」에 의한 수산업협동조합중앙회의 신용사업부문 〈개정 2013. 12. 3.〉 3. 「자본시장과 금융투자업에 관한 법률」에 의한 투자매매업자·투자중개업자(다만, 「자본시장과 금융투자업에 관한 법률」 제12조에 의해 인가를 받은 외국 투자매매업자·투자중개업자의 지점 등은 제외한다) 4. 「자본시장과 금융투자업에 관한 법률」에 의한 증권금융회사 및 한국예탁결제원

평가 항목ID	통제구분	평가항목	위험도	[근거조항] 전자금융감독규정 (금융위원회고시 제2018-36호, 2018. 12. 21) 전자금융감독규정시행세칙 (금융감독원세칙, 2021. 2. 25)
				5.「자본시장과 금융투자업에 관한 법률」에 의한 거래소 〈개정 2013. 12. 3.〉 6.「여신전문금융업법」에 의한 신용카드업자(다만, 법인신용카드 회원에 한하여 신용카드업을 영위하는 자는 제외한다) 7.「보험업법」에 의한 보험요율산출기관 8.「상호저축은행법」에 의한 상호저축은행중앙회 9.「신용협동조합법」에 의한 신용협동조합중앙회 10.「보험업법」에 의한 보험회사
FISM-232	8.1 업무 지속성 확보방안	재해복구 목표시간 내 재해복구 가능 여부	5	○ **(전자금융감독규정)** - 제23조(비상대책 등의 수립·운용)제9항 ⑨ 제8항 각 호의 금융회사는 업무별로 업무지속성 확보의 중요도를 분석하여 핵심 업무를 선정하여야 하며, 업무별 복구목표시간을 정하여야 한다. 이 경우 핵심 업무의 복구목표시간은 3시간 이내로 하되,「보험업법」에 의한 보험회사의 핵심 업무의 경우에는 24시간 이내로 한다. 〈신설 2015. 6. 24.〉
FISM-233	8.1 업무 지속성 확보방안	매년 1회 이상 재해복구센터로 재해복구전환훈련 실시 여부	5	○ **(전자금융감독규정)** - 제23조(비상대책 등의 수립·운용)제10항 ⑩ 제8항의 규정에 따른 재해복구센터를 운영하는 금융회사는 매년 1회 이상 재해복구센터로 실제 전환하는 재해복구전환훈련을 실시하여야 한다. 〈개정 2013. 12. 3.〉, 〈종전의 제9항에서 이동 2015. 6. 24.〉
FISM-234	8.2 비상지원 인력 확보관리	업무지속성 확보대책에 핵심전산업무의 비상지원인력에 관한 확보 및 운영방안 포함 여부	5	○ **(전자금융감독규정)** - 제23조(비상대책 등의 수립·운용)제2항제1호 ② 제1항에 따른 업무지속성 확보대책에는 비상사태에 대비한 다음 각 호의 안전대책이 반영되어야 한다.

평가 항목ID	통제구분	평가항목	위험도	[근거조항] 전자금융감독규정 (금융위원회고시 제2018-36호, 2018. 12. 21) 전자금융감독규정시행세칙 (금융감독원세칙, 2021. 2. 25)
				1. 파업 시 핵심전산업무 종사자의 근무지 이탈에 따른 정보처리시스템의 마비를 방지하기 위하여 비상지원인력을 확보·운영할 것
FISM-235	8.2 비상지원 인력 확보관리	업무지속성 확보대책에 비상지원인력 또는 외부전문업체 활용방안 수립 및 운영 여부	5	○ **(전자금융감독규정)** - 제23조(비상대책 등의 수립·운용) ② 제1항에 따른 업무지속성 확보대책에는 비상사태에 대비한 다음 각 호의 안전대책이 반영되어야 한다. 2. 비상사태 발생 시에도 정보처리시스템의 마비를 방지하고 신속히 원상복구가 될 수 있도록 정보처리시스템 운영에 대한 비상지원인력 또는 외부 전문업체를 활용하는 방안을 수립·운영할 것
FISM-236	8.2 비상지원 인력 확보관리	업무지속성 확보대책에 전산시스템 운영지침서, 사용자매뉴얼 등이 최신 상태로 유지되고 있는지 여부	5	○ **(전자금융감독규정)** - 제23조(비상대책 등의 수립·운용)제2항제3호 ② 제1항에 따른 업무지속성 확보대책에는 비상사태에 대비한 다음 각 호의 안전대책이 반영되어야 한다. 3. 비상지원인력이 사용법을 충분히 이해하고 업무운용이 가능한 수준으로 전산시스템 운영지침서, 사용자매뉴얼 등을 쉽고 자세하게 작성하고 최신상태로 유지할 것
FISM-237	8.2 비상지원 인력 확보관리	업무지속성 확보대책에 비상지원인력에 대한 연수 실시 여부 포함 여부	5	○ **(전자금융감독규정)** - 제23조(비상대책 등의 수립·운용)제2항제4호 ② 제1항에 따른 업무지속성 확보대책에는 비상사태에 대비한 다음 각 호의 안전대책이 반영되어야 한다. 4. 핵심전산업무 담당자 부재 시에도 비상지원 인력이 업무를 수행할 수 있도록 비상지원인력에 대한 연수를 실시할 것

평가 항목ID	통제구분	평가항목	위험도	[근거조항] 전자금융감독규정 (금융위원회고시 제2018-36호, 2018. 12. 21) 전자금융감독규정시행세칙 (금융감독원세칙, 2021. 2. 25)
FISM-238	8.3 위기대응 행동매뉴얼 수립	위기대응 행동매뉴얼 또는 비상대책 수립 여부	5	○ **(전자금융감독규정)** - 제23조(비상대책 등의 수립·운용)제4항,제5항 ④ 「국가위기관리기본지침」에 따라 금융위원회가 지정한 금융회사는 금융위원회의 「금융전산분야위기대응실무매뉴얼」에 따라 위기대응행동매뉴얼(이하 "행동매뉴얼"이라 한다)을 수립·준수하고 이를 금융위원회에 알려야 한다. 〈개정 2013. 12. 3., 2016. 10. 5.〉 ⑤ 금융위원회가 별도로 지정하지 아니한 금융회사 또는 전자금융업자는 자연재해, 인적 재해, 기술적 재해, 전자적 침해 등으로 인한 전산시스템의 마비 방지와 신속한 복구를 위한 비상대책을 수립·운영하여야 한다. 〈개정 2013. 12. 3., 2016. 10. 5.〉
FISM-240	8.3 위기대응 행동매뉴얼 수립	위기대응 행동매뉴얼 또는 비상대책이 업무 지속성 확보대책에 반영 여부	5	○ **(전자금융감독규정)** - 제23조(비상대책 등의 수립·운용)제6항 ⑥ 제4항에 따른 행동매뉴얼 또는 제5항에 따른 비상대책에는 제1항의 규정에 따른 업무지속성 확보대책이 반영되어야 한다.
FISM-241	11.2 침해사고 대응	연 1회 해킹, 디도스공격 등 침해사고 대응 및 복구훈련 실시와 침해사고 대응기관에 제출 여부	5	○ **(전자금융감독규정)** - 제37조의4(침해사고대응기관 지정 및 업무범위 등) ⑤ 금융회사 및 전자금융업자는 침해사고에 대한 대응능력 확보를 위하여 연 1회 이상 침해사고 대응 및 복구훈련 계획을 수립·시행하여야 하며 그 계획 및 결과를 침해사고대응기관의 장에게 제출하여야 한다. 다만 다음 각 호의 어느 하나에 해당하는 금융회사는 그러하지 아니한다. 〈개정 2016. 10. 5.〉 1. 법 제2조제3호가목의 금융회사 중 신용협동조합 2. 법 제2조제3호다목·라목의 금융회사 3. 시행령 제2조제4호부터 제6호까지의 조합 4. 시행령 제5조제2항의 요건을 충족한 금융회사

평가 항목ID	통제구분	평가항목	위험도	[근거조항] 전자금융감독규정 (금융위원회고시 제2018-36호, 2018. 12. 21) 전자금융감독규정시행세칙 (금융감독원세칙, 2021. 2. 25)
FISM-242	8.3 위기대응 행동매뉴얼 수립	금융위원회 주관 금융분야 합동비상대응훈련 실시 여부	5	○ **(전자금융감독규정)** - 제24조(비상대응훈련 실시) ① 금융회사 또는 전자금융업자는 제23조제4항에 따른 행동매뉴얼 또는 같은 조 제5항에 따른 비상대책에 따라 연 1회의 비상대응훈련을 실시하고 그 결과를 금융위원회에 보고하여야 한다. 이때, 제23조제10항에 따른 재해복구전환훈련을 포함하여 실시할 수 있다. 〈개정 2013. 12. 3., 2016. 6. 30.〉 ② 금융위원회는 금융분야의 비상대응능력을 강화하기 위하여 금융회사 또는 전자금융업자를 선별하여 금융분야 합동비상대응훈련을 실시할 수 있다. 〈개정 2013. 12. 3.〉 ③ 금융위원회는 제2항의 규정에 따른 합동비상대응훈련을 실시할 때, 다음 각 호의 기관에게 지원을 요청할 수 있다. 1. 「정부조직법」 제15조에 따른 "국가정보원(국가사이버안전센터)" 2. 「경찰법」 제2조에 따른 "경찰청(사이버테러대응센터)" 3. 침해사고대응기관 〈개정 2013. 12. 3.〉 4. 그밖에 비상대응훈련의 실효성 확보를 위하여 금융위원회가 필요하다고 인정하는 기관 ④ 금융회사 또는 전자금융업자는 제1항 및 제2항에 따른 의무의 이행을 위하여 전자금융보조업자에게 협조를 요청할 수 있다. 〈신설 2018. 12. 21.〉
FISM-243	9.1 전자금융거래 시 준수사항	전자금융거래 시 암호화 통신 여부	5	○ **(전자금융감독규정)** - 제34조(전자금융거래 시 준수사항)제1호 금융회사 또는 전자금융업자는 전자금융거래와 관련하여 다음 각 호의 사항을 준수하여야 한다. 1. 전화 등 거래수단 성격상 암호화가 불가능한 경우를 제외한 전자금융거래는 암호화 통신을 할 것(다만, 전용선을 사용하는 경우로서 제36조의 규정에 따라 자체 보안성심의를 실시한 경우에는 그러하지 아니하다)

평가 항목ID	통제구분	평가항목	위험도	[근거조항] 전자금융감독규정 (금융위원회고시 제2018-36호, 2018. 12. 21) 전자금융감독규정시행세칙 (금융감독원세칙, 2021. 2. 25)
FISM-244	9.1 전자금융거래 시 준수사항	전자금융거래 시 비대면 전자금융거래를 허용하지 않는 계좌개설 서비스를 제공할 수 있도록 시스템 구축 여부	5	○ **(전자금융감독규정)** - 제34조(전자금융거래 시 준수사항)제2호 금융회사 또는 전자금융업자는 전자금융거래와 관련하여 다음 각 호의 사항을 준수하여야 한다. 2. 전자금융사고를 예방하기 위하여 비대면 전자금융거래를 허용하지 않는 계좌개설, 중요거래정보에 대한 문자메시지 및 이메일(e-mail) 통지 등의 서비스를 이용자가 요청하는 경우, 동 서비스를 제공할 수 있도록 시스템을 갖출 것
FISM-245	9.1 전자금융거래 시 준수사항	전자금융거래 시 중요거래정보에 대한 문자메시지 및 이메일서비스를 제공할 수 있도록 시스템 구축 여부	5	○ **(전자금융감독규정)** - 제34조(전자금융거래 시 준수사항)제2호 금융회사 또는 전자금융업자는 전자금융거래와 관련하여 다음 각 호의 사항을 준수하여야 한다. 2. 전자금융사고를 예방하기 위하여 비대면 전자금융거래를 허용하지 않는 계좌개설, 중요거래정보에 대한 문자메시지 및 이메일(e-mail) 통지 등의 서비스를 이용자가 요청하는 경우, 동 서비스를 제공할 수 있도록 시스템을 갖출 것
FISM-246	9.1 전자금융거래 시 준수사항	전자금융거래 시 전자금융거래에 사용되는 접근매체의 본인 실명증표 확인 후 교부 여부	5	○ **(전자금융감독규정)** - 제34조(전자금융거래 시 준수사항)제3호 금융회사 또는 전자금융업자는 전자금융거래와 관련하여 다음 각 호의 사항을 준수하여야 한다. 3. 전자금융거래에 사용되는 접근매체를 발급받기 위해서는 반드시 실명확인 후 교부할 것

평가 항목ID	통제구분	평가항목	위험도	[근거조항] 전자금융감독규정 (금융위원회고시 제2018-36호, 2018. 12. 21) 전자금융감독규정시행세칙 (금융감독원세칙, 2021. 2. 25)
FISM-247	9.1 전자금융거래 시 준수사항	전자금융거래에 관한 거래인증수단 채택시 안전성, 보안성, 이용편의성 등을 충분히 고려 여부	5	○ **(전자금융감독규정)** - 제34조(전자금융거래 시 준수사항)제4호 금융회사 또는 전자금융업자는 전자금융거래와 관련하여 다음 각 호의 사항을 준수하여야 한다. 4. 거래인증수단 채택시 안전성, 보안성, 이용편의성 등을 충분히 고려할 것
FISM-248	9.1 전자금융거래 시 준수사항	전자금융거래 프로그램의 위/변조 등 무결성 검증방법 제공 여부	5	○ **(전자금융감독규정)** - 제34조(전자금융거래 시 준수사항)제5호 금융회사 또는 전자금융업자는 전자금융거래와 관련하여 다음 각 호의 사항을 준수하여야 한다. 5. 금융회사 또는 전자금융업자는 전자금융거래에서 이용자에게 제공하거나 거래를 처리하기 위한 전자금융거래프로그램(거래전문포함)의 위·변조 여부 등 무결성을 검증할 수 있는 방법을 제공할 것
FISM-249	9.1 전자금융거래 시 준수사항	전자금융거래의 종류·성격·위험수준 등을 고려한 인증방법 사용 여부	5	○ **(전자금융감독규정)** - 제37조(인증방법 사용기준) 금융회사 또는 전자금융업자는 전자금융거래의 종류·성격·위험수준 등을 고려하여 안전한 인증방법을 사용하여야 한다. 〈개정 2015. 3. 18.〉
FISM-250	9.4 이용자 정보보호	사용자 단말기에서 이용자 정보 조회 내역(사용자, 사용일시, 변경/조회 내용, 접속방법)이 정보처리시스템에 자동 기록되고 관련 기록의 1년 이상 보관여부	5	○ **(전자금융감독규정)** - 제13조(전산자료 보호대책)제3항 ③ 금융회사 또는 전자금융업자는 단말기를 통한 이용자 정보 조회 시 사용자, 사용일시, 변경·조회내용, 접속방법이 정보처리시스템에 자동적으로 기록되도록 하고, 그 기록을 1년 이상 보존하여야 한다. 〈개정 2013. 12. 3.〉

평가 항목ID	통제구분	평가항목	위험도	[근거조항] 전자금융감독규정 (금융위원회고시 제2018-36호, 2018. 12. 21) 전자금융감독규정시행세칙 (금융감독원세칙, 2021. 2. 25)
FISM-251	9.4 이용자 정보보호	이용자 비밀번호 유출위험 및 관리에 관한 사항 공지 여부	5	○ **(전자금융감독규정)** - 제35조(이용자 유의사항 공지)제1호 금융회사 또는 전자금융업자는 전자금융거래의 안전한 수행을 위하여 이용자에게 다음 각 호의 사항을 준수하도록 공지하여야 한다. 〈개정 2013. 12. 3.〉 1. 비밀번호 유출위험 및 관리에 관한 사항
FISM-252	9.4 이용자 정보보호	금융기관 등이 제공하는 이용자 보호 제도에 관한 사항 공지 여부	5	○ **(전자금융감독규정)** - 제35조(이용자 유의사항 공지)제2호 금융회사 또는 전자금융업자는 전자금융거래의 안전한 수행을 위하여 이용자에게 다음 각 호의 사항을 준수하도록 공지하여야 한다. 〈개정 2013. 12. 3.〉 2. 금융기관 또는 전자금융업자가 제공하고 있는 이용자 보호제도에 관한 사항
FISM-253	9.4 이용자 정보보호	해킹/피싱 등 전자적 침해방지에 관한 사항 공지 여부	5	○ **(전자금융감독규정)** - 제35조(이용자 유의사항 공지)제3호 금융회사 또는 전자금융업자는 전자금융거래의 안전한 수행을 위하여 이용자에게 다음 각 호의 사항을 준수하도록 공지하여야 한다. 〈개정 2013. 12. 3.〉 3. 해킹·피싱 등 전자적 침해 방지에 관한 사항
FISM-254	9.4 이용자 정보보호	본인확인절차 후 비밀번호 변경 가능한 정보처리시스템 구축 여부	5	○ **(전자금융감독규정)** - 제35조(이용자 유의사항 공지)제4호 금융회사 또는 전자금융업자는 전자금융거래의 안전한 수행을 위하여 이용자에게 다음 각 호의 사항을 준수하도록 공지하여야 한다. 〈개정 2013. 12. 3.〉 4. 본인확인 절차를 거쳐 비밀번호 변경이 가능하도록 정보처리시스템을 구축하고 비밀번호 변경 시 같은 번호를 재사용하지 않도록 할 것

평가 항목ID	통제구분	평가항목	위험도	[근거조항] 전자금융감독규정 (금융위원회고시 제2018-36호, 2018. 12. 21) 전자금융감독규정시행세칙 (금융감독원세칙, 2021. 2. 25)
FISM-255	9.4 이용자 정보보호	이용자 비밀번호 변경시 동일 비밀번호 재사용 금지 여부	5	○ **(전자금융감독규정)** - 제35조(이용자 유의사항 공지)제4호 금융회사 또는 전자금융업자는 전자금융거래의 안전한 수행을 위하여 이용자에게 다음 각 호의 사항을 준수하도록 공지하여야 한다. 〈개정 2013. 12. 3.〉 4. 본인확인 절차를 거쳐 비밀번호 변경이 가능하도록 정보처리시스템을 구축하고 비밀번호 변경 시 같은 번호를 재사용하지 않도록 할 것
FISM-256	10.1 외부주문 계약 준수사항	IT외부주문 업무에 대한 업무적정성 검토 여부	5	○ **(전자금융감독규정)** - 제8조(인력, 조직 및 예산)제1항제2호 ① 금융회사 또는 전자금융업자는 인력 및 조직의 운용에 관하여 다음 각 호의 사항을 준수하여야 한다. 〈개정 2013. 12. 3.〉 2. 외부주문등에 관한 계약을 체결하는 때에는 계약내용의 적정성을 검토하고 자체적으로 통제가 가능하도록 회사내부에 조직과 인력을 갖출 것
FISM-257	10.1 외부주문 계약 준수사항	IT외부주문 계약 체결시 계약내용의 적정성 검토 여부	5	○ **(전자금융감독규정)** - 제8조(인력, 조직 및 예산)제1항제2호 ① 금융회사 또는 전자금융업자는 인력 및 조직의 운용에 관하여 다음 각 호의 사항을 준수하여야 한다. 〈개정 2013. 12. 3.〉 2. 외부주문등에 관한 계약을 체결하는 때에는 계약내용의 적정성을 검토하고 자체적으로 통제가 가능하도록 회사내부에 조직과 인력을 갖출 것
FISM-258	10.1 외부주문 계약 준수사항	외부주문 등의 입찰·계약·수행·완료 등 각 단계별로 금융감독원장이 정하는 보안관리 방안 준수 여부	5	○ **(전자금융감독규정)** - 제60조(외부주문등에 대한 기준)제1항제7호 ① 금융회사 또는 전자금융업자는 전자금융거래를 위한 외부주문등의 경우에는 다음

평가 항목ID	통제구분	평가항목	위험도	[근거조항] 전자금융감독규정 (금융위원회고시 제2018-36호, 2018. 12. 21) 전자금융감독규정시행세칙 (금융감독원세칙, 2021. 2. 25)
				각 호의 사항을 준수하여야 한다. 〈개정 2013. 12. 3.〉 7. 외부주문등의 입찰·계약·수행·완료 등 각 단계별로 금융감독원장이 정하는 보안관리방안을 따를 것 〈개정 2015. 2. 3.〉 ○ **(전자금융감독규정시행세칙)** - 제9조의2(외부주문등에 대한 기준) ① 규정 제60조제1항제7호에 따라 감독원장이 정하는 보안관리방안은 별표 5-2와 같다.
FISM-259	10.1 외부주문 계약 준수사항	외부주문 시 내부통제방안 수립 및 운용 여부	5	○ **(전자금융감독규정)** - 제8조(인력, 조직 및 예산) ① 금융회사 또는 전자금융업자는 인력 및 조직의 운용에 관하여 다음 각 호의 사항을 준수하여야 한다. 〈개정 2013. 12. 3.〉 2. 외부주문등에 관한 계약을 체결하는 때에는 계약내용의 적정성을 검토하고 자체적으로 통제가 가능하도록 회사내부에 조직과 인력을 갖출 것 - 제60조(외부주문등에 대한 기준) ① 금융회사 또는 전자금융업자는 전자금융거래를 위한 외부주문등의 경우에는 다음 각 호의 사항을 준수하여야 한다. 〈개정 2013. 12. 3.〉 9. 정보관리의 취약점을 최소화하고 보안유지를 위한 내부통제방안을 수립·운용하고, 통제는 제8조제1항제2호의 조직에서 수행 〈개정 2015. 2. 3.〉
FISM-260	10.2 외부주문 시 보호대책	외부주문 시 정보처리시스템 개발 업무에 사용되는 업무장소 및 전산설비는 내부 업무용과 분리하여 설치·운영 여부	5	○ **(전자금융감독규정)** - 제60조(외부주문등에 대한 기준)제1항제1호 ① 금융회사 또는 전자금융업자는 전자금융거래를 위한 외부주문등의 경우에는 다음 각 호의 사항을 준수하여야 한다. 〈개정 2013. 12. 3.〉

평가 항목ID	통제구분	평가항목	위험도	[근거조항] 전자금융감독규정 (금융위원회고시 제2018-36호, 2018. 12. 21) 전자금융감독규정시행세칙 (금융감독원세칙, 2021. 2. 25)
				1. 외부주문등에 의한 정보처리시스템의 개발업무에 사용되는 업무장소 및 전산설비는 내부 업무용과 분리하여 설치·운영 〈개정 2015. 2. 3.〉
FISM-261	10.2 외부주문 시 보호대책	외부주문 시 금융기관과 이용자간 암호화정보 해독 및 원장 등 중요 데이터 변경 금지 여부	5	○ **(전자금융감독규정)** - 제60조(외부주문등에 대한 기준)제1항제2호 ① 금융회사 또는 전자금융업자는 전자금융거래를 위한 외부주문등의 경우에는 다음 각 호의 사항을 준수하여야 한다. 〈개정 2013. 12. 3.〉 2. 금융회사와 이용자 간 암호화정보 해독 및 원장 등 중요 데이터 변경 금지 〈개정 2013. 12. 3.〉
FISM-262	10.2 외부주문 시 보호대책	외부주문 시 계좌번호, 비밀번호 등 이용자 금융정보 보관 및 유출 금지 여부	5	○ **(전자금융감독규정)** - 제60조(외부주문등에 대한 기준)제1항제3호 ① 금융회사 또는 전자금융업자는 전자금융거래를 위한 외부주문등의 경우에는 다음 각 호의 사항을 준수하여야 한다. 〈개정 2013. 12. 3.〉 3. 계좌번호, 비밀번호 등 이용자 금융정보 무단보관 및 유출 금지
FISM-263	10.2 외부주문 시 보호대책	외부주문 시 접근매체 위/변조, 해킹, 개인정보 유출 등에 대비한 보안대책 수립 여부	5	○ **(전자금융감독규정)** - 제60조(외부주문등에 대한 기준)제1항제4호 ① 금융회사 또는 전자금융업자는 전자금융거래를 위한 외부주문등의 경우에는 다음 각 호의 사항을 준수하여야 한다. 〈개정 2013. 12. 3.〉 4. 접근매체 위·변조, 해킹, 개인정보유출 등에 대비한 보안대책 수립
FISM-264	10.2 외부주문 시 보호대책	외부주문 시 금융기관과 전자금융보조업자간의 접속은 전용회선 사용 여부	5	○ **(전자금융감독규정)** - 제60조(외부주문등에 대한 기준)제1항제5호 ① 금융회사 또는 전자금융업자는 전자금융거래를 위한 외부주문등의 경우에는 다음 각 호의 사항을 준수하여야 한다. 〈개정 2013. 12. 3.〉

평가 항목ID	통제구분	평가항목	위험도	[근거조항] 전자금융감독규정 (금융위원회고시 제2018-36호, 2018. 12. 21) 전자금융감독규정시행세칙 (금융감독원세칙, 2021. 2. 25)
				5. 금융회사와 전자금융보조업자 간의 접속은 전용회선(전용회선과 동등한 보안 수준을 갖춘 가상의 전용회선을 포함한다)을 사용 〈개정 2013. 12. 3., 2016. 10. 5.〉
FISM-265	10.2 외부주문 시 보호대책	외부주문 시 정보처리시스템 장애 등 서비스 중단에 대비한 비상대책 수립 여부	5	○ **(전자금융감독규정)** - 제60조(외부주문등에 대한 기준) ① 금융회사 또는 전자금융업자는 전자금융거래를 위한 외부주문등의 경우에는 다음 각 호의 사항을 준수하여야 한다. 〈개정 2013. 12. 3.〉 6. 정보처리시스템 장애 등 서비스 중단에 대비한 비상대책 수립
FISM-266	10.2 외부주문 시 보호대책	외부주문 시 중요전산자료의 백업자료 보존 및 백업설비 확보 등 백업대책 수립	5	○ **(전자금융감독규정)** - 제60조(외부주문등에 대한 기준)제1항제8호 ① 금융회사 또는 전자금융업자는 전자금융거래를 위한 외부주문등의 경우에는 다음 각 호의 사항을 준수하여야 한다. 〈개정 2013. 12. 3.〉 8. 업무지속성을 위한 중요 전산자료의 백업(backup)자료 보존 및 백업설비 확보 등 백업대책 수립
FISM-267	10.3 외부주문 등에 대한 기준	외부주문 사항에 대해 연1회 이상 재무건전성 평가 및 주요 경영활동 상시모니터링 여부	5	○ **(전자금융감독규정)** - 제60조(외부주문등에 대한 기준)제1항제10호 ① 금융회사 또는 전자금융업자는 전자금융거래를 위한 외부주문등의 경우에는 다음 각 호의 사항을 준수하여야 한다. 〈개정 2013. 12. 3.〉 10. 전자금융보조업자에 대한 재무건전성을 연1회 이상 평가하여 재무상태 악화에 따른 도산에 대비하고 전자금융보조업자의 주요 경영활동에 대해 상시 모니터링을 실시

평가 항목ID	통제구분	평가항목	위험도	[근거조항] 전자금융감독규정 (금융위원회고시 제2018-36호, 2018. 12. 21) 전자금융감독규정시행세칙 (금융감독원세칙, 2021. 2. 25)
FISM-268	10.3 외부주문 등에 대한 기준	외부주문 사항에 대해 연1회 이상 서비스 품질수준 평가 여부	5	○ **(전자금융감독규정)** - 제60조(외부주문등에 대한 기준)제1항제11호 ① 금융회사 또는 전자금융업자는 전자금융거래를 위한 외부주문등의 경우에는 다음 각 호의 사항을 준수하여야 한다. 〈개정 2013. 12. 3.〉 11. 전자금융보조업자가 제공하는 서비스의 품질수준을 연1회 이상 평가할 것
FISM-269	10.3 외부주문 등에 대한 기준	외부주문 사항에 대해 사전 동의 없는 재위탁, 계약업체 변경 금지 (사전 동의시 계약서 기재사항 포함) 여부	5	○ **(전자금융감독규정)** - 제60조(외부주문등에 대한 기준)제1항제12호 ① 금융회사 또는 전자금융업자는 전자금융거래를 위한 외부주문등의 경우에는 다음 각 호의 사항을 준수하여야 한다. 〈개정 2013. 12. 3.〉 12. 전자금융보조업자가 사전 동의 없이 다시 외부주문등 계약을 체결하거나 계약업체를 변경하지 못하도록 하고, 사전 동의시 해당 계약서에 제7호의 사항을 기재하도록 통제 〈개정 2016. 6. 30.〉
FISM-270	10.3 외부주문 등에 대한 기준	외부주문 사항에 대해 위탁회사가 전자금융거래정보 보호와 관련된 전산장비·소프트웨어 개발, 운영, 유지관리 업무 재위탁 시, 금융거래정보 변경사항에 대해 위탁회사 또는 원수탁업자가 이를 관리, 통제할 수 있는 절차 마련 여부	5	○ **(전자금융감독규정)** - 제60조(외부주문등에 대한 기준)제4항제1호 ④ 법 제40조제6항 단서에서 "금융위원회가 인정하는 경우"란 전자금융거래정보의 보호와 관련된 전산장비·소프트웨어에 대한 개발·운영 및 유지관리 업무를 재위탁하는 경우로서 다음 각 호의 사항을 준수하는 경우를 말한다. 1. 재수탁업자가 재위탁된 업무를 처리함에 있어 금융거래 정보의 변경이 필요한 경우에는 위탁회사 또는 원수탁업자의 개별적 지시에 따라야 하며, 위탁회사 또는 원수탁업자는 변경된 정보가 지시 내용에 부합하는지 여부를 확인하여야 함

평가 항목ID	통제구분	평가항목	위험도	[근거조항] 전자금융감독규정 (금융위원회고시 제2018-36호, 2018. 12. 21) 전자금융감독규정시행세칙 (금융감독원세칙, 2021. 2. 25)
FISM-271	10.3 외부주문 등에 대한 기준	외부주문 사항에 대해 위탁된 금융거래정보가 위탁회사의 전산실 내 관리 및 보관 여부	5	○ **(전자금융감독규정)** - 제60조(외부주문등에 대한 기준)제4항제2호 ④ 법 제40조제6항 단서에서 "금융위원회가 인정하는 경우"란 전자금융거래정보의 보호와 관련된 전산장비·소프트웨어에 대한 개발·운영 및 유지관리 업무를 재위탁하는 경우로서 다음 각 호의 사항을 준수하는 경우를 말한다. 2. 위탁업무와 관련된 이용자의 금융거래정보는 위탁회사의 전산실 내에 두어야 함. 다만, 재수탁업자가 이용자의 이용자 정보를 어떠한 경우에도 알지 못하도록 위탁회사 또는 원수탁업자가 금융거래정보를 처리하여 제공한 경우에는 위탁회사의 관리·통제 하에 재수탁회사 등 제3의 장소로 이전 가능함
FISM-272	10.3 외부주문 등에 대한 기준	외부주문 시 업무 수행인력에 대한 사전 신원조회 실시, 대표자 신원보증서 징구, 인력변경시 인수인계에 관한사항 등 업무수행인력에 관한 관리방안 수립 여부	5	○ **(전자금융감독규정)** - 제60조(외부주문등에 대한 기준)제1항제13호 ① 금융회사 또는 전자금융업자는 전자금융거래를 위한 외부주문등의 경우에는 다음 각 호의 사항을 준수하여야 한다. 〈개정 2013. 12. 3.〉 13. 업무수행인력에 대하여 사전 신원조회 실시(이 경우 신원보증보험 증권 징구로 갈음할 수 있다) 또는 대표자의 신원보증서 징구, 인력변경시 인수인계에 관한 사항 등을 포함한 업무수행인력 관리방안 수립 〈개정 2018. 12. 21.〉
FISM-273	10.3 외부주문 등에 대한 기준	외부주문 시 자체 보안성 검토 및 정기 보안점검 실시 여부	5	○ **(전자금융감독규정)** - 제60조(외부주문등에 대한 기준)제1항제14호 ① 금융회사 또는 전자금융업자는 전자금융거래를 위한 외부주문등의 경우에는 다음 각 호의 사항을 준수하여야 한다. 〈개정 2013. 12. 3.〉 14. 외부주문등은 자체 보안성검토 및 정기(금융감독원장이 정하는 중요 점검사항에 대해서는 매일) 보안점검 실시 〈개정 2015. 2. 3.〉

평가 항목ID	통제구분	평가항목	위험도	[근거조항] 전자금융감독규정 (금융위원회고시 제2018-36호, 2018. 12. 21) 전자금융감독규정시행세칙 (금융감독원세칙, 2021. 2. 25)
				○ **(전자금융감독규정시행세칙)** - 제9조의2(외부주문등에 대한 기준) ② 규정 제60조제1항제14호에 따라 감독원장이 정하는 중요 점검사항은 별표 5-3과 같다.
FISM-274	11.1 정보기술부문 및 전자금융 사고보고	정보처리시스템 또는 통신회선 등의 장애로 10분 이상 전산 업무가 중단 또는 지연 사고에 대한 금융감독원장 보고 여부	5	○ **(전자금융감독규정)** - 제73조(정보기술부문 및 전자금융 사고보고)제1항제1호 ① 금융회사 및 전자금융업자는 다음 각 호와 관련된 중대한 사고가 발생한 경우에는 지체 없이 금융감독원장에게 보고하여야 한다. 〈개정 2013. 12. 3., 2015. 2. 3.〉 1. 정보처리시스템 또는 통신회선 등의 장애로 10분 이상 전산업무가 중단 또는 지연된 경우 ○ **(전자금융감독규정시행세칙)** - 제12조(정보기술부문 사고보고) ① 금융회사 및 전자금융업자는 규정 제73조에 따른 정보기술부문 및 전자금융 사고가 발생한 경우 별지 제2호서식 별첨1에 따라 즉시 보고하여야 한다. 다만, 규정 제73조제1항제4호의 사고 중 사고금액이 3억원 미만인 사고의 경우 매월 발생한 사고를 익월 15일까지 별지 제2호서식 별첨2에 따라 일괄 보고할 수 있다. ② 제1항에 따른 사고보고는 최초보고, 중간보고 및 종결보고로 구분한다. 1. 최초보고 : 사고를 인지 또는 발견한 즉시 감독원의 전자금융사고 대응시스템(Electronic Financial Accident Response System : EFARS), 서면, 팩시밀리 또는 전화로 보고하되, 전화로 보고한 경우에는 즉시 전자금융사고 대응시스템, 서면 또는 팩시밀리로 보고한다. 2. 중간보고 : 제1호의 즉시보고 후 사고내용 보완할 필요가 있는 경우에는 즉시

평가 항목ID	통제구분	평가항목	위험도	[근거조항] 전자금융감독규정 (금융위원회고시 제2018-36호, 2018. 12. 21) 전자금융감독규정시행세칙 (금융감독원세칙, 2021. 2. 25)
				중간보고를 하여야 하며, 제3호의 조치완료 시까지 2월 이상 소요될 경우에는 인지·발견일로부터 2월 이내 및 종결 시까지 매 6월마다 제1호의 방법에 따라 보고한다. 다만, 즉시보고 후 조치완료 시까지 2월 미만이 소요될 경우에는 중간보고를 생략할 수 있다. 3. 종결보고 : 사고금액에 대한 배상조치가 완료되거나 사고조치 등이 완료되어 정상적인 업무를 수행하게 된 때 제1호의 방법에 따라 보고한다. 다만, 최초보고 시 조치가 이미 완료된 경우에는 종결보고를 생략할 수 있다. ③ 감독원장은 금융회사 및 전자금융업자 정보기술부문의 사고보고 등을 전담할 비상연락 담당자를 회사별로 지정할 수 있다. ④ 금융회사 및 전자금융업자는 비상연락 담당자가 제3항에 따라 지정되거나 변경된 경우에는 제2항제1호에서 정한 보고방법에 따라 감독원장에게 즉시 보고하여야 한다.
FISM-275	11.1 정보기술부문 및 전자금융 사고보고	전산자료 또는 프로그램의 조작과 관련 금융사고 보고에 대한 금융감독원장 보고 여부	5	○ **(전자금융감독규정)** - 제73조(정보기술부문 및 전자금융 사고보고)제1항제2호 ① 금융회사 및 전자금융업자는 다음 각 호와 관련된 중대한 사고가 발생한 경우에는 지체 없이 금융감독원장에게 보고하여야 한다. 〈개정 2013. 12. 3., 2015. 2. 3.〉 2. 전산자료 또는 프로그램의 조작과 관련된 금융사고가 발생한 경우 ○ **(전자금융감독규정시행세칙)** - 제12조(정보기술부문 사고보고) ① 금융회사 및 전자금융업자는 규정 제73조에 따른 정보기술부문 및 전자금융 사고가 발생한 경우 별지 제2호서식 별첨1에 따라 즉시 보고하여야 한다. 다만, 규정 제73조제1항제4호의 사고 중 사고금액이 3억원 미만인 사고의 경우 매월 발생한 사고를 익월 15일까지 별지 제2호서식 별첨2에 따라 일괄 보고할 수 있다. ② 제1항에 따른 사고보고는 최초보고, 중간보고 및 종결보고로 구분한다. 1. 최초보고 : 사고를 인지 또는 발견한 즉시 감독원의 전자금융사고 대응시스템

평가 항목ID	통제구분	평가항목	위험도	[근거조항] 전자금융감독규정 (금융위원회고시 제2018-36호, 2018. 12. 21) 전자금융감독규정시행세칙 (금융감독원세칙, 2021. 2. 25)
				(Electronic Financial Accident Response System : EFARS), 서면, 팩시밀리 또는 전화로 보고하되, 전화로 보고한 경우에는 즉시 전자금융사고 대응시스템, 서면 또는 팩시밀리로 보고한다. 2. 중간보고 : 제1호의 즉시보고 후 사고내용 보완할 필요가 있는 경우에는 즉시 중간보고를 하여야 하며, 제3호의 조치완료 시까지 2월 이상 소요될 경우에는 인지·발견일로부터 2월 이내 및 종결 시까지 매 6월마다 제1호의 방법에 따라 보고한다. 다만, 즉시보고 후 조치완료 시까지 2월 미만이 소요될 경우에는 중간보고를 생략할 수 있다. 3. 종결보고 : 사고금액에 대한 배상조치가 완료되거나 사고조치 등이 완료되어 정상적인 업무를 수행하게 된 때 제1호의 방법에 따라 보고한다. 다만, 최초 보고 시 조치가 이미 완료된 경우에는 종결보고를 생략할 수 있다. ③ 감독원장은 금융회사 및 전자금융업자 정보기술부문의 사고보고 등을 전담할 비상연락 담당자를 회사별로 지정할 수 있다. ④ 금융회사 및 전자금융업자는 비상연락 담당자가 제3항에 따라 지정되거나 변경된 경우에는 제2항제1호에서 정한 보고방법에 따라 감독원장에게 즉시 보고하여야 한다.
FISM-276	11.1 정보기술부문 및 전자금융 사고보고	전자적 침해행위로 인한 정보처리시스템 사고에 대한 금융감독원장 보고 여부	5	○ **(전자금융감독규정)** - 제73조(정보기술부문 및 전자금융 사고보고)제1항제3호 ① 금융회사 및 전자금융업자는 다음 각 호와 관련된 중대한 사고가 발생한 경우에는 지체 없이 금융감독원장에게 보고하여야 한다. 〈개정 2013. 12. 3., 2015. 2. 3.〉 3. 전자적 침해행위로 인해 정보처리시스템에 사고가 발생하거나 이로인해 이용자가 금전적 피해를 입었다고 금융회사 또는 전자금융업자에게 통지한 경우 〈개정 2013. 12. 3.〉 ○ **(전자금융감독규정시행세칙)** - 제12조(정보기술부문 사고보고)

평가 항목ID	통제구분	평가항목	위험도	[근거조항] 전자금융감독규정 (금융위원회고시 제2018-36호, 2018. 12. 21) 전자금융감독규정시행세칙 (금융감독원세칙, 2021. 2. 25)
				① 금융회사 및 전자금융업자는 규정 제73조에 따른 정보기술부문 및 전자금융 사고가 발생한 경우 별지 제2호서식 별첨1에 따라 즉시 보고하여야 한다. 다만, 규정 제73조제1항제4호의 사고 중 사고금액이 3억원 미만인 사고의 경우 매월 발생한 사고를 익월 15일까지 별지 제2호서식 별첨2에 따라 일괄 보고할 수 있다. ② 제1항에 따른 사고보고는 최초보고, 중간보고 및 종결보고로 구분한다. 1. 최초보고 : 사고를 인지 또는 발견한 즉시 감독원의 전자금융사고 대응시스템(Electronic Financial Accident Response System : EFARS), 서면, 팩시밀리 또는 전화로 보고하되, 전화로 보고한 경우에는 즉시 전자금융사고 대응시스템, 서면 또는 팩시밀리로 보고한다. 2. 중간보고 : 제1호의 즉시보고 후 사고내용 보완할 필요가 있는 경우에는 즉시 중간보고를 하여야 하며, 제3호의 조치완료 시까지 2월 이상 소요될 경우에는 인지·발견일로부터 2월 이내 및 종결 시까지 매 6월마다 제1호의 방법에 따라 보고한다. 다만, 즉시보고 후 조치완료 시까지 2월 미만이 소요될 경우에는 중간보고를 생략할 수 있다. 3. 종결보고 : 사고금액에 대한 배상조치가 완료되거나 사고조치 등이 완료되어 정상적인 업무를 수행하게 된 때 제1호의 방법에 따라 보고한다. 다만, 최초보고 시 조치가 이미 완료된 경우에는 종결보고를 생략할 수 있다. ③ 감독원장은 금융회사 및 전자금융업자 정보기술부문의 사고보고 등을 전담할 비상연락 담당자를 회사별로 지정할 수 있다. ④ 금융회사 및 전자금융업자는 비상연락 담당자가 제3항에 따라 지정되거나 변경된 경우에는 제2항제1호에서 정한 보고방법에 따라 감독원장에게 즉시 보고하여야 한다.
FISM-277	11.1 정보기술부문	이용자가 전자적 침해행위로 인해 금전적 피해를 입었다고 통지한	5	○ **(전자금융감독규정)** - 제73조(정보기술부문 및 전자금융 사고보고)제1항제3호

평가 항목ID	통제구분	평가항목	위험도	[근거조항] 전자금융감독규정 (금융위원회고시 제2018-36호, 2018. 12. 21) 전자금융감독규정시행세칙 (금융감독원세칙, 2021. 2. 25)
	및 전자금융 사고보고	사고에 대한 금융감독원장 보고 여부		① 금융회사 및 전자금융업자는 다음 각 호와 관련된 중대한 사고가 발생한 경우에는 지체 없이 금융감독원장에게 보고하여야 한다. 〈개정 2013. 12. 3., 2015. 2. 3.〉 3. 전자적 침해행위로 인해 정보처리시스템에 사고가 발생하거나 이로인해 이용자가 금전적 피해를 입었다고 금융회사 또는 전자금융업자에게 통지한 경우 〈개정 2013. 12. 3.〉 ○ **(전자금융감독규정시행세칙)** - 제12조(정보기술부문 사고보고) ① 금융회사 및 전자금융업자는 규정 제73조에 따른 정보기술부문 및 전자금융 사고가 발생한 경우 별지 제2호서식 별첨1에 따라 즉시 보고하여야 한다. 다만, 규정 제73조제1항제4호의 사고 중 사고금액이 3억원 미만인 사고의 경우 매월 발생한 사고를 익월 15일까지 별지 제2호서식 별첨2에 따라 일괄 보고할 수 있다. ② 제1항에 따른 사고보고는 최초보고, 중간보고 및 종결보고로 구분한다. 1. 최초보고 : 사고를 인지 또는 발견한 즉시 감독원의 전자금융사고 대응시스템(Electronic Financial Accident Response System : EFARS), 서면, 팩시밀리 또는 전화로 보고하되, 전화로 보고한 경우에는 즉시 전자금융사고 대응시스템, 서면 또는 팩시밀리로 보고한다. 2. 중간보고 : 제1호의 즉시보고 후 사고내용 보완할 필요가 있는 경우에는 즉시 중간보고를 하여야 하며, 제3호의 조치완료 시까지 2월 이상 소요될 경우에는 인지·발견일로부터 2월 이내 및 종결 시까지 매 6월마다 제1호의 방법에 따라 보고한다. 다만, 즉시보고 후 조치완료 시까지 2월 미만이 소요될 경우에는 중간보고를 생략할 수 있다. 3. 종결보고 : 사고금액에 대한 배상조치가 완료되거나 사고조치 등이 완료되어 정상적인 업무를 수행하게 된 때 제1호의 방법에 따라 보고한다. 다만, 최초

평가 항목ID	통제구분	평가항목	위험도	[근거조항] 전자금융감독규정 (금융위원회고시 제2018-36호, 2018. 12. 21) 전자금융감독규정시행세칙 (금융감독원세칙, 2021. 2. 25)
				보고 시 조치가 이미 완료된 경우에는 종결보고를 생략할 수 있다. ③ 감독원장은 금융회사 및 전자금융업자 정보기술부문의 사고보고 등을 전담할 비상연락 담당자를 회사별로 지정할 수 있다. ④ 금융회사 및 전자금융업자는 비상연락 담당자가 제3항에 따라 지정되거나 변경된 경우에는 제2항제1호에서 정한 보고방법에 따라 감독원장에게 즉시 보고하여야 한다.
FISM-278	11.1 정보기술부문 및 전자금융 사고보고	접근매체의 위조나 변조로 발생한 사고에 대한 금융감독원장 보고 여부	5	○ **(전자금융감독규정)** - 제73조(정보기술부문 및 전자금융 사고보고)제1항제4호 ① 금융회사 및 전자금융업자는 다음 각 호와 관련된 중대한 사고가 발생한 경우에는 지체 없이 금융감독원장에게 보고하여야 한다. 〈개정 2013. 12. 3., 2015. 2. 3.〉 4. 법 제9조제1항의 규정에서 정하는 사고 ○ **(전자금융감독규정시행세칙)** - 제12조(정보기술부문 사고보고) ① 금융회사 및 전자금융업자는 규정 제73조에 따른 정보기술부문 및 전자금융 사고가 발생한 경우 별지 제2호서식 별첨1에 따라 즉시 보고하여야 한다. 다만, 규정 제73조제1항제4호의 사고 중 사고금액이 3억원 미만인 사고의 경우 매월 발생한 사고를 익월 15일까지 별지 제2호서식 별첨2에 따라 일괄 보고할 수 있다. ② 제1항에 따른 사고보고는 최초보고, 중간보고 및 종결보고로 구분한다. 1. 최초보고 : 사고를 인지 또는 발견한 즉시 감독원의 전자금융사고 대응시스템(Electronic Financial Accident Response System : EFARS), 서면, 팩시밀리 또는 전화로 보고하되, 전화로 보고한 경우에는 즉시 전자금융사고 대응시스템, 서면 또는 팩시밀리로 보고한다. 2. 중간보고 : 제1호의 즉시보고 후 사고내용 보완할 필요가 있는 경우에는 즉시 중간보고를 하여야 하며, 제3호의 조치완료 시까지 2월 이상 소요될 경우에는

평가 항목ID	통제구분	평가항목	위험도	[근거조항] 전자금융감독규정 (금융위원회고시 제2018-36호, 2018. 12. 21) 전자금융감독규정시행세칙 (금융감독원세칙, 2021. 2. 25)
				인지·발견일로부터 2월 이내 및 종결 시까지 매 6월마다 제1호의 방법에 따라 보고한다. 다만, 즉시보고 후 조치완료 시까지 2월 미만이 소요될 경우에는 중간보고를 생략할 수 있다. 3. 종결보고 : 사고금액에 대한 배상조치가 완료되거나 사고조치 등이 완료되어 정상적인 업무를 수행하게 된 때 제1호의 방법에 따라 보고한다. 다만, 최초 보고 시 조치가 이미 완료된 경우에는 종결보고를 생략할 수 있다. ③ 감독원장은 금융회사 및 전자금융업자 정보기술부문의 사고보고 등을 전담할 비상연락 담당자를 회사별로 지정할 수 있다. ④ 금융회사 및 전자금융업자는 비상연락 담당자가 제3항에 따라 지정되거나 변경된 경우에는 제2항제1호에서 정한 보고방법에 따라 감독원장에게 즉시 보고하여야 한다.
FISM-279	11.1 정보기술부문 및 전자금융 사고보고	계약체결 또는 거래지시의 전자적 전송이나 처리과정에서 발생한 사고에 대한 금융감독원장 보고 여부	5	○ **(전자금융감독규정)** - 제73조(정보기술부문 및 전자금융 사고보고)제1항제4호 ① 금융회사 및 전자금융업자는 다음 각 호와 관련된 중대한 사고가 발생한 경우에는 지체 없이 금융감독원장에게 보고하여야 한다 〈개정 2013. 12. 3., 2015. 2. 3.〉 4. 법 제9조제1항의 규정에서 정하는 사고 ○ **(전자금융감독규정시행세칙)** - 제12조(정보기술부문 사고보고) ① 금융회사 및 전자금융업자는 규정 제73조에 따른 정보기술부문 및 전자금융 사고가 발생한 경우 별지 제2호서식 별첨1에 따라 즉시 보고하여야 한다. 다만, 규정 제73조제1항제4호의 사고 중 사고금액이 3억원 미만인 사고의 경우 매월 발생한 사고를 익월 15일까지 별지 제2호서식 별첨2에 따라 일괄 보고할 수 있다.

평가 항목ID	통제구분	평가항목	위험도	[근거조항] 전자금융감독규정 (금융위원회고시 제2018-36호, 2018. 12. 21) 전자금융감독규정시행세칙 (금융감독원세칙, 2021. 2. 25)
				② 제1항에 따른 사고보고는 최초보고, 중간보고 및 종결보고로 구분한다. 1. 최초보고 : 사고를 인지 또는 발견한 즉시 감독원의 전자금융사고 대응시스템(Electronic Financial Accident Response System : EFARS), 서면, 팩시밀리 또는 전화로 보고하되, 전화로 보고한 경우에는 즉시 전자금융사고 대응시스템, 서면 또는 팩시밀리로 보고한다. 2. 중간보고 : 제1호의 즉시보고 후 사고내용 보완할 필요가 있는 경우에는 즉시 중간보고를 하여야 하며, 제3호의 조치완료 시까지 2월 이상 소요될 경우에는 인지·발견일로부터 2월 이내 및 종결 시까지 매 6월마다 제1호의 방법에 따라 보고한다. 다만, 즉시보고 후 조치완료 시까지 2월 미만이 소요될 경우에는 중간보고를 생략할 수 있다. 3. 종결보고 : 사고금액에 대한 배상조치가 완료되거나 사고조치 등이 완료되어 정상적인 업무를 수행하게 된 때 제1호의 방법에 따라 보고한다. 다만, 최초보고 시 조치가 이미 완료된 경우에는 종결보고를 생략할 수 있다. ③ 감독원장은 금융회사 및 전자금융업자 정보기술부문의 사고보고 등을 전담할 비상연락 담당자를 회사별로 지정할 수 있다. ④ 금융회사 및 전자금융업자는 비상연락 담당자가 제3항에 따라 지정되거나 변경된 경우에는 제2항제1호에서 정한 보고방법에 따라 감독원장에게 즉시 보고하여야 한다.
FISM-280	11.1 정보기술부문 및 전자금융 사고보고	사고보고의 고의 지연 및 숨긴 자에 대한 징계절차 수립 여부	5	○ **(전자금융감독규정)** - 제73조(정보기술부문 및 전자금융 사고보고)제2항 ② 금융회사 및 전자금융업자는 제1항에 따른 사고보고를 고의로 지연하거나 숨긴 자에 대하여 소정절차에 따라 징계 등 필요한 조치를 취하여야 한다. 〈개정 2013. 12. 3.〉 ○ **(전자금융감독규정시행세칙)** - 제12조(정보기술부문 사고보고)

평가 항목ID	통제구분	평가항목	위험도	[근거조항] 전자금융감독규정 (금융위원회고시 제2018-36호, 2018. 12. 21) 전자금융감독규정시행세칙 (금융감독원세칙, 2021. 2. 25)
				① 금융회사 및 전자금융업자는 규정 제73조에 따른 정보기술부문 및 전자금융사고가 발생한 경우 별지 제2호서식 별첨1에 따라 즉시 보고하여야 한다. 다만, 규정 제73조제1항제4호의 사고 중 사고금액이 3억원 미만인 사고의 경우 매월 발생한 사고를 익월 15일까지 별지 제2호서식 별첨2에 따라 일괄 보고할 수 있다. ② 제1항에 따른 사고보고는 최초보고, 중간보고 및 종결보고로 구분한다. 1. 최초보고 : 사고를 인지 또는 발견한 즉시 감독원의 전자금융사고 대응시스템(Electronic Financial Accident Response System : EFARS), 서면, 팩시밀리 또는 전화로 보고하되, 전화로 보고한 경우에는 즉시 전자금융사고 대응시스템, 서면 또는 팩시밀리로 보고한다. 2. 중간보고 : 제1호의 즉시보고 후 사고내용 보완할 필요가 있는 경우에는 즉시 중간보고를 하여야 하며, 제3호의 조치완료 시까지 2월 이상 소요될 경우에는 인지·발견일로부터 2월 이내 및 종결 시까지 매 6월마다 제1호의 방법에 따라 보고한다. 다만, 즉시보고 후 조치완료 시까지 2월 미만이 소요될 경우에는 중간보고를 생략할 수 있다. 3. 종결보고 : 사고금액에 대한 배상조치가 완료되거나 사고조치 등이 완료되어 정상적인 업무를 수행하게 된 때 제1호의 방법에 따라 보고한다. 다만, 최초보고 시 조치가 이미 완료된 경우에는 종결보고를 생략할 수 있다. ③ 감독원장은 금융회사 및 전자금융업자 정보기술부문의 사고보고 등을 전담할 비상연락 담당자를 회사별로 지정할 수 있다. ④ 금융회사 및 전자금융업자는 비상연락 담당자가 제3항에 따라 지정되거나 변경된 경우에는 제2항제1호에서 정한 보고방법에 따라 감독원장에게 즉시 보고하여야 한다.
FISM-281	11.2 침해사고 대응	해킹 등 전자적 침해행위로 인한 피해 발생시 즉시 대처할 수 있도록 적절한 대책 마련 여부	5	○ **(전자금융감독규정)** - 제15조(해킹 등 방지대책)제4항

평가 항목ID	통제구분	평가항목	위험도	[근거조항] 전자금융감독규정 (금융위원회고시 제2018-36호, 2018. 12. 21) 전자금융감독규정시행세칙 (금융감독원세칙, 2021. 2. 25)
				④ 금융회사 또는 전자금융업자는 해킹 등 전자적 침해행위로 인한 피해 발생시 즉시 대처할 수 있도록 적절한 대책을 마련하여야 한다. 〈개정 2013. 12. 3.〉
FISM-282	11.3 손해배상	전자금융사고 시 책임이행을 위한 보험 등 가입 여부	5	**○ (전자금융감독규정)** - 제5조(전자금융사고 책임이행을 위한 보험 등의 가입에 관한 기준)제1항 ① 금융회사 또는 전자금융업자가 법 제9조제4항에 따라 전자금융사고 책임이행을 위한 보험 또는 공제에 가입하는 경우 보상한도는 다음 각 호에서 정하는 금액 이상이어야 한다. 〈개정 2013. 12. 3.〉 1. 「금융위원회의 설치 등에 관한 법률」 제38조제1호(다만, 「은행법」에 의한 지방금융회사 및 같은 법 제58조에 의해 인가를 받은 외국금융회사의 국내 지점은 제외한다) 및 제7호의 회사, 「전자금융거래법 시행령」 제2조제2호의 회사 : 20억원 2. 「금융위원회의 설치 등에 관한 법률」 제38조제8호의 회사, 「전자금융거래법」 제2조제3호나목(신용카드업자에 한한다) 및 다목의 회사, 「전자금융거래법 시행령」 제2조제1호의 회사, 「은행법」에 따른 지방금융회사 및 같은 법 제58조에 의해 인가를 받은 외국금융회사의 국내지점 : 10억원 〈개정 2013. 12. 3.〉 3. 「금융위원회의 설치 등에 관한 법률」 제38조제2호(다만, 명의개서대행업무를 수행하는 회사는 제외)의 회사 : 5억원 〈개정 2013. 12. 3.〉 4. 제1호 부터 제3호 이외의 금융회사 : 1억원. 다만, 제1호 부터 제3호 이외의 금융회사들이 관련 법령에 의해 당해 금융회사를 구성원으로 하는 금융회사를 통해 전자금융거래 관련 정보기술부문의 주요부분을 공동으로 이용하는 경우, 정보기술부문의 주요부문을 제공하는 금융회사가 공동 이용 금융회사 전체의 사고를 보장하는 내용으로 제2호의 금액(시행령 제2조제5호의 금융회사는 제1호의 금액) 이상의 보험 또는 공제에 가입하면 공동 이용 금융회사는 본호의 보험 또는 공제에 가입한 것으로 본다. 〈개정 2013. 12. 3.〉 5. 법 제28조제2항제1호 및 제2호의 전자금융업자 : 2억원

평가 항목ID	통제구분	평가항목	위험도	[근거조항] 전자금융감독규정 (금융위원회고시 제2018-36호, 2018. 12. 21) 전자금융감독규정시행세칙 (금융감독원세칙, 2021. 2. 25)
				6. 법 제28조제2항제4호의 전자금융업자 중 제1호 또는 제2호에 속하는 금융회사가 발급한 신용카드, 직불카드 등 거래지시에 사용되는 접근매체의 정보를 저장하는 전자금융업자 : 10억원 〈개정 2016. 10. 5.〉 7. 제5호, 제6호 이외의 전자금융업자 : 1억원 〈종전의 제6호에서 이동〉
FISM-283	11.3 손해배상	전자금융사고시 보상한도설정의 적정성 여부	5	○ **(전자금융감독규정)** - 제5조(전자금융사고 책임이행을 위한 보험 등의 가입에 관한 기준)제1항 ① 금융회사 또는 전자금융업자가 법 제9조제4항에 따라 전자금융사고 책임이행을 위한 보험 또는 공제에 가입하는 경우 보상한도는 다음 각 호에서 정하는 금액 이상이어야 한다. 〈개정 2013. 12. 3.〉 1. 「금융위원회의 설치 등에 관한 법률」 제38조제1호(다만, 「은행법」에 의한 지방금융회사 및 같은 법 제58조에 의해 인가를 받은 외국금융회사의 국내지점은 제외한다) 및 제7호의 회사, 「전자금융거래법 시행령」 제2조제2호의 회사 : 20억원 〈개정 2013. 12. 3.〉 2. 「금융위원회의 설치 등에 관한 법률」 제38조제8호의 회사, 「전자금융거래법」 제2조제3호나목(신용카드업자에 한한다) 및 다목의 회사, 「전자금융거래법 시행령」 제2조제1호의 회사, 「은행법」에 따른 지방금융회사 및 같은 법 제58조에 의해 인가를 받은 외국금융회사의 국내지점 : 10억원 〈개정 2013. 12. 3.〉 3. 「금융위원회의 설치 등에 관한 법률」 제38조제2호(다만, 명의개서대행업무를 수행하는 회사는 제외)의 회사 : 5억원 〈개정 2013. 12. 3.〉 4. 제1호 부터 제3호 이외의 금융회사 : 1억원. 다만, 제1호 부터 제3호 이외의 금융회사들이 관련 법령에 의해 당해 금융회사를 구성원으로 하는 금융회사를 통해 전자금융거래 관련 정보기술부문의 주요부분을 공동으로 이용하는 경우, 정보기술부문의 주요부문을 제공하는 금융회사가 공동 이용 금융회사 전체의 사고를 보장하는 내용으로 제2호의 금액(시행령 제2조제5호의 금융회사는 제1호의 금액) 이상의 보험 또는 공제에 가입하면 공동 이용 금융회사는 본호의

평가 항목ID	통제구분	평가항목	위험도	[근거조항] 전자금융감독규정 (금융위원회고시 제2018-36호, 2018. 12. 21) 전자금융감독규정시행세칙 (금융감독원세칙, 2021. 2. 25)
				보험 또는 공제에 가입한 것으로 본다. 〈개정 2013. 12. 3.〉 5. 법 제28조제2항제1호 및 제2호의 전자금융업자 : 2억원 6. 법 제28조제2항제4호의 전자금융업자 중 제1호 또는 제2호에 속하는 금융회사가 발급한 신용카드, 직불카드 등 거래지시에 사용되는 접근매체의 정보를 저장하는 전자금융업자 : 10억원 〈개정 2016. 10. 5.〉 7. 제5호, 제6호 이외의 전자금융업자 : 1억원 〈종전의 제6호에서 이동〉
FISM-284	11.3 손해배상	전자금융사고 시 책임이행을 위한 준비금 관리 및 지급에 관한 내부절차 수립 및 운영 여부	5	○ **(전자금융감독규정)** - 제5조(전자금융사고 책임이행을 위한 보험 등의 가입에 관한 기준)제2항 ② 금융회사 또는 전자금융업자가 전자금융사고 책임이행을 위한 준비금을 적립하는 경우에는 제1항 각 호에서 정한 금액 이상의 금액을 보유하고 책임이행이 신속히 이루어질 수 있도록 준비금 관리 및 지급에 관한 내부 절차를 수립하여 운영하여야 한다. 〈개정 2013. 12. 3., 2016. 10. 5.〉
FISM-285	8.3 위기대응 행동매뉴얼 수립	위기대응 행동매뉴얼 또는 비상대책에 따라 연 1회의 비상대응훈련을 실시하고 그 결과를 금융위원회에 보고하는지 여부 확인	5	○ **(전자금융감독규정)** - 제24조(비상대응훈련 실시)제1항 ① 금융회사 또는 전자금융업자는 제23조제4항에 따른 행동매뉴얼 또는 같은 조 제5항에 따른 비상대책에 따라 연 1회의 비상대응훈련을 실시하고 그 결과를 금융위원회에 보고하여야 한다. 이때, 제23조제10항에 따른 재해복구전환훈련을 포함하여 실시할 수 있다. 〈개정 2013. 12. 3., 2016. 6. 30.〉 ② 금융위원회는 금융분야의 비상대응능력을 강화하기 위하여 금융회사 또는 전자금융업자를 선별하여 금융분야 합동비상대응훈련을 실시할 수 있다. 〈개정 2013. 12. 3.〉 ③ 금융위원회는 제2항의 규정에 따른 합동비상대응훈련을 실시할 때, 다음 각 호의

평가 항목ID	통제구분	평가항목	위험도	[근거조항] 전자금융감독규정 (금융위원회고시 제2018-36호, 2018. 12. 21) 전자금융감독규정시행세칙 (금융감독원세칙, 2021. 2. 25)
				기관에게 지원을 요청할 수 있다. 1.「정부조직법」 제15조에 따른 "국가정보원(국가사이버안전센터)" 2.「경찰법」 제2조에 따른 "경찰청(사이버테러대응센터)" 3. 침해사고대응기관 〈개정 2013. 12. 3.〉 4. 그밖에 비상대응훈련의 실효성 확보를 위하여 금융위원회가 필요하다고 인정하는 기관 ④ 금융회사 또는 전자금융업자는 제1항 및 제2항에 따른 의무의 이행을 위하여 전자금융보조업자에게 협조를 요청할 수 있다. 〈신설 2018. 12. 21.〉
FISM-286	11.1 정보기술부문 및 전자금융 사고보고	전자금융거래를 위한 전자적 장치 또는 정보통신망에 침입하여 부정한 방법으로 획득한 접근매체의 이용으로 발생한 사고에 대한 금융감독원장 보고 여부	5	○ **(전자금융감독규정)** - 제73조(정보기술부문 및 전자금융 사고보고)제1항제4호 ① 금융회사 및 전자금융업자는 다음 각 호와 관련된 중대한 사고가 발생한 경우에는 지체 없이 금융감독원장에게 보고하여야 한다. 〈개정 2013. 12. 3., 2015. 2. 3.〉 4. 법 제9조제1항의 규정에서 정하는 사고 ○ **(전자금융감독규정시행세칙)** - 제12조(정보기술부문 사고보고) ① 금융회사 및 전자금융업자는 규정 제73조에 따른 정보기술부문 및 전자금융 사고가 발생한 경우 별지 제2호서식 별첨1에 따라 즉시 보고하여야 한다. 다만, 규정 제73조제1항제4호의 사고 중 사고금액이 3억원 미만인 사고의 경우 매월 발생한 사고를 익월 15일까지 별지 제2호서식 별첨2에 따라 일괄 보고할 수 있다. ② 제1항에 따른 사고보고는 최초보고, 중간보고 및 종결보고로 구분한다. 1. 최초보고 : 사고를 인지 또는 발견한 즉시 감독원의 전자금융사고 대응시스템(Electronic Financial Accident Response System : EFARS), 서면, 팩시밀리 또는 전화로 보고하되, 전화로 보고한 경우에는 즉시 전자금융사고 대응시스템, 서면 또는 팩시밀리로 보고한다. 2. 중간보고 : 제1호의 즉시보고 후 사고내용 보완할 필요가 있는 경우에는 즉시

평가 항목ID	통제구분	평가항목	위험도	[근거조항] 전자금융감독규정 (금융위원회고시 제2018-36호, 2018. 12. 21) 전자금융감독규정시행세칙 (금융감독원세칙, 2021. 2. 25)
				중간보고를 하여야 하며, 제3호의 조치완료 시까지 2월 이상 소요될 경우에는 인지·발견일로부터 2월 이내 및 종결 시까지 매 6월마다 제1호의 방법에 따라 보고한다. 다만, 즉시보고 후 조치완료 시까지 2월 미만이 소요될 경우에는 중간보고를 생략할 수 있다. 3. 종결보고 : 사고금액에 대한 배상조치가 완료되거나 사고조치 등이 완료되어 정상적인 업무를 수행하게 된 때 제1호의 방법에 따라 보고한다. 다만, 최초 보고 시 조치가 이미 완료된 경우에는 종결보고를 생략할 수 있다. ③ 감독원장은 금융회사 및 전자금융업자 정보기술부문의 사고보고 등을 전담할 비상연락 담당자를 회사별로 지정할 수 있다. ④ 금융회사 및 전자금융업자는 비상연락 담당자가 제3항에 따라 지정되거나 변경된 경우에는 제2항제1호에서 정한 보고방법에 따라 감독원장에게 즉시 보고하여야 한다.
FISM-287	5.4 취약점 분석·평가	오픈뱅킹 운영기관 등에서 정한 기준에 따라 보안 점검을 실시*하고, 결과에 따른 미흡사항의 제거 또는 그에 상응하는 조치시행 여부 * 오픈뱅킹 서비스 개시 1년 이상 경과한 금융회사 등에 해당	5	○ **(전자금융감독규정)** - 제37조의2(전자금융기반시설의 취약점 분석·평가 주기, 내용 등) ① 전자금융기반시설의 취약점 분석·평가는 총자산이 2조원 이상이고, 상시 종업원 수(「소득세법」에 따른 원천징수의무자가 근로소득세를 원천징수한 자를 기준으로 한다. 이하 같다) 300명 이상인 금융회사 또는 전자금융업자이거나 「수산업협동조합법」, 「산림조합법」, 「신용협동조합법」, 「상호저축은행법」 및 「새마을금고법」에 따른 중앙회의 경우 연 1회 이상(홈페이지에 대해서는 6개월에 1회 이상) 실시하여야 한다. ⑤ 금융회사 또는 전자금융업자는 취약점 분석·평가에 따라 이행계획을 수립·시행하여야 하며 다음 각 호의 사항을 준수하여야 한다. 1. 취약점 분석·평가 결과에 따른 취약점의 제거 또는 이에 상응하는 조치의 시행

【서버】

■ 평가대상

A	B	C	D	E
AIX 계열	HP-UX 계열	LNIUX 계열	Solaris 계열	Windows 계열

■ 평가기준

평가 항목ID	A	B	C	D	E	통제 구분	평가항목	위험도	상세설명
SRV-001	○	○	○	○	○	5.3.2 보안 관리	SNMP Community 스트링 설정 미흡	3	○ SNMP 서비스는 네트워크 관리 및 네트워크 장치의 동작을 감시/통할하는 SNMP 프로토콜을 기반으로 하는 서비스로, SNMP 통신 시 접근 허용 여부를 결정하기 위한 SNMP community string의 복잡도가 낮게 설정 되었는지 점검
SRV-003					○	5.3.2 보안 관리	SNMP 접근 통제 미설정	3	○ SNMP 서비스는 네트워크 관리 및 네트워크 장치의 동작을 감시/통할하는 SNMP 프로토콜을 기반으로 하는 서비스로, SNMP서비스를 사용할 수 있는 호스트를 특정하여 접근통제를 수행하고 있는지 점검
SRV-004	○	○	○	○	○	5.3.2 보안 관리	불필요한 SMTP 서비스 실행	3	○ SMTP 서비스는 인터넷에서 메일을 전송하는 SMTP 프로토콜을 기반으로 하는 서비스로, 악의적인 공격자가 SMTP 서비스를 실행 중인 서버의 정보를 획득하는 등 다양한 공격이 가능하므로 불필요한 SMTP 서비스 가동 여부를 점검
SRV-005	○	○	○	○		5.3.2 보안 관리	SMTP 서비스의 expn/vrfy 명령어 실행 제한 미비	3	○ SMTP 서비스에서 제공하는 expn/vrfy 명령어는 시스템 계정명 수집 가능성이 존재하므로, 해당 명령의 허용 여부를 점검

평가 항목ID	A	B	C	D	E	통제 구분	평가항목	위험도	상세설명
SRV-006	○	○	○	○		5.3.2 보안 관리	SMTP 서비스 로그 수준 설정 미흡	2	○ SMTP 서비스는 일반적으로 로그 설정을 할 때, 중요한 이벤트만 기록하는 수준부터 발생한 모든 이벤트를 기록하는 수준까지 로그의 기록 정도를 설정할 수 있다. 로그 수준이 너무 낮게 설정되었을 경우, 오류 또는 침해 행위로 인한 서비스 장애의 원인을 추적하지 못할 위협이 있기 때문에 로그 수준 설정의 적절성을 점검
SRV-007	○	○	○	○		5.3.2 보안 관리	취약한 버전의 SMTP 서비스 사용	5	○ 특정 SMTP 서비스 버전에서 공개된 취약점이 존재할 경우, 악의적인 사용자가 이를 활용한 공격을 수행할 위협이 있으므로 취약한 SMTP 서비스 버전의 사용 여부 점검
SRV-008	○	○	○	○		5.3.2 보안 관리	SMTP 서비스의 DoS 방지 기능 미설정	1	○ 네트워크 회선 용량 및 서버 처리 용량 초과로 인한 메일 서비스 거부 및 시스템 다운을 방지하기 위한 보안설정의 적정성을 점검
SRV-009	○	○	○	○		5.3.2 보안 관리	SMTP 서비스 스팸 메일 릴레이 제한 미설정	4	○ SMTP 서비스는 인터넷에서 메일을 전송하는 프로토콜로, 다른 메일 서버가 보낸 메일을 다시 발송하는 relay 기능을 제공하는데 해당 기능은 공격자가 정당한 인증 과정 없이 다량의 메일(스팸 메일 등) 발송을 할 위협이 존재하므로 이에 대한 설정을 점검
SRV-010	○	○	○	○		5.3.2 보안 관리	7SMTP 서비스의 메일 queue 처리 권한 설정 미흡	4	○ SMTP 서비스 운영 시 메일 queue 처리 기능이 임의의 사용자에게 허용되어 있을 경우, 비인가자가 악의적으로 queue의 데이터를 삭제하는 등의 공격 발생 위협이 존재하므로 적절한 보안 설정이 되어있는지 점검
SRV-011	○	○	○	○		5.3.2 보안 관리	시스템 관리자 계정의 FTP 사용 제한 미비	3	○ FTP 서비스는 단독으로 사용 시 네트워크에서 계정과 패스워드가 암호화 되지 않으므로, 중요한 시스템 관리자 계정들을 보호하기 위해 해당 계정들의 FTP 접속을 ftpusers 파일을 활용하여 제한하고 있는지 점검
SRV-012	○	○	○	○		5.3.2 보안 관리	.netrc 파일 내 중요 정보 노출	4	○ .netrc 파일은 ftp 나 rexec 사용 시 자동 로그인을 위한 계정과 패스워드를 저장할 수 있는 파일로 계정 정보를 평문으로 저장하는 취약한 설정이므로, 해당 설정 파일이 존재하는지 점검

평가 항목ID	A	B	C	D	E	통제 구분	평가항목	위험도	상세설명
SRV-013	○	○	○	○	○	5.3.2 보안 관리	FTP 서비스의 Anonymous 인증 허용	5	○ FTP 서비스는 파일을 전송하기 위한 프로토콜을 기반으로 하는 서비스로, 임의의 사용자가 FTP 서비스를 이용할 수 있는 익명(Anonymous) FTP 기능이 활성화된 경우 악의적인 사용자도 손쉽게 접근이 가능하므로 해당 기능의 허용 여부를 점검
SRV-014	○	○	○	○		5.3.2 보안 관리	NFS 접근 통제 미비	5	○ NFS 서비스는 원격지의 시스템에 위치한 파일을 공유할 수 있는 서비스로 잘못된 설정에 의해 원치 않는 파일 또는 디렉터리 등이 외부에 노출되고 있는지 여부를 점검
SRV-015	○	○	○	○		5.3.2 보안 관리	불필요한 NFS 서비스 실행	4	○ NFS 서비스는 원격지의 시스템에 위치한 파일을 공유할 수 있는 서비스로 해당 서비스가 업무와 관계없이 불필요하게 실행되고 있는지 여부를 점검
SRV-016	○	○	○	○		5.3.2 보안 관리	불필요한 RPC서비스 활성화	4	○ RPC(Remote Procedure Call) 서비스는 손쉬운 분산 처리 환경을 제공하지만, 오래된 버전의 특정 서비스들은 알려진 취약점이 존재하거나 잠재적인 취약점 발견 가능성이 있으므로 해당 서비스가 업무와 관계없이 불필요하게 활성화 되어 있는지 점검
SRV-018					○	5.3.2 보안 관리	하드디스크 기본 공유 활성화	4	○ Windows는 프로그램 및 서비스를 네트워크나 컴퓨터 환경에서 관리하기 위해 시스템 기본 공유 항목을 자동으로 생성하며, 이러한 공유 기능을 이용하여 비인가자가 불법적으로 모든 시스템 자원에 접근할 수 있는 위협이 있으므로 해당 서비스가 업무에 관계없이 활성화 되어 있는지 점검
SRV-020					○	5.3.2 보안 관리	공유에 대한 접근 통제 미비	5	○ Windows의 공유 기능은 폴더, 디스크 드라이브, 프린터 등을 공유하여 다른 사용자들과 함께 사용 가능하며 접근통제가 미흡한 공유는 비인가 접근 위협이 존재하므로, 사용자 권한 및 사용자 그룹 설정 등 보안 설정의 적절성을 점검
SRV-021					○	5.3.2 보안 관리	FTP 서비스 접근 제어 설정 미비	5	○ FTP는 파일을 전송하기 위한 프로토콜로 계정과 패스워드를 암호화하지 않고 평문 전송을 하며, 적절한 접근통제 정책 미적용 시 비인가자에게 시스템 파일이 노출될 수 있으므로 FTP 접근 제어 설정의 적절성 여부를 점검

평가 항목ID	A	B	C	D	E	통제 구분	평가항목	위험도	상세설명
SRV-022	○	○	○	○	○	5.3.2 보안 관리	계정의 비밀번호 미설정, 빈 암호 사용 관리 미흡	3	○ 시스템 접속 계정에 대한 비밀번호가 설정되어 있지 않은 경우 비인가자가 계정을 도용하여 인가되지 않은 파일 및 서비스에 접근할 수 있는 위협이 존재하므로, 계정에 비밀번호가 설정되어 있지 않거나 빈 비밀번호를 설정하였는지를 점검
SRV-023					○	5.3.2 보안 관리	원격 터미널 서비스의 암호화 수준 설정 미흡	3	○ 원격 터미널 서비스는 원격지에 있는 서버를 관리하기 위한 유용한 도구이지만 원격 터미널 서비스의 암호화 수준이 낮을 경우, 계정 탈취 위협이 증가하므로 해당 설정의 적절성을 점검
SRV-024					○	5.3.2 보안 관리	취약한 Telnet 인증 방식 사용	3	○ Telnet 서비스는 평문으로 데이터를 송수신하므로 패스워드 방식으로 인증을 수행할 경우 계정 및 패스워드가 노출될 위험성이 존재함. 네트워크상으로 패스워드를 전송하지 않는 NTLM 인증 설정을 적용하고 있는지 점검
SRV-025	○	○	○	○		5.3.2 보안 관리	취약한 hosts.equiv 또는 .rhosts 설정 존재	5	○ hosts.equiv, .rhosts 파일 내에 등록된 시스템이나 사용자는 시스템 접근 시 인증 절차 없이 r 계열 명령어(rexec, rlogin등)를 사용이 가능함. 특히 hosts.equiv, .rhosts 파일 내에 `+ +` 구문 존재 시 시스템 root를 제외한 모든 사용자가 인증절차 없이 r 계열 명령어를 실행할 수 있는 등 보안 수준이 낮으므로 이러한 설정이 존재하는지 점검
SRV-026	○	○	○	○		5.3.2 보안 관리	root 계정 원격 접속 제한 미비	5	○ 시스템 관리를 위한 root 계정의 원격 접속 허용은 악의적인 사용자가 무작위 대입 공격을 통해 시스템의 관리자 권한을 획득할 수 있는 위협을 증가시키므로, root 계정의 직접적인 원격 접속을 차단하고 있는지 여부를 점검
SRV-027	○	○	○	○	○	5.3.2 보안 관리	서비스 접근 IP 및 포트 제한 미비	4	○ 서비스로의 접근이 통제되지 않을 경우 악의적인 사용자의 공격 목표가 될 수 있기 때문에 보안상 접근통제가 필요함. 방화벽, 3rd-party 제품 또는 tcpwrapper를 활용하여 서비스에 대한 IP 및 포트 접근제어를 수행하고 있는지 점검
SRV-028	○	○	○	○	○	5.3.2 보안 관리	원격 터미널 접속 타임아웃 미설정	2	○ 사용자 부재시, 비인가자에 의한 시스템 무단 사용을 방지하기 위해 일정시간 사용하지 않는 세션에 대한 자동 종료시간 설정 여부를 점검하고, 세션 종료 시간이 설정되어 있을 경우 과도하게 설정 되어 있는지 점검

평가 항목ID	A	B	C	D	E	통제 구분	평가항목	위험도	상세설명
SRV-029					○	5.3.2 보안 관리	SMB 세션 중단 관리 설정 미비	3	○ SMB 세션은 서버 리소스를 소모하므로 세션 수가 많으면 서버 속도가 느려지거나 성능저하가 발생할 수 있음. 공격자가 악의적으로 SMB 세션을 반복 설정하는 등의 방법을 활용하여 SMB 서비스에 대한 서비스 거부 공격을 감행할 수 있으므로 유효한 로그온 시간이 초과된 세션이 자동으로 종료되도록 설정되었는지 점검
SRV-031					○	5.3.2 보안 관리	계정 목록 및 네트워크 공유 이름 노출	5	○ SAM(보안계정관리자) 계정과 공유의 익명 열거가 허용된 경우, 악의적인 사용자가 계정 이름 목록을 확인하고 사회공학 공격 및 기타 공격에 활용할 수 있으므로, 계정과 공유의 익명 열거를 방지하고 있는지 점검
SRV-034	○	○	○	○	○	5.3.2 보안 관리	불필요한 서비스 활성화	3	○ 시스템 운영 중 불필요한 서비스들이 설치되어 실행되고 있는 경우, 시스템의 성능 저하를 야기하거나 잠재적인 보안 취약점이 발생할 수 있으므로 업무와 관계 없이 활성화되어 있는 서비스를 점검 (취약한 버전의 automountd, NetBIOS, DMI, WebDAV, RDS 등 일반적으로 불필요한 서비스 점검)
SRV-035	○	○	○	○		5.3.2 보안 관리	취약한 서비스 활성화	5	○ 알려진 취약점이 존재하는 서비스를 실행할 경우, 공격자의 침입 경로로 활용될 수 있기 때문에 취약한 서비스나 취약한 버전의 서비스가 실행되고 있는지 점검(tftp, talk, ntalk, finger, r 계열 서비스, echo, discard, daytime, chargen, NIS, NIS+ 서비스 등)
SRV-037	○	○	○	○	○	5.3.2 보안 관리	취약한 FTP 서비스 실행	3	○ FTP는 파일을 전송하기 위한 프로토콜로 계정과 패스워드를 암호화하지 않고 평문 전송을 하여 네트워크 스니핑의 위협이 존재하므로, 해당 서비스가 업무와 관계없이 불필요하게 실행되고 있는지 점검
SRV-040	○	○	○	○	○	5.3.2 보안 관리	웹 서비스 디렉터리 리스팅 방지 설정 미흡	5	○ 디렉터리 리스팅은 디렉터리에 대한 요청 시 그 디렉터리에 기본 문서가 존재하지 않을 경우 디렉터리 내에 존재하는 모든 파일들의 목록을 출력함. 해당 기능이 활성화 되어 있는 경우 백업 파일이나 소스 파일 등 중요 파일이 외부에 노출될 수 있으므로 해당 기능의 활성화 여부를 점검

평가 항목ID	A	B	C	D	E	통제 구분	평가항목	위험도	상세설명
SRV-041					○	5.3.2 보안 관리	웹 서비스의 CGI 스크립트 관리 미흡	5	○ CGI(Common Gateway Interface)는 동적 컨텐츠를 생성하기 위해 호출하는 처리 프로그램과 통신하기 위해 정의된 인터페이스 명세이다. CGI 도입 초기에 취약점이 있는 스크립트들이 존재하였으므로 취약 스크립트가 있는지 확인하고, 악성 CGI 스크립트의 비인가 생성을 방지하기 위해 CGI 디렉터리의 권한이 적절하게 설정되어 있는지 여부를 점검
SRV-042	○	○	○	○	○	5.3.2 보안 관리	웹 서비스 상위 디렉터리 접근 제한 설정 미흡	5	○ 상위 디렉터리로 이동이 가능하면 하위경로에 접속한 후 상위로 이동하여 중요 파일들에 대한 접근이 가능한 위협이 존재하므로 ".." 와 같은 상위 경로를 사용하지 못하도록 적절하게 설정하였는지 점검
SRV-043	○	○	○	○	○	5.3.2 보안 관리	웹 서비스 경로 내 불필요한 파일 존재	4	○ 웹 서비스 설치 시 기본으로 생성되는 설명 파일 또는 테스트 페이지로 인한 불필요한 정보 노출이 발생할 수 있으므로, 불필요한 파일의 존재 여부를 점검
SRV-044	○	○	○	○	○	5.3.2 보안 관리	웹 서비스 파일 업로드 및 다운로드 용량 제한 미설정	4	○ 웹 서버에 불필요한 대량의 파일 업로드, 다운로드로 인한 서비스 거부 공격 위협이 존재하므로, 서버에 영향을 줄 정도의 대량의 업로드와 다운로드에 대한 통제 여부를 점검
SRV-045	○	○	○	○	○	5.3.2 보안 관리	웹 서비스 프로세스 권한 제한 미비	5	○ 웹 서버에 대한 요청을 처리하는 프로세스의 권한을 제한하지 않을 경우, 취약점 존재 시 공격자가 해당 서버의 높은 권한을 획득 가능한 위협이 존재함. 웹 서버 요청을 처리하는 프로세스 권한이 적절하게 설정되어 있는지 여부를 점검
SRV-046	○	○	○	○	○	5.3.2 보안 관리	웹 서비스 경로 설정 미흡	4	○ 웹 서비스 경로를 기타 업무와 영역이 분리되지 않은 경로로 설정하거나, 불필요한 경로가 존재할 경우 외부에서 시스템의 중요 파일이나 기능에 비인가 접근이 발생할 위협이 존재하므로 웹 서비스 경로 설정의 적절성을 점검
SRV-047	○	○	○	○	○	5.3.2 보안 관리	웹 서비스 경로 내 불필요한 링크 파일 존재	4	○ 웹 서버에 설정된 웹 서비스 루트 경로를 벗어나는 외부 링크 파일이 있다면, 공격자에 의한 비인가 접근 가능성이 존재하므로 불필요한 링크 파일 존재 여부를 점검

평가 항목ID	A	B	C	D	E	통제 구분	평가항목	위험도	상세설명
SRV-048	○	○	○	○	○	5.3.2 보안 관리	불필요한 웹 서비스 실행	3	○ 웹 서비스는 구동 중일 경우 잠재적인 보안 취약점이 발생할 수 있고 흔히 공격의 목표가 되는 서비스이므로, 업무와 관계 없이 불필요하게 활성화되어 있는지 여부를 점검
SRV-055					○	5.3.2 보안 관리	웹 서비스 설정 파일 노출	5	[IIS] ○ Global.asa 파일에는 데이터베이스 관련 정보(IP주소, DB명, 패스워드), 내부 IP주소, 웹 애플리케이션 환경설정 정보 및 기타 정보 등 중요 정보가 포함될 수 있으므로 해당 파일에 대한 접근통제의 적절성 여부 등을 점검 * .asa 파일을 매핑하여 Global.asa 파일이 요청되었을 때 웹 서버가 평문으로 응답하지 않도록 조치 필요
SRV-057					○	5.3.2 보안 관리	웹 서비스 경로 내 파일의 접근 통제 미흡	5	○ 웹 서비스 경로 내 파일의 접근 권한을 확인하여 비인가자에 의한 웹 서비스 파일의 실행 및 읽기 방지가 이루어지고 있는지 점검
SRV-058					○	5.3.2 보안 관리	웹 서비스의 불필요한 스크립트 매핑 존재	4	○ 웹 서비스에서 사용하지 않는 스크립트 매핑은 잠재적 보안 위협이 될 수 있으므로, 업무와 관계없는 불필요한 스크립트가 매핑되어 있는지 여부를 점검
SRV-059					○	5.3.2 보안 관리	웹 서비스 서버 명령 실행 기능 제한 설정 미흡	5	○ 웹 서버에서 임의의 명령을 실행할 수 있도록 설정되어 있는 경우, 비인가자에 의한 임의 파일 수정 및 시스템 관리자 권한 획득이 가능한 위협이 있어 이에 대한 보안설정 적절성 여부를 점검
SRV-060	○	○	○	○	○	5.3.2 보안 관리	웹 서비스 기본 계정(아이디 또는 비밀번호) 미변경	5	[Tomcat] ○ Tomcat은 Apache 웹 서버에 JSP와 자바 서블릿을 실행시킬 수 있는 기능을 제공하는 자바 애플리케이션 서버로 Tomcat이 설치될 때 기본으로 설정되는 계정을 변경하지 않을 경우 비인가자에 의한 시스템 접근이 발생할 수 있으므로 기본 계정에 대한 보안 설정의 적절성 여부를 점검
SRV-062	○	○	○	○		5.3.2 보안 관리	DNS 서비스 정보 노출	1	○ DNS 서버 종류 및 버전 등의 정보가 노출될 경우 공격자가 기타 공격에 활용할 가능성이 있으므로, 적절한 보안 설정이 되었는지 점검

평가 항목ID	A	B	C	D	E	통제 구분	평가항목	위험도	상세설명
SRV-063	○	○	○	○	○	5.3.2 보안 관리	DNS Recursive Query 설정 미흡	3	○ 공격자가 스푸핑 IP 주소(IP Spoofing)로 다량의 DNS 응답을 보내는 공격(DNS Cache Poisoning-DNS 캐시에 거짓정보가 들어가게 하는 공격) 등의 DNS 공격 위협이 존재하므로 DNS 서버가 불필요하게 Recursive Query를 지원하고 있는지 점검
SRV-064	○	○	○	○		5.3.2 보안 관리	취약한 버전의 DNS 서비스 사용	5	○ DNS 서비스 운영 시 낮은 버전을 사용하고 있을 경우 Cache Poisoning (CVE-2008-1447) 공격, 서비스 거부 공격, 버퍼 오버플로우(Buffer Overflow), DNS 원격 침입 등의 알려진 취약점이 존재하므로 주기적인 DNS 보안 패치를 통해 안전한 서비스를 운영하고 있는지에 대한 점검
SRV-066	○	○	○	○	○	5.3.2 보안 관리	DNS Zone Transfer 설정 미흡	4	○ DNS 서버에 저장되어 있는 도메인 정보의 사본을 전송하는 DNS Zone Transfer 기능이 내부 DNS 서버만 접근할 수 있도록 통제되어 있지 않다면, 임의의 공격자가 도메인 내 호스트 목록 정보를 획득하여 공격에 활용할 수 있기 때문에 해당 기능의 설정 적절성을 점검
SRV-069	○	○	○	○	○	5.3.3 사용자 인증	비밀번호 관리정책 설정 미비	5	○ 사용자 비밀번호에 대한 관리정책 설정이 미흡할 경우 유추하기 쉬운 비밀번호 설정, 주기적인 비밀번호 미변경 등 비인가자에 의한 계정 탈취 가능성이 높아지는 위협이 존재하므로 적절한 비밀번호 관리정책이 설정되어 있는지 여부를 점검
SRV-070	○	○	○	○	○	5.3.2 보안 관리	취약한 패스워드 저장 방식 사용	5	○ 취약한 패스워드 저장 방식을 사용할 경우, 공격자에게 계정의 로그인 정보가 탈취되어 악용될 위협이 존재하므로 관련 설정의 적절성 여부를 점검
SRV-072					○	5.3.3 사용자 인증	기본 관리자 계정명(Administrator) 존재	4	○ Windows는 널리 알려진 관리자 계정(Administrator)명이 디폴트로 생성되어, 공격자가 쉽게 계정명을 유추하고 탈취 시도를 할 수 있으므로 Administrator 계정의 계정명 변경 유무를 점검
SRV-073	○	○	○	○	○	5.3.2 보안 관리	관리자 그룹에 불필요한 사용자 존재	4	○ 시스템에 다수의 관리자 계정이 존재할 경우, 공격자가 탈취를 시도할 수 있는 관리자 계정이 많아지므로 관리자 그룹에 업무상 필요한 최소한의 사용자만 등록하여 사용하고 있는지 여부를 점검

평가 항목ID	A	B	C	D	E	통제 구분	평가항목	위험도	상세설명
SRV-074	○	○	○	○	○	5.3.3 사용자 인증	불필요하거나 관리되지 않는 계정 존재	4	○ 시스템 설치 시 기본으로 생성되는 계정, 업무상 더 이상 사용되지 않는 계정 등 불필요한 계정이나 장기간 비밀번호가 변경되지 않은 계정이 존재할 경우 비인가자의 계정 탈취 위협이 증가하므로 불필요한 계정 삭제 및 내부 정책에 따른 주기적인 비밀번호 변경을 실시하고 있는지 여부를 점검
SRV-075	○	○	○	○	○	5.3.3 사용자 인증	유추 가능한 계정 비밀번호 존재	5	○ 패스워드 설정 시 문자/숫자/특수문자를 모두 포함하여 강력한 패스워드가 설정될 수 있도록 암호 복잡성을 설정하여야 하며 영/숫자만으로 이루어진 암호는 현재 공개된 패스워드 크랙 유틸리티 및 무작위 공격에 의해 쉽게 유추할 수 있으므로 회사에서 정한 비밀번호 관리정책 준수 여부를 점검
SRV-078					○	5.3.3 사용자 인증	불필요한 Guest 계정 활성화	4	○ Guest 계정이 활성화 되어있을 경우 시스템에 대한 접근 권한을 보유하지 않은 사용자가 Guest 계정 권한으로 접근할 위협이 존재하므로, Guest 계정을 비활성화하여 접근 권한이 없는 사용자의 접근을 제한하고 있는지를 점검
SRV-079					○	5.3.2 보안 관리	익명 사용자에게 부적절한 권한(Everyone) 적용	5	○ 익명 사용자가 Everyone 그룹에게 접근 권한이 부여된 모든 리소스에 접근 가능한지를 결정하는 설정으로 "사용"으로 설정할 경우, 공격자가 익명의 비인가 접근으로 정보를 획득할 위협이 존재하므로 해당 정책 설정의 적절성을 점검
SRV-080					○	5.3.2 보안 관리	일반 사용자의 프린터 드라이버 설치 제한 미비	3	○ 프린터 드라이버 설치 권한이 부여된 경우 악의적인 사용자가 고의적으로 잘못된 프린터 드라이버를 설치하여 서버를 손상시킬 수도 있고, 프린터 드라이버로 위장한 악성코드를 설치할 가능성도 존재하므로 일반 사용자의 프린터 드라이버 설치를 제한하고 있는지 점검
SRV-081	○	○	○	○		5.3.2 보안 관리	Crontab 설정파일 권한 설정 미흡	4	○ cron은 특정 시간에 특정 작업을 수행할 수 있는 데몬으로 공격에 악용되거나 정보가 노출될 위협이 존재함. 이에 따라 cron 서비스를 보호하기 위해 서비스의 설정 파일들에 부여된 권한의 적절성을 점검

평가 항목ID	A	B	C	D	E	통제 구분	평가항목	위험도	상세설명
SRV-082	○	○	○	○	○	5.3.2 보안 관리	시스템 주요 디렉터리 권한 설정 미흡	4	○ 시스템 주요 디렉터리에 대한 권한 설정 미흡으로 인하여 중요 파일에 대한 접근 및 변조가 발생할 위협이 존재하므로, 시스템 주요 디렉터리에 부여된 권한의 적절성을 점검
SRV-083	○	○	○	○		5.3.2 보안 관리	시스템 스타트업 스크립트 권한 설정 미흡	3	○ 시스템 스타트업 스크립트의 소유권 및 권한 설정이 미흡할 경우, 임의의 공격자가 스크립트의 내용 변경 등을 통해 시스템 침입에 악용할 위협이 존재하므로, 해당 파일에 대한 권한 설정의 적절성을 점검
SRV-084	○	○	○	○	○	5.3.2 보안 관리	시스템 주요 파일 권한 설정 미흡	5	○ 시스템 중요 파일에 대한 권한 설정이 미흡할 경우, 중요 정보가 유출, 다른 공격에 활용, 또는 파일 자체가 변조될 위협이 존재하므로 주요 중요 파일의 권한이 일반적으로 권장되는 권한 수준으로 부여되었는지 점검
SRV-087	○	○	○	○		5.3.2 보안 관리	C 컴파일러 존재 및 권한 설정 미흡	3	○ 공격자가 시스템에 침입 후 공격 코드가 작성된 소스 파일을 컴파일하여 시스템 공격(관리자 권한 획득, 서비스 거부 유발 등)에 악용 가능하므로, 시스템에 C 컴파일러 존재 여부 및 권한 부여의 적절성을 점검
SRV-090					○	5.3.2 보안 관리	불필요한 원격 레지스트리 서비스 활성화	5	○ 원격 레지스트리 서비스는 권한 있는 사용자가 원격으로 접근하여 레지스트리 값을 변경할 수 있는 서비스로, 악의적인 사용자가 권한을 탈취한 경우 레지스트리 값 변경을 통한 침해 행위가 발생할 수 있으므로 불필요한 경우 서비스를 비활성화하고 있는지 점검
SRV-091	○	○	○	○		5.3.2 보안 관리	불필요하게 SUID, SGID bit가 설정된 파일 존재	4	○ SUID(Set User-ID)와 SGID(Set Group-ID)가 설정된 파일은 취약점이 존재할 경우, 권한 상승 공격에 활용될 수 있으므로 불필요한 SUID, SGID가 설정된 파일이 존재하는지 점검
SRV-092	○	○	○	○	○	5.3.2 보안 관리	사용자 홈 디렉터리 설정 미흡	4	○ 사용자 계정별 홈 디렉터리 경로 및 권한이 올바로 설정되지 않을 경우, 비인가 접근이 발생할 가능성이 존재하므로 사용자별 홈 디렉터리 경로 및 접근 권한의 적절성을 점검
SRV-093	○	○	○	○		5.3.2 보안 관리	불필요한 world writable 파일 존재	4	○ World Writable 파일 또는 디렉터리가 존재할 경우 이를 임의의 사용자가 변경하여 추가적인 공격에 활용할 위협이 존재하므로, 모든 사용자가 변경할 수 있는 불필요한 World Writable 파일 및 디렉터리 권한이 존재하는지 점검

평가 항목ID	A	B	C	D	E	통제 구분	평가항목	위험도	상세설명
SRV-094	○	○	○	○		5.3.2 보안 관리	Crontab 참조파일 권한 설정 미흡	4	○ Crontab에 정의된 작업에서 실행 또는 참조하는 파일에 others 쓰기 권한이 있는 경우, 파일 내용을 수정하여 악의적인 작업의 수행이 가능하므로 해당 파일 권한의 적절성을 점검
SRV-095	○	○	○	○		5.3.2 보안 관리	존재하지 않는 소유자 및 그룹 권한을 가진 파일 또는 디렉터리 존재	4	○ 사용하지 않는 디렉터리나 파일의 존재는 시스템 자원의 낭비 및 관리의 부재가 발생할 수 있으므로, 불필요한 계정이 삭제된 이후 해당 계정이 생성한 디렉터리 및 파일 등이 서버에 불필요하게 남아있는지 점검
SRV-096	○	○	○	○		5.3.2 보안 관리	사용자 환경파일의 소유자 또는 권한 설정 미흡	4	○ 사용자 shell 환경 파일에 others 권한이 부여되어 있으면 사용자 정보가 유출되거나 다른 공격에 활용될 수 있으므로, 관련 파일에 대한 권한 설정의 적절성을 점검
SRV-097					○	5.3.2 보안 관리	FTP 서비스 디렉터리 접근권한 설정 미흡	4	○ FTP 홈 디렉터리에 Everyone 그룹 접근 허용과 같이 불필요한 권한이 부여되어있는 경우 비인가 접근 위협이 존재하기 때문에, FTP 홈 디렉터리의 접근 권한 설정 적절성을 점검
SRV-101					○	5.3.2 보안 관리	불필요한 예약된 작업 존재	3	○ 미리 설정해둔 프로그램을 실행할 수 있는 예약 작업은 시작프로그램과 더불어 공격자가 악성코드 설치 등에 자주 활용하는 경로이므로 예약 작업 목록에 의심스러운 작업이 존재하는지 점검
SRV-103					○	5.3.2 보안 관리	LAN Manager 인증 수준 미흡	3	○ Lan Manager 인증 수준 설정을 통해 네트워크 로그온에 사용할 Challenge/Response 인증 프로토콜의 보안 강도를 설정할 수 있음. 이 설정은 클라이언트가 사용하는 인증 프로토콜 수준, 협상된 세션 보안 수준, 서버가 사용하는 인증 수준에 영향을 주기 때문에 보다 안전한 인증을 위한 NTLMv2 사용 설정 여부를 점검
SRV-104					○	5.3.2 보안 관리	보안 채널 데이터 디지털 암호화 또는 서명 기능 비활성화	3	○ 보안 채널 데이터 디지털 암호화 또는, 서명 설정을 통해 도메인 구성원이 시작한 모든 보안 채널 트래픽의 서명과 암호화 여부를 설정함. 인증 트래픽 끼어들기 공격, 재전송 공격 및 기타 유형의 네트워크 공격으로부터 보호하기 위해 Windows는 NetLogon 보안 통신 채널을 만들어 컴퓨터 및 사용자 계정 인증을 함. 이 정책을 활성화하면 모든 보안 채널의 서명 또는, 암호화가 협상되지 않는 한 보안 채널이 생성되지 않으며, 비활성화할 경우 모든 보안 채널 트래픽의 암호화 및 서명이 가능할 경우에만 수행하기 때문에 적절한 보안 설정이 되어 있는지 점검

평가 항목ID	A	B	C	D	E	통제 구분	평가항목	위험도	상세설명
SRV-105					○	5.3.2 보안 관리	불필요한 시작프로그램 존재	3	○ 시작프로그램 목록에 공격자가 악의적으로 설치한 악성 프로그램이나 공격 도구 등이 포함되어 시스템에 피해를 줄 수 있으므로, 시작프로그램 목록을 수시로 검사하여 불필요하거나 의심스러운 프로그램이 존재하는지 점검
SRV-108	○	○	○	○	○	5.3.2 보안 관리	로그에 대한 접근통제 및 관리 미흡	3	○ 로그에 대한 접근통제가 미흡할 경우, 비인가자가 로그에서 정보를 획득하거나 로그 자체를 변조할 수 있는 위협이 존재하므로, 로그에 대한 접근 권한의 적절성을 점검
SRV-109	○	○	○	○	○	5.3.2 보안 관리	시스템 주요 이벤트 로그 설정 미흡	3	○ 시스템 문제 발생 시 원활한 원인 파악/문제 해결 등을 위해서 각종 보안 로그가 저장 및 관리되어야 하며, 특히 인증 관련이나 중요 이벤트 로그가 남도록 설정되었는지 점검
SRV-112				○		5.3.2 보안 관리	Cron 서비스 로깅 미설정	2	○ Cron 서비스 실행에 대한 로깅 미설정 시 비인가자에 의한 시스템 행위를 추적할 수 없으므로 적절한 로깅 설정이 되어있는지 점검
SRV-115	○	○	○	○	○	5.3.2 보안 관리	로그의 정기적 검토 및 보고 미수행	4	○ 각종 공격이나 시스템 오류에 대해 원활히 추적이 가능하려면, 로그에 대한 관리와 분석이 중요하므로 정기적으로 로그에 대한 검토 및 보고가 이루어지고 있는지 점검
SRV-116					○	5.3.2 보안 관리	“보안 감사를 수행할 수 없는 경우, 즉시 시스템 종료” 기능 설정 미흡	5	○ 보안 감사 로그 불가 시 시스템 종료가 설정되어 있으면 보안 감사 로그가 가득차거나 기타 에러 등의 이유로 로그를 기록하지 못할 경우 시스템이 재부팅되어 서비스 가용성의 문제가 발생할 수 있으므로 적절한 보안설정을 적용하여 운영하고 있는지 점검
SRV-118	○	○	○	○	○	5.3.4 패치 관리	주기적인 보안패치 및 벤더 권고사항 미적용	5	○ 공개된 취약점에 의한 침해를 방지하고, 시스템에 대한 안전성 향상을 위해 최신/긴급 패치에 대한 검토, 계획 수립, 계획에 따른 이행(또는 보호방안 수립) 여부 등을 점검
SRV-119					○	5.3.4 패치 관리	백신 프로그램 업데이트 미흡	5	○ 지속적으로 기존에 없던 신종 악성코드가 개발 및 배포되는 위협이 존재하므로, 악성코드 정보에 대한 주기적인 업데이트가 적절하게 이루어지고 있는지 점검

평가 항목ID	A	B	C	D	E	통제 구분	평가항목	위험도	상세설명
SRV-121	○	○	○	○		5.3.2 보안 관리	root 계정의 PATH 환경변수 설정 미흡	5	○ 사용자가 특정 명령어를 실행할 때 PATH에 지정된 디렉터리를 검색하여 해당 명령어를 찾기 때문에, 관리자의 PATH 환경변수에 현재 디렉터리 또는 알 수 없는 디렉터리가 포함되지 않았는지 점검이 필요함. PATH에 현재 디렉터리 또는 임의의 디렉터리가 포함되어 있고 실행할 명령(예 : ls, cd 등)과 동일한 이름을 가진 악성 프로그램이 해당 디렉터리에 숨겨져 있다면 실행시키고자 했던 원래의 프로그램 대신 악성 프로그램이 실행되어 시스템이 침해 당할 수 있는 위협이 존재하므로, 시스템의 PATH 설정이 적절한지 점검
SRV-122	○	○	○	○		5.3.2 보안 관리	UMASK 설정 미흡	3	○ umask 값은 신규 파일이나 디렉터리 생성 시 기본으로 설정되는 권한을 결정하는 값으로, umask 설정에 따라 특정 사용자가 새로운 파일 또는 디렉터리를 생성했을 때 다른 사용자에게 의도치 않은 접근 권한이 부여될 가능성이 존재하므로 적절한 umask 값이 설정되었는지 점검
SRV-123					○	5.3.2 보안 관리	최종 로그인 사용자 계정 노출	3	○ 최종 로그인한 사용자 계정이 로그온 창에 표시되도록 설정된 경우, 해당 계정명의 계정이 존재한다는 정보가 노출될 수 있고, 이후 추가적인 계정 탈취 시도가 발생할 수 있기 때문에 해당 설정이 적절하게 설정 되었는지 점검
SRV-125					○	5.3.2 보안 관리	화면보호기 미설정	4	○ 화면 보호기 설정이 되어 있지 않으면, 관리자가 자리를 비운 사이 임의의 사용자가 서버에 접근할 수 있는 위협이 존재하므로 적절하게 화면보호기를 설정하였는지 점검
SRV-126					○	5.3.3 사용자 인증	자동 로그온 방지 설정 미흡	4	○ 자동 로그온은 시스템 시작 시 미리 설정되어 있는 사용자로 자동으로 로그온 하도록 하는 기능으로 관리자 권한으로 자동 로그온 설정이 되어있는 경우, 임의의 사용자가 관리자 권한 획득이 가능한 위협이 존재하므로 불필요한 자동 로그온 설정이 존재하는지 점검
SRV-127	○	○	○	○	○	5.3.3 사용자 인증	계정 잠금 임계값 설정 미비	4	○ 계정 비밀번호에 대한 무작위 대입 공격으로 비인가자가 계정 정보를 탈취할 위협이 존재하므로 로그인 입력 횟수 제한 등의 임계값 설정 여부를 점검
SRV-128					○	5.3.2 보안 관리	NTFS 파일 시스템 미사용	3	○ FAT 파일 시스템은 NTFS 파일 시스템에 비하여 지원되는 보안 기능이 제한되어 접근 통제의 어려움이 존재하므로 보다 강화된 보안 기능을 지원하는 NTFS 파일시스템 사용 여부를 점검

평가 항목ID	A	B	C	D	E	통제 구분	평가항목	위험도	상세설명
SRV-129					○	5.3.2 보안 관리	백신 프로그램 미설치	5	○ 악성코드 감염 시 정보 유출/삭제 등 뿐만 아니라 악성코드 확산 등의 위험성이 있으므로, 악성코드 감염 대비 및 치료 수행을 위한 백신 프로그램의 설치 여부를 점검
SRV-131	○	○	○	○		5.3.2 보안 관리	SU 명령 사용가능 그룹 제한 미비	3	○ su(set user or superuser or switch user) 명령은 로그아웃 하지 않고 다른 사용자로 전환할 수 있게 해주는 명령으로, 관리자 비밀번호를 알고 있을 때 이 명령을 통해 관리자 권한을 획득(관리자로 전환) 가능하므로 su 명령을 사용할 수 있는 그룹을 설정하여 해당 그룹에 속한 사용자에게만 명령을 허용하고 있는지 여부를 점검
SRV-133	○	○	○	○		5.3.2 보안 관리	Cron 서비스 사용 계정 제한 미비	3	○ cron은 특정 시간에 특정 작업을 수행할 수 있는 데몬으로 공격에 악용되거나 정보가 노출될 위협이 존재함. 이에 따라 cron 서비스를 이용할 수 있는 계정을 정의하는 방식 등의 접근 통제를 수행하고 있는지 점검
SRV-134				○		5.3.2 보안 관리	스택 영역 실행 방지 미설정	2	○ 스택 영역에서의 실행이 가능한 경우, "stack smashing" 등의 버퍼 오버플로우 공격에 취약하므로, 스택 영역 실행 기능에 대한 보안설정의 적절성을 점검
SRV-135				○	○	5.3.2 보안 관리	TCP 보안 설정 미비	2	○ 하이재킹 공격이나 IP Spoofing, DoS 와 같은 네트워크 공격 위협을 감소시키기 위해, TCP 연결의 보안을 강화하는 설정이 활성화되어 있는지 점검
SRV-136					○	5.3.2 보안 관리	시스템 종료 권한 설정 미흡	5	○ 로그온 단계에서 "시스템 종료" 가 허용될 경우, 로그온을 하지 않더라도 시스템 종료가 가능하여 비인가 서버 종료 위협 등이 존재하므로 로그온 단계에서의 시스템 종료 기능 비활성화 여부를 점검
SRV-137					○	5.3.2 보안 관리	네트워크 서비스의 접근 제한 설정 미흡	3	○ 네트워크에서 이 컴퓨터 액세스 정책은 다수의 네트워크 프로토콜(SMB 기반 프로토콜, NetBIOS, CIFS(Common Internet File System) 및 COM+ 등) 접근에 필요한 정책으로 해당 권한 설정이 미흡할 경우, 임의의 사용자 또는 그룹이 네트워크 서비스로 접근이 가능하여 시스템 침해 위협이 증가하므로 접근 권한 설정의 적절성을 점검

평가 항목ID	A	B	C	D	E	통제 구분	평가항목	위험도	상세설명
SRV-138					○	5.3.2 보안 관리	백업 및 복구 권한 설정 미흡	2	○ 백업 및 복구 권한은 해당 권한을 활용하여 실제 객체에 대해 필요한 접근 권한을 우회하여 정보를 획득하거나 시스템 무결성을 침해할 위협이 존재하므로, 불필요한 사용자 및 그룹에게 부여된 권한이 존재하는지 점검
SRV-139					○	5.3.2 보안 관리	시스템 자원 소유권 변경 권한 설정 미흡	3	○ 시스템 자원(Active Directory 개체, 프린터, 레지스트리 키, 서비스 등)은 서비스 운영에 영향을 주기 때문에 관리자 또는 관리자 그룹이 아닌, 일반 사용자가 권한을 보유하면 데이터 및 자원 보호 정책 설정 등의 인가되지 않은 변경이 발생할 위협이 존재하므로 해당 정책의 설정 적절성을 점검
SRV-140					○	5.3.2 보안 관리	이동식 미디어 포맷 및 꺼내기 허용 정책 설정 미흡	4	○ 이동식 미디어(USB 등) 포맷 및 꺼내기 허용 권한이 불필요한 사용자에게 권한이 주어질 경우 비인가 데이터 복사/삭제 등의 행위가 발생할 위협이 증가하므로 해당 보안 정책의 설정 적절성을 점검
SRV-142	○	○	○	○		5.3.2 보안 관리	중복 UID가 부여된 계정 존재	4	○ 시스템에 중복 UID가 존재하는 경우, 접근통제와 감사 추적의 어려움이 발생할 수 있으므로, 동일한 UID가 부여된 계정의 존재 여부를 점검
SRV-144	○	○	○	○		5.3.2 보안 관리	/dev 경로에 불필요한 파일 존재	4	○ 디바이스가 존재하지 않거나 이름이 잘못 입력된 경우 시스템은 /dev 디렉터리에 계속해서 파일이 생성되거나, 에러가 발생할 가능성이 존재함. 또한 /dev 디렉터리는 악의적인 공격자가 rootkit을 숨기는 경로로 사용되는 경우도 있음. 따라서 파일 시스템 손상 및 장애 등의 문제를 방지하기 위해 실제 존재하지 않는 디바이스 파일이 해당 경로에 있는지 점검
SRV-147	○	○	○	○	○	5.3.2 보안 관리	불필요한 SNMP 서비스 실행	3	○ SNMP(Simple Network Management Protocol)서비스는 시스템을 모니터링 하기 위한 프로토콜로써, 불필요하게 운영할 경우 정보노출 위협이 존재하므로 불필요한 SNMP서비스가 구동 중인지에 대한 점검
SRV-148	○	○	○	○	○	5.3.2 보안 관리	웹 서비스 정보 노출	3	○ 웹 서버 종류 및 버전 등에 대한 정보가 노출될 경우 공격자가 기타 공격에 활용할 가능성이 있으므로 적절한 보안 설정이 되었는지 점검
SRV-149					○	5.3.2 보안 관리	디스크 볼륨 암호화 미적용	4	○ 디스크 볼륨이 암호화 되어 있지 않는 경우, 비인가자가 데이터에 물리적으로 직접 접근하여 데이터를 획득할 위협이 존재하므로 암호화 여부를 점검

평가 항목ID	A	B	C	D	E	통제 구분	평가항목	위험도	상세설명
SRV-150					○	5.3.3 사용자 인증	로컬 로그온 허용	3	○ 로컬 로그온이 불필요한 계정의 로컬 로그온이 허용된 경우 해당 계정이 탈취되었을 때 추가적인 침해 행위를 수행하는 등 피해가 커질 가능성이 존재하기 때문에, 불필요하게 로컬 로그온이 허용된 계정이 존재하는지 점검
SRV-151					○	5.3.2 보안 관리	익명 SID/이름 변환 허용	3	○ 익명 SID/이름 반환 허용 정책 설정 시 잘 알려진 Administrator SID를 요청하여 해당 계정의 실제 이름을 알아낼 수 있으며 암호 추측 공격을 통해 계정 권한을 획득할 위협이 존재하므로 해당 정책의 활성화 여부를 점검
SRV-152					○	5.3.2 보안 관리	원격터미널 접속 가능한 사용자 그룹 제한 미비	3	○ 원격 서비스는 서버 관리를 위한 서비스로 접근 가능한 그룹이나 계정을 제한하지 않을 경우 임의의 사용자가 서버에 접근하여 정보 변경, 유출 등이 발생할 위협이 있으므로 해당 설정을 점검
SRV-158	○	○	○	○	○	5.3.2 보안 관리	불필요한 Telnet 서비스 실행	3	○ Telnet 서비스는 Password 인증 방식 사용 시 데이터를 평문으로 송수신하기 때문에 인증 시 아이디/패스워드가 노출될 수 있는 위협이 존재하므로 가급적 사용하지 않는 것이 바람직하여, 업무와 관계없이 불필요하게 활성화되어 있는지 점검
SRV-161	○	○	○	○		5.3.2 보안 관리	ftpusers 파일의 소유자 및 권한 설정 미흡	3	○ ftpusers 파일에서 FTP 서비스에 접근 가능한 사용자 계정을 관리할 수 있으므로, 해당 파일에 대한 권한 설정의 적절성을 점검
SRV-163	○	○	○	○	○	5.3.2 보안 관리	시스템 사용 주의사항 미출력	1	○ 비인가자의 부적절한 로그인 권한 획득을 사전에 방지하기 위하여 로그인 시 경고 및 시스템 사용 주의사항 등의 문구를 표시하고 있는지 점검
SRV-164	○	○	○	○		5.3.2 보안 관리	구성원이 존재하지 않는 GID 존재	2	○ 계정이 존재하지 않는 그룹 권한(GID)이 존재할 경우, 해당 그룹이 소유한 파일이 비인가자에게 노출될 위협이 존재하므로 소속된 계정이 없는 GID가 존재하는지 점검

평가 항목ID	A	B	C	D	E	통제 구분	평가항목	위험도	상세설명
SRV-165	○	○	○	○		5.3.2 보안 관리	불필요하게 Shell이 부여된 계정 존재	1	○ 로그인이 불필요한 계정들에 /bin/false 등을 부여하여 계정 탈취 시의 피해를 감소시키기 위한 설정을 적용하고 있는지 여부를 점검
SRV-166	○	○	○	○		5.3.2 보안 관리	불필요한 숨김 파일 또는 디렉터리 존재	1	○ 악의적인 목적으로 생성한 파일 혹은 디렉터리를 숨김파일로 저장하는 경우가 많으므로, 숨김 파일 및 디렉터리 중 침해 행위로 인해 생성된 파일이 존재하는지 점검
SRV-170					○	5.3.2 보안 관리	SMTP 서비스 정보 노출	1	○ SMTP 접속 시 노출되는 배너에서 공격자가 유용한 정보를 획득할 가능성이 존재하므로, 불필요하게 노출되는 정보 유무를 점검
SRV-171					○	5.3.2 보안 관리	FTP 서비스 정보 노출	1	○ FTP 접속 시 노출되는 배너에서 공격자가 유용한 정보 획득할 가능성이 존재하므로, 불필요하게 노출되는 정보 존재 유무를 점검
SRV-172					○	5.3.2 보안 관리	불필요한 시스템 자원 공유 존재	3	○ Windows의 공유 기능은 폴더, 디스크 드라이브, 프린터 등을 공유하여 다른 사용자들과 함께 사용이 가능한 서비스이지만, 불필요한 공유의 활성화는 여러가지 공격의 목표가 될 가능성이 존재하므로, 불필요한 공유의 존재 여부를 점검
SRV-173					○	5.3.2 보안 관리	DNS 서비스의 취약한 동적 업데이트 설정	3	○ DNS(Domain Name Service) 서비스의 동적 업데이트 기능이 불필요하게 활성화되어 있고 신뢰할 수 있는 출처 이외에도 업데이트가 가능한 경우, 악의적인 사용자에 의해 DNS 레코드가 변조될 위협이 존재하므로, 해당 기능의 설정 적절성을 점검
SRV-174	○	○	○	○	○	5.3.2 보안 관리	불필요한 DNS 서비스 실행	3	○ DNS(Domain Name Service)는 도메인 이름과 IP간의 변환을 위한 서비스로, 불필요하게 운영할 경우 잠재적인 보안 취약점으로 인한 공격의 경로가 될 수 있으므로 해당 서비스가 업무와 관계없이 활성화되어 있는지 여부를 점검

【데이터베이스】

■ **평가대상**

A	B	C	D	E	F
ORACLE 계열	MSSQL 계열	MYSQL 계열	PostgreSQL 계열	MariaDB 계열	Tibero 계열

■ 평가기준

평가 항목ID	A	B	C	D	E	F	통제 구분	평가항목	위험도	상세설명
DBM-001	○	○	○	○	○	○	5.3.3 사용자 인증	취약하게 설정된 비밀번호 존재	4	○ 계정의 비밀번호가 취약하게 설정된 경우, 비인가자가 비밀번호를 유추하거나 무작위 대입 공격을 통해 계정을 탈취하여 데이터베이스에 접근할 수 있는 위협이 존재하므로 취약하게 설정된 비밀번호가 있는지 여부를 점검
DBM-003	○	○	○	○	○	○	5.3.3 사용자 인증	업무상 불필요한 계정 존재	4	○ 업무상 사용되지 않는 계정 등 불필요한 계정이 존재할 경우, 비인가자가 해당 계정 탈취를 통해 데이터베이스에 접근할 수 있는 위협이 존재하므로 불필요한 계정이 존재하는지 여부를 점검
DBM-004	○	○	○	○	○	○	5.3.2 보안 관리	업무상 불필요하게 관리자 권한이 부여된 계정 존재	5	○ 관리자 권한이 업무상 불필요하게 부여된 계정이 존재할 경우, 해당 계정을 통해 비인가자가 관리자 권한을 도용할 수 있는 위협이 존재하므로 업무상 불필요하게 관리자 권한이 부여된 계정이 존재하는지 여부를 점검
DBM-005	○	○	○	○	○	○	5.3.2 보안 관리	데이터베이스 내 중요정보 암호화 미적용	5	○ 데이터베이스 내에 주민등록번호, 비밀번호 등 중요 정보가 암호화되지 않은 평문 형태로 저장되어 있는 경우, 중요 정보가 외부로 유출될 수 있는 위협이 존재하므로 중요 정보를 암호화하여 보관하고 있는지 여부를 점검

평가 항목ID	A	B	C	D	E	F	통제 구분	평가항목	위험도	상세설명
DBM-006	○	○	○	○	○	○	5.3.3 사용자 인증	로그인 실패 횟수에 따른 접속 제한 설정 미흡	3	○ 계정의 로그인 시도에 대한 제한이 없는 경우, 비인가자가 비밀번호의 무작위 대입 공격을 통해 계정을 탈취하여 데이터베이스에 접근할 수 있는 위협이 존재하므로 계정의 로그인 실패 횟수에 따라 일시 또는 영구적으로 접속을 제한하고 있는지 여부를 점검
DBM-007	○	○	○	○	○	○	5.3.3 사용자 인증	비밀번호의 복잡도 정책 설정 미흡	5	○ 비밀번호의 복잡도 설정이 미흡한 경우, 비인가자가 비밀번호를 유추하거나 무작위 대입 공격을 통해 계정을 탈취하여 데이터베이스에 접근할 수 있는 위협이 존재하므로 비밀번호 설정 시 복잡도 정책이 적절하게 설정되어 있는지 여부를 점검
DBM-008	○	○	○	○	○	○	5.3.3 사용자 인증	주기적인 비밀번호 변경 미흡	4	○ 장기간 비밀번호가 변경되지 않은 계정이 존재할 경우, 비인가자에 의해 계정의 비밀번호가 탈취될 수 있는 위협이 증가하므로 회사 내부 정책에 따라 주기적으로 비밀번호 변경을 실시하고 있는지 여부를 점검
DBM-009	○	○	○	○	○	○	5.3.2 보안 관리	사용되지 않는 세션 종료 미흡	3	○ 사용되지 않는 불필요한 세션이 관리되지 않을 경우, 세션 도용을 통한 비인가 접근, 다수의 세션 생성을 통한 서비스 장애 등의 위협이 존재함에 따라, 자동 세션종료 설정을 통해 사용되지 않는 세션 종료 여부를 점검
DBM-011	○	○	○	○	○	○	5.3.2 보안 관리	감사 로그 수집 및 백업 미흡	5	○ 데이터베이스에서 수행한 주요 행위를 기록 및 백업하지 않는 경우, 장애 및 침해사고 발생 시 이를 효과적으로 대처할 수 없으므로 로그 수집 및 백업이 적절하게 이루어지고 있는지 점검
DBM-012	○						5.3.2 보안 관리	Listener Control Utility(lsnrnctl) 보안 설정 미흡	5	○ Listener Control Utility(lsnrnctl) 보안 설정이 미흡한 경우, 비인가자가 TNS(Trasnparent Network Substrate) Listener 에 접근하여 서비스를 중지하는 등의 위협이 존재하므로 Listener Control Utility(lsnrnctl)의 보안 설정 여부를 점검
DBM-013	○	○	○	○	○	○	5.3.2 보안 관리	원격 접속에 대한 접근 제어 미흡	5	○ 업무상 불필요한 원격 접속을 허용하는 경우, 이를 통해 비인가자가 원격으로 데이터베이스에 접근할 수 있는 위협이 존재하므로 원격 접속에 대한 통제 여부를 점검

평가 항목ID	A	B	C	D	E	F	통제 구분	평가항목	위험도	상세설명
DBM-014	○						5.3.2 보안 관리	취약한 운영체제 역할 인증 기능(OS_ROLES, REMOTE_OS_ROLES) 사용	4	○ 운영체제 역할 인증 기능(OS_ROLES, REMOTE_OS_ROLES)을 사용하는 경우, 비인가된 OS 사용자 및 그룹이 데이터베이스에 접근하여 데이터베이스 역할(Role)을 제어할 수 있으므로 해당 기능이 사용중으로 설정되어 있는지 점검
DBM-015	○	○				○	5.3.2 보안 관리	Public Role에 불필요한 권한 존재	4	○ Public Role에 응용프로그램 관리 권한, DBA 권한 등이 존재할 경우, 해당 업무와 직접적인 연관이 없는 사용자에게 동일한 권한이 부여될 수 있는 위협이 존재하므로 불필요한 권한이 Public Role에 부여되어 있는지 점검
DBM-016	○	○	○	○	○	○	5.3.4 패치 관리	최신 보안패치와 벤더 권고사항 미적용	4	○ 최신 보안패치 및 벤더 권고사항을 적용하지 않은 경우, 알려진 취약점에 노출될 수 있는 위협이 존재하므로 최신 보안 패치 및 권고사항 이행 여부를 점검
DBM-017	○	○	○	○	○	○	5.3.2 보안 관리	업무상 불필요한 시스템 테이블 접근 권한 존재	5	○ 시스템 테이블에 접근할 수 있는 권한이 업무상 불필요하게 부여된 경우, 비인가자가 이를 통하여 시스템의 주요 정보를 획득하거나 주요 데이터 베이스 설정 변경할 수 있는 위협이 존재하므로 인가되지 않은 사용자에게 시스템 테이블 접근 권한이 부여되어있는지 점검
DBM-019	○	○	○	○	○	○	5.3.3 사용자 인증	비밀번호 재사용 방지 설정 미흡	3	○ 이전에 사용된 비밀번호의 재사용이 가능할 경우, 기존에 유출된 비밀번호를 이용하여 비인가자에 의해 계정이 탈취될 수 있는 위협이 증가하므로 이전에 사용된 비밀번호의 재사용 방지 설정 여부를 점검
DBM-020	○	○	○	○	○	○	5.3.3 사용자 인증	사용자별 계정 분리 미흡	3	○ 계정을 사용자별로 분리하여 사용하지 않을 경우, 침해사고시 감사 추적이 어려울 수 있으므로 계정을 사용자별로 분리하여 사용하고 있는지 여부를 점검
DBM-021		○					5.3.2 보안 관리	업무상 불필요한 ○DBC/OLE-DB 데이터 소스 및 드라이버 존재	3	○ 업무상 불필요한 ODBC, OLE-DB 데이터 소스 및 드라이버가 존재하는 경우, 이를 통해 비인가자가 데이터베이스에 접근할 가능성이 존재하므로 해당 ODBC, OLE-DB 데이터 소스 및 드라이브를 제거하였는지 여부를 점검

평가 항목ID	A	B	C	D	E	F	통제 구분	평가항목	위험도	상세설명
DBM-022	○	○	○	○	○	○	5.3.2 보안 관리	설정 파일 및 중요정보가 포함된 파일의 접근 권한 설정 미흡	3	○ 데이터베이스 주요 설정 파일 및 중요정보(데이터베이스 비밀번호, 로그 등)가 포함된 파일의 접근 권한이 적절하지 않은 경우, 비인가자가 이를 수정/삭제 할 수 있는 위협이 있으므로 해당 파일들의 접근권한이 적절한지 여부를 점검
DBM-024	○	○	○	○	○	○	5.3.2 보안 관리	불필요하게 WITH GRANT OPTION 옵션이 설정된 권한 존재	3	○ 운영상 불필요하게 WITH GRANT OPTION 이 설정된 권한이 있는 경우, 해당 권한을 가진 사용자가 다른 사용자에게 동일한 권한을 부여할 수 있으므로 불필요하게 WITH GRANT OPTION 옵션이 설정되어 있는 권한이 있는지 점검
DBM-025	○	○	○	○	○	○	5.3.4 패치 관리	서비스 지원이 종료된(EoS) 데이터베이스 사용	3	○ 서비스 지원이 종료된(EoS)버전을 사용하는 경우, 알려진 취약점 또는 신규로 발견되는 취약점으로 부터 발생하는 보안위협에 대처할 수 없는 위협이 존재하므로 서비스 지원이 종료된(EoS) 버전의 데이터베이스를 사용중인지 여부를 점검
DBM-026	○		○	○	○	○	5.3.2 보안 관리	데이터베이스 구동 계정의 umask 설정 미흡	2	○ 데이터베이스 구동 계정이 파일(로그 등) 생성 시 기본적으로 적용되는 권한이 적절하지 않은 경우, 비인가자가 데이터베이스의 주요 파일들에 접근 및 수정 가능한 위협이 존재하므로 해당 파일들이 적절한 권한을 가지고 생성하도록 설정하였는지 여부를 점검
DBM-028	○	○	○	○	○	○	5.3.2 보안 관리	업무상 불필요한 데이터베이스 Object 존재	1	○ 업무상 불필요한 데이터베이스 Object가 존재하는 경우, 비인가자가 이를 이용하여 데이터베이스에 접근할 수 있는 위협이 있으므로 업무상 불필요한 데이터베이스 Object가 존재하는지 점검
DBM-029	○						5.3.2 보안 관리	데이터베이스의 자원 사용 제한 설정 미흡	1	○ Oracle 프로파일 옵션 중 자원 사용 제한 설정(RESOURCE_LIMIT)이 활성화 되어있지 않은 경우, 비밀번호 관련 제한 설정을 제외한 프로파일 제한 옵션 값들이 동작하지 않으므로 이를 점검
DBM-030	○					○	5.3.2 보안 관리	Audit Table에 대한 접근 제어 미흡	1	○ 감사 로그가 저장되는 Audit Table에 대하여 일반 사용자의 수정/삭제 권한이 존재할 경우, 해당 계정을 이용해 비인가자가 감사 로그를 수정/삭제할 수 있는 위협이 존재하므로 Audit Table의 수정/삭제 권한을 관리자 계정으로 제한하는지 여부를 점검

평가 항목ID	A	B	C	D	E	F	통제 구분	평가항목	위험도	상세설명
DBM-031		○					5.3.2 보안 관리	SA 계정에 대한 보안설정 미흡	3	○ SA계정은 MS-SQL(SQL SERVER)에서 기본적으로 제공하는 관리자 계정으로서 비인가자에게 탈취당할 경우, 데이터베이스의 모든 권한을 탈취 당할 위협이 있으므로 해당 계정이 활성화 되어있는 경우 적절한 보안 정책이 적용되고 있는지 여부를 점검
DBM-032				○			5.3.2 보안 관리	데이터베이스 접속 시 통신구간에 비밀번호 평문 노출	3	○ 데이터베이스 접속시 통신구간에서 계정의 비밀번호가 평문으로 노출되는 경우, 네트워크 스니핑을 통해 비인가자가 계정 정보를 탈취할 수 있는 위협이 존재하므로 데이터베이스 접속시 비밀번호가 평문으로 노출되는지 여부 점검

【네트워크 인프라】

■ 평가기준

평가 항목ID	통제 구분	평가항목	위험도	상세설명
INF-001	5.5.2 보안 관리	네트워크 회선(ISP) 이중화 구성	3	○ 네트워크(ISP) 회선이 단일화 구성되어 있어 회선 장애시 서비스 장애가 발생할 우려가 있으므로 네트워크 회선(ISP)을 이중화하여 구성하고 있는지 점검
INF-002	5.5.2 보안 관리	네트워크 장비 이중화 구성	3	○ 네트워크 장비가 단일장비 구성으로 운영 중 장비 장애시 서비스 장애가 발생할 우려가 있으므로 네트워크 장비를 이중화 구성하고 있는지 점검
INF-003	5.5.2 보안 관리	정보보호시스템 이중화 구성	3	○ 정보보호시스템이 단일장비 구성으로 운영 중 장비 장애시 서비스 장애가 발생할 우려가 있으므로 정보보호시스템을 이중화 구성하고 있는지 점검
INF-004	5.5.2 보안 관리	중요 서버 이중화 구성	3	○ 서버의 단일장비 구성으로 운영 중 장비 장애시 서비스 장애가 발생할 우려가 있으므로 중요서버를 이중화 구성하고 있는지 점검
INF-005	5.5.2 보안 관리	소프트웨어 및 하드웨어 지원 서비스가 종료(EOS)된 노후장비 존재	3	○ 벤더의 소프트웨어 및 하드웨어의 지원이 종료된 경우 장비의 성능저하 및 장애, 신규 취약점 패치 등이 원할하지 않을 수 있으므로 지원이 종료(End of Service)된 노후장비가 존재하는지 점검
INF-006	5.5.2 보안 관리	재해 또는 장애발생 시 복구를 위한 별도 구간 확보 여부	3	○ 재해, 장애 등의 비상시를 대비해 재해복구센터 또는 백업센터 등의 네트워크 구간 마련 여부
INF-007	5.5.2 보안 관리	업무 특성별 네트워크 망분리 구성	5	○ 업무 특성별로 네트워크 구간이 분리되지 않을 경우 침해사고 발생 시, 전체 네트워크가 위험에 노출될 가능성이 있으므로 네트워크 구간을 업무 특성별로 적절하게 분리하고 있는지 점검

평가 항목ID	통제 구분	평가항목	위험도	상세설명
INF-008	5.5.2 보안 관리	개발/테스트와 운영 네트워크 망분리 구성	5	○ 개발 및 테스트(검증계) 서버의 경우 보안설정의 강도가 운영서버에 비해 낮게 설정될 소지가 있고, 정보보호시스템의 보호범위에서도 벗어나 있는 경우가 있으므로 동 구간을 별도로 분리하여 운영하고 있는지 점검
INF-009	5.5.2 보안 관리	사용자들의 주요 서버구간으로의 접근통제	4	○ 사용자 단말에서 주요서버구간으로 접근통제가 실시되지 않을 경우 허용되지 않은 접근 및 악성코드 등에 노출될 위험이 존재하므로 사용자 단말에서 주요 서버 접근 시 해당 사용자의 권한에 맞는 접속만 허용되도록 통제를 수행하고 있는지 점검
INF-010	5.5.2 보안 관리	분리된 각 네트워크 구간 사이에 접근통제	4	○ 업무 특성에 맞게 분리한 네트워크 구간 사이에 비인가 접근이 발생하지 않도록 최소한의 허용정책을 통해 적절한 접근통제를 수행하고 있는지 점검
INF-011	5.5.2 보안 관리	보안 정책 미적용 우회 경로 유무 여부	4	○ 분리된 네트워크 구간내 접근통제를 거치지 않는 네트워크 접점의 우회경로가 있는지 점검
INF-012	5.5.2 보안 관리	외부통신망에서 접근이 불필요한 구간에 대한 접근통제 미흡	5	○ 외부통신망에서 접근이 허용된 DMZ구간 이외에 접근통제가 적절히 수행되지 않아 외부로부터 직접 접근이 가능한 구간 또는 시스템이 있는지 점검
INF-013	5.5.2 보안 관리	내부통신망 공인IP 사용 통제	3	○ 공인IP는 외부에서 직접 접속이 가능하여 부적절한 접근을 허용할 위험이 있으므로 내부 통신망에 불필요하게 공인IP가 할당되어 있는지 점검
INF-015	5.5.2 보안 관리	내부구간에 위치한 정보시스템(서버,DB)에 대한 외부통신망 차단 여부	5	○ 내부서버에서 외부통신망에 접속이 가능한 경우 정보유출 또는 바이러스 감염 등에 대한 위험이 존재하므로 내부구간 정보시스템에서 외부로의 허용 여부 점검
INF-016	5.5.2 보안 관리	중요 단말기에서 외부통신망 및 내부통신망(그룹웨어 등)에 대한 접근통제의 적절성	5	○ 중요단말기에서 외부통신망 접속으로 인한 악성코드 감염의 위험이 있으며, 중요정보 유출 또는 파괴의 가능성이 있음

평가 항목ID	통제 구분	평가항목	위험도	상세설명
INF-017	5.5.2 보안 관리	장애 인지 및 대응 방안 수립 여부	1	○ 장애 발생시 담당자가 인지하지 못하는 경우 즉각적인 상황파악 및 대처가 어려우므로 모니터링 시스템을 통해 장애 발생에 대한 즉각적인 인지 및 대응 방안이 마련되어 있는지 점검
INF-018	5.5.2 보안 관리	네트워크 구간별 침입탐지시스템 구성의 적절성	4	○ 네트워크 구간별 침입탐지시스템이 없거나 부적절한 위치에 설치되어 있을 경우 침입시도 및 비정상 트래픽 탐지가 불가능하므로 탐지예외 구간이 있는지 점검
INF-019	5.5.2 보안 관리	외부통신망과 통신을 하는 서버(웹 서버 등)의 DMZ 구성의 적절성	3	○ DMZ구간에 위치해야할 공개용 서버가 내부구간에 위치할 경우 해당 구간 및 전체 구간에 대한 침해가 발생할 수 있으므로 공개용 서버 내부구간 존재여부 점검
INF-020	5.5.2 보안 관리	네트워크 관리시스템의 작업내역, 로그관리 및 사용자권한 설정에 대한 보안설정의 적절성	3	○ 네트워크 관리시스템의 권한 설정이 제대로 되어 있지 않아 중요정보가 비인가자에게 노출될 위험이 있으며, 작업이력 및 로그관리가 제대로 이루어지지 않아 장애발생시 원인 파악이 어려울 수 있음

【네트워크 장비】

■ **평가대상**

A	B	C	D
CISCO 계열	A10 계열	BROCADE, ALTEON, NOTEL, BIGIP, CITRIX, PIOLINK 계열	3COM, JUNIPER 계열

■ 평가기준

평가 항목ID	스위치	라우터	A	B	C	D	통제 구분	평가항목	위험도	상세설명
NET-001	○	○	○	○	○	○	5.5.2 보안 관리	네트워크 장비 설정 백업 여부	4	○ 네트워크 장비의 장애, 가동중지 등 비상상황 발생 시 신속하게 시스템의 정상복구가 가능하도록 하기 위함
NET-003	○	○	○	○	○	○	5.5.2 보안 관리	SNMP 커뮤니티 이름 복잡성 설정	4	○ SNMP Community String 설정 시 복잡도를 준수하여 설정하여 비인가자에 의해 쉽게 유추되지 않도록 하기 위함
NET-004	○	○	○	○	○	○	5.5.2 보안 관리	SNMP 커뮤니티 권한 설정	4	○ SNMP Community String 권한을 RO(Read Only)로 설정하여 비인가자가 Community String을 탈취하여도 네트워크 설정 정보를 변경할 수 없도록 하기 위함
NET-005	○	○	○	○	○	○	5.5.2 보안 관리	SNMP 접근통제(ACL) 설정	5	○ SNMP ACL(Access list)을 설정하여 비인가자의 SNMP 접근을 차단하는 등 네트워크 정보 노출을 제한하기 위함
NET-006		○	○		○		5.5.2 보안 관리	외부인터페이스 SNMP 접근 차단	1	○ 네트워크 장비 외부인터페이스에 SNMP 서비스 포트에 대한 ACL(Access list) 차단 설정을 적용하여 비인가자의 접근을 제한하기 위함

평가 항목ID	스위치	라우터	A	B	C	D	통제 구분	평가항목	위험도	상세설명
NET-007	○	○	○	○	○	○	5.5.3 사용자 인증	Local 사용자 생성 및 권한관리 여부	3	○ 장비 접속 시 Local 사용자를 생성하여 비인가자의 접근을 차단하기 위함
NET-008	○	○	○	○	○	○	5.5.3 사용자 인증	강화된 인증기능(AAA) 사용 여부	3	○ 장비 접속 시 AAA(Authentication Authorization Accounting) 인증 기능을 활성화하여 비인가자의 접근을 차단하기 위함
NET-009	○	○	○	○	○	○	5.5.3 사용자 인증	취약한 비밀번호 중복 사용	5	○ 사용자, 관리자 등이 사용하는 비밀번호를 중복으로 사용할 경우 비인가자에 의해 계정정보 유출이 가능함에 따라 비밀번호 중복 사용 여부를 점검
NET-010	○	○	○	○	○		5.5.3 사용자 인증	enable secret 설정 여부	5	○ 네트워크 장비 설정(Configuration)이 노출될 경우 평문으로 노출되었던 Enable 비밀번호를 암호화 적용하여 비인가자가 쉽게 식별할 수 없도록 하기 위함
NET-011	○	○	○	○	○	○	5.5.3 사용자 인증	안전한 암호화 알고리즘 설정 여부	5	○ 사용자 및 관리자의 비밀번호를 암호화하여 네트워크 장비 설정 (Configuration) 파일이 외부로 노출될 경우 비인가자의 장비 내 비밀번호 식별을 어렵게 하기 위함
NET-012	○	○	○	○	○	○	5.5.3 사용자 인증	비밀번호 복잡도 설정	5	○ 비밀번호 복잡도 정책을 준수하여 공격자가 네트워크 장비에 접속 시도 시 접근이 용이하지 않게 하기 위함
NET-013	○	○	○	○	○	○	5.5.2 보안 관리	원격 관리 접근 통제	5	○ 원격에서 네트워크 장비 접근 시 접근이 허가된 사용자 외에 비인가자의 접근을 차단하기 위함
NET-014	○	○	○	○	○	○	5.5.2 보안 관리	세션 타임아웃 설정 여부	4	○ 사용자 부재 시, 비인가자에 의한 시스템 무단 사용을 방지하기 위해 일정시간 사용하지 않는 세션에 대한 자동 종료시간 설정 여부를 점검하고, 세션 종료시간이 설정되어 있을 경우 과도하게 설정 되어 있는지를 점검

평가 항목ID	스위치	라우터	A	B	C	D	통제 구분	평가항목	위험도	상세설명
NET-015	○	○	○	○	○	○	5.5.2 보안 관리	VTY 접속 시 안전하지 않은 프로토콜(TELNET 등) 사용	4	○ 원격 터미널(vty)을 통해 네트워크 장비 접근 시 암호화프로토콜을 사용하여, 네트워크 스니핑 공격에 의해 평문데이터가 공격자에게 노출되지 않게 하기 위함
NET-016	○	○	○				5.5.2 보안 관리	불필요한 보조 입출력 포트(AUX) 차단 여부	2	○ 사용하지 않는 입출력 포트 사용을 중지하여 비인가자의 접근을 차단하기 위함
NET-022		○	○	○			5.5.2 보안 관리	불필요한 Source 라우팅 차단 설정 여부	2	○ Source 라우팅은 라우팅 경로를 통하지 않고 패킷 발송자가 원하는 경로로 패킷을 보낼 수 있는 기능으로 비인가자에 의해 공격에 악용되는 것을 차단하기 위함
NET-026		○	○			○	5.5.2 보안 관리	Proxy ARP 차단 설정 여부	3	○ 비인가자가 패킷 주소를 위조하여 Proxy ARP를 요청할 수 있으며 이에 응답하는 것을 이용하여 라우터와 네트워크 관련 정보를 획득할 수 있으므로 이를 차단하기 위함
NET-027	○	○	○	○			5.5.2 보안 관리	IP Directed Broadcast 차단 점검 - IOS 11	3	○ IP Directed Broadcast를 비활성화 하여 DoS 공격(Smurf 공격 등)을 차단하기 위함
NET-030	○	○	○	○	○	○	5.5.2 보안 관리	불필요한 서비스 구동 여부	2	○ 운영에 필요하지 않는 서비스가 불필요하게 설정되어 있을 경우 의도치 않는 공격의 대상이 될 수 있으므로 잠재적인 위험을 제거하기 위함
NET-031	○	○	○	○	○	○	5.5.2 보안 관리	NTP 설정 및 시각 동기화 여부	3	○ 시스템 시간 정확성 및 이벤트 발생 시 정확한 로그 분석을 하기 위함
NET-033	○	○	○	○	○	○	5.5.2 보안 관리	로깅 활성화 설정	3	○ 네트워크 장비 운영 및 보안을 위한 모니터링이 가능하도록 하기 위함
NET-034	○	○	○	○		○	5.5.2 보안 관리	로깅 메시지 시간 설정 여부	1	○ 로그 메시지에 정확한 시간을 포함시켜 공격에 대한 분석이 가능하도록 하기 위함

평가 항목ID	스위치	라우터	A	B	C	D	통제 구분	평가항목	위험도	상세설명
NET-035	○	○	○	○	○	○	5.5.2 보안 관리	로깅 버퍼 사이즈 설정 여부	2	○ 시스코 라우터는 Log 메시지를 메모리 버퍼에 저장하는데 버퍼의 용량을 일정 수준 이상으로 설정하여 디버깅이나 모니터링 시에 활용하기 위함
NET-036	○	○	○	○	○	○	5.5.2 보안 관리	원격 로그서버 연동 설정	3	○ 네트워크 장비에 로그를 저장하는 데 한계가 있어, 로그가 삭제될 수 있으므로 원격에 로그서버를 설치하여 별도의 로그 파일을 관리하기 위함
NET-037	○	○	○	○			5.5.2 보안 관리	콘솔로깅 레벨 설정	1	○ 로그 메시지가 콘솔 메시지에 출력되는 경우 콘솔에만 출력될 뿐 운영상 불필요한 경우가 있으므로 불필요한 로그 메시지 출력을 방지하기 위함
NET-038		○	○				5.5.2 보안 관리	외부 인터페이스에 ingress 필터 설정	5	○ 외부 인터페이스에 ingress 필터를 설정하여 내부 네트워크로 유입되는 패킷을 필터링하기 위함
NET-039		○	○				5.5.2 보안 관리	외부 인터페이스에 egress 필터 설정	3	○ 외부 인터페이스에 egress 필터를 설정하여 내부에서 외부로 전송되는 패킷을 필터링하기 위함
NET-040		○	○				5.5.2 보안 관리	스푸핑방지 필터 설정	4	○ 내부 네트워크 IP 대역을 소스 IP로 사용하여 들어오는 패킷을 외부 인터페이스에서 필터하여 스푸핑 공격을 차단하기 위함
NET-041		○	○				5.5.2 보안 관리	IP 멀티캐스트 차단 설정	1	○ IP 멀티캐스트를 사용하지 않는 경우 멀티캐스트 패킷을 필터하여 공격에 악용되는 것을 차단하기 위함
NET-042		○	○				5.5.2 보안 관리	ICMP 차단 미설정	2	○ 외부에서 내부로 유입되는 ICMP 패킷을 차단하여 내부의 정보가 유출되지 않도록 하고 서비스 거부공격 등을 차단하기 위함
NET-043		○	○				5.5.2 보안 관리	ICMP redirect 차단 미설정	2	○ 외부 인터페이스에 ICMP redirect 패킷을 차단하여 라우팅 테이블이 변경되는 것을 방지하기 위함

평가 항목ID	스위치	라우터	A	B	C	D	통제 구분	평가항목	위험도	상세설명
NET-044		○	○				5.5.2 보안 관리	ICMP unreachable 차단 미설정	2	○ ICMP unreachable 메시지를 이용하여 스캐닝 시 네트워크 장비의 특정 포트 활성화 여부 노출 및 DoS 공격에 악용되는 것을 차단하기 위함
NET-045		○	○				5.5.2 보안 관리	ICMP mask-reply 차단 미설정	2	○ ICMP mask-reply 서비스를 차단하여 비인가자에게 네트워크 구성정보가 노출되는 것을 차단하기 위함
NET-046		○	○				5.5.2 보안 관리	ICMP Timestamp, Information Requests 차단 미설정	1	○ ICMP Timestamp, Information Requests를 차단하여 비인가자에게 네트워크 정보가 노출되지 않게 하기 위함
NET-047		○	○				5.5.2 보안 관리	서비스 거부(DDoS) 공격 차단 필터링 설정	4	○ 서비스 거부 공격을 발생할 수 있는 포트를 차단하기 위함
NET-048	○	○	○	○	○	○	5.5.4 패치 관리	최신/긴급 보안 패치 및 업데이트 적용 여부	5	○ 네트워크 장비 운영체제의 최신 버전 및 마지막으로 발표된 보안 패치를 검토(운영체제 안정 버전 및 최신 보안 패치에 대한 테스트 등) 및 수행하였는지 확인하기 위함
NET-049	○	○	○	○			5.5.2 보안 관리	명령어 실행 권한 제한 여부	3	○ 사용자에 명령어별 권한 수준을 Level 15로 설정하여 비인가자의 접근을 차단하기 위함
NET-050	○	○	○	○	○	○	5.5.2 보안 관리	로그온 시 경고메시지 미설정	3	○ 라우터에 접근하는 사용자에게 배너를 통하여 적절한 경고 메시지를 보여주기 위함
NET-051		○	○				5.5.2 보안 관리	tcp keepalives 사용 설정 여부	3	○ 원격 사용자가 종료되었을 때 tcp keepalives를 사용하여 세션을 차단함으로써 하이재킹을 통한 공격 차단 및 세션의 정상적인 종료를 위함
NET-052	○	○	○	○	○	○	5.5.2 보안 관리	미사용 인터페이스 비활성화 설정	4	○ 비인가자에 의해 사용하지 않는 인터페이스를 통해 통신장비와 연결된 네트워크 정보 파악 및 장애 유발을 차단하기 위함

평가 항목ID	스위치	라우터	A	B	C	D	통제 구분	평가항목	위험도	상세설명
NET-054	○		○	○	○	○	5.5.2 보안 관리	스위치 허브 보안강화	1	○ 보안설정을 통해 네트워크 트래픽이 비인가자에게 노출 또는 변조되는 것을 차단하기 위함
NET-056	○	○	○	○	○	○	5.5.2 보안 관리	비밀번호의 주기적인 변경관리 여부	3	○ 네트워크 장비 접근자의 비밀번호를 장기간 변경하지 않을 경우 비밀번호 대입공격으로 인한 비밀번호 탈취 위협이 존재함으로 보안장비의 비밀번호를 주기적으로 변경/관리하는지 여부를 점검
NET-057	○	○	○				5.5.2 보안 관리	취약한 서비스 구동 여부	2	○ 취약한 서비스*가 구동 될 경우 장비정보 노출, 전송 정보 노출 등의 위협이 존재함에 따라 취약한 서비스 구동 여부를 점검 * CDP, LLDP, TFTP, Finger, identd, Smart Install 등

【정보보호시스템 장비】

■ **평가대상**

A	B	C	D	E	F
침입차단시스템 (FW)	가상사설망 (VPN)	침입탐지시스템 (IDS)	침입방지시스템 (IPS)	DDoS대응장비 (DDoS)	웹방화벽 (WAF)

■ 평가기준

평가 항목ID	A	B	C	D	E	F	통제 구분	평가항목	위험도	상세설명
ISS-001	○	○	○	○	○	○	5.5.2 보안 관리	보안장비 정책 및 로그 백업 설정	4	○ 보안장비 장애, 가동중지 등 비상상황 발생 시 신속하게 시스템의 정상복구가 가능하도록 하기 위함
ISS-002	○	○	○	○	○	○	5.5.2 보안 관리	원격 로그 서버 사용	3	○ 정보보호시스템에 로그를 저장하는데 한계가 있어, 로그가 삭제될 수 있으므로 원격에 로그서버를 설치하여 별도의 로그파일을 관리하기 위함
ISS-003	○	○					5.5.2 보안 관리	DMZ 구간 설정	4	○ 공개용 서버 구간의 DMZ 설정을 통해 내부서버 및 사용자 구간과 분리하여 비인가자가 공개용 서버 구간의 호스트를 통해 내부 네트워크로 접근하는 것을 차단하기 위함
ISS-004	○	○					5.5.2 보안 관리	외부구간 NAT 설정	4	○ 외부에 연결될 필요가 없는 시스템에 대해 NAT(Network Address Translation) 설정을 하여 비인가자가 내부 네트워크에 접근하는 것을 차단하기 위함
ISS-005	○	○	○	○	○	○	5.5.4 패치 관리	최신/긴급 보안 패치 및 업데이트 적용	5	○ 정보보호시스템 장비 OS 및 보안패턴에 대해 최신 버전으로 적용하였는지 확인하기 위함

평가 항목ID	A	B	C	D	E	F	통제 구분	평가항목	위험도	상세설명
ISS-006	○	○	○	○	○	○	5.5.2 보안 관리	보안장비 사용량의 주기적인 점검 및 보고	4	○ 보안장비에 사용량을 검토하여 CPU, 메모리 등 장비 가용성을 확보하기 위함
ISS-007	○	○	○	○	○	○	5.5.2 보안 관리	보안장비 장애/보안이벤트 모니터링 실시	4	○ 장애 및 보안 이벤트에 대한 모니터링을 설정하여 해킹 등 공격 징후 또는 시스템 운영상 장애 발생에 대해 실시간 대응을 하기 위함
ISS-008			○	○	○	○	5.5.2 보안 관리	탐지된 이벤트 및 로그에 대한 정기적 분석 및 보고	3	○ 탐지된 이벤트 및 로그에 대한 분석을 실시하여 침해사고 발생을 점검하기 위함
ISS-009			○	○	○	○	5.5.2 보안 관리	위험도가 높은 이벤트 및 로그에 대한 RAW 패킷저장	2	○ 침해사고 발생 시 RAW 패킷이 저장되지 않는 경우 정확한 분석에 어려움이 있으므로, 정확한 분석을 위해 탐지된 패킷에 대한 RAW 데이터 저장 여부를 확인하기 위함
ISS-010			○	○	○		5.5.2 보안 관리	TCP/UDP/ICMP 탐지/차단 패턴 적용 여부	2	○ TCP/UDP/ICMP Flooding 공격에 대한 탐지 및 차단 패턴을 적용하여 외부 인터넷망을 통한 공격 시 내부 서버 및 단말기 등을 보호하기 위함
ISS-011			○	○	○		5.5.2 보안 관리	Port Scan 탐지/차단 패턴 적용	2	○ 외부 인터넷 망을 통해 내부 시스템에 대한 접근 정보 획득을 차단하기 위함
ISS-012			○	○		○	5.5.2 보안 관리	해킹 툴 탐지/차단 패턴 적용	2	○ 악성코드에 대한 탐지 및 차단패턴을 적용하여 첨부파일 등을 통한 악성코드 감염을 차단하기 위함
ISS-013	○	○					5.5.2 보안 관리	불필요한 Source Routing 설정	2	○ 정해진 경로가 아닌 특정 경로를 통한 공격을 차단하기 위함
ISS-014	○	○	○	○	○	○	5.5.2 보안 관리	사용하지 않는 SNMP 설정	4	○ 사용하지 않는 SNMP 서비스를 중지하여 SNMP 서비스 취약점(장비의 소프트웨어 정보 및 하드웨어 정보 제공, DoS 등 각종 공격에 노출)을 이용한 공격을 차단하기 위함

평가 항목ID	A	B	C	D	E	F	통제 구분	평가항목	위험도	상세설명
ISS-015	○	○	○	○	○	○	5.5.2 보안 관리	SNMP Community String 복잡성 설정	4	○ SNMP Community String 설정 시 복잡도를 준수하여 설정하여 비인가자에 의해 쉽게 유추되지 않도록 하기 위함
ISS-016	○	○	○	○	○	○	5.5.2 보안 관리	보안장비 보안 접속	5	○ 암호화 접속을 통해 비인가자에 의한 스니핑 공격에 노출되는 것을 방지하기 위함
ISS-017	○	○	○	○	○	○	5.5.3 사용자 인증	보안장비 Default 계정 변경	4	○ 외부에서 쉽게 계정정보 획득이 가능한 보안장비의 Default 계정을 이용하여 비인가자가 보안장비에 접근하는 것을 차단하기 위함
ISS-018	○	○	○	○	○	○	5.5.3 사용자 인증	보안장비 Default 비밀번호 변경	4	○ 외부에서 쉽게 획득이 가능한 보안장비의 초기 Default 비밀번호를 사용하여 비인가자가 보안장비에 접근하는 것을 차단하기 위함
ISS-019	○	○	○	○	○	○	5.5.3 사용자 인증	보안장비 계정 관리	5	○ 침해사고 발생 시 계정별 권한에 대한 관리 및 감사증적 기록을 남기기 위함
ISS-020	○	○	○	○	○	○	5.5.3 사용자 인증	보안장비 계정별 권한 설정	4	○ 보안장비 계정을 용도별로 권한을 부여함으로써 권한 없는 사용자의 의도하지 않은 보안정책 수정이나 설정값 변경을 방지하기 위함
ISS-021	○	○	○	○	○	○	5.5.2 보안 관리	보안장비 원격 관리 접근 통제	5	○ 관리용도로 허용된 IP에 대해서만 보안장비에서 허용하여 비인가자에 대한 접근을 차단하기 위함
ISS-022	○	○	○	○	○	○	5.5.2 보안 관리	보안장비 접속 성공/실패 로깅	3	○ 보안장비 접근 권한에 대해 계정의 로그인 성공/실패 로그를 저장하여 비인가자의 접근을 확인하기 위함
ISS-023	○	○	○	○	○	○	5.5.2 보안 관리	로그인 실패횟수 제한	3	○ 비인가자가 자동화된 방법을 통해 사용자 계정에 반복적인 대입을 시도하여 계정 및 비밀번호를 탈취하여 접근하는 것을 방지하기 위함

평가 항목ID	A	B	C	D	E	F	통제 구분	평가항목	위험도	상세설명
ISS-024	○	○	○	○	○	○	5.5.2 보안 관리	세션 타임아웃 설정	4	○ 사용자 부재 시, 비인가자에 의한 시스템 무단 사용을 방지하기 위해 일정시간 사용하지 않는 세션에 대한 자동 종료시간 설정 여부를 점검하고, 세션 종료시간이 설정되어 있을 경우 과도하게 설정 되어 있는지를 점검
ISS-025	○	○	○	○	○	○	5.5.2 보안 관리	NTP 설정 및 시각 동기화	2	○ 시스템 시각 정확성 및 이벤트 발생 시 정확한 로그 분석을 하기 위함
ISS-026	○	○	○	○	○	○	5.5.2 보안 관리	주요 파일에 대한 주기적인 무결성 검사	2	○ 주요 파일(설정, 로그 등)이 불법 변조되어 있는 것을 확인하기 위함
ISS-027	○	○	○	○	○	○	5.5.2 보안 관리	보안장비 기능 외 서비스 미제한	2	○ 정보보호시스템 장비 기능 외 다른 서비스가 시스템에서 실행되는 경우 비인가자에 의해 공격에 활용될 수 있으므로 이를 차단하기 위함
ISS-028	○	○					5.5.2 보안 관리	보안장비 정책 변경통제 절차 수립	4	○ 보안장비 관리자가 사용자 편의 등을 위해 정책을 임의적으로 생성, 변경, 삭제하는 것을 차단하기 위함
ISS-029	○	○					5.5.2 보안 관리	보안장비 변경요청 정책의 기술적 검토	4	○ 보안장비 정책을 생성, 변경, 삭제 시 네트워크 및 시스템 운영에 영향을 미칠 수 있으므로, 보안정책 신청에 대해 관리자가 적정성 여부 등을 검토 후 적용하고 있는지 확인하기 위함
ISS-030	○	○					5.5.2 보안 관리	모든 목적지 및 서비스로의 허용 오류	5	○ 신뢰할 수 있는 내부 시스템인 경우에도, 모든 목적지의 모든 서비스로의 허용정책은 비인가자에 의한 불필요한 접근을 허용하여 잠재적인 위험에 노출될 수 있으므로 이를 차단하기 위함
ISS-031	○	○					5.5.2 보안 관리	취약한 서비스의 네트워크 대역 단위 허용	5	○ 관리용도 또는 취약한 서비스 포트로 출발지나 목적지 IP를 광범위하게 허용할 경우 비인가자에 의한 불필요한 접근을 허용하여 잠재적인 위험에 노출될 수 있으므로 이를 방지하기 위함

평가 항목ID	A	B	C	D	E	F	통제 구분	평가항목	위험도	상세설명
ISS-032	○	○					5.5.2 보안 관리	과도한 서비스 포트 허용	5	○ 신뢰할 수 있는 내부 시스템인 경우에도, 과도한 서비스로의 허용 정책은 비인가자에 의한 불필요한 접근을 허용하여 잠재적인 위험에 노출될 수 있으므로 이를 차단하기 위함
ISS-033	○	○					5.5.2 보안 관리	불필요한 양방향 정책 허용	4	○ 불필요하게 양방향으로 설정된 정책은 비인가자에 의한 불필요한 접근을 허용하여 잠재적인 위험에 노출될 수 있으므로 이를 방지하기 위함
ISS-034	○	○					5.5.2 보안 관리	정책적용 순서 오류	4	○ 잘못된 정책 적용으로 인해 비인가자에 의한 불필요한 접근을 허용할 수 있으므로 이를 차단하기 위함
ISS-035	○	○					5.5.2 보안 관리	출발지 포트 기반의 정책 허용	5	○ 공격자로 하여금 출발지 포트를 속여 목적지 서버의 임의의 서비스 포트에 접속하는 것을 차단하기 위함
ISS-036	○	○					5.5.2 보안 관리	취약한 원격서비스 허용	5	○ 비밀번호 없이 서버에 접근이 가능하거나 보안 취약점에 노출된 원격 서비스를 허용하고 있는지 점검하기 위함
ISS-037	○	○					5.5.2 보안 관리	기타 불필요한 정책 적용	4	○ 테스트용도 혹은 현재 사용하지 않은 서비스에 대한 허용정책 등 불필요한 포트 및 사용하지 않는 정책을 점검하기 위함
ISS-038	○	○					5.5.2 보안 관리	서버간 관리포트 허용	5	○ 서버간 관리포트 허용 등 취약한 정책 존재여부를 점검하기 위함
ISS-039	○	○					5.5.2 보안 관리	단말과 서버간 접근통제를 우회한 접속 허용	5	○ 사용자 단말과 서버간에 비인가 접속용 관리포트 허용정책 등 취약한 정책이 존재하는지 점검하기 위함
ISS-040	○	○	○	○	○	○	5.5.2 보안 관리	보안장비 비밀번호의 주기적인 변경	3	○ 보안장비 접근자의 비밀번호를 장기간 변경하지 않을 경우 비밀번호 대입공격으로 인한 비밀번호 탈취 위협이 존재함으로 보안장비의 비밀번호를 주기적으로 변경/관리하는지 여부를 점검

평가 항목ID	A	B	C	D	E	F	통제 구분	평가항목	위험도	상세설명
ISS-041	○	○					5.5.2 보안 관리	불필요한 네트워크 대역 단위 허용	4	○ 출발지나 목적지 IP를 불필요하게 네트워크 대역 단위로 허용할 경우 비인가자에 의한 접근을 허용하여 잠재적인 위험에 노출될 수 있으므로 이를 방지하기 위함

【웹·모바일·HTS 애플리케이션】

■ 평가기준

평가항목ID			Sub NUM	통제구분	평가항목	위험도	상세설명
WEB	Mobile	HTS					
WEB-FIN-	MOB-FIN-	HTS-FIN-	001	5.8.2 (전자금융) 거래정보 검증	[전자금융] 거래 인증수단 검증 오류	5	○ 전자금융거래에 적용된 거래 인증수단 검증의 적절성 여부를 점검 * (평가 예시) - 잘못된 인증정보(비밀번호, OTP, 보안카드 번호 등) 입력 후 정상 거래 가능 여부 점검 - 폐기된 인증수단(인증서, 보안카드, OTP 등)을 통해 인증 시도 후 정상 거래 가능 여부 점검 - SMS, ARS, 계좌 등의 인증수단 이용 시, 인증 유효시간 제한 여부 점검 - 인증 매체를 통해 전달받은 인증정보를 금융회사에서 정한 시간 이후에 인증 요청 시 정상 처리 가능 여부를 점검
WEB-FIN-	MOB-FIN-	HTS-FIN-	004	5.8.2 (전자금융) 거래정보 검증	[전자금융] 거래정보 무결성 검증	5	○ 전자금융거래 시 이용되는 거래정보의 무결성 검증 여부를 점검 * (평가 예시) - 예비거래에 이용된 거래정보와 본거래에서 이용된 거래정보의 일치 여부 점검 - 본 거래정보와 최종 승인된 거래정보의 일치 여부 점검 - 전자서명기술 이용 시 타인인증서로 서명 후 거래 가능 여부 점검 - 전자서명기술 이용 시 전자서명 검증절차 오류 여부 점검 - 전자서명기술 이용 시 전자서명 무결성 검증 오류 여부 점검 - 전자서명기술 이용 시 매번 동일한 전자서명값 이용 여부 점검 등 - 계좌 인증 수행 시 이체 금액을 변조하여 전송 가능 여부를 점검 - 유료 인증수단(범용 인증서) 발급 시, 발급 비용 변조 가능 여부를 점검 등 * 거래정보의 무결성 : 이용자가 단말기(PC/모바일 등)를 통해 입력한 거래정보가 금융회사 시스템으로 안전하게 전송됨을 의미

평가항목ID			Sub NUM	통제구분	평가항목	위험도	상세설명
WEB	Mobile	HTS					
WEB-FIN-	MOB-FIN-	HTS-FIN-	005	5.8.2 (전자금융) 거래정보 검증	[전자금융] 거래정보 재사용	5	○ 전자금융거래 시 이용되는 거래정보의 재사용 가능 여부를 점검 * (평가 예시) - 기 사용된 거래정보(이체 전문, 결제 전문 등)를 재전송하여 정상거래 가능 여부를 점검 등
WEB-FIN-	MOB-FIN-	HTS-FIN-	006	5.8.2 (전자금융) 거래정보 검증	[전자금융] 거래시 소유주 확인 여부	5	○ 전자금융거래 시 이용자의 이용 권한 검증 여부를 점검 * (평가 예시) - 계좌(카드,계약)정보 조회 시 타 이용자의 계좌(카드,계약)번호 입력 후 타 이용자 계좌 조회 가능 여부 점검 - 거래 요청 시 계좌 번호를 현재 로그인 중인 이용자가 아닌 다른 이용자의 계좌번호로 변조하여 거래 시도 등
WEB-FIN-	MOB-FIN-	HTS-FIN-	007	5.8.2 (전자금융) 거래정보 검증	[전자금융] 사전에 정한 조회기간 이상으로 거래내역 조회가능 여부	5	○ 거래내역 조회 시 금융회사가 정한 기간 이상의 내역 조회 가능 여부를 점검 * (평가 예시) - 3개월로 정한 거래내역 조회기능을 3개월 이상으로 변경 후 응답 여부 점검 - 거래가 종료된 계좌에 대해 거래내역을 임의 조회 가능 여부 점검 등
WEB-FIN-	MOB-FIN-	HTS-FIN-	009	5.8.1 (전자금융) 거래 인증	[전자금융] 비밀번호 변경 시 본인확인 절차 실시 여부	5	○ 전자금융거래 시 사용되는 비밀번호 변경 시 본인확인 절차의 존재 여부를 점검 * (평가 예시) - 비밀번호 변경 시 본인확인 절차 존재 여부 점검 등
WEB-FIN-	MOB-FIN-	HTS-FIN-	010	5.8.1 (전자금융) 거래 인증	[전자금융] 비밀번호 변경 시 이전 비밀번호 재사용 여부	5	○ 전자금융거래 시 사용되는 비밀번호 변경 시 동일 비밀번호 재사용 가능 여부를 점검 * (평가 예시) - 비밀번호 변경 시 과거에 이용했던 비밀번호의 재사용 여부 점검 등

평가항목ID			Sub NUM	통제구분	평가항목	위험도	상세설명
WEB	Mobile	HTS					
	MOB-FIN-		011	5.8.3 (전자금융) 단말 보안	[전자금융] OS 변조 탐지 기능 적용 여부	5	○ OS가 변조(루팅, 탈옥) 된 단말 이용 시 보안 위협이 증대됨에 따라, OS변조 시 전자금융 서비스 이용 가능 여부를 점검 * (평가 예시) - 권한이 상승된 OS변조 단말에서 서비스 이용 가능 여부 점검 등
	MOB-FIN-		012	5.8.3 (전자금융) 단말 보안	[전자금융] 악성코드 방지	5	○ 악성코드에 대한 대응이 필요함에 따라, 전자금융서비스 이용 시 악성코드 차단 및 탐지 프로세스 동작 여부를 점검 * (평가 예시) - 애플리케이션 이용 시 악성코드 방지 프로세스 동작 여부 점검 - 악성코드 방지 프로세스 강제 종료 후 재구동 여부 점검 등
		HTS-FIN-	013	5.8.3 (전자금융) 단말 보안	[전자금융] 보안프로그램 최초 설치 시 미동작으로 설정	5	○ 보안 프로그램이 동작하지 않을 경우 이용자의 입력값 및 중요정보와 파일이 유출 될 수 있는 위협을 점검 * (평가 예시) - 최초 설치 시 보안프로그램 동작 여부 점검 등
		HTS-FIN-	014	5.8.3 (전자금융) 단말 보안	[전자금융] 보안프로그램 임의 해제 가능 여부	5	○ 보안 프로그램이 임의해제되는 경우 이용자의 입력값 및 중요정보와 파일이 유출 될 수 있는 위협을 점검 * (평가 예시) - 보안 프로그램 강제종료, 레지스트리 변조, 환경 파일 변조 등의 방법 또는 이용자가 임의로 해제 가능 여부 점검 - 이용자가 직접 해제를 요청하는 경우 위협에 대한 주의사항 등의 내용을 이용자 고지 여부 점검 등

평가항목ID			Sub NUM	통제구분	평가항목	위험도	상세설명
WEB	Mobile	HTS					
		HTS-FIN-	015	5.8.3 (전자금융) 단말 보안	[전자금융] 프로그램 실행 명령줄(Command Line) 내 중요정보 평문 노출 여부	5	○ 프로그램 실행을 위해 전달되는 명령줄(Command Line) 내 이용자 중요정보 노출 여부를 점검 * (평가 예시) - 실행 명령줄 내 중요정보 평문 여부를 확인
		HTS-FIN-	016	5.8.3 (전자금융) 단말 보안	[전자금융] HTS 구동시 실행 파라미터 재사용 가능 여부	5	○ 노출된 실행 파라미터 정보를 이용하여 인증절차 없이 타인의 HTS계정으로 로그인 할 수 있는 위협을 점검 * (평가 예시) - 실행 파라미터를 재사용하여, 별도의 인증절차없이 로그인 가능 여부를 확인
WEB-FIN-	MOB-FIN-	HTS-FIN-	017	5.8.3 (전자금융) 단말 보안	[전자금융] 이용자 입력정보 보호	4	○ 이용자 거래입력 수단(手段)을 보호하기 위한 금융회사 대응수단 및 적용범위 등을 점검 * (평가 예시) - 이용자 거래정보 입력보호 범위가 금융회사가 정한 범위와 달리 적용되어 있거나 또는 일관성 확인 - 이용자 거래정보 입력보호에 대응하기 위한 절차 또는 방법 존재 여부 점검 등
	MOB-FIN-	HTS-FIN-	018	5.8.3 (전자금융) 단말 보안	[전자금융] 프로그램 무결성 검증	5	○ 변조된 프로그램이 정상실행 될 경우 악성코드가 포함되어 재배포 되는 등의 보안 위협이 존재함에 따라, 변조 프로그램 이용 시 정상 실행 가능 여부를 점검 * (평가 예시) - 설치파일(APK, IPA) 변조 후 재 설치 시, 정상 실행 가능 여부 점검 - 애플리케이션 설치 후 실행파일 및 관련 라이브러리 변조를 통해 정상 실행 가능 여부 점검 등

평가항목ID			Sub NUM	통제구분	평가항목	위험도	상세설명
WEB	Mobile	HTS					
	MOB-FIN-	HTS-FIN-	020	5.8.3 (전자금융) 단말 보안	[전자금융] 소스코드 난독화 적용 여부	4	○ 디컴파일(DeCompile) 기술을 이용하여 복구된 소스코드의 분석(프로그램 흐름 파악, 중요정보 획득 등)을 어렵게 하기 위해, 소스코드(또는 실행파일) 난독화 여부를 점검 * (평가 예시) - 실행 프로그램 또는 소스코드 난독화 미적용으로 인한 중요 로직의 해독 가능 여부를 점검
	MOB-FIN-	HTS-FIN-	021	5.8.3 (전자금융) 단말 보안	[전자금융] 디버깅 탐지기능 적용 여부	4	○ 디버깅을 통한 코드 흐름, 메모리 상태 분석 등 프로그램 역분석을 어렵게 하기 위해, 안티디버깅 기능 적용 여부를 점검 * (평가 예시) - 동적 디버깅 프로그램(gdb, lldb, windbg 등)을 통해 디버깅 시 정상 실행 가능 여부 점검 등
		HTS-FIN-	022	5.8.3 (전자금융) 단말 보안	[전자금융] 보안프로그램 구동 시(최초) 최신 업데이트 미수행	4	○ 보안 프로그램이 최신 버전으로 업데이트되지 않은 경우 새로운 보안 취약점을 통해 이용자의 입력값 및 중요정보와 파일이 유출 될 수 있는 위협을 점검 * (평가 예시) - 보안프로그램 최신 버전 업데이트 여부 점검 등
WEB-SER-	MOB-SER-	HTS-FIN-	001	5.8.4 (일반공통) 서비스 보호	SQL Injection	5	○ 사용자가 간섭 가능한 매개변수(URL 파라미터, XML 등)에 의해 SQL 질의문이 완성되는 점을 이용하여, 해당 매개변수 변조를 통해 비정상 질의 가능 여부를 점검 * (평가 예시) - URL 파라미터 또는 XML 등 입력하는 부분에 SQL 구문 입력 후 서버에서 응답한 값에 대한 위험성 점검 - SQL문으로 해석될 수 있는 값(글번호, 검색 내용 등)을 입력하여 데이터베이스 내에 저장된 정보 열람 및 시스템 명령 실행가능 여부 점검 - 조작된 XPath 쿼리를 보내어 비정상적인 질의 가능 여부 점검 등

평가항목ID			Sub NUM	통제구분	평가항목	위험도	상세설명
WEB	Mobile	HTS					
WEB-SER-	MOB-SER-	HTS-FIN-	002	5.8.4 (일반공통) 서비스 보호	악성파일 업로드	5	○ 웹쉘 등과 같은 악성파일이 업로드 될 경우 시스템 명령어 실행 및 인접 서버에 대한 침입 가능성이 존재함에 따라, 악성파일 업로드 및 실행 가능 여부를 점검 * (평가 예시) - 이미지, 한글(hwp) 등의 파일을 업로드 할 수 있는 부분에 JSP, ASP 등의 스크립트 파일 업로드 가능 여부 점검 - 업로드 된 파일의 위치 및 실행 가능 여부 점검 등 * 웹쉘(web shell) : 업로드 취약점을 통하여 해커가 원격에서 웹서버를 조종할 수 있도록 작성한 웹 스크립트(단체표준 TTAK.KO-12.0002/R3 정보 보호 기술 용어)
WEB-SER-	MOB-SER-	HTS-SER-	003	5.8.4 (일반공통) 서비스 보호	부적절한 이용자 인가 여부	5	○ 접근 권한에 대한 검증 과정이 구현되지 않아 다른 이용자의 민감한 정보나 권한이 노출 될 수 있으므로 이에 대한 검증절차 존재 여부를 점검 * (평가 예시) - 현재 로그인 중인 이용자가 중요 정보가 포함된 페이지에 대해 접근권한 확인 여부 점검 - 중요 정보 페이지에서 이용자 파라미터 변경으로 타인의 정보를 열람, 수정이 가능 여부 점검 - 통상 파라미터 변조에 따른 비정상적인 권한상승/조회/변경 가능 여부 등을 점검
WEB-SER-	MOB-SER-	HTS-SER-	004	5.8.5 (일반공통) 이용자 인증	이용자 인증정보 재사용	5	○ 중간자 공격 등에 의해 탈취된 인증정보가 재사용되는 것을 방지하기 위해 이미 사용된 인증정보(전자서명값 등)에 대해 재사용 가능 여부를 점검 * (평가 예시) - 이용자 인증 수행을 위해 생성된 전자서명 값의 재사용 가능 여부를 점검 - OTP/SMS/계좌 인증에 사용되는 일회성 값의 재사용 가능 여부를 점검 - 비대면 실명인증(신분증 사본 제출) 수행 시, 서버에 전송되는 신분증 사진 및 신분증 정보(주민등록번호, 이름, 발급일자 등)에 대해 재사용 가능 여부를 점검 등

평가항목ID			Sub NUM	통제구분	평가항목	위험도	상세설명
WEB	Mobile	HTS					
WEB-SER-	MOB-SER-	HTS-SER-	005	5.8.5 (일반공통) 이용자 인증	고정된 인증정보 이용	5	○ SMS 등 이용자 인증을 위해 생성되는 값에 대해 인증정보 탈취 방지를 위해 가변적인 데이터 사용 여부를 점검 * (평가 예시) - SMS, ARS 등 이용자 인증 시 매번 동일한 인증코드 생성 여부 점검 등
WEB-SER-	MOB-SER-	HTS-SER-	006	5.8.5 (일반공통) 이용자 인증	유추가능한 인증정보 이용	5	○ 비인가자에 의한 인증정보 유추에 대응하기 위해, 인증정보(로그인 비밀번호, 계좌원장 비밀번호, PIN번호 등)의 등록 또는 변경 시 해당 값의 적절성 및 복잡성을 점검 * (평가 예시) - 이용자의 주민등록번호, 전화번호 등과 같이 쉽게 유추 가능한 개인 신상정보를 이용한 인증정보 사용 가능 여부를 점검 - 연속숫자, 연속문자, 동일숫자, 이름 등과 같이 제 3자가 비밀번호를 쉽게 유추할 수 있는 인증정보 사용 가능 여부를 점검 - 로그인 및 ARS 등에 사용되는 인증정보가 계좌 원장 비밀번호와 동일하게 사용 가능한지를 점검 - 복잡도를 준수하지 않는 비밀번호를 등록 및 변경 가능 여부를 점검 등 ※ 비밀번호 복잡도 : 영문 대문자, 영문 소문자, 숫자, 특수문자 2개 조합시 10자리 이상, 3개 조합시 8자리 이상
WEB-SER-	MOB-SER-	HTS-SER-	007	5.8.5 (일반공통) 이용자 인증	유추가능한 초기화 비밀번호 이용	5	○ 비밀번호 복구 매커니즘(비밀번호 찾기 등) 이용 시 복구된 비밀번호의 고정성 및 규칙성을 통해 타 이용자의 비밀번호 획득, 변경, 복구 등에 대한 가능 여부를 점검 * (평가 예시) - 비밀번호 찾기 또는 복구 메뉴에서 신규 비밀번호 생성 시 패스워드 생성 규칙 점검 - 타인의 비밀번호 초기화 가능 여부 점검 - 앞서 발견한 비밀번호 생성 규칙을 통해 타인의 계정으로 접속 가능 여부 점검 등

평가항목ID			Sub NUM	통제구분	평가항목	위험도	상세설명
WEB	Mobile	HTS					
	MOB-SER-	HTS-SER-	008	5.8.6 (일반공통) 단말 보안	단말기 내 중요정보 저장 여부	5	○ 애플리케이션 사용 폴더 및 외부 저장소에 존재하는 파일 내 중요정보 저장 여부를 점검 * (평가 예시) - 애플리케이션 사용 폴더 및 외부 저장소에 존재하는 파일에 중요정보 저장 여부 점검 등 * 중요정보 : 개인정보(주민등록번호), 금융정보(비밀번호, 카드번호, OTP, 보안카드 번호 등), 기타 중요정보라 판단되는 정보 * 중요정보 주요 검색영역 : 해당 애플리케이션 동작과 연관된 파일/폴더 등
	MOB-SER-	HTS-SER-	009	5.8.6 (일반공통) 단말 보안	메모리 내 중요정보 노출 여부	5	○ 이용자 단말기 메모리 영역에서 이용자 중요정보의 평문노출 여부를 점검 * (평가 예시) - GDB 등 메모리 덤프를 이용하여 이용자 입력 정보(중요정보)의 평문노출 여부 점검 등 * 중요정보 : 개인정보(주민등록번호), 금융정보(비밀번호, 카드번호, OTP, 보안카드 번호 등), 기타 중요정보라 판단되는 정보 * 중요정보 주요 검색영역 : 해당 애플리케이션 동작과 관련된 메모리 영역 등
WEB-SER-	MOB-SER-	HTS-SER-	010	5.8.4 (일반공통) 서비스 보호	파일 다운로드	5	○ 파일 다운로드 인터페이스를 이용하여 서버의 주요파일 다운로드 가능 여부 점검 * (평가 예시) - 파일 다운로드 시 파일이 저장된 디렉터리 이외에 경로에 접근하여 주요 파일의 다운로드 가능 여부 점검 등 * 주요파일 : 소스코드, 서버설정파일 등

평가항목ID			Sub NUM	통제구분	평가항목	위험도	상세설명
WEB	Mobile	HTS					
WEB-SER-	MOB-SER-	HTS-SER-	011	5.8.4 (일반공통) 서비스 보호	외부사이트에 의한 시스템 운영 정보 노출 여부	5	○ 검색엔진 또는 외부 사이트에 분석 대상과 연관된 중요정보 노출 여부를 점검 * (평가 예시) - 검색 엔진 및 외부 사이트에서 제공하는 분석 도구를 이용하여 분석 대상과 연관된 중요정보의 노출 여부 점검 등
WEB-SER-			012	5.8.5 (일반공통) 이용자 인증	유추 가능한 세션ID	5	○ 세션ID에 대한 무차별 대입공격에 대응하기 위해, 세션ID에 대한 복잡성을 점검 * (평가 예시) - 세션 ID가 무차별 대입 공격에 용이한 약한 강도 설정 여부 점검 - 세션 ID가 단순히 숫자가 증가하는 등의 규칙성 존재 여부 점검 등
WEB-SER-			013	5.8.5 (일반공통) 이용자 인증	쿠키변조	5	○ 쿠키 정보를 통해 이용자 검증 또는 데이터 입력에 사용되는 점을 악용하여, 쿠키 정보 조작을 통해 타이용자 권한 획득 또는 기타 중요정보 유출 가능 여부를 점검 * (평가 예시) - 쿠키에 계정, 권한 구분자, 인증ID 등 이용자의 권한을 식별할 수 있는 내용에 대한 조작을 통해 타 이용자의 권한으로 정상이용 가능 여부 점검 등
WEB-SER-	MOB-SER-	HTS-SER-	014	5.8.4 (일반공통) 서비스 보호	운영체제 명령실행	5	○ 운영체제 내 임의 명령어 실행이 가능한 인터페이스의 존재 여부를 점검 * (평가 예시) - 내부 서버에 명령어를 내릴 수 있는 인터페이스가 존재할 경우, 지정된 명령어 이외의 임의 명령 실행 가능 여부 점검 등

평가항목ID			Sub NUM	통제구분	평가항목	위험도	상세설명
WEB	Mobile	HTS					
WEB-SER-	MOB-SER-	HTS-SER-	015	5.8.4 (일반공통) 서비스 보호	XML 외부객체 공격 (XXE)	5	○ XML 구문 분석기의 입력값 검증 누락으로 인해 시스템의 자원에 접근 가능한 취약점으로, XML 구문에 대한 검증 여부를 점검 * (평가 예시) - XML 에 정의 되지 않은 구문을 삽입하여 서버로 전송 후 해당 내용이 실행 가능 여부 점검 등
WEB-SER-	MOB-SER-		016	5.8.4 (일반공통) 서비스 보호	리다이렉트 기능을 이용한 피싱 공격	4	○ 리다이렉트 기능이 존재 시 URL 인자값에 대한 검증 누락으로 인해 임의 페이지로 이동 가능성이 존재 하여 해당 기능 및 인자값 검증 여부를 점검 * (평가 예시) - 리다이렉트 기능이 존재할 경우 URL 인자값을 임의의 페이지로 지정하여 이동 가능 여부 점검 등
WEB-SER-			017	5.8.4 (일반공통) 서비스 보호	LDAP Injection	5	○ 이용자 입력을 기반으로 LDAP(Lightweight Directory Access Protocol) 구문을 구축하여 웹 기반 응용 프로그램 악용 여부를 점검 * (평가 예시) - 쿼리를 주입함으로써 개인정보 등의 내용이 유출 가능 여부 점검 - 입력 값에 대해 특수문자(=, +, 〈, 〉, #, :, / 등)를 입력하여 LDAP 명령어가 실행되는지 여부 점검 등
WEB-SER-			018	5.8.4 (일반공통) 서비스 보호	SSI Injection	5	○ CGI 또는 서버사이드 스크립트를 통해 만들어진 웹사이트에서 입력값에 부적절한 명령문을 삽입하여 실행 가능 여부를 점검 * (평가 예시) - 변수 값에 부적절한 명령문을 삽입하여 실행 가능 여부 점검 - 〈!--#echo var="DOCUMENT_NAME"--〉, 〈!--#exec cmd="ls" --〉, 〈!--#exec cmd="dir"--〉 과 같은 명령어 삽입 시 실행 가능 여부 점검 등

평가항목ID			Sub NUM	통제구분	평가항목	위험도	상세설명
WEB	Mobile	HTS					
WEB-SER-	MOB-SER-	HTS-SER-	019	5.8.4 (일반공통) 서비스 보호	불충분한 이용자 인증	4	○ 민감한 데이터 또는 이용자 인증이 필요한 경로에 임의의 이용자가 접근할 수 있으므로 이에 대한 인증절차가 존재 또는 우회가능한지 여부를 점검 * (평가 예시) - 개인정보 및 비밀번호 수정 기능 페이지 접근 전에 본인인증에 대한 재인증 여부 확인 - 인증 절차 후 접근이 가능한 페이지의 URL을 수집하여 인증절차 없이 접근 시도, 클라이언트 스크립트를 통한 접근 제어 시 해당 스크립트를 삭제하여 인증 없이 해당 페이지에 접근 가능 여부 점검 - 플로우 통제 우회 가능 여부 점검 등 * 플로우 통제 : 이용자 인증 시 단계별 인증을 통해 하는 경우 전 단계의 요건을 갖춰야 다음 단계로 진입하도록 된 구조 - ex) step 1. 연락처 작성 〉 step 2. 주소 작성 〉 step 3. 개인정보 작성 〉 step 4. 완료
	MOB-SER-	HTS-SER-	020	5.8.6 (일반공통) 단말 보안	화면 내 중요정보 평문노출 여부	5	○ 이용자 단말기에서 화면 내에 이용자 중요정보의 평문 노출 여부를 점검 * (평가 예시) - 화면 내 중요정보 평문 노출 여부 점검 등(화면캡처 등) * 중요정보 : 개인정보(주민등록번호), 금융정보(비밀번호, 카드번호, OTP, 보안카드 번호 등), 기타 중요정보라 판단되는 정보 등
WEB-SER-	MOB-SER-	HTS-SER-	021	5.8.4 (일반공통) 서비스 보호	자동화공격	5	○ 시스템 자원 고갈, 비용 발생 등 서비스 운영상 영향을 미칠 수 있는 기능(SMS, 이메일 발송, 계좌인증 호출, 글쓰기, 파일 업로드 등)에 대해 반복된 호출 가능 여부를 점검 * (평가 예시) - 자동화 도구를 이용하여 SMS 발송, 계좌인증(1원이체) 호출, 글쓰기 등의 반복된 작업 수행 가능 여부 점검 등

평가항목ID			Sub NUM	통제구분	평가항목	위험도	상세설명
WEB	Mobile	HTS					
WEB-SER-		HTS-SER-	022	5.8.4 (일반공통) 서비스 보호	버퍼오버플로우 (Buffer Overflow Attack)	5	○ C언어의 strcpy, gets 등과 같이 버퍼의 경계 검사를 하지 않는 취약한 함수를 사용함으로써 발생되는 취약점으로, 해당 취약점을 통해 시스템 권한 획득, 프로그램 흐름 변경 등의 악의적인 행위 가능 여부를 점검 * (평가 예시) - 파라미터 입력 값에 허용 이상의 데이터 삽입 시 결함 발생 여부 점검 등
WEB-SER-		HTS-SER-	023	5.8.4 (일반공통) 서비스 보호	포맷스트링 (Format String Attack)	5	○ C언어의 printf와 같은 함수에서 검증되지 않은 입력값을 사용함으로써 발생되는 취약점으로, 해당 취약점을 통해 다른 메모리 공간에 대한 접근 가능 여부를 점검 * (평가 예시) - printf 와 같은 취약한 함수 사용 시 별도의 문자열 검증 수행 여부 점검 등
WEB-SER-			024	5.8.7 (일반공통) 데이터 보호	단말기 브라우저 영역 내에서의 중요정보 노출	5	○ 단말기 브라우저 영역 내에서의 중요정보 평문 노출 유무 여부를 점검 * (평가 예시) - 개발자 도구 등을 통해 이용자 구간 내 중요정보 평문 노출 유무 점검 등 * 웹 영역 : 웹을 구성하는 HTML, Javascript, DOM 등 웹을 표현하기 위한 영역 * 중요정보 : 비밀번호(로그인 비밀번호 등)
	MOB-SER-		025	5.8.6 (일반공통) 단말 보안	앱 소스코드 내 운영정보 노출 여부	5	○ 앱 소스코드 내 운영정보 노출 여부를 점검 * (평가 예시) - 애플리케이션을 디컴파일 및 역분석하여 코드상에 운영정보의 노출 여부 점검 등 * 운영정보 : 서버정보(ID/PW), 고정된 암호키 등

평가항목ID			Sub NUM	통제구분	평가항목	위험도	상세설명
WEB	Mobile	HTS					
	MOB-SER-		026	5.8.6 (일반공통) 단말 보안	화면 강제실행에 의한 인증단계 우회	5	○ 화면강제 실행, 인증관련 파일 조작 등을 통해 인증단계 우회 가능 여부를 점검 * (평가 예시) - 인텐트(Intent), Cycript 등 화면 강제 실행이 가능한 기능 및 도구를 이용하여 화면강제 실행 시 서비스 정상 사용가능 여부 점검 - 인증 관련 파일 존재 시 해당파일 조작을 통해 인증단계 우회 가능 여부 점검 등
WEB-SER-	MOB-SER-	HTS-SER-	027	5.8.7 (일반공통) 데이터 보호	데이터 평문전송	4	○ 네트워크 데이터 전송 시 중요정보 평문전송 여부를 점검 * (평가 예시) - 패킷 스니핑 및 웹 프록시 도구를 이용하여 중요정보 평문 노출 여부 점검 등 * 중요정보 : 고유식별정보(주민등록번호), 비밀번호(로그인 비밀번호, 계좌 비밀번호, 공인인증서 비밀번호 등), 신용정보(보안카드번호, OTP번호, 카드번호 등) 등
WEB-SER-	MOB-SER-		028	5.8.4 (일반공통) 서비스 보호	크로스사이트 요청변조 (CSRF)	4	○ 공격자가 업로드 한 악의적 행위 구문으로 인해 타 이용자의 권한 도용이 가능한지에 대한 점검 * (평가 예시) - 타 이용자의 권한으로 실행하고자 하는 구문*을 업로드 후 해당 이용자 권한으로 구문이 실행되는지 가능 여부 점검 등 ※ 일반적으로는 스크립트 구문이 많이 사용되나, 다른 방식 사용 가능

평가항목ID			Sub NUM	통제구분	평가항목	위험도	상세설명
WEB	Mobile	HTS					
WEB-SER-	MOB-SER-		029	5.8.4 (일반공통) 서비스 보호	디렉토리 목록 노출	4	○ 인덱스 파일로 지정한 파일이 존재하지 않거나, 디렉토리 리스팅을 허락하도록 설정했을 경우 디렉토리 리스트가 출력됨에 따라 하위 파일 및 디렉토리 목록의 출력 여부를 점검 * (평가 예시) - URL에 디렉터리 명을 입력 했을 경우 하위 파일 및 디렉터리의 목록의 출력 여부 점검 등
WEB-SER-			030	5.8.4 (일반공통) 서비스 보호	서버 인증서 무결성 검증	3	○ 서버 인증서의 무결성 조건이 위배될 경우, 웹브라우저에서 안전하지 않은 웹사이트로 경고하여 이용자의 신뢰를 떨어트릴 수 있음으로 서버 인증서 무결성 점검 * (평가 예시) - 이용자PC 브라우저에서 서버 인증서 유효기간이 만료되어 안전하지 않은 웹사이트로 경고 여부 점검 - CN값과 서비스URL이 일치하지 않아 안전하지 않은 웹사이트로 경고 여부 점검 - 서버 인증서 발급기관(CA)이 신뢰할 수 없는 기관이거나, 자체 서명(Self-signed)된 인증서를 사용 여부 점검 등
WEB-SER-	MOB-SER-	HTS-SER-	031	5.8.4 (일반공통) 서비스 보호	시스템 운영정보 노출 여부	4	○ 웹 서버의 소스 코드 및 오류 메시지를 통한 정보 노출 가능성이 존재하며, 시스템 운영정보 노출 여부를 점검 * (평가 예시) - 개발자 도구 및 웹 프록시 도구를 이용하여 서버로 부터 중요정보의 전달 여부 점검 - 에러 발생 시 절대 경로 주소나 웹서버 버전 정보 등이 발생 여부 점검 등

평가항목ID			Sub NUM	통제구분	평가항목	위험도	상세설명
WEB	Mobile	HTS					
WEB-SER-	MOB-SER-	HTS-SER-	032	5.8.5 (일반공통) 이용자 인증	인증 오류 횟수 제한기능 제공 여부	3	○ 무작위 대입 공격에 의한 인증 우회, 인증정보 유출 등의 위협에 대응하기 위해, 이용자가 입력하는 인증 요청에 대한 오류 횟수 제한 여부를 점검 * (평가 예시) - 금융회사가 정한 오류횟수 이상으로 오인증 후 해당 계정의 상태 (서비스 이용 제한, 인증수단 폐기, 다른 인증방법으로 전환 등)를 확인 - 전자금융거래에 사용되는 비밀번호의 경우 5회 이내의 범위에서 미리 정한 횟수 이상의 비밀번호 입력 오류가 발생할 경우 즉시 사용 금지 필요(전자금융감독규정 제33조 이용자 비밀번호 관리)
WEB-SER-	MOB-SER-	HTS-SER-	033	5.8.5 (일반공통) 이용자 인증	불충분한 세션종료 처리	4	○ 세션종료 시간 미설정 또는 과도한 세션 종료 설정 여부를 점검 * (평가 예시) - 이용자 로그인 후 일정시간 이후 동일 세션으로 접속 가능 여부 점검 등 (참고) 주요 통신기반시설 가이드에는 세션 종료 시간을 10분 설정할 것을 권고
WEB-SER-			034	5.8.7 (일반공통) 데이터 보호	취약한 HTTPS 프로토콜 이용	3	○ 취약한 버전의 암호 프로토콜 사용 시 암호화된 통신 내용이 유출될 수 있어 취약한 버전의 SSL(SSL 2.0, 3.0) 사용 여부를 점검 * (평가 예시) - 취약한 버전의 SSL(SSL 2.0, 3.0) 사용 가능 여부 점검 등
WEB-SER-			035	5.8.7 (일반공통) 데이터 보호	취약한 HTTPS 암호 알고리즘 이용	3	○ 보안강도가 낮은 암호 알고리즘을 사용할 경우, 중간자 공격 등에 의해 암호화된 통신 내용이 유출 될 수 있는 위협이 발생될 수 있으므로, 암호 알고리즘의 보안 강도의 적절성 여부를 점검 * (평가 예시) - 보안 강도가 낮은 암호알고리즘 사용 여부 점검 등

평가항목ID			Sub NUM	통제구분	평가항목	위험도	상세설명
WEB	Mobile	HTS					
WEB-SER-			036	5.8.7 (일반공통) 데이터 보호	취약한 HTTPS 컴포넌트 사용	3	○ 취약한 HTTPS 확장 모듈 사용 시 암호화된 정보 노출 등의 위협이 존재함에 따라 이에 대한 취약점 존재 유무 점검 * (평가 예시) - HTTPS 관련 주요 취약점(CVE-2014-0160:Heartbleed, CVE-2014-0224: OpenSSL, SSL Strip)의 존재 여부 점검 등 * CVE-2014-0160 : OpenSSL의 라이브러리에 버그가 존재하여 서버내 중요 메모리 데이터가 노출될 수 있는 취약점 * CVE-2014-0224 : OpenSSL 통신 상의 CCS(ChangeCipherSpec) 메시지 처리과정 중 취약점이 있어 암호화된 정보의 노출 및 변조 가능성이 존재하는 취약점 * SSL Strip : 서버에서 HSTS 기능을 설정하지 않아, HTTP프로토콜로 접속이 가능한 취약점
WEB-SER-			037	5.8.7 (일반공통) 데이터 보호	취약한 HTTPS 재협상 허용	2	○ 암호화된 통신내용이 노출될 가능성이 존재하는 취약한 방식의 HTTPS 재협상(Renegotiation)을 허용 여부를 점검 * (평가 예시) - SSLTEST 결과 insecure client-initiated renegotiation 값 점검 등 (ex. No - 양호, supported - 미흡)
WEB-SER-			038	5.8.4 (일반공통) 서비스 보호	불필요한 웹 메서드 허용	1	○ 웹 서비스에서 사용하지 않는 메서드 허용 여부를 점검 * (평가 예시) - 메서드를 변경하여 실제 요청 시 정상 기능 작동 여부 점검 - 최상위 경로 외에 하위 경로에서도 동일하게 테스트 수행(설정 환경이 다른 경우가 존재) 등

평가항목ID			Sub NUM	통제구분	평가항목	위험도	상세설명
WEB	Mobile	HTS					
WEB-SER-	MOB-SER-	HTS-SER-	039	5.8.4 (일반공통) 서비스 보호	관리자 페이지 노출 여부	4	○ 일반 이용자에 의한 관리자 페이지 접근 가능 여부를 점검 * (평가 예시) - 알려진 관리자 페이지 및 유추 가능한 페이지 경로에 대해 접근 가능 여부 점검 등
WEB-SER-	MOB-SER-	HTS-SER-	040	5.8.4 (일반공통) 서비스 보호	불필요한 파일 노출 여부	4	○ 서버 운영상 불필요한 파일의 존재 여부를 점검 * (평가 예시) - 무작위 대입 또는 잘 알려진 경로 대입 등을 통해 불필요한 파일(샘플 파일, 테스트 파일, 백업 파일 등)의 존재 여부 점검 등
WEB-SER-	MOB-SER-		041	5.8.4 (일반공통) 서비스 보호	크로스 사이트 스크립팅 (XSS)	4	○ 공격자가 업로드한 스크립트가 타 이용자의 사용환경(브라우저, 웹뷰 등)에서의 실행 가능 여부를 점검 * (평가 예시) - 크로스사이트 스크립팅 문자열을 데이터베이스에 저장된 값을 확인할 수 있는 페이지에 업로드 시, 해당 스크립트의 실행 여부 점검 등
	MOB-SER-		042	5.8.6 (일반공통) 단말 보안	디버그 로그 내 중요정보 노출 여부	5	○ 디버그 로그 내 중요정보 노출 여부를 점검 * (평가 예시) - DDMS 등 디버그 로그를 확인 할 수 있는 도구를 이용하여 디버그 로그 내 중요정보 노출 여부 점검 등 * 중요정보 : 개인정보(주민등록번호), 금융정보(비밀번호, 카드번호, OTP, 보안카드 번호 등), 기타 중요정보라 판단되는 정보

평가항목ID			Sub NUM	통제구분	평가항목	위험도	상세설명
WEB	Mobile	HTS					
	MOB-SER-		043	5.8.6 (일반공통) 단말 보안	백그라운드 화면 보호	3	○ 실행 중이던 애플리케이션이 백그라운드 상태로 진입할 때 저장되는 스냅샷 파일 내 중요정보 노출 여부를 점검 * (평가 예시) - 별도의 화면 또는 뷰속성 변경없이 백그라운드 상태 진입 이전 화면이 스냅샷이 파일 내 중요정보 존재 여부 점검 등
WEB-FIN-			025	5.8.3 (전자금융) 단말 보안	[전자금융] 단말기 브라우저 영역 내에서의 중요정보 노출	5	○ 단말기 브라우저 영역 내에서의 중요정보 기밀성 확보 여부를 점검 * (평가 예시) - 개발자 도구 등을 통해 이용자 구간 내 중요정보 평문 노출 유무 점검 등 * 웹 영역 : 웹을 구성하는 HTML, Javascript, DOM 등 웹을 표현하기 위한 영역 * 중요정보 : 고유식별정보(주민등록번호), 비밀번호(로그인 비밀번호, 계좌 비밀번호, 공인인증서 비밀번호 등), 신용정보(보안카드번호, OTP번호, 카드번호 등) 등
WEB-SER-	MOB-SER-		046	5.8.4 (일반공통) 서비스 보호	서버 사이드 요청 위조 (SSRF)	4	○ 외부에서 접근 가능한 서버에서 전송하는 요청 메시지 파라미터(IP,URL 등) 값을 변조하여, 공격자가 직접 접근할 수 없는 네트워크 대역(내부망 등)에 위치한 서버에서 변조된 요청 메시지에 대해 응답값이 반환되는지 여부를 점검
WEB-SER-	MOB-SER-	HTS-SER-	048	5.8.4 (일반공통) 서비스 보호	세션정보 재사용	3	○ 세션ID, 토큰 등을 절취 후 타 이용자의 이용 환경에서 해당 값을 이용하여 권한이 필요한 페이지에 정상 접근 및 권한 우회 가능 여부를 점검 * (평가 예시) - 로그인 수행 후 해당 세션ID를 획득 후, 별도의 IP 주소를 사용하는 단말에서 사용 시 해당 이용자의 권한으로 서비스 이용 가능 여부를 점검 등 - OAuth, SSO 등에서 사용하는 토큰 정보를 획득 후, 별도의 IP 주소를 사용하는 단말에서 사용 시 해당 이용자의 권한으로 서비스 이용 가능 여부를 점검 등

평가항목ID			Sub NUM	통제구분	평가항목	위험도	상세설명
WEB	Mobile	HTS					
WEB-SER-	MOB-SER-	HTS-SER-	026	5.8.3 (전자금융) 단말 보안	[전자금융] 통신구간 암호화 적용 여부	5	○ 이용자 단말과 거래 및 인증을 수행하는 서버간 데이터 보호를 위해 안전한 통신 프로토콜 이용 여부를 점검 * (평가 예시) - 전자금융거래 시 통신구간 암호화(tls) 적용 여부를 점검
WEB-FIN-	MOB-FIN-	HTS-FIN-	027	5.8.1 (전자금융) 거래 인증	[전자금융] 접근매체 발급 시 실명확인 수행 여부	5	○ 비인가자에 의한 접근매체 무단 발급에 대응하기 위해 접근매체 발급 시 실명확인 수행 여부를 점검 * (평가 예시) - 접근매체 발급 시 실명확인 수행 여부를 점검 ※ 실명확인 수행 방법 - (필수) ① 신분증 사본 제출, ② 영상통화, ③ 접근매체 전달시 확인, ④ 기존계좌 활용, ⑤ 기타 이에 준하는 새로운 방식(생체인증 등) 중 2가지 이상 의무 적용 - (권고) ⑥ 타 기관 신원확인 결과 활용(휴대폰 본인확인 등), ⑦ 다수의 개인정보 검증 ※ 접근매체 : 전자금융거래에 있어서 거래지시를 하거나 이용자 및 거래내용의 진실성과 정확성을 확보하기 위하여 사용되는 수단 또는 정보
WEB-SER-	MOB-SER-	HTS-SER-	049	5.8.4 (일반공통) 서비스 보호	인증수단 소유자 검증 여부	5	○ 타 이용자 소유의 인증수단을 이용한 인증 수행 가능 여부를 점검 * (평가 예시) - 인증서 사전 등록(등록·변경) 시, 타 이용자 명의의 인증서 등록 후 인증 우회 가능 여부 점검 - 타 이용자 명의의 전화번호 이용 또는 사전 등록하여 인증(SMS, ARS 등) 수행 가능 여부 점검 - 타 이용자 명의의 계좌 번호를 입력하여 계좌 인증 수행 가능 여부 점검 - 타 이용자 명의의 OTP 등록 가능 여부 점검 - 타 이용자의 인증서를 이용한 전자서명 가능 여부 점검 등

전자금융기반시설
보안 취약점 평가기준 안내서 (제2022-1호)

발 행 : 2021년 12월
발행인 : 김 철 웅
발행처 : 금융보안원, 보안평가부 (보안평가기술팀)
주 소 : 경기도 용인시 수지구 대지로 132

〈비 매 품〉

• 상기 내용과 관련하여 궁금한 사항은 이메일(fsat@fsec.or.kr)로 문의하시기 바랍니다.

금융미래를 열어가는 금융보안파트너

안전하고 편리한 금융미래, 금융보안원이 열어가겠습니다.

금융보안원
FINANCIAL SECURITY INSTITUTE

(본원) 경기도 용인시 수지구 대지로 132 금융보안원
(교육센터) 서울특별시 영등포구 의사당대로 143 금투센터 8층
TEL 1577-6659 **FAX** 02-3495-9789