로보어드바이저 테스트베드 설명회

○ 일시 : 2017년 3월 10일(금) 10시

○ 장소 : 코스콤 3층 핀테크 세미나룸

Robo Advisor
TEST BED CENTER

목 차

1. 참여 요강

2. 자가 평가서

3. 제출자료 목록

4. 시스템 보안성심사 안내

5. RA테스트베드 관련 한국예탁결제원 업무 프로세스 안내

6. [보도자료]로보어드바이저 테스트베드 기본운영방안

로보어드바이저 테스트베드
참여 요강

- 제2차 정기심사 -

Robo Advisor
TEST BED CENTER

1 참여자 자격조건

□ 다음 유형에 해당하는 로보어드바이저(이하 RA) 기술을 보유한 업체에 한해 로보어드바이저 테스트베드에 참여가능 함

○ **RA 기술보유 업체**(자문·일임업 未등록자, 법인)

○ 자체 개발한 RA 기술을 이용하여 직접 자문·일임서비스를 제공하고자 하는 **자문·일임업자**(겸영 은행·증권사 포함)

○ **RA 기술보유 주체**(RA 전문자문사, RA 기술업체 등)와 **서비스 제공 주체**(자문·일임 겸영 은행·증권사 등)로 구성된 **컨소시움**

2 참여 알고리즘 조건

□ 알고리즘별로 참여하여야 하며, 한 업체가 복수의 알고리즘도 신청 가능

□ 테스트베드 참여 알고리즘은 자동화 요건과 운용자산 요건을 기본적으로 충족하여야 함

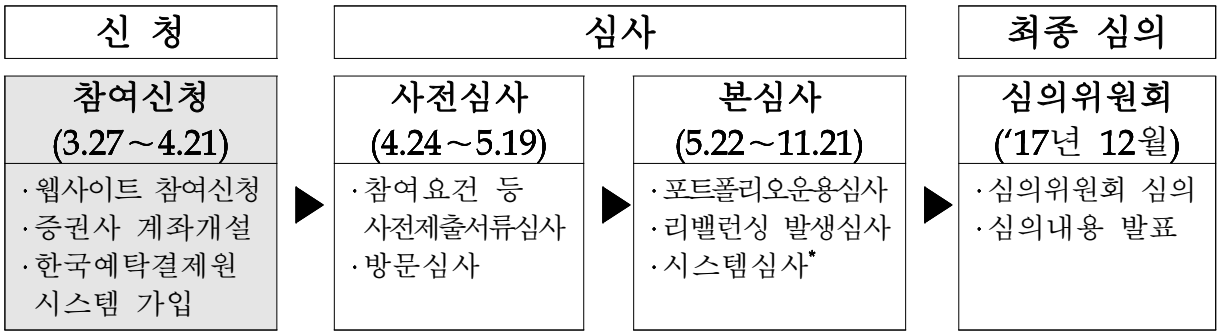
○ **(자동화 요건)** 원칙적으로 투자자 성향분석(프로파일링), 자산배분, 포트폴리오 산출, 리밸런싱 등의 과정에서 사람의 개입 없이 전산시스템만으로 서비스 제공이 가능해야 함

○ **(운용자산 요건)** 펀드(ETF 포함), 파생결합증권(ELS, ETN, DLS 등), 주식으로 운용하여야 하며, 하나 또는 복수의 자산군으로 포트폴리오 구성 가능

- 대기성 자금인 경우 예금, RP 등의 포트폴리오 편입 허용
  * 채권, 파생상품은 운용대상 자산에서 제외
- 사전심사시작일 기준 거래 가능한 금융투자자산만 편입 가능

※ 금융위원회 2016.8.29 보도자료 [맞춤형 자산관리서비스의 대중화 시대를 열게 될 로보어드바이저 테스트베드 기본 운영방안] 참고

3 심사 프로세스



* 상용화시 **로보어드바이저 서비스의 대고객 전달체계**에 대한 **안정성·보안성** 등 시스템 심사

1 **(참여신청)** 테스트베드 웹사이트를 통해 **참여신청서와 신청서류**를 **온라인으로 제출**

○ 일정 : '17. 3. 27 ~ 4. 21 (18시 마감)

2 **(사전심사) 참여 업체 유형에 따른 요건, 알고리즘의 자동화 요건, 운용자산 요건** 등에 대한 서류 및 현장 심사

○ 일정 : '17. 4. 24 ~ 5. 19

* 사전심사 통과참여자만 본심사 진행가능

3 **(본심사)** 일정기간 동안 실제 자금을 운용하여 **알고리즘의 안정성**을 심사

○ 일정 : '17. 5. 22 ~ 11. 21

○ 수익률 등 공개정보는 웹사이트를 통해 공표

4 **(심의위원회)** 테스트베드 참여 RA 알고리즘에 대한 심사보고서 심의 및 **테스트베드 통과여부 최종 결정**

○ 일정 : '17년 12월 (예정)

4 참여 신청 절차

① 테스트베드 웹사이트 회원가입 및 알고리즘 심사 참여신청
② 증권사 및 한국예탁결제원 계좌 개설
③ 테스트베드 웹사이트 정보입력 및 접수확인

웹사이트 회원가입 및 심사 참여신청	① 테스트베드 웹사이트(www.RAtestbed.kr) 회원가입 (컨소시움인 경우 서비스 제공주체의 명의) ② 알고리즘 심사 참여신청 ③ 심사 참여신청 확인증 발급 (한국예탁결제원 제출용) ④ 사전심사용 자료제출(별도 목록 참고)
증권사 및 한국예탁결제원 계좌개설	⑤ 한국예탁결제원 RA테스트베드 참가용 계좌개설 및 업무 참가신청, 업무대리인 등록신청* - 한국예탁결제원 서울사옥 방문 - 자산관리플랫폼(MAP) 이용 계좌 개설 ⑥ 한국예탁결제원 RA테스트베드 참가용 수익률산출(PICA) 서비스 계약체결 및 시스템 설치 - MAP 미사용자산군(예:해외주식, 해외ETF 등) 운용 시 투자 유니버스(Investment Universe) 목록 제출
	⑦ 증권사에 참여자 명의계좌**(일임투자계좌 또는 MAP 시스템을 사용가능한 계좌) 총 9개 개설 (동일 증권사에 개설)
	⑧ 한국예탁결제원 MAP시스템에 RA 투자일임업자 정보 및 일임계좌정보 등록
웹사이트 정보입력 및 접수확인	⑨ 한국예탁결제원 개설정보(투자자문사별 전용계좌번호 등) 증권사 계좌정보 입력 및 사전심사자료 보완제출 ⑩ 사무국 접수확인

* 첨부된 "RA 테스트베드 계좌 수익률 산출을 위한 한국예탁결제원 업무 프로세스 안내" 참조

** RA기술보유업체 단독참여인 경우 임원자금으로 운용 가능

5 운용 자료 제출 및 확인

□ **(자료 제출 의무)** 일일 거래 종료 후 거래내역/잔고내역 등을 한국예탁결제원을 통해 사무국에 제출하여야 하며, 증권사를 통해 대행 제출하더라도 자료의 정합성에 대해서는 참여자가 확인하여야 함

- ㅇ 일일 거래 종료 후 한국예탁결제원 시스템(MAP 및 PICA)을 통해 **거래내역·잔고내역 등의 정상 반영여부를 확인**하고 오류발생시 수정 및 등록 처리
- ㅇ **테스트베드 웹사이트의 공개되는 자료의 정합성을 확인**하고, 오류발생시 관련기관과 협의하여 수정 되도록 요청

□ **(리밸런싱)** 포트폴리오 운용 중 분기별 1회 이상 리밸런싱이 발생하여야 하며 발생내역을 웹사이트를 통해 사무국에 제출

6 유의 사항

□ **(심사 범위)** RA테스트베드 심사는 알고리즘의 안정성 뿐만 아니라 투자자 성향분석(프로파일링), 자산배분, 리밸런싱 등의 과정에서 **사람의 개입없이 전산시스템**만으로 **서비스 제공이 가능한지**를 중점적으로 심사함

□ **(MAP 미활용 자산) 펀드, 해외자산**을 운용중인 참여자는 증권사에서 한국예탁결제원에 자료가 대행 제출되지 않으므로, 한국예탁결제원 수익률산출시스템(PICA)에 일일 거래내역·잔고내역 등을 직접 등록하여야 하며, 이를 확인하기 위하여 사무국 요청 시 관련 증빙자료를 제출하여야 함

□ **(사후관리)** 심사 종료 후에도 테스트베드에 참여하여야 함

- ㅇ 심사 종료 후 운용중인 포트폴리오를 유형별로 1계좌씩 유지
- ㅇ 알고리즘 변경 시 테스트베드를 통해 변경내역을 공개

□ **(채권평가사와 업무 계약)** 투자유니버스에 ELS상품을 포함하여 운용할 참여자는 반드시 채권평가사와 계약을 하여야 함

□ **(계좌 재활용 불가)** 이전 테스트베드에서 사용하던 계좌 재활용 불가. 반드시 계좌를 신규 개설하여 참여하여야 함

□ **(입출금 처리)** 예탁금 사전 입금 금지. 포트폴리오 운용심사시작 직전 영업일(2017.5.19)에 입금하여야 하며, 포트폴리오 운용심사 기간 중에는 예탁금 입출금 불가

- ㅇ 동일유형 3계좌 간 30%이상 차등화된 금액으로 입금

  예) 안정추구형 3계좌 입금금액 : 70만원, 100만원, 130만원

8 참여 수수료

□ 참여수수료 : 50만원(알고리즘별, 부가세 포함)

□ 납부기한 : 사전심사 시작 후 2주 이내 납부('17.5.8까지)

○ 회원가입 시 등록한 담당자 이메일로 세금계산서 발행 예정

※ 참여수수료 미납 시 신청취소 처리함(본심사 참여 불가)

9 접수 및 문의처

□ 접수 : 로보어드바이저 테스트베드 사무국

○ 접수 홈페이지 : www.RAtestbed.kr

○ 이 메 일 : RAtestbed@koscom.co.kr

□ 문의처

○ 사 무 국 : 02) 767-7979

○ 금융감독원 : 02) 3145-6703

○ 금융보안원 : 02) 3495-9621

로보어드바이저 테스트베드
자가 평가서

- 제2차 정기심사 -

Robo Advisor
TEST BED CENTER

로보어드바이저 테스트베드 자가 평가서

Ver 1.1

2017년 4월 27일

○ 본 자가 평가서는 RA테스트베드 상세심사지침을 활용하여 심사참여시 참고해야 할 사항을 정리한 문서입니다.

Robo Advisor
TEST BED CENTER

1. 주요 심사 항목

심사 항목	심사항목의 주요 내용
테스트베드 참여요건	테스트베드 참여 업체 요건, 알고리즘의 자동화, 운용자산 요건을 충족해야 함
알고리즘의 합리성	알고리즘의 운용목표, 주요전제 등에 대해 설명이 가능하고, 알고리즘 테스트 결과가 신뢰 가능한 수준이어야 함
개인 맞춤성	투자자성향 분석 도구가 투자자의 투자목적, 위험감수능력 등 다양한 측면을 고려하여야 하며, 투자자성향 분석에 따라 유의미하게 구분되는 복수의 포트폴리오가 산출되어야 함
포트폴리오 산출	최소 5개 이상의 상품·종목으로 구성된 포트폴리오가 자동으로 산출되어야 함
유지·보수 전문인력	알고리즘, 시스템을 시의 적절하게 업그레이드하고 지속적으로 관리할 수 있는 IT 전문 인력을 1인 이상 보유하여야 함
합리적인 리밸런싱	리밸런싱 발생기준·원칙이 수립되어 있고, 이에 기반하여 리밸런싱이 유효하게 발생하여야 함
다계좌 동시 관리	복수 계좌를 동시에 운용하더라도 알고리즘이 오류 없이 정상적으로 작동하여야 함
법규 준수성	알고리즘이 법령에서 금지하는 투자(예: 투자자 동의 없는 계열회사 증권 투자)를 자체적으로 제한할 수 있어야 함
시스템 보안성	알고리즘, 주문내역, 투자자 개인정보 등 RA의 핵심정보에 대한 해킹 방지 시스템을 보유해야함
시스템 안정성	알고리즘, 시스템 장애 발생시 체계적으로 대응할 수 있는 비상조치매뉴얼·시스템 등 보유해야 함

2. 심사항목 상세

심사항목	주요 심사 내용	심사번호	심사방법	심사주체	심사자료
테스트베드 참여요건	① 테스트베드 참여업체 요건을 충족해야 함	P0-01-DE	서면	사무국	법인등기부 등본 자문·일임업 등록 증빙서류
	② 알고리즘 자동화 요건을 충족해야 함	P0-02-DE	서면	사무국	각 단계별 증빙화면
알고리즘의 합리성	① 알고리즘의 운용목표, 주요전제 등에 대해 합리적인 수준에서 설명 가능해야 함	P1-01-DE	서면	사무국	알고리즘 설명서
	② 백테스팅 결과가 합리적으로 신뢰 가능한 수준이어야 함	P1-02-DE	서면	사무국	백테스팅 결과자료
	③ 리밸런싱 발생기준·원칙이 수립되어 있으며 사용자에게 쉽게 전달되어야 함	P1-03-DE	서면	사무국	알고리즘 설명서
개인 맞춤성 I	① 투자자의 투자목적, 재산상황, 투자경험, 위험감수 능력 등 다양한 측면을 고려하여 투자자성향을 분석해야 함	P2-01-DE	서면	금감원	알고리즘 설명서
	② 설명된 투자자성향 분석 툴이 알고리즘으로 구현되어 있어야 함	P2-03-PE	현장실사	사무국	알고리즘 설명서 전산화면
	③ 입력한 다양한 투자자정보에 따라 차별화된 포트폴리오가 자동 산출되어야 함	P2-04-PE	현장실사	사무국	알고리즘 설명서 전산화면
포트폴리오 산출	① 포트폴리오별 최소 5개 이상의 상품·종목이 산출되어야 함	P3-01-PE	현장실사	사무국	알고리즘 설명서
유지·보수 전문인력	① IT 전문인력을 1인 이상 보유하고 있어야 함	P4-01-PE	현장실사	사무국	경력확인서
개인 맞춤성 II	① 산출된 자산배분 비율대로 실제 운용되어야 함	P5-01-EE	운용	사무국	알고리즘 설명서 매매/잔고내역 운용전 포트폴리오 산출내역
	② 투자자 성향에 따라 산출된 포트폴리오는 운용과정에서 차별성을 유지하여야 함	P5-02-EE	운용	사무국	
합리적인 리밸런싱	① 사전에 제시된 리밸런싱 원칙에 부합하도록 리밸런싱이 발생되어야 함	O1-01-EE	운용	사무국	리밸런싱 발생내역 알고리즘 설명서 투자유니버스 자료
	② 리밸런싱 후 금융상품별 배분된 투자금액이 자산군별 투자비중에 부합되어야 함	O1-02-EE	운용	사무국	
	③ 리밸런싱 실시 결과 자료는 정합성을 확인한 후 기한 내 제출하여야 함	O1-03-EE	운용	사무국	

심사항목	주요 심사 내용	심사번호	심사방법	심사주체	심사자료
다계좌 동시관리	① 동일한 포트폴리오를 다수 계좌에서 운용함에 있어 알고리즘 오류가 발생하지 않아야 함	O2-01-EE	운용	사무국	계좌별 운용내역 전산화면
법규 준수	① 알고리즘이 자본시장법상 불건전 영업행위 금지조항에 저촉되지 않도록 설계되어 있어야 함	O3-01-DE	서면	금감원	법규준수 설명자료
	② 설명된 법규준수 장치들이 알고리즘에 제대로 구현되어 운용되어야 함	O3-02-PE	현장실사	사무국	일일 운용내역
시스템 안정성	① 시스템운영매뉴얼과 비상조치매뉴얼이 적정하게 유지관리되어야 함	S1-01-SE	현장실사	사무국	시스템운용매뉴얼 비상조치매뉴얼
	② 알고리즘, 시스템 장애발생을 신속히 인지할 수 있는 모니터링 체계를 갖춰야 함	S1-02-SE	현장실사	사무국	시스템운용매뉴얼 장애상황기록부
	③ 비인가자에 대한 시스템 접근통제 방안을 수립하고 주기적 예방관리를 실시해야 함	S1-03-SE	현장실사	사무국	시스템운용매뉴얼 비밀번호 관리대장 유지보수 관리대장
	④ 변경을 위한 절차가 마련되어 있어야 함	S1-04-SE	현장실사	사무국	형상관리절차서
	⑤ 상용화를 위한 화면이 구현되어 있어야 함	S1-05-SE	현장실사	사무국	전산구현화면
시스템 보안성	① 이용자 및 계좌 소유주 인증 과정이 적정하게 설계되어 있어야 함	S2-01-DE	서면	금보원	보안대책명세서
	② 중요정보(개인정보, 금융정보, 패스워드 등)의 보호대책이 적정하게 수립·이행되어야 함	S2-02-DE	서면	금보원	보안대책명세서
	③ 시스템에 대한 물리적 통제가 적정하게 관리되어야 함	S2-03-SE	서면,현장실사	금보원	보안대책명세서 보호구역 출입자 관리 기록부 보호구역 작업관리 기록부 보호구역 시스템 반출반입 기록부
	④ 시스템에 대한 기술적 통제가 적정하게 관리되어야 함	S2-04-SE	서면,현장실사	금보원	보안대책명세서
	⑤ 중요PC(관리자 PC, 개발 PC 등)가 적정하게 통제·관리되어야 함	S2-05-SE	서면,현장실사	금보원	보안대책명세서
	⑥ 네트워크가 적정하게 통제·관리되어야 함	S2-06-SE	서면,현장실사	금보원	보안대책명세서

[○○○] 자가 평가서

□ 업체명 :

항 목	심사번호	상세 심사 내용	확인결과
① 자동화요건	P0-02-DE	① 투자자 위험성향・투자목적 분석(프로파일링)이 자동화 되어 있는가?	□예 □아니오
		② 투자자성향・투자목적에 따른 자산군별 투자비중 결정(자산배분)이 자동화 되어 있는가?	□예 □아니오
		③ 투자대상 금융상품 선정(포트폴리오 셀렉션)이 자동화 되어 있는가?	□예 □아니오
		④ (선택)주문집행 처리과정이 자동화 되어 있는가? ⇒ 참여 업체의 선택에 따라 자동화 시스템 구축 여부에 대한 심사 가능	□예 □아니오
		⑤ 리밸런싱 처리과정이 자동화 되어 있는가?	□예 □아니오
② 알고리즘 합리성	P1-01-DE	① 알고리즘 설명 자료에 적용기술・특징・운용목표 등이 기재되어 있는가?	□예 □아니오
		② 자산 배분의 주요 전제사항이 설명되어 있는가? ⇒ 예: 동일 자산군(집합투자증권 제외)에는 50%를 초과하지 않고 동일 종목에는 30%를 초과하지 않는다	□예 □아니오
		③ 포트폴리오 유형에 따라 금융상품의 종류・비중・위험도 등 자산을 배분하는 방법 등이 기재되어 있는가?	□예 □아니오
		④ 투자유니버스가 적정하게 기재되어 있는가?	□예 □아니오
		⑤ 포트폴리오 유형에 따른 포트폴리오간 차별성에 관한 사항이 설명되고 있는가?	□예 □아니오
		⑥ 포트폴리오별 위험도 산정방식이 기재되어 있는가?	□예 □아니오
		⑦ 운용중 위험을 회피하는 방안이 제시되고 있는가?	□예 □아니오
③ 백테스팅 결과	P1-02-DE	① 백테스팅 결과자료에 과거 일정기간(2008년 이후, 1년 이상) 동안의 자산배분 및 포트폴리오에 대한 모의실험 결과가 포함되어 있는가?	□예 □아니오
		② 포트폴리오 유형(안정추구형/위험중립형/적극투자형 등)별로 실험 결과가 나뉘어 있는가?	□예 □아니오
		③ 과거 자산배분 모의실험 결과는 포트폴리오유형별 자산배분 규칙 내에 있는가? ⇒ 포트폴리오 유형별 자산배분 규칙에 채권형ETF를 30% 초과할 수 없도록 했다면 결과자료에서 이의 확인이 가능 할 것	□예 □아니오

항 목	심사번호	상세 심사 내용	확인결과
		④ 과거 포트폴리오 모의실험 결과는 포트폴리오유형별 금융상품의 종류·비중·위험도 등 자산 배분하는 규칙 내에 있는가? ⇒ 금융상품의 자산배분 규칙에 단일 종목이 30%를 못 넘도록 했다면 결과자료에서 이의 확인이 가능할 것	□예 □아니오
		⑤ (자산별 비중 또는 종목별 비중이 목표비중 이탈시) 리밸런싱을 통해 조정되고 있는가? ⇒ 알고리즘 설명서에 리밸런싱 주기가 목표비중 이탈이라고 기재되어 있을 경우에 한함	□예 □아니오
		⑥ 과거 모의실험 결과가 리밸런싱 원칙에 부합하는지 기술되어 있는가? ⇒ 리밸런싱 주기가 1개월이라면 1개월 단위로 리밸런싱된 결과가 확인 가능할 것	□예 □아니오
		⑦ 과거 모의실험 결과가 포트폴리오 유형(안정추구형/위험중립형/적극투자형 등)의 목표에 적합한지 기술되어 있는가? ⇒ 누적수익률 그래프 및 변동성 측면에서 포트폴리오 유형별 차이가 충분히 확인 가능할 것	□예 □아니오
④ 리밸런싱	P1-03-DE	① 알고리즘 설명 자료에 리밸런싱 발생기준 및 절차가 기재되어 있는가?	□예 □아니오
		② 분기별 1회 이상 리밸런싱 실시를 명시하고 있는가?	□예 □아니오
		③ 리밸런싱 시 투자자문의 내용 또는 투자일임재산의 안정성 및 수익성 평가를 하고 있는가?	□예 □아니오
		④ 리밸런싱 시 투자 대상자산의 종목·수량 등을 산출하는 방법은 투자자성향 분석결과를 고려하고 있는가?	□예 □아니오
		⑤ 리밸런싱 처리 결과의 투자자 통지방법을 명시하고 있는가?	□예 □아니오
⑤ 투자자 성향분석 설문내용	P2-01-DE	① 투자목적 관련 설문항목이 포함되어 있는가?	□예 □아니오
		② 재산상황 관련 설문항목이 포함되어 있는가?	□예 □아니오
		③ 투자경험 관련 설문항목이 포함되어 있는가?	□예 □아니오
		④ 투자위험 감수능력 관련 설문항목이 포함되어 있는가?	□예 □아니오
		⑤ 투자자의 연령에 대한 설문이 포함되어 있는가?	□예 □아니오
		⑥ 투자예정기간에 대한 설문이 포함되어 있는가?	□예 □아니오
		⑦ 투자자의 금융이해도(지식)에 대한 설문이 포함되어 있는가?	□예 □아니오
		⑧ 상기 항목 이외에 투자자 성향분석을 위한 설문항목이 있는가?	□예 □아니오
		⑨ 투자자 성향에 따른 분류기준 등이 설명되어 있는가?	□예 □아니오

항 목	심사번호	상세 심사 내용	확인결과
⑥ 투자자 성향분석 화면	P2-03-PE	① 투자자성향 분석을 위한 문답 절차를 투자자에게 전산화면으로 제공하고 있는가?	□예 □아니오
		② 전산화면의 질문 내용이 旣 제출한 문서상의 내용과 동일하게 구성되어 있는가?	□예 □아니오
		③ 질문에 대한 답변 입력완료 후 자동으로 투자자성향 분석결과를 투자자에게 전산화면으로 제공하고 있는가?	□예 □아니오
		④ 질문에 대한 답변 입력완료 후 제시된 투자자성향 분석결과는 旣 제출한 문서상의 투자자성향 분류에 포함되어 있는가?	□예 □아니오
		⑤ 旣 제출한 문서상의 모든 투자자성향 분류를 시연할 수 있는가?	□예 □아니오
⑦ 포트폴리오 산출	P2-04-PE	① 투자자 성향분석 화면이 구현되어 있는가?	□예 □아니오
		② 자산배분 화면이 구현되어 있는가?	□예 □아니오
		③ 포트폴리오 산출 화면(투자자용 또는 관리자용)이 구현되어 있는가?	□예 □아니오
		④ 리밸런싱 전/후 자산배분 및 포트폴리오 산출화면(투자자용 또는 관리자용)이 구현되어 있는가? ⇒ 포트폴리오 산출화면에는 종목코드, 종목명, 투자비중, 수량 등이 출력되어야 함	□예 □아니오
		⑤ 매매결과를 조회할 수 있는 화면이 구현되어 있는가?	□예 □아니오
		⑥ 투자자성향에 맞게 적합한 포트폴리오가 제시되었는지 설명 가능한가?	□예 □아니오
⑧ 포트폴리오 요건	P3-01-PE	① 포트폴리오별 5개 이상의 종목·상품이 산출되고 있는가? ⇒ 개별주식종목으로만 구성할 경우 10개 이상으로 산출하여야 함(대기성 현금은 종목・상품 수에 포함하지 않음)	□예 □아니오
		② 포트폴리오유형별 투자유니버스내 종목·상품으로 구성되어 있는가?	□예 □아니오
		③ 투자 불가능한 종목(채권, 파생상품)이 포함되지 않게 구성되어 있는가?	□예 □아니오
		④ 반복 수행(3번 이상)시에도 정상적으로 상품·종목이 산출되고 있는가? ⇒ 반복해서 화면에 정상적으로 표시되는지 여부를 확인. 실시간 데이터를 기반으로 작동되는 알고리즘의 경우 입력하는 시점에 따라 포트폴리오의 결과가 달라질 수 있으므로 결과 값이 바뀌는 부분은 정상으로 인정함)	□예 □아니오
		⑤ 포트폴리오의 예측되는 위험도를 제시하고 있는가? ⇒ 백테스트 결과를 기반으로 최대손실폭 또는 표준편차 등을 제시	□예 □아니오
		⑤-1 (위험도를 제시하지 않고 있다면) 위험도를 제시하지 않는 타당한 사유가 있는가?	□예 □아니오

항 목	심사번호	상세 심사 내용	확인결과
⑨ 유지·보수 전문인력	P4-01-PE	① 증빙서류상의 인력 현황과 동일한 인력을 보유하고 있는가?	□예 □아니오
		② 증빙서류상의 인력이 유지·보수 전문인력의 자격(첨부1참조)을 보유하고 있는가?	□예 □아니오
		③ 해당 인력이 RA관련 유지보수업무를 실제 수행하고 있는지 증명할 수 있는가?	□예 □아니오
⑩ 자산배분 비율대로 집행	P5-01-EE	① 구성된 포트폴리오가 실제로 운용되고 있는가?	□예 □아니오
		② 동일 포트폴리오를 운용하는 모든 계좌의 실제 자산취득 내역이 해당 포트폴리오의 구성 원칙대로 구성되어 있는가?	□예 □아니오
		②-1 (포트폴리오 구성 원칙대로 운용되지 않은 경우) 그 사유를 합리적으로 설명할 수 있는가?	□예 □아니오
⑪ 포트폴리오 차별성유지	P5-02-EE	① 투자자 성향에 따라 산출된 안정추구, 위험중립, 적극투자형 포트폴리오가 운용과정에서도 차별성이 유지되고 있는가?	□예 □아니오
		①-1 (차별성이 유지되지 않는 경우) 그 사유를 합리적으로 설명할 수 있는가?	□예 □아니오
⑫ 리밸런싱 발생원칙	O1-01-EE	① 포트폴리오 운용기간 중 분기당 1회 이상 리밸런싱의 발생내역이 있는가? ⇒ 리밸런싱 발생내역에는 포트폴리오 변경내역, 잔고 변경내역, 로그 등이 포함되어야 함.	□예 □아니오
		①-1 (리밸런싱이 발생되지 않았다면) 그 사유를 설명할 수 있는가? ⇒ 리밸런싱 처리하였으나 포트폴리오에 변동사항이 없을 경우 등	□예 □아니오
		② 리밸런싱 원칙에 부합하여 리밸런싱이 처리되고 있는가?	□예 □아니오
		②-1 (리밸런싱이 원칙에 부합하지 않는 경우) 그 사유를 설명할 수 있는가?	□예 □아니오
		③ 정기 리밸런싱 외 수시 리밸런싱을 하고 있는가?	□예 □아니오
		③-1 시장 이벤트 발생시 리밸런싱을 통해 조정되고 있는가?	□예 □아니오
		③-2 목표비중 이탈시 리밸런싱을 통해 조정되고 있는가?	□예 □아니오
⑬ 리밸런싱 처리	O1-02-EE	① 리밸런싱 후에도 최소 5개 이상의 종목·상품으로 구성되어 있는가? ⇒ 개별주식종목으로만 구성할 경우 10개 이상으로 산출하여야 함(대기성 현금은 종목·상품 수에 포함하지 않음)	□예 □아니오
		② 리밸런싱 후 재설정된 포트폴리오가 포트폴리오 산출기준에 부합되고 있는가?	□예 □아니오
		③ 리밸런싱 처리 후 포트폴리오 변경이 발생하였는가?	□예 □아니오

항 목	심사번호	상세 심사 내용	확인결과
		③-1 (리밸런싱 처리 후에도 포트폴리오 변경이 없다면) 포트폴리오 변경이 발생하지 않는 사유에 대해 설명할 수 있는가?	□예 □아니오
		④ 투자유니버스는 변경 없이 처음 그대로 유지되었나?	□예 □아니오
		④-1 (투자유니버스 변경이 있을 경우) 투자유니버스 변경을 통보하였는가?	□예 □아니오
		⑤ 리밸런싱 후 편입된 종목들이 투자유니버스 내에 있는가?	□예 □아니오
		⑤-1 (투자유니버스에 없는 종목이 새로 편입되었다면) 타당한 근거를 제시할 수 있는가?	□예 □아니오
		⑥ 리밸런싱 후 재설정된 포트폴리오에서 금융상품별 배분된 투자 금액이 자산군별 투자금액에 부합되고 있는가?	□예 □아니오
		⑦ 리밸런싱 발생 후 포트폴리오 산출까지의 과정을 증명할 근거자료를 제시할 수 있는가?(방문 확인)	□예 □아니오
⑭ 리밸런싱 결과제출	O1-03-EE	① 리밸런싱 발생 후 매매결과 및 관련 자료를 기한 내 제출하였는가? ⇒ 리밸런싱에 의한 매매결과는 발생 당일 한국예탁결제원 PICA에 등록 및 정합성 검증을 하여야 하며(해외자산은 익영업일까지), 리밸런싱 관련 자료(21.리밸런싱 발생내역)는 익영업일까지 사무국 공표사이트에 등록하여야 함	□예 □아니오
		② 리밸런싱 관련 자료에 오류가 없으며 발생 주기 및 시점은 알고리즘 설명서와 일치하는가?	□예 □아니오
		③ 홈페이지에 공개되는 자료의 정합성을 매일 확인하였으며 오류 발견시 관련기관과 협의하여 즉시 수정하였는가?	□예 □아니오
		④ 리밸런싱 미 발생에 대한 근거 자료 제출 요청시 기한 내 제출하였는가? ⇒ 근거자료 형태 : 로그, 화면, DB데이터 등 ※ ①, ②, ③, ④ 각항목별 3회 이상 미준수시 부적합 처리	□예 □아니오
⑮ 다계좌 운용	O2-01-EE	① 동일 포트폴리오 유형별 3개 계좌씩 생성하여 운용하고 있는가? ⇒ 다계좌(9개)의 투자자성향분석부터 포트폴리오 종목 산출, 주문 집행이 개별적으로 처리되었는지 확인할 수 있어야 함	□예 □아니오
		② 동일 포트폴리오 유형으로 등록된 3개 계좌가 유사한 형태로 운용되고 있는가?	□예 □아니오
		②-1 (각 계좌별 운용결과가 유사하지 않을 경우) 사유를 합리적으로 설명할 수 있는가?	□예 □아니오
		③ 다수계좌(2)를 동시에 운용 가능하도록 구현되어 있는가?	□예 □아니오

항 목	심사번호	상세 심사 내용	확인결과
⑯ 법규준수	O3-01-DE	① 자기 또는 관계인수인이 인수한 증권이 있는가?	□예 □아니오
		①-1 (인수 증권이 있을 경우) 투자일임재산으로 매수하는 행위를 금지하는 알고리즘이 구현되어 있는가?	□예 □아니오
		② 자기가 운용하는 다른 투자일임재산, 집합투자재산 또는 신탁재산이 있는가?	□예 □아니오
		②-1 (동 재산이 있을 경우) 투자일임재산으로 동 재산과 거래하는 행위를 금지하는 알고리즘이 구현되어 있는가?	□예 □아니오
		③ 투자일임재산으로 투자일임업자 또는 그 이해관계인의 고유재산과 거래하는 행위를 금지하는 알고리즘이 구현되어 있는가?	□예 □아니오
		④ 투자일임업자 또는 그 이해관계인이 발행한 증권이 있는가?	□예 □아니오
		④-1 (동 증권이 있을 경우) 투자자의 동의 없이 투자일임재산으로 동 증권에 투자하는 행위를 금지하는 알고리즘이 구현되어 있는가?	□예 □아니오
		④-2 (동 증권에 투자하는 경우) 투자자 동의를 받는 절차가 구축되어 있는가?	□예 □아니오
		⑤ 투자일임재산을 각각의 투자자별로 운용하지 아니하고 여러 투자자의 자산을 집합하여 운용하는 행위를 금지하는 시스템이 구축되어 있는가?	□예 □아니오
		⑥ 기타 불건전 영업행위 방지를 위해 알고리즘에 추가로 설계되어 있는 부분이 있는지?	□예 □아니오
⑰ 시스템 매뉴얼 / 비상조치 매뉴얼	S1-01-SE	① 각 매뉴얼 개정이력이 관리되고 있는가? ⇒ 매뉴얼 개정 시 변경내역, 변경사항 승인이 포함되어야 함	□예 □아니오
		② 각 매뉴얼에 최근 시스템 및 운영 변경사항이 반영되어 있는가?	□예 □아니오
		③ 비상조치매뉴얼에 예상 장애유형별 대응 시나리오 및 예상 복구시간이 포함되어 있는가? ⇒ 예상 장애유형에는 네트워크 및 H/W 장애에 대비한 업무연속성계획(BCP:Business Continuity Planning)이 포함되어야 하며, 장애발생 후부터 정상화까지 복구시간을 명시하여야 함	□예 □아니오
		④ 비상조치매뉴얼에 외부 데이터 송/수신 불가시 조치방안이 기술되어 있는가?	□예 □아니오
		⑤ 시스템운영매뉴얼에 시스템구성도, 구동·조작방법, 운용순서가 포함되어 있는가?	□예 □아니오
		⑥ 시스템운영매뉴얼에 비상연락체계와 시스템 담당자 연락처 등이 포함되어 있는가?	□예 □아니오

항 목	심사번호	상세 심사 내용	확인결과
⑱ 모니터링	S1-02-SE	① 장애발생을 즉시 인지할 수 있는 모니터링 수단이 있는가?(전담 인원 또는 경보 기능)	□예 □아니오
		② 모니터링 내용이 이해하기 쉽고 신속히 인지할 수 있도록 표현되어 있는가?	□예 □아니오
		③ 시스템 자원 상태의 감시, 경고 및 제어가 가능하도록 체계가 구축되어 있는가?	□예 □아니오
		④ 장애상황기록부를 기록 관리하고 있는가? ⇒ 장애상황기록부에는 장애일시, 장애내용, 조치사항 등을 상세히 작성하여 보관하여야 함	□예 □아니오
⑲시스템 접근통제	S1-03-SE	① 시스템(DB 포함)에 대한 접근권한이 사용자 그룹별로 제한되어 관리되고 있는가?	□예 □아니오
		② H/W, DBMS, OS에 대한 주기적 유지보수가 이루어지며, 작업내용은 기록되어 관리되고 있는가?	□예 □아니오
		③ 시스템 관리자 권한이 IT전문인력에 의해 통제되고 있는가?	□예 □아니오
⑳ 형상관리	S1-04-SE	① 형상관리절차서(첨부2참조)가 있으며 현행화가 되어 있는가?	□예 □아니오
		② 형상관리 대상이 형상관리절차서에 포함되어 있는가?	□예 □아니오
		③ 원본 프로그램 및 데이터베이스 변경을 위한 절차가 있으며 관리자의 승인을 거치고 있는가?	□예 □아니오
		④ 프로그램 변경은 운영시스템과 분리된 별도의 시스템에서 수정되어 테스트를 거치고 있는가?	□예 □아니오
		⑤ 프로그램 배포 후 문제 발생 시 이전 버전으로 복원할 수 있는 대책 및 절차가 있는가?	□예 □아니오
㉑ 상용화 화면	S1-05-SE	① 상용화를 위한 포트폴리오 산출 화면(투자자용 또는 관리자용)이 구현되어 있는가?	□예 □아니오
		② 상용화를 위한 리밸런싱 전/후 자산배분 화면(투자자용 또는 관리자용)이 구현되어 있는가?	□예 □아니오
		③ 상용화를 위한 리밸런싱 전/후 포트폴리오 산출화면(투자자용 또는 관리자용)이 구현되어 있는가? ⇒ 포트폴리오 산출화면에는 종목코드, 종목명, 투자비중, 수량등이 출력되어야 함	□예 □아니오
		④ 투자자에게 매매결과를 조회할 수 있는 화면이 구현되어 있는가?	□예 □아니오
㉒ 이용자 및 계좌소유주 인증	S2-01-DE	① 이용자 인증 방법이 적정하게 설계되어 있는가? ⇒ 인증 우회 가능성에 대한 보호대책 및 인증정보 탈취를 위한 공격(세션 가로채기, 비밀번호 무작위 대입공격, 인증정보 재활용 등)에 대한 대책 필요	□예 □아니오
		② 계좌 소유주 인증 방법이 적정하게 설계되어 있는가? ⇒ 타인의 계좌를 등록할 수 없도록 대책(특히, 휴대폰 인증의 경우 메시지 탈취, 전화번호 변조, 휴대폰 도난 등의 대책) 필요	□예 □아니오

항 목	심사번호	상세 심사 내용	확인결과
		③ 인증 및 거래관련 기록(인증시도 및 결과, 접속정보 등)을 보존하고 관련기록의 변경에 대한 보호대책이 마련되어 있는가? ⇒ 인증 및 거래관련 정보가 기록된 데이터베이스, 로그 등은 인가된 사용자만 접근 가능하도록 보호대책 필요	□예 □아니오
㉓ 중요정보 보호대책	S2-02-DE	① 중요정보(개인정보, 금융정보, 패스워드 등)는 안전하게 암호화하여 기밀성을 보장할 수 있도록 설계되어 있는가? ⇒ 시스템 내에서 처리되는 중요정보(개인정보, 금융정보, 패스워드 등)는 기밀성 유지를 위해 암호화 등의 대책이 마련 필요	□예 □아니오
		② 중요정보(운용지시 등)는 위변조 여부 등 무결성을 확인할 수 있도록 설계되어 있는가? ⇒ 시스템 내에서 처리되는 무결성이 요구되는 중요정보(운용지시 등)는 무결성을 확인할 수 있도록 대책 필요(암호화, 체크섬 등)	□예 □아니오
		③ ①, ②에 적용된 암호화 알고리즘은 국내외 전문기관(NIST, KISA 등)에서 권고한 암호화 알고리즘 및 키길이를 사용하고 안전하게 관리되고 있는가? ⇒ 암호화 연산은 112비트 이상의 보안강도를 갖는 암호알고리즘 및 암호키 길이 적용 필요. 암호키는 생성, 분배, 접근, 파기 전반에 걸쳐 안전하게 관리될 수 있도록 절차 필요.	□예 □아니오
㉔ 시스템 물리적통제	S2-03-SE	① 전산설비에 대한 보호구역 설정이 되어있는가? ⇒ 전산설비 설치장소를 보호구역으로 설정하고, 보호구역 내 작업(시스템 유지보수, 시스템 도입 등)이 필요한 경우 작업기록을 관리하며, 보호구역 내 시스템 반출 및 반입 내역 관리 필요	□예 □아니오
		② 전산설비에 대한 출입통제대책(카드키 혹은 지문인식 등)이 수립되어 있는가? ⇒ 사전 인가자 인증을 위한 대책(카드키 혹은 지문인식 등)이 마련되어 있어야 하며, 사전 인가자 외 인원은 책임자의 승인을 받아 출입하며(내부 담당자 동행) 출입자 관리기록부에 기록(신원, 방문목적, 방문일시 등) 필요	□예 □아니오
		③ 중요서버는 잠금장치로 보호되어 있는가? ⇒ 중요 서버는 잠금장치로 보호되어 해당 서버 관리자만 접근할 수 있도록 대책이 마련 필요. 단, 출입통제대책이 마련된 전산실에 관리자만 출입할 수 있는 경우에는 제외	□예 □아니오
		④ 전산설비를 클라우드 및 IDC에 위탁 운영하는 경우, ①~③항목에 대한 물리적 통제 관련 요구사항을 계약서에 반영하고 운영상태를 주기적으로 검토하고 있는가? ⇒ 위탁운영기관이 정보보호 인증서(ISMS, ISO 27001, 클라우드 보안인증제도 등 관련 인증	□예 □아니오

항 목	심사번호	상세 심사 내용	확인결과
		서 中1개 이상)를 보유하고 위탁전산설비가 해당 인증서 범위 내에 포함되는 경우 계약서 반영사항을 인증서로 갈음	
㉕ 시스템 기술적통제	S2-04-SE	① 중요서버(중요도를 고려하여 사전 지정 필수 (예: DB, 웹 등))에 접근하는 계정은 안전한 비밀번호를 사용하도록 설정 및 적용되고 있는가? ⇒ 중요서버에 접근하는 계정 중 root계정은 원격 접속을 제한하여야 하며, 비밀번호는 적절한 조합규칙(아이디, 생년월일, 주민번호 등을 포함하지 않은 영문자, 특수문자, 숫자를 혼합한 8자리 이상), 분기별 1회 이상 변경, 보관시 암호화, 시스템마다 관리자 비밀번호가 다르게 지정, 비밀번호 연속오류에 대한 대응 등 필요	□예 □아니오
		② 중요서버에 대한 접근은 중요PC 및 지정된 서버 등에 대해서만 허용하고 있는가? ⇒ 기본적으로 외부통신망과 연결이 차단되어있어야 하며, 중요 PC 및 서버 등이 외부에 있어 부득이하게 통신해야할 경우 침입차단시스템 등의 접근통제 방안 마련 필요	□예 □아니오
		③ 중요서버는 업무상의 용도를 제외하고 외부통신망(인터넷 등)의 연결 및 불필요한 서비스가 차단되어 있는가? ⇒ 외부통신망과 물리적 혹은 논리적 망분리 적용이 되어 있는지 확인하며, 서버 내 불필요한 서비스(Finger서비스, r계열서비스, NFS서비스, tftp서비스 등)가 열려 있지 않도록 설정 필요	□예 □아니오
		④ 중요서버에 대해 최신보안패치를 적용하고 있는가? ⇒ 중요서버에 적용할 패치의 중요도에 따라 긴급하고 중요한 패치의 경우 즉시, 보통레벨의 패치 사항의 경우 일정기간 내 적용할 수 있도록 관련 절차 마련 필요	□예 □아니오
		⑤ 중요서버에 대해 악성코드 대응 방안을 적용하고 있는가? ⇒ 중요서버에 악성코드탐지 프로그램을 설치하고 정기적으로 악성코드탐지 프로그램을 업데이트 하며 실시간 검사가 이뤄질 수 있도록 설정 필요	□예 □아니오
		⑥ 중요서버는 독립서버로 운영하고, 정보보안시스템(차단시스템 등)을 적용하여 보호하고 있는가? ⇒ 시스템 용도(웹/WAS, 어플리케이션, DB 등)별로 독립된 서버로 운영하며, 서버 가상화(가상머신 등)를 이용하는 경우 별도의 보호대책 수립 필요 (예: 가상머신별 접근관리, 데이터 분리 및 보호, 하이퍼바이저와 가상머신사이의 인터페이스 취약점에 대한 보호대책 수립 등)	□예 □아니오
		⑦ 정보보호시스템(침입차단시스템 등)내 취약한 정책이 존재하지 않는가? ⇒ 기본적으로 All Deny정책이 적용되어 있고, 접근이 필요한 최소한의 서비스만 허용되어 있어야 하며, 취약한 정책(네트워크IP주소 단위로 허용된 정책, 출발지 포트 기반의 정책, 양방향으로 설	□예 □아니오

항 목	심사번호	상세 심사 내용	확인결과
		정된 정책 등)이 없는지 주기적으로 확인 필요	
		⑧ 인터넷에 공개된 웹 서버에 대해 웹 취약점 점검을 수행하였는가? ⇒ 자체 혹은 외부기관에서 점검한 수행결과 및 조치계획서 첨부 필요	□예 □아니오
㉖ 중요PC 통제	S2-05-SE	① 중요PC(관리자 PC, 개발 PC 등)는 업무상의 용도를 제외하고 외부통신망(인터넷 등)의 연결이 차단되고 및 불필요한 프로그램이 제거되어 있는가? ⇒ 중요PC는 사전 지정 필수 (예: 중요서버에 접근 가능한 PC, 개인정보를 취급하는 PC 등). 중요PC는 외부통신망과 물리적 혹은 논리적 망분리 적용이 필요하며, 불필요한 프로그램(상용 메신저 등)의 제거 필요.	□예 □아니오
		② 중요PC에 대한 계정은 안전한 비밀번호를 사용하도록 설정 및 적용되고 있는가? ⇒ 비밀번호는 적절한 조합규칙(아이디, 생년월일, 주민번호 등을 포함하지 않은 영문자, 특수문자, 숫자를 혼합한 8자리이상), 분기별 1회 이상 변경, 보관시 암호화 등이 적용되어 있는지 확인 필요	□예 □아니오
		③ 중요PC에 대해 최신보안패치를 적용하고 있는가? ⇒ 중요PC는 HOT Fix등 최신보안패치를 적용하며, 설치된 응용 프로그램(한글, MS-Office, 어도브 아크로뱃 등)에 대해 정기적으로 패치할 수 있도록 관련 절차 필요	□예 □아니오
		④ 중요PC에 대해 악성코드 대응 방안을 적용하고 있는가? ⇒ 악성코드탐지 프로그램을 설치하고 정기적으로 악성코드탐지 프로그램을 업데이트 하며, 실시간 검사 및 OS에서 제공하는 침입차단 기능 활성화 필요	□예 □아니오
		⑤ 중요PC에 대해 외부반출을 통제하고 있는가? ⇒ 중요PC는 원칙적으로 외부로 반출하지 않도록 통제하여야 하며, 외부반출 시 중요서버에 접근금지 및 중요데이터 삭제 등의 조치 필요	□예 □아니오
		⑥ 중요PC에서 보조기억매체 및 휴대용전산장비에 접근하는 것을 통제하고 있는가? ⇒ 중요PC의 보조기억매체 및 휴대용전산장비 접근은 원칙적으로 금지하나, 필요가 불가피한 경우 별도의 보호대책 마련 필요 (예: 악성코드탐지, 접근관리대장 관리, 관리자 통제하에서만 사용 등)	□예 □아니오
		⑦ 비중요 PC 내에 중요정보(개인정보, 암호키 등) 저장을 제한하고 있는가? ⇒ 주기적으로 비중요 PC내에 중요정보가 저장되어 있는지 여부를 확인할 수 있는 관련 절차 필요	□예 □아니오

항 목	심사번호	상세 심사 내용	확인결과
㉖ 네트워크 통제	S2-06-SE	① 시스템 용도(웹, DB 등)에 따라 네트워크 구간이 분리되어 있는가? ⇒ 웹, DB 등 시스템 용도별로 네트워크를 분리하여야 하며, 네트워크 가상화(가상 스위치 등)를 이용하는 경우 별도의 보호대책 필요 (예: 가상 스위치별 VLAN설정 등)	□예 □아니오
		② 네트워크 구간별로 접근제어가 설정되어 있는가? ⇒ 웹은 DMZ, DB는 내부망 등 네트워크 구간별로 허용 IP 및 포트를 관리를 통한 접근제어 필요	□예 □아니오
		③ 대외기관(금융회사 등)과의 통신 시 보안통신(전용회선 혹은 VPN 등)이 적용되어 있는가?	□예 □아니오
		④ 무선네트워크는 통제 하에 이용을 최소화하며, 이용 시 보호대책을 적용하였는가? ⇒ 무선네트워크 이용 시 SSID는 hidden, 암호정책은 WPA이상, MAC필터링 적용 등 필요	□예 □아니오
		⑤ 중요서버 원격 통신 시 보안통신(전용회선 혹은 VPN 등)이 적용되어 있는가? ⇒ IDC 및 클라우드 등에 위치한 중요서버와의 원격 통신 시 전용회선 혹은 VPN(SSH등 포함) 및 사용 필요	□예 □아니오
		⑥ 인가된 사용자만이 중요서버가 위치한 네트워크에 접근할 수 있도록 통제하고 있는가? ⇒ 내부망에 접근 가능한 네트워크장비(스위치, 라우터, VPN 등)에 비인가자가 접근할 수 없도록 물리적, 관리적, 혹은 기술적 통제 필요 (예: 네트워크 포트에 접근할 수 없도록 포트잠금장치 설치, 인가된 사용자만 네트워크 식별자(IP 혹은 MAC 등)할당 등)	□예 □아니오

첨부 1) 유지·보수 전문인력의 자격요건

1. 정보보호 또는 정보기술(IT) 분야의 학력 또는 기술자격을 가진 사람으로서 다음 각 목의 어느 하나에 해당하는 사람.
   가. 정보보호 또는 정보기술(IT) 분야의 전문학사학위를 취득한 후 3년 이상 해당 분야 업무를 수행한 경력이 있는 사람
   나. 정보보호 또는 정보기술(IT) 분야의 학사학위 또는 다음 전문자격을 취득한 후 1년 이상 해당 분야 업무를 수행한 경력이 있는 사람
   다. 정보보호 또는 정보기술(IT) 분야의 석사학위 이상 취득한 사람
   1) 「전자정부법」 제2조제15호에 따른 감리원
   2) 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제47조제5항에 따른 정보보호 관리체계 인증기관의 인증 심사원
   3) 「자격기본법」에 따라 공인을 받은 정보보호전문가(Specialist for Information Security)
   4) 국제정보시스템감사통제협회(Information Systems Audit and Control Association)의 정보시스템감사사(Certified Information Systems Auditor)
   5) 국제정보시스템보안자격협회(International Information System Security Certification Consortium)의 정보시스템보호전문가(Certified Information System Security Professional)

2. 다음 각 목의 어느 하나에 해당하는 사람
   가. 7년 이상 정보보호 분야 업무 또는 정보기술(IT) 분야 업무를 수행한 경력이 있는 사람
   나. 전문학사학위를 취득한 후 5년 이상 정보보호 분야 업무 또는 정보기술(IT) 분야 업무를 수행한 경력이 있는 사람
   다. 학사학위를 취득한 후 3년 이상 정보보호 분야 업무 또는 정보기술(IT) 분야 업무를 수행한 경력이 있는 사람
   라. 석사학위를 취득한 후 1년 이상 정보보호 분야 업무 또는 정보기술(IT) 분야 업무를 수행한 경력이 있는 사람

< 비고 >
1. “정보보호 또는 정보기술(IT) 분야 학력”이란 「고등교육법」에 따른 해당 학교에서 다음 각 목에 해당하는 학과의 과정을 이수하고 졸업하거나 그 밖의 관계법령에 따라 국내 또는 외국에서 이와 같은 수준 이상으로 인정되는 학력을 말한다.

가. 전자 관련 학과: 전기전자, 전기전자정보, 전기전자제어, 전자, 전자계산, 전자전기정보, 전자정보, 전자제어, 전자재료, 전자컴퓨터, 전자컴퓨터전기제어, 정보전자, 반도체, 메카트로닉스, 제어계측, 컴퓨터과학

나. 정보통신 관련 학과: 통신, 국제정보통신, 무선통신, 방송통신, 이동통신, 전기전자통신, 전기전자정보통신, 정보통신, 전자통신, 전자정보통신, 전자제어통신, 전파통신, 컴퓨터통신, 항공통신정보, 전기통신설비, 전자정보통신반도체, 전파, 전기전자전파, 방송설비, 통신컴퓨터, 컴퓨터네트워크, 컴퓨터정보기술

다. 정보보호 또는 정보처리기술 관련 학과: 전산, 전산통계, 정보전산, 정보처리, 시스템, 정보시스템, 구조시스템, 컴퓨터응용, 컴퓨터응용설계, 컴퓨터제어, 컴퓨터응용제어, 컴퓨터정보, 멀티미디어

라. 그 밖에 교육부장관이나 해당 교육기관의 장으로부터 전자, 정보통신, 정보보호 또는 정보처리기술 관련 학과로 인정받은 학과

2. “정보보호 또는 정보기술(IT) 분야 기술자격”이란 「국가기술자격법」 제2조제3호, 제8조의2제2항 및 같은 법 시행규칙 별표 2의 전기·전자 직무분야 중 전자계산기 종목의 자격과 정보통신 직무분야 중 기술·기능 분야의 자격을 말한다.

3. “정보보호 분야 업무”란 공공기관, 민간기업, 교육기관 등에서 수행하는 다음 각 목에 해당하는 분야의 계획·분석·설계·개발·운영·유지보수·컨설팅·감리 또는 연구개발 업무 등을 말한다.

가. 정보보호를 위한 공통기반기술 분야: 암호 기술, 인증 기술 등

나. 시스템·네트워크 보호 분야: 시스템 보호, 해킹·바이러스 대응, 네트워크 보호 등

다. 응용서비스 보호 분야: 전자거래 보호, 응용서비스 보호, 정보보호 표준화 등

4. “정보기술(IT) 분야 업무”란 공공기관, 민간기업, 교육기관 등에서 수행하는 다음 각 목에 해당하는 분야의 계획·분석·설계·개발·운영·유지보수·컨설팅·감리 또는 연구개발 업무 등을 말한다.

가. 정보통신서비스 분야: 기간통신, 별정통신, 부가통신, 방송서비스 등

나. 정보통신기기 분야: 정보기기, 방송기기, 부품 등

다. 소프트웨어 및 컴퓨터 관련 서비스 분야: 범용 패키지 소프트웨어, 특정 업무용 프로그램, 디지털콘텐츠, 데이터베이스의 개발·구축·운영·활용 및 컴퓨터 관련 서비스

5. 외국에서 취득한 기술자격, 학력 또는 경력은 제1호부터 제4호까지의 기준에 따라 산정한다.

첨부 2) 형상관리절차서

○ 형상관리절차서에는 다음의 내용이 포함되어야 함

1. 형상관리 대상
   - 중요문서(각종 매뉴얼)
   - 프로그램 목록 및 설계서, 데이터베이스 목록 및 설계서, 파일 목록 및 정의서
   - 내/외부 시스템간 I/F 목록 및 정의서
2. 원본 프로그램 및 데이터베이스 관리방안
   - 보관 위치
   - 프로그램 반입/반출 절차(개인의 임의 반출/반입 통제)
   - 데이터베이스 변경 절차
3. 프로그램 변경절차
   - 변경대상 프로그램 및 변경사항에 대한 관리자 승인
   - 변경 프로그램 운영시스템에서 반출
   - 운영시스템과 분리된 별도의 시스템에서 수정 및 테스트 진행
   - 테스트결과 검토를 통해 변경 프로그램의 안정성을 관리자가 확인 후 운영시스템으로 이행 및 이행결과 확인
   - 변경업무로 인한 형상관리 대상 문서 변경
4. 프로그램 버전 관리방안
   - 변경업무에 따른 프로그램 버전관리 방안
   - 변경업무 이행 후 오류발생 시 이전 버전으로 복원 절차
5. 프로그램 변경 내역 관리
   - 변경업무 적용일, 변경사유, 변경 대상 프로그램, 변경 승인자
   - 변경 업무 단위로 관리

로보어드바이저 테스트베드
제출자료 목록

- 제2차 정기심사 -

Robo Advisor
TEST BED CENTER

□ 제출자료 목록

자료번호	자료명		문서형태	제출시기(방법)	심사번호	비고
0	참여신청서		웹사이트 입력	참여 신청 후 사전심사 개시전 까지 (웹사이트 제출)	-	
1	테스트베드 이용 약정서★		전자(화)문서		-	사전심사 현장방문시 원본제출
2	법인등기사항전부증명서 사본 1부		전자(화)문서		P0-01-DE	(자문·일임업 미등록자 대상)
3	자문·일임업 등록 증빙서류		전자(화)문서		P0-01-DE	(자문·일임업 기등록자 대상) 금융투자업등록통보서 등
4	사업자등록증 사본 1부		전자(화)문서		-	
5	계좌개설증명가능한 문서 (계좌개설확인서, 증권통장사본, 계좌별 잔고증명서 등) 9부		전자(화)문서		-	계좌별 각 1부씩. 총 9부
11	알고리즘 설명서★	① 알고리즘 설명	전자(화)문서		P1-01-DE P5-01-EE	적용기술, 특징, 운용목표, 주요전제, 위험도 및 위험도 측정에 관한 내용, 포트폴리오 구성 원칙 등
		② 리밸런싱 설명	전자(화)문서		P1-03-DE O1-01-EE O1-02-EE	발생원칙, 발생기준, 발생주기 등
		③ 투자자성향분석 설명	전자(화)문서		P2-01-DE P2-02-DE P2-03-PE	투자자성향유형 분류기준, 유형별 특징, 투자성향별 자산구성 기준
12	투자유니버스 자료★		전자(화)문서		P1-01-DE P3-01-PE O1-01-EE O1-02-EE	알고리즘명, 자산군구분, 종목코드, 종목명 등

자료번호	자료명		문서형태	제출시기(방법)	심사번호	비고
13	법규준수 설명 자료★		전자(화)문서		O3-01-DE	자본시장법상 불건전 영업행위 금지조항에 저촉되지 않도록 설계되어 있음을 설명
14	백테스팅 결과분석 자료★		전자(화)문서		P1-02-DE	과거 1년 이상 동안의 모의실험 결과 포함
15	단계별 증빙화면★	① 투자자 프로파일링	캡쳐화면		P0-02-DE	첫페이지만 첨부 가능
		② 자산배분	캡쳐화면		P0-02-DE	상세화면 첨부
		③ 포트폴리오 셀렉션	캡쳐화면		P0-02-DE	상세화면 첨부
		④ 주문집행(자동)	캡쳐화면		P0-02-DE	상세화면 첨부(선택)
		⑤ 포트폴리오 리밸런싱	캡쳐화면		P0-02-DE	상세화면 첨부
16	자가평가서 점검 결과★		전자(화)문서		-	자체 점검결과 작성 제출
17	주식 종목정보 변경시 처리방법★		전자(화)문서			권리락 등 발생시 처리방법이며 투자유니버스에 '주식'종목 포함된 경우에만 제출
20	포트폴리오 운용개시 현황★		전자(화)문서	포트폴리오 운용 중 (웹사이트 제출)	-	포트폴리오 운용개시 후 2영업일 內 제출
21	리밸런싱 발생내역★		전자(화)문서		O1-01-EE	매일 리밸런싱 발생시 발생사실은 매일 등록하며 자료는 1주단위로 제출 가능
22	시스템운영매뉴얼 * 개인정보 및 IP 등 시스템 보안사항은 마스킹 처리 후 제출		전자(화)문서	시스템심사 신청시 (일정 별도 통보. 웹사이트 제출)	S1-01-SE	이력관리, 현행화, 시스템구성도, 구동·조작방법, 운영순서 등 포함
23	비상조치매뉴얼 * 개인정보 및 IP 등 시스템 보안사항은 마스킹 처리 후 제출		전자(화)문서		S1-01-SE	장애유형별 대응 시나리오 및 예상 복구시간 등 포함

자료번호	자료명	문서형태	제출시기(방법)	심사번호	비고
24	형상관리절차서	전자(화)문서		S1-04-SE	자가평가서 첨부2 참조
25	보안대책명세서	전자(화)문서		S2-01-DE 등	
31	장애상황기록부	현장실사시 확인	시스템심사 현장실사시	S1-02-SE	
32	유지보수 관리대장			S1-03-SE	
33	보호구역 출입자명부			S2-03-SE	
34	전문인력 증빙서류	서면제출		P4-01-PE	자가평가서 첨부 1 참조

* 별표(★) 자료는 별도양식 참조(웹사이트 '공지사항' 게시)

□ 제출파일명 생성규칙 : [알고리즘명]자료번호.자료명_회사명_작성일자

ex) [코스콤로보1]11.알고리즘설명서_코스콤_20170310.hwp
[코스콤로보1]11.알고리즘설명서_1_알고리즘설명_코스콤_20170310.hwp

※ '제출파일명 생성규칙'을 반드시 준수할 것. 미준수시 제출파일 반려함.

□ 제출방법 : (웹사이트) '알고리즘 참여신청' 후 '심사진행현황'메뉴 → '파일첨부관리' 이용

* 기 제출파일 변경 등록 시 기존파일 삭제 후 변경파일 첨부
* 파일크기 10MB 초과 시 분할 압축하여 첨부

로보어드바이저 테스트베드
시스템 보안성심사 안내

- 제2차 정기심사 -



금융보안원
FINANCIAL SECURITY INSTITUTE

로보어드바이저 시스템 보안성심사 안내

(금융보안원, 2017.3.10.)

1 심사개요

□ **(심사목표) 보안사고 예방·대응수준 확인 (상용 서비스 대비)**

□ **(심사기업) 테스트베드 참여업체 중 상용서비스 제공 예정자**

□ **(심사대상) 심사기업이 보유한 로보어드바이저 시스템 전반**

※ 알고리즘 운영 서버, DB 서버, 웹 서버, 정보보호시스템, 중요 PC 등

□ **(심사방향) 2단계 심사 (서면 및 현장), 서비스 유형별* 맞춤 점검**

* [참고1]『로보어드바이저 시스템 서비스 유형』참조

○ **(2단계 심사)** 서면심사(1단계)에서 보완사항 권고, 현장심사(2단계) 시 보안대책현황 및 보완조치 이행여부 등 점검

○ **(서비스 유형별 맞춤 점검)** 온라인에서의 고객 맞춤형 서비스* 제공유무에 따라 온라인형과 오프라인형으로 구분하여 점검 기준을 적용

* 고객이 홈페이지 등에 직접 접속하여 고객별 수익률 조회, 포트폴리오 조회 등을 제공

□ **(심사기준) 6개 분야 31개 기준***

* [참고2]『로보어드바이저 시스템 보안성심사 기준』참조

○ 온라인 서비스 제공 시 31개 기준, 미 제공시 27개 기준 점검

2 심사 절차 및 구분

□ (심사절차) 『서면 심사』 및 『현장 심사』로 구분

○ **(서면 심사)** 로보어드바이저 시스템의 보안대책 현황을 서면(보안대책명세서)으로 심사

※ **(자료제출)** 심사기업이 사무국 홈페이지로 보안대책명세서를 제출
(결과송부) 금융보안원이 서면심사 후 결과보고서를 심사기업에게 전달

○ **(현장 심사)** 시스템 운영 **현장을 방문하여 시스템 보안현황 일치성, 보완조치 이행여부 등 심사**

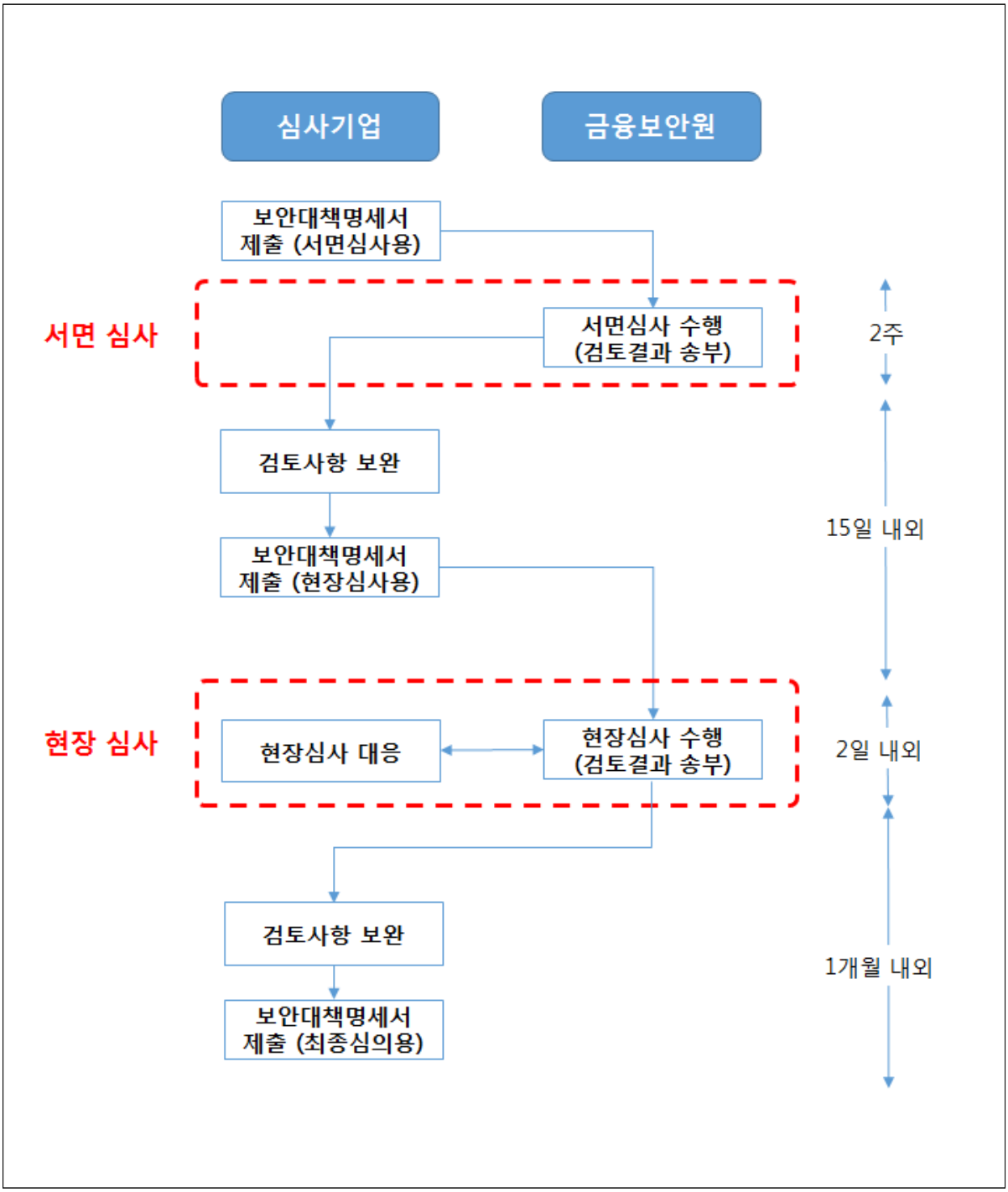
※ 최종(보완) 보안대책명세서, 보완조치의견 등을 토대로 심사진행

□ 심사기업 유형에 따른 서면·현장심사 대상 여부

심사기업유형 / 심사구분	자문일임업, 로보어드바이저 기술보유업체 (단독, 컨소시엄형)	은행 · 증권	
		단독형	컨소시엄형
서면심사	대상	대상	대상
현장심사	대상	비대상	일부대상*

* 자문일임업, 로보어드바이저 기술보유업체가 보유한 시스템은 현장심사 대상

< 참고 : 시스템 보안성심사 세부절차 >



3 제출 서류

□ **(제출서류)** 『보안대책명세서*』 (서면심사와 현장심사용 양식 동일)

※ [참고4] 『 로보어드바이저 테스트베드 보안대책명세서 샘플』 참고

○ **(구성)** 서비스 개요, 서비스 유형, 서비스 절차, 시스템 및 네트워크 구성도, 심사기준 별 보호대책

□ **(제출마감일자)**

○ **(서면심사) 심사기업 권역별로 3차에 걸쳐 마감**

- **(1차)** 은행('17.6.9.) **(2차)** 증권('17.6.23.) **(3차)** 기타('17.7.7.)

※ 마감일정은 변동가능

○ **(현장심사) 현장심사 시작 일주일 전 마감**

※ 현장심사 일정은 개별통보 예정

□ **(제출방식) 테스트베드 홈페이지에 전자파일로 업로드(hwp 등)**

4 문의

□ **(문의처) 금융보안원 핀테크보안팀**

○ **(절차) 02-3495-9623 (심사기준) 02-3495-9625**

※ 로보어드바이저 기업의 질의응답에 관한 사항은 필요한 경우 FAQ(참고3) 등으로 지속적인 안내 예정

참고 1 로보어드바이저 시스템 서비스 유형

□ 온라인 고객 맞춤형 서비스 제공 유무에 따라 『온라인형』과 『오프라인형』으로 구분

○ **(온라인형)** 고객계정을 기반으로 맞춤형 정보를 웹서비스 등 온라인으로 제공하는 경우

○ **(오프라인형)** 온라인 기반의 고객 맞춤형 서비스가 없는 경우

※ 참고 : 로보어드바이저 유형별 예시

1 온라인형

- 로보어드바이저 홈페이지 내 회원가입 후, 고객별 수익률 조회, 포트폴리오 조회 등을 제공

※ 고객이 회원가입 후 개인정보(핸드폰 번호 등), 금융정보(계좌번호 등)를 조회할 수 있는 경우에도 온라인형에 해당

2 오프라인형

- 로보어드바이저 홈페이지 내 회원가입 없이, 회사 소개, 일반적인 투자성향 분석 등의 서비스만 제공

※ 고객 맞춤형 정보(수익률 및 포트폴리오 정보 등)는 우편, 대면 등의 방식으로 제공

참고 2 로보어드바이저 시스템 보안성심사 기준

□ 시스템 보안성심사 기준

분야	심사기준	온라인형	오프라인형
1. 이용자 및 계좌 소유주 인증 (S2-01-DE)	① 이용자 인증	√	
	② 계좌 소유주 인증	√	
	③ 기록관리	√	
2. 중요정보 보호대책 (S2-02-DE)	① 기밀성 보장	√	√
	② 무결성 보장	√	√
	③ 암호화 알고리즘	√	√
3. 시스템 물리적 통제 (S2-03-DE)	① 보호구역 설정	√	√
	② 출입통제	√	√
	③ 잠금장치 보호	√	√
	④ IDC 계약사항	√	√
4. 시스템 기술적 통제 (S2-04-DE)	① 안전한 비밀번호 적용	√	√
	② 접속단말 지정	√	√
	③ 불필요 통신 및 서비스 차단	√	√
	④ 보안패치 적용	√	√
	⑤ 악성코드 대응	√	√
	⑥ 안전한 서버운영	√	√
	⑦ 정보보호시스템 취약정책 제거	√	√
	⑧ 웹 취약점 점검	√	
5. 중요 PC 통제 (S2-05-DE)	① 불필요 통신 및 프로그램 차단	√	√
	② 안전한 비밀번호 적용	√	√
	③ 보안패치 적용	√	√
	④ 악성코드 대응	√	√
	⑤ 외부반출 통제	√	√
	⑥ 보조기억매체 통제	√	√
	⑦ 중요정보 저장제한	√	√
6. 네트워크 통제 (S2-06-DE)	① 네트워크 분리	√	√
	② 구간별 접근제어	√	√
	③ 대외통신 보호	√	√
	④ 무선 네트워크 통제	√	√
	⑤ 원격통신 통제	√	√
	⑥ 내부 네트워크 통제	√	√

※ 전자금융거래법, 전자금융감독규정 등 관련 법규에 서술된 내용이 본 심사기준과 상충될 경우 관련법규의 내용이 우선되며, 로보어드바이저 서비스 특성에 따라 심사기준 적용대상 변동 가능

□ 시스템 보안성심사 기준 상세

분야	심사기준
1. 이용자 및 계좌 소유주 인증 (S2-01-DE)	**① (이용자 인증)** 이용자 인증을 위한 방법이 적정하게 설계되어 있는가? - 인증방법(패스워드, 생체인증, OTP 등) 자체의 안전성(메커니즘, 알고리즘 등)과 인증 프로세스 전반의 안전성을 함께 고려하여 설계해야 하며, 서비스 이용 시 타인의 명의를 도용할 수 없도록 대책 (특히, 휴대폰 인증의 경우 메시지 탈취, 전화번호 변조, 휴대폰 도난 등의 대책) 필요 - 인증정보 탈취를 위한 공격(세션 가로채기, 비밀번호 무작위 대입공격, 인증정보 재활용 등)에 대한 대책 필요
	② (계좌 소유주 인증) 계좌 소유주 인증을 위한 방법이 적정하게 설계되어 있는가? - 인증방법(계좌 비밀번호, 계좌 입금 금액 입력 등) 자체의 안전성 (메커니즘, 알고리즘 등)과 인증 프로세스 전반의 안전성을 함께 고려하여 설계해야 하며, 계좌 소유주 인증 시 타인의 계좌를 등록할 수 없도록 대책(특히, 휴대폰 인증의 경우 메시지 탈취, 전화번호 변조, 휴대폰 도난 등의 대책) 필요
	③ (기록관리) 인증 및 거래관련 기록(인증시도 및 결과, 접속정보 등)을 보존하고 관련기록의 변경에 대한 보호대책이 마련되어 있는가? - 인증관련 정보가 기록된 데이터베이스, 로그 등은 인가된 사용자만 접근 가능하도록 보호대책 필요
2. 중요정보 보호대책 (기밀성, 무결성) (S2-02-DE)	**① (기밀성 보장)** 중요정보(개인정보, 금융정보, 패스워드 등)는 안전하게 암호화하여 기밀성을 보장할 수 있도록 설계되어 있는가? - 시스템 내에서 처리되는 기밀성이 요구되는 중요정보(개인정보, 금융정보, 패스워드 등)는 기밀성 유지를 위해 암호화 필요
	② (무결성 보장) 중요정보(운용지시 등)는 위변조 여부 등 무결성을 검증할 수 있도록 설계되어 있는가? - 시스템 내에서 처리되는 무결성이 요구되는 중요정보(운용지시 등)는 무결성을 검증할 수 있도록 대책 필요(암호화, 체크섬 등)

분야	심사기준
	③ **(암호화 알고리즘)** S2-02-DE ①, ②에 적용된 암호화 알고리즘은 국내외 전문기관(NIST, KISA 등)에서 권고한 암호화 알고리즘 및 키길이를 사용하고 안전하게 관리되고 있는가? - 암호화 연산은 112비트 이상의 보안강도를 갖는 암호알고리즘 및 암호키 길이 적용 필요 ※ 국내에서 권고하는 112비트 이상의 보안강도를 갖는 암호알고리즘의 목록은 '암호 알고리즘 및 키 길이 이용 안내서(KISA)' 참조 - 암호키는 생성, 분배, 접근, 파기 전반에 걸쳐 안전하게 관리될 수 있도록 절차가 필요하며, 필요 시 암호키 관리를 위한 안전한 물리적 관리적 절차(HSM, 잠금장치가 있는 금고 등) 필요
	* 고려사항 : 관련 법령(개인정보보호법, 정보통신망 이용촉진 및 정보보호 등에 관한 법률, 전자금융거래법 등)의 준수여부는 심사기준서 제외
3. 시스템 물리적 통제 (S2-03-DE)	① **(보호구역 설정)** 전산설비에 대한 보호구역 설정이 되어있는가? - 전산설비 설치장소를 보호구역으로 설정하고, 보호구역 내 작업(시스템 유지보수, 시스템 도입 등)이 필요한 경우 작업기록을 관리하며, 보호구역 반출 및 반입 내역 관리 필요
	② **(출입통제)** 전산설비에 대한 출입통제대책(카드키 혹은 지문인식 등)이 수립되어 있는가? - 사전 인가자 인증을 위한 대책(카드키 혹은 지문인식 등)이 마련되어 있어야 하며, 사전 인가자 외 인원은 책임자의 승인을 받아 출입하며(내부 담당자 동행) 출입자 관리기록부에 기록(신원, 방문목적, 방문일시 등) 필요
	③ **(잠금장치 보호)** 중요서버는 잠금장치로 보호되어 있는가? - 중요 서버는 잠금장치로 보호되어 해당 서버 관리자만 접근할 수 있도록 대책 필요. 단, 출입통제대책이 마련된 전산실에 관리자만 출입할 수 있는 경우에는 제외

분야	심사기준
	④ **(IDC 계약사항)** 전산설비를 클라우드 및 IDC에 위탁 운영하는 경우, S2-03-DE ①~③기준에 대한 물리적 통제 관련 요구사항을 계약서에 반영하고 운영상태를 주기적으로 검토하고 있는가? - S2-03-DE ①~③기준에 대한 시스템 물리적 보안요구사항을 위탁운영기관과의 계약서에 반영 필요. 다만 위탁운영기관이 정보보호 인증서(ISMS, ISO 27001, 클라우드 보안인증제도 등 관련 인증서 中1개 이상)를 보유하고 위탁전산설비가 해당 인증서 범위 내에 포함되는 경우 계약서 반영사항을 인증서로 갈음
4. 시스템 기술적 통제 (S2-04-DE)	① **(안전한 비밀번호 적용)** 중요서버에 접근하는 계정은 안전한 비밀번호를 사용하도록 설정 및 적용되고 있는가? - 중요서버에 접근하는 계정 중 root계정은 원격 접속을 제한하여야 하며, 패스워드는 적절한 조합규칙(아이디, 생년월일, 주민번호 등을 포함하지 않은 영문자, 특수문자, 숫자를 혼합한 8자리 이상)으로 설정하고, 분기별 1회 이상 변경, 보관 시 암호화, 시스템마다 관리자 비밀번호가 다르게 지정, 비밀번호 연속오류에 대한 대응 등 필요
	② **(접속단말 지정)** 중요서버에 대한 접근은 중요PC 및 지정된 서버 등에 대해서만 허용하고 있는가? - 중요서버에 접근하는 단말(중요PC 및 지정된 서버)이 중요서버와 다른 네트워크 구간에 위치하는 경우, 침입차단시스템 등의 접근제어를 통해 해당 단말로부터 중요서버의 특정포트로만 통신할 수 있도록 설정 필요
	③ **(불필요 통신 및 서비스 차단)** 중요서버는 업무상의 용도를 제외하고 외부통신망(인터넷 등)의 연결 및 불필요한 서비스가 차단되어 있는가? - 기본적으로 외부통신망과 연결이 차단되어있어야 하며, 중요 PC 및 서버 등이 외부에 있어 부득이하게 통신해야할 경우 침입차단시스템 등의 접근통제 방안이 적용 필요. 서버 내 불필요한 서비스(Finger서비스, r계열서비스, NFS서비스, tftp서비스 등)가 열려 있지 않도록 설정 필요 ※ 불필요한 서비스를 해제하는 방법은 '주요정보통신기반시설 취약점 분석·평가 방법 상세가이드(KISA)' 참조
	④ **(보안패치 적용)** 중요서버에 대해 최신보안패치를 적용하고 있는가? - 중요서버에 적용할 패치의 중요도에 따라 긴급하고 중요한 패치의 경우 즉시, 보통레벨의 패치 사항의 경우 일정기간 내 적용할 수 있도록 관련 절차 필요

분야	심사기준
	⑤ **(악성코드 대응)** 중요서버에 대해 악성코드 대응 방안을 적용하고 있는가? - 중요서버에 악성코드탐지 프로그램을 설치하고 정기적으로 악성코드탐지 프로그램을 업데이트 하며 실시간 검사가 이뤄질 수 있도록 설정필요. 단, UNIX계열의 서버는 제외
	⑥ **(안전한 서버운영)** 중요서버는 독립서버로 운영하고, 정보보안시스템(차단시스템 등)을 적용하여 보호하고 있는가? - 시스템 용도(웹/WAS, 어플리케이션, DB 등)별로 독립된 서버의 운영이 필요하며 서버 가상화(가상머신 등)를 이용하는 경우 별도의 보호대책 필요 (예: 가상머신별 접근관리, 데이터 분리 및 보호, 하이퍼바이저와 가상머신사이의 인터페이스 취약점에 대한 보호대책 수립 등)
	⑦ **(정보보호시스템 취약정책 제거)** 정보보호시스템(침입차단시스템 등)내 취약한 정책이 존재하지 않는가? - 기본적으로 All Deny정책이 적용되어 있고, 접근이 필요한 최소한의 서비스만 허용되어 있어야 하며, 취약한 정책(네트워크IP주소 단위로 허용된 정책, 출발지 포트 기반의 정책, 양방향으로 설정된 정책 등)이 없는지 주기적으로 확인 필요.
	⑧ **(웹 취약점 점검)** 인터넷에 공개된 웹 서버에 대해 웹 취약점 점검을 수행하였는가? - 자체 혹은 외부기관에서 점검한 수행결과 및 조치계획서 첨부
	* 고려사항 : 중요서버는 중요도를 고려하여 사전 지정 필수(예: DB, 웹 등)
5. 중요 PC 통제 (S2-05-DE)	① **(불필요 통신 및 프로그램 차단)** 중요PC(관리자 PC, 개발 PC 등)는 업무상의 용도를 제외하고 외부통신망(인터넷 등)의 연결 및 불필요한 프로그램이 설치되어 있는가? - 중요PC는 외부통신망과 물리적 혹은 논리적 망분리가 적용되어야 하며, 불필요한 프로그램(상용 메신저 등)의 제거 필요
	② **(안전한 비밀번호 적용)** 중요PC에 대한 계정은 안전한 비밀번호를 사용하도록 설정 및 적용되고 있는가?

분야	심사기준
	- 패스워드는 적절한 조합규칙(아이디, 생년월일, 주민번호 등을 포함하지 않은 영문자, 특수문자, 숫자를 혼합한 8자리 이상)으로 설정하고, 분기별 1회 이상 변경, 보관시 암호화 등 필요
	③ **(보안패치 적용)** 중요PC에 대해 최신보안패치를 적용하고 있는가? - 중요PC는 HOT Fix등 최신보안패치를 적용하며, 설치된 응용 프로그램(한글, MS-Office, 어도브 아크로뱃 등)에 대해 정기적으로 패치할 수 있도록 관련 절차 필요
	④ **(악성코드 대응)** 중요PC에 대해 악성코드 대응 방안을 적용하고 있는가? - 중요서버에 악성코드탐지 프로그램을 설치하고 정기적으로 악성코드탐지 프로그램을 업데이트 하며, 실시간 검사 및 OS에서 제공하는 침입차단 기능 활성화 필요
	⑤ **(외부반출 통제)** 중요PC에 대해 외부반출을 통제하고 있는가? - 중요PC는 원칙적으로 외부로 반출하지 않도록 통제하여야 하며, 외부반출 시 중요서버에 접근금지 및 중요데이터 삭제 등의 조치 필요
	⑥ **(보조기억매체 통제)** 중요PC에서 보조기억매체 및 휴대용전산장비에 접근하는 것을 통제하고 있는가? - 중요PC의 보조기억매체 및 휴대용전산장비 접근은 원칙적으로 금지하나, 필요가 불가피한 경우 별도의 보호대책 마련 필요 (예: 악성코드탐지, 접근관리대장 관리, 관리자 통제 하에서만 사용 등)
	⑦ **(중요정보 저장제한)** 비중요 PC 내에 중요정보(개인정보, 암호키 등) 저장을 제한하고 있는가? - 주기적으로 비중요 PC내에 중요정보가 저장되어 있는지 여부를 확인할 수 있는 관련 절차 필요
	* 고려사항 : 중요PC 사전 지정 필수 (예: 중요서버에 접근 가능한 PC, 개인정보를 취급하는 PC 등)
6. 네트워크 통제	① **(네트워크 분리)** 시스템 용도(웹, DB 등)에 따라 네트워크 구간이 분리되어 있는가?

분야	심사기준
(S2-06-DE)	- 웹, DB 등 시스템 용도별로 네트워크를 분리하여야 하며, 네트워크 가상화(가상 스위치 등)를 이용하는 경우 별도의 보호대책 필요 (예: 가상 스위치별 VLAN설정 등)
	② **(구간별 접근제어)** 네트워크 구간별로 접근제어가 설정되어 있는가? - 웹은 DMZ, DB는 내부망 등 네트워크 구간별로 허용 IP 및 포트를 관리를 통해 접근제어 필요
	③ **(대외통신 보호)** 대외기관(금융회사 등)과의 통신 시 보안통신(전용회선 혹은 VPN 등)이 적용되어 있는가? - 대외기관과의 통신 시에는 전용회선 혹은 VPN을 사용하여야 하나, 전송계층에서의 보안통신(SSL등)을 사용하여야할 경우 해당 별도의 보호대책 필요 (예 : 취약한 버전의 SSL 프로토콜 사용 금지 등) - 단, 대외기관과 HTS 등 별도의 통신프로토콜을 사용하여야 하는 경우, 정해진 프로토콜 내에서 중요정보가 암호화되어 전송되도록 보호대책 필요
	④ **(무선네트워크 통제)** 무선네트워크는 통제 하에 이용을 최소화하며, 이용 시 보호대책을 적용하였는가? - 무선네트워크 이용 시 SSID는 hidden, 암호정책은 WPA이상, MAC필터링 적용, 중요서버가 위치한 네트워크에서는 사용금지 확인
	⑤ **(원격통신 통제)** 중요서버 원격 통신 시 보안통신(전용회선 혹은 VPN 등)이 적용되어 있는가? - IDC 및 클라우드 등에 위치한 중요서버와의 원격 통신 시 전용회선 혹은 VPN(SSH등 포함) 사용 여부 확인
	⑥ **(내부 네트워크 통제)** 인가된 사용자만이 중요서버가 위치한 네트워크에 접근할 수 있도록 통제하고 있는가? - 내부망에 접근가능한 네트워크장비(스위치, 라우터, VPN 등)에 비인가자가 접근할 수 없도록 물리적, 관리적, 혹은 기술적 통제 필요 (예: 네트워크 포트에 접근할 수 없도록 포트잠금장치 설치, 인가된 사용자만 네트워크 식별자(IP 등)할당 등)

참고 3 자주하는 질문(FAQ)

Q1) 단독, 컨소시엄 두 가지 방식으로 신청하려 합니다. 시스템 보안성심사를 두 번 받아야 하나요?

⇒ 원칙적으로 각각 시스템 보안성심사를 받아야 하며, 시스템 및 네트워크의 구성이 동일한 경우에는 한번으로 갈음할 수 있습니다.

Q2) 로보어드바이저 시스템을 자체전산설비가 아닌 클라우드, IDC 등 외부환경에 운영 중입니다. 현장심사(2단계)는 어떻게 하게 되나요?

⇒ 서비스제공자(클라우드, IDC 등)와 로보어드바이저 기업 간 계약서 및 서비스제공자의 관련인증서 보유여부 등을 종합적으로 고려하여 일부 심사기준은 서면심사(1단계)로 갈음할 수 있습니다.

Q3) 시스템 보안성심사 시 서면심사(1단계)는 필수인가요?

⇒ 서면심사(1단계)는 사전에 보안 취약점을 점검하여 로보어드바이저 기업이 보완할 수 있도록 함으로써 로보어드바이저 기업의 현장심사(2단계)를 지원하는 목적으로 필수입니다.

Q4) 보안시스템 구축에 필요한 예산은 대략 얼마인가요?

⇒ 보안시스템 구축 시 예산에 관한 사항은 금융보안원의 보안성심사와 관련이 없습니다.

Q5) 온라인 및 오프라인 형을 구분하는 기준은 어떻게 됩니까?

⇒ 웹 서비스 상에서 고객 계정을 기반으로 고객 맞춤형 정보를 제공하는 경우가 온라인에 해당됩니다.

Q6) IDC 및 클라우드서비스 이용 시 시스템 물리적 통제 요구사항 대해 어떻게 증빙자료를 제출해야하나요?

⇒ IDC 및 클라우드에서 물리적 통제를 위해 마련한 보안대책을 증빙할 수 있다면 어떤 형식(계약서, 홈페이지, 이메일 등)의 증빙자료이던 괜찮습니다. 만일 ISO 27001과 같은 인증서 보유 시 해당 인증서로도 갈음할 수 있습니다.

Q7) 기존 인터넷뱅킹을 이용한 고객을 대상으로 상품을 추천하는 경우, '온라인형' 인가요 '오프라인형' 인가요?

⇒ '온라인' 형이며, 이때 사용자인증 및 계좌소유주인증의 증빙자료는 기존 사용자인증방식(공인인증서 등)을 기술함으로써 갈음할 수 있습니다.

Q8) 기존 금융회사 내부의 보안성심사를 받은 시스템을 대부분 이용하는데, 이때에도 해당 시스템에 대한 심사자료를 제출해야하나요?

⇒ 기본적으로 심사자료는 제출해야하며, 편의에 따라 자체보안성 심사를 받은 자료를 첨부하고, 심사기준별로 해당되는 부분을 표기하여 제출해 주시면 됩니다.

Q9) 금융회사 내부의 모든 시스템에 대해 시스템 및 네트워크 구성도를 작성해야하나요?

⇒ 로보어드바이저와 관계된 서버(운용지시 서버 등)를 중심으로 해당 서버가 어떻게 보호되고 있는지 알 수 있도록 시스템 및 네트워크 구성도를 작성하시면 됩니다.

Q10) 금융회사가 자문·일임업 및 로보어드바이저 기술보유업체(이하 핀테크 업체)와 컨소시엄으로 참여하려 합니다. 현장심사(2단계)는 어떤 경우에 받아야 하나요?

⇒ 핀테크 업체가 금융회사 밖에서 별도의 시스템을 운영하는 경우 핀테크 업체가 운영하는 시스템은 현장심사를 받으셔야 합니다.

참고 4 로보어드바이저 테스트베드 보안대책명세서 샘플

보안대책명세서

심사기업 : ○○○○

[심사알고리즘 : ○○○○**]**

1. 서비스 개요

○ 서비스 명

— ABC 로보어드바이저

○ 서비스 특징

— 고객의 일임동의를 얻은 후, 펀드 및 주식을 운용자산으로 하여 고객의 자산을 운용하는 서비스로 고객은 홈페이지 회원가입 후 매매내역 및 수익률 등을 조회할 수 있으며, 필요시 포트폴리오 구성을 다시 할 수 있도록 지시할 수 있다.

2. 서비스 유형

○ 온라인형 *(오프라인형인 경우에는 '오프라인'으로 표시)*

— 서버 운영 형태 : IDC위탁 (위탁 업체명 : XYZ)

— 고객 맞춤형 서비스 종류 : 회원가입, 수익률 및 포트폴리오 조회

○ 컨소시엄형 *(단독형인 경우에는 '단독형'으로 표시)*

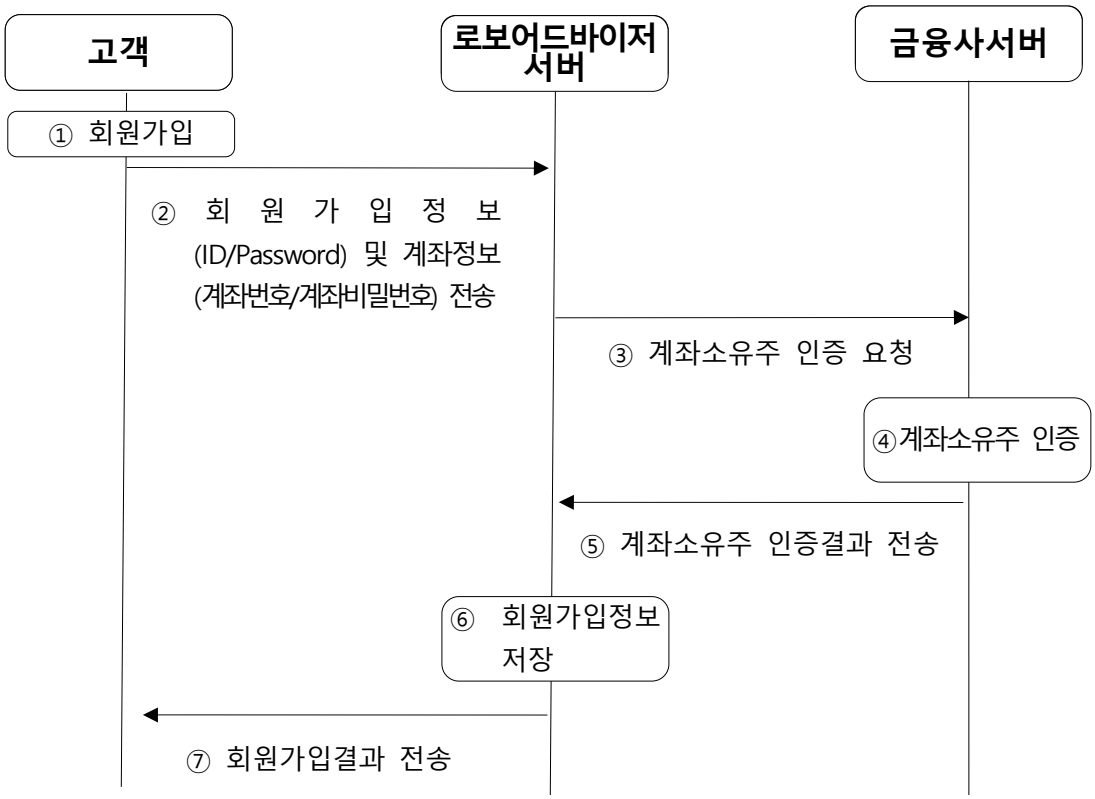
— ○○금융사 : 고객정보 제공 및 운용지시

— ○○자문사 : 포트폴리오 제공
(시스템 위치 : 금융회사 내부)
(금융회사 외부에 위치한 경우에는 '외부'로 표시)

3. 서비스 절차

○ 회원가입 *(모든 서비스 절차(포트폴리오 제공, 운용지시 등)에 대해 기술)*

— 서비스 프로세스



절차	상세 내용	비고
① 회원가입	- 고객이 로보어드바이저 홈페이지를 방문하여 회원가입 진행	
② 회원가입정보 및 계좌정보 전송	- Password는 고객 입력부터 로보어드바이저 서버까지 E2E암호화 솔루션을 적용하여 전송 - 계좌정보는 고객 입력부터 금융사서버까지 E2E암호화 솔루션을 적용하여 전송	적용한 E2E암호화 제품은 ABC사의 DEF 임
③ 계좌 소유주 인증 요청	- 로보어드바이저 서버는 E2E암호화한 계좌정보를 금융사서버로 전달	

절차	상세 내용	비고
④ 계좌 소유주 인증	- 금융사서버는 E2E암호화된 계좌정보를 복호화하여 원장에 기록된 계좌정보와의 일치여부 확인	
⑤ 계좌 소유주 인증결과 전송	- 계좌소유주 인증결과를 로보어드바이저 서버로 전달	
⑥ 회원가입정보 저장	- 로보어드바이저 서버는 계좌소유주 인증을 통과한 고객에 한하여 회원 ID 및 단방향으로 암호화한 Password를 저장	단방향 암호화는 SHA-256 이용
⑦ 회원가입결과 전송	- 금융사 서버는 회원가입 여부를 고객에게 전송	

— 화면정의서

//회원가입화면

— 주요 보호정보 및 보호방안

주요 보호정보	보호방안
계좌정보	- 계좌정보는 입력부터 전송 및 처리완료시점까지 E2E암호화 적용 - 입력시 가상키패드 활용
회원 Password	- Password는 입력부터 전송 및 처리완료시점까지 E2E암호화 적용 - Password는 8자리이상 문자, 숫자 및 특수문자를 포함하도록 설정 - 주기적으로 Password를 변경할 수 있도록 관리

○ 포트폴리오 제공

(회원가입과 동일한 방식으로 기술하며, 특히 고객, 로보어드바이저 서버, 금융사 서버간 주고받는 중요정보의 처리, 저장, 전송 내역은 반드시 포함)

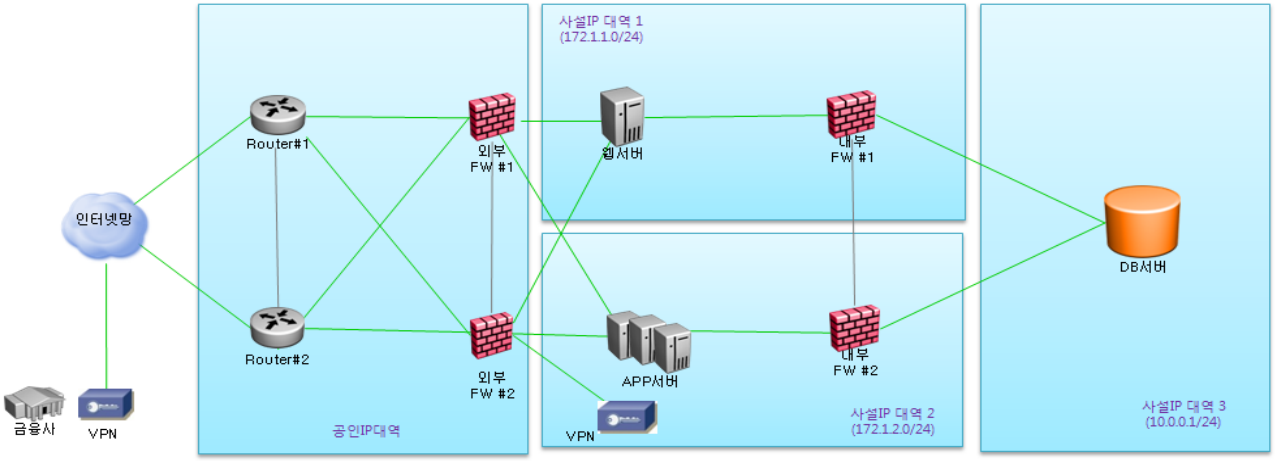
○ 운용지시

(회원가입과 동일한 방식으로 기술하며, 특히 고객, 로보어드바이저 서버, 금융사 서버간 주고받는 중요정보의 처리, 저장, 전송 내역은 반드시 포함)

4. 시스템 및 네트워크 구성도

(중요서버 리스트 및 각각의 역할을 기술하고, 중요서버에서 처리되는 중요정보, 중요서버 보호를 위한 보호조치(정보보호시스템, 네트워크 통제사항 등) 표기)

(컨소시엄 형태로 한 개 이상의 사이트에서 시스템 운영 시 각 사이트별로 시스템 및 네트워크 구성도 표기)



중요서버	역할	중요 처리정보	보호조치
웹서버	– 회원 로그인 – 수익률 조회	– 인증정보 – 개인정보 – 금융정보	– 방화벽 적용 – 최신 보안패치, 악성코드 탐지프로그램 적용 – 인터넷 차단 및 불필요한 통신포트 차단
APP서버	– 시세정보 수집 – 로보어드바이저 알고리즘 엔진 탑재 – 매매지시	– 개인정보 – 금융정보 – 운용지시	– 방화벽 적용 – 최신 보안패치, 악성코드 탐지프로그램 적용 – 금융사 통신시 VPN이용 – 인터넷 차단 및 불필요한 통신포트 차단
DB서버	– 데이터 저장	– 개인정보 – 금융정보 – 인증정보	– 2중 방화벽 적용 – 최신 보안패치, 악성코드 탐지프로그램 적용 – 인터넷 차단 및 불필요한 통신포트 차단

5. 심사기준 별 보호대책

○ 검토결과 요약

(단위 : 개)

총 심사기준	적합(예)	부적합(아니오)	N/A*
31	31	0	0

* N/A : 로보어드바이저 유형이 심사기준에 부합하지 않는 경우 N/A처리가능

○ 상세 검토내역

분야	심사 번호	심사기준	확인결과	증적자료*
이용자 및 계좌소유주 인증	S2-01-DE	① 이용자 인증 방법이 적정하게 설계되어 있는가?	□예 □아니오 □N/A	
		② 계좌 소유주 인증 방법이 적정하게 설계되어 있는가?	□예 □아니오 □N/A	
		③ 인증 및 거래관련 기록(인증시도 및 결과, 접속정보 등)을 보존하고 관련기록의 변경에 대한 보호대책이 마련되어 있는가?	□예 □아니오 □N/A	
중요정보 보호대책	S2-02-DE	① 중요정보(개인정보, 금융정보, 패스워드 등)는 안전하게 암호화하여 기밀성을 보장할 수 있도록 설계되어 있는가?	□예 □아니오 □N/A	
		② 중요정보(운용지시 등)는 위변조 여부 등 무결성을 검증할 수 있도록 설계되어 있는가?	□예 □아니오 □N/A	
		③ S2-02-DE ①, ②에 적용된 암호화 알고리즘은 국내외 전문기관(NIST, KISA 등)에서 권고한 암호화 알고리즘 및 키길이를 사용하고 안전하게 관리되고 있는가?	□예 □아니오 □N/A	

분야	심사 번호	심사기준	확인결과	증적자료*
시스템 물리적통제	S2-03-SE	① 전산설비에 대한 보호구역 설정이 되어 있는가?	□예 □아니오 □N/A	
		② 전산설비에 대한 출입통제대책(카드키 혹은 지문인식 등)이 수립되어 있는가?	□예 □아니오 □N/A	
		③ 중요서버는 잠금장치로 보호되어 있는가?	□예 □아니오 □N/A	
		④ 전산설비를 클라우드 및 IDC에 위탁 운영하는 경우, S2-03-SE ①~③기준에 대한 물리적 통제 관련 요구사항을 계약서에 반영하고 운영상태를 주기적으로 검토하고 있는가?	□예 □아니오 □N/A	
시스템 기술적통제	S2-04-SE	① 중요서버(중요도를 고려하여 사전 지정 필수(예: DB, 웹 등))에 접근하는 계정은 안전한 비밀번호를 사용하도록 설정 및 적용되고 있는가?	□예 □아니오 □N/A	
		② 중요서버에 대한 접근은 중요PC 및 지정된 서버 등에 대해서만 허용하고 있는가?	□예 □아니오 □N/A	
		③ 중요서버는 업무상의 용도를 제외하고 외부통신망(인터넷 등)의 연결 및 불필요한 서비스가 차단되어 있는가?	□예 □아니오 □N/A	
		④ 중요서버에 대해 최신보안패치를 적용하고 있는가?	□예 □아니오 □N/A	
		⑤ 중요서버에 대해 악성코드 대응 방안을 적용하고 있는가?	□예 □아니오 □N/A	
		⑥ 중요서버는 독립서버로 운영하고, 정보보안 시스템(차단시스템 등)을 적용하여 보호하고 있는가?	□예 □아니오 □N/A	
		⑦ 정보보호시스템(침입차단시스템 등)내 취약한 정책이 존재하지 않는가?	□예 □아니오 □N/A	
		⑧ 인터넷에 공개된 웹 서버에 대해 웹 취약점 점검을 수행하였는가?	□예 □아니오 □N/A	

분야	심사 번호	심사기준	확인결과	증적자료*
중요PC 통제	S2-05-SE	① 중요PC(관리자 PC, 개발 PC 등)는 업무상의 용도를 제외하고 외부통신망(인터넷 등)의 연결이 차단되고 및 불필요한 프로그램이 제거되어 있는가?	□예 □아니오 □N/A	
		② 중요PC에 대한 계정은 안전한 비밀번호를 사용하도록 설정 및 적용되고 있는가?	□예 □아니오 □N/A	
		③ 중요PC에 대해 최신보안패치를 적용하고 있는가?	□예 □아니오 □N/A	
		④ 중요PC에 대해 악성코드 대응 방안을 적용하고 있는가?	□예 □아니오 □N/A	
		⑤ 중요PC에 대해 외부반출을 통제하고 있는가?	□예 □아니오 □N/A	
		⑥ 중요PC에서 보조기억매체 및 휴대용전산장비에 접근하는 것을 통제하고 있는가?	□예 □아니오 □N/A	
		⑦ 비중요 PC 내에 중요정보(개인정보, 암호키 등) 저장을 제한하고 있는가?	□예 □아니오 □N/A	
네트워크 통제	S2-06-SE	① 시스템 용도(웹, DB 등)에 따라 네트워크 구간이 분리되어 있는가?	□예 □아니오 □N/A	
		② 네트워크 구간별로 접근제어가 설정되어 있는가?	□예 □아니오 □N/A	
		③ 대외기관(금융회사 등)과의 통신 시 보안통신(전용회선 혹은 VPN 등)이 적용되어 있는가?	□예 □아니오 □N/A	
		④ 무선네트워크는 통제 하에 이용을 최소화하며, 이용 시 보호대책을 적용하였는가?	□예 □아니오 □N/A	
		⑤ 중요서버 원격 통신 시 보안통신(전용회선 혹은 VPN 등)이 적용되어 있는가?	□예 □아니오 □N/A	
		⑥ 인가된 사용자만이 중요서버가 위치한 네트워크에 접근할 수 있도록 통제하고 있는가?	□예 □아니오 □N/A	

* 증적자료는 표 안에 입력하거나, 자유형식으로 별도 첨부 가능

증적자료 작성 시 고려사항

① **(보안대책 기술)** 각 기준별로 보안대책을 **육하원칙으로 상세히 기재**

※「시스템 보안성심사 기준 상세」(p7 ~ 12)를 참고하여 **각 세부심사기준에 보안대책이 어떻게 부합하는지를 기술**

확인결과에 **'예'**를 선택하지 않은 경우 **미선택의 사유를 반드시 작성**

② **(객관적 증빙자료 첨부)** 기술한 내용을 객관적으로 증빙할 수 있는 자료를 첨부

※ (증빙자료의 예) 스크린 샷, 소스코드 일부발췌, 심사기준을 만족하는 내용이 포함되어있는 운영기록(증적자료)의 제목(파일명), 관련 증적이 시스템으로 관리되는 경우 해당 시스템 위치, 시스템명 등

※ 심사기준별 증적자료 작성 예시

[심사기준]
1.1 (이용자 인증) 이용자 인증을 위한 방법이 적정하게 설계되어 있는가?

- 인증방법(패스워드, 생체인증, OTP 등) 자체의 안전성(메커니즘, 알고리즘 등)과 인증 프로세스 전반의 안전성을 함께 고려하여 설계해야 하며, 서비스 이용 시 타인의 명의를 도용할 수 없도록 대책 (특히, 휴대폰 인증의 경우 메시지 탈취, 전화번호 변조, 휴대폰 도난 등의 대책) 필요
- 인증정보 탈취를 위한 공격(세션 가로채기, 비밀번호 무작위 대입공격, 인증정보 재활용 등)에 대한 대책 필요

[증적자료]

(보안대책) 사용자 인증을 위해 패스워드인증 및 구글에서 지원하는 OTP인증을 사용하고 있으며, 패스워드의 경우 8자리 이상(특수문자, 영문, 숫자 혼합)을 요구하고 있음. 비밀번호 탈취공격을 막기 위해, 패스워드 및 OTP입력부터 검증까지 모든 과정을 세션으로 관리하고 있으며, 세션 유효시간을 30분으로 한정하고 있음. 또한 5회 이상 패스워드 및 OTP인증이 틀릴 경우, 사용자의 웹서비스 이용을 차단

(증빙자료)

패스워드 인증화면	OTP사용화면

RA 테스트베드 계좌 수익률 산출을 위한 한국예탁결제원 업무 프로세스 안내

- 제2차 정기심사 -

KSD 한국예탁결제원

RA 테스트베드 계좌 수익률 산출을 위한 한국예탁결제원 업무 프로세스 안내

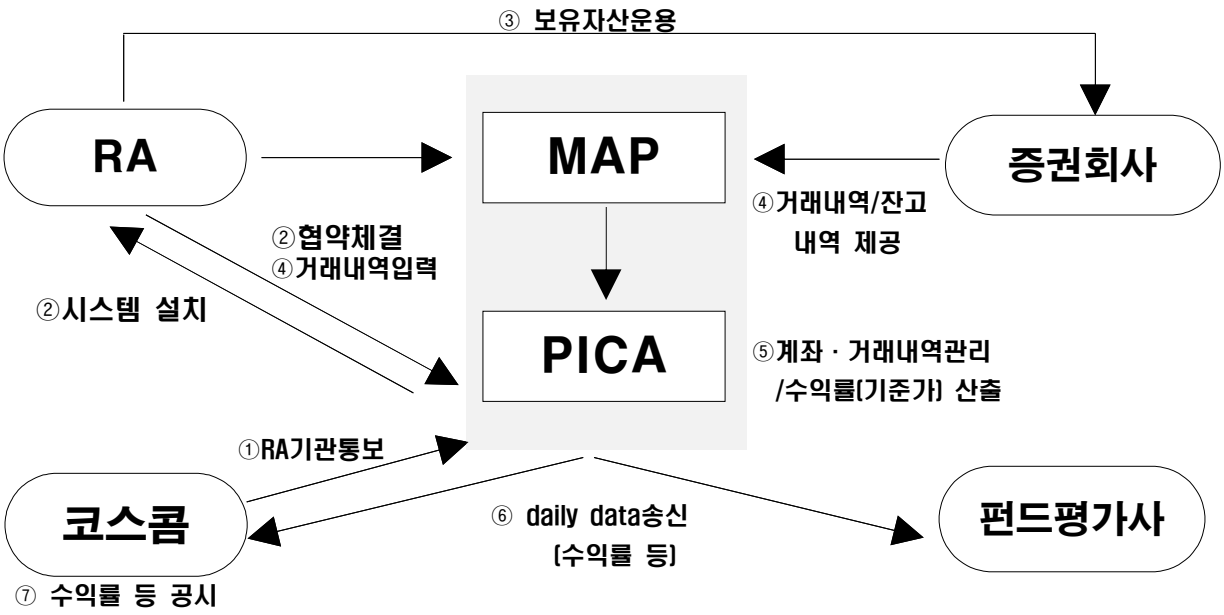
(2017. 3. 한국예탁결제원)

1 업무정의

테스트베드에 참가하는 RA(이하 "RA" 라 함)의 투자 운용성과 등의 투명한 관리를 위해 펀드의 기준가격 산출 전문기관인 한국예탁결제원이 RA를 대신하여 운용계좌별 매매내역, 입출금내역, 잔고내역 등에 대한 정보를 전용 네트워크를 이용하여 증권사로부터 수신하고, 이를 기반으로 수익률을 산출하여 관련기관에 통보하는 업무

2 업무처리 운용구조

2.1 업무 프로세스 흐름도



2.2 수익률 산출을 위한 협약 체결 및 시스템(PICA) 설치(펀드서비스부)

2.3 MAP(Managed Asset Platform)* 이용을 위한 계좌개설(증권예탁부)

* MAP : 투자자문사 투자일임재산의 매매주문 확인 등 백오피스 업무의 표준화 및 자동화 지원 필요성에 따라 투자자문사를 대상으로 예탁결제원(SAFE+) 네트워크를 이용하여 증권사로부터 수신한 매매주문에 따른 거래내역, 잔고내역 등을 제공하는 업무

- 계좌개설 및 업무참가 신청, 공인인증서 및 SAFE+사용 신청

2.4 MAP상 RA 정보 및 증권회사 운용(위탁)계좌 정보 등 등록(펀드업무부)

2.5 MAP상 거래시 매매자료 등에 대한 자료 확인 및 승인(펀드업무부)

2.6 PICA 수익률 산출을 위한 각종 거래내역 정보 등록(펀드서비스부)

2.7 MAP 미사용 자산 거래내역/잔고내역 PICA 등록(펀드서비스부)

2.8 PICA 최종 수익률 산출 검증 및 승인(펀드서비스부)

2.9 펀드평가사, 사무국에 거래내역 및 수익률 등 데이터 전송(펀드서비스부)

3 관련부서 연락처

업무구분		문의처		
		부서	팀	연락처
SAFE+	계좌개설	증권예탁부	예탁총괄팀	02) 3774-3094
	공인인증서			02) 3774-3084
자산관리 플랫폼 (MAP)	RA정보 및 계좌등록	펀드업무부	펀드운용지원팀	051) 519-1752
	매매자료/잔고내역 송수신 등			051) 519-1757
PICA	RA수익률산출 업무계약체결	펀드서비스부	펀드컨설팅팀	02) 3774-3490
	MAP미사용자산 거래/잔고내역 송수신 등		펀드회계팀	02) 3774-3699
				02) 3774-3487
			펀드지원(IT)팀	02) 3774-3493

로보어드바이저 테스트베드
기본 운영방안

금융위원회 자산운용과

금융위원회

보 도 자 료

보도	2016.08.29.(월) 조간 이후	배포	2016.08.26(금)

책 임 자	금융위 자산운용과장 김 기 한(02-2100-2660)	담 당 자	송 병 관 사무관 (02-2100-2665) 박 보 라 사무관 (02-2100-2668)
	금감원 자산운용감독실장 오 용 석(02-3145-6700)		김 진 옥 부국장 (02-3145-6702)
	코스콤 기술연구소장 정 동 윤(02-767-8008)		강 석 희 부장 (02-767-7979)
	금융보안원 보안전략본부장 전 융(02-3495-9004)		박 진 석 부장 (02-3495-9600)
	한국예탁결제원 투자지원본부장 강 보 선(02-3774-3106)		신 명 희 부장 (02-3774-3480)

제 목 : 맞춤형 자산관리서비스의 대중화 시대를 열게 될 「로보어드바이저 테스트베드 기본 운영방안」

■ 자산관리산업에 혁신을 불러일으키고, 투자자에게 보다 효율적이고 넓은 선택의 기회를 제공하게 될 로보어드바이저 테스트베드를 실시합니다.

○ 시장에 알려질 기회가 많지 않았던 창업초기 로보어드바이저 업체도 테스트베드를 통해 우수한 기술과 역량을 마음껏 발휘할 수 있습니다.

○ 테스트베드 웹사이트를 통해 다양한 전략을 가진 로보어드바이저를 직접 비교할 수 있게 됩니다.

○ 테스트베드에 참여한 로보어드바이저에 대해 알고리즘의 합리성, 투자자 맞춤성, 법규준수성, 시스템 보안성·안정성 등을 중점적으로 심사합니다.

■ 금융회사는 내년 상반기 중 로보어드바이저가 자문·운용인력을 대신하는 로보어드바이저 자문·일임서비스를 시작할 수 있습니다.

■ 테스트베드를 통과한 로보어드바이저의 자문·일임서비스가 시작되면, 소액을 투자하는 일반 국민도 저렴한 비용으로 자문·일임서비스를 이용할 수 있습니다.

➡ 맞춤형 자산관리서비스의 대중화, 그 첫걸음이 시작됩니다.

I. 추진 경과

□ IT, 인공지능 등 기술발전 등에 힘입어 **국내·외에서 로보어드바이저 자산관리서비스가 빠르게 성장 중***

* (미) $157억('14.6) → $190억('14.12) → $210억('15.6) → $867억('17, 예상), MyPrivateBanking

□ 다만, 로보어드바이저에 적합한 규율체계가 완비되지 못하여 **로보어드바이저의 신뢰성 및 안정성 등에 대한 시장의 우려**가 제기

□ 이에, 금융위는「서비스경제 발전전략」등을 통해 **로보어드바이저 테스트베드 운영계획을 발표하고 규제개선을 추진**해 왔으며,

○ 금번에, 금융당국, 학계, 업계로 구성된 TF를 통해 **공정하고 내실 있는 테스트베드 운영방안을 준비·발표**

< 로보어드바이저의 개요 및 주요 특징 >

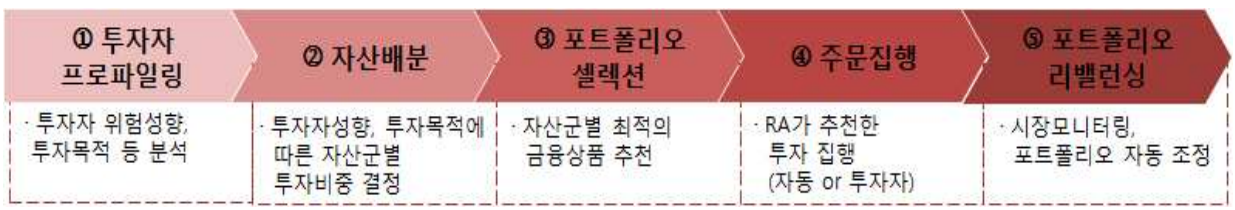
□ **(개념)** 알고리즘, 빅데이터 분석 등에 기반한 **컴퓨터 프로그램을 활용**하여 **자동적으로 포트폴리오 자문.운용서비스를 제공**하는 **온라인 상의 자산관리서비스**

□ **(주요 특징)** 사람의 개입을 최소화한 **자동화된 알고리즘**과 **온라인 플랫폼을 기반**으로 **자산관리 서비스에 대한 접근성 제고**

① 전통적인 자산관리서비스에 비해 **낮은 수수료와 최소가입금액**으로 일반 국민도 **큰 부담 없이** 자문·일임서비스 향유 가능

② **온라인·모바일 기기**를 통해 **언제, 어디서나 편리**하게 서비스이용이 가능

③ 투자자성향 분석 및 포트폴리오 산출 **프로그램을 기반**으로 **체계적인 포트폴리오 자문·일임서비스**



II. 「로보어드바이저 테스트베드 기본 운영방안」 주요 내용

◇ **[테스트베드 운영 목적]** 분산투자, 투자자성향 분석, 해킹방지체계 등 **투자자문·일임을 수행하기 위한 최소한의 규율이 제대로 작동하는지 여부를 확인**하는 절차로, **RA의 수익성 검증이 목적이 아님**

1. [신청 요건] 누가, 무엇을 가지고 신청할 수 있는가?

1 **(참여가능 업체 유형)** 순수 RA 기술업체(자문·일임 未등록), RA 기술을 보유한 자문·일임업자, 업체간 컨소시움 등 다양한 업체가 참여할 수 있도록 **참가유형을 폭넓게 인정**

2 **(신청대상 알고리즘) 펀드, 파생결합증권, 주식으로 구성***(운용자산 요건)된 **포트폴리오를 자동으로 산출·운용**(자동화 요건)하는 알고리즘이 참여할 수 있으며, 한 업체가 **복수의 알고리즘 신청도 가능**

* 대기성 자금을 예금, RP 등으로 운용하는 것은 허용되나, 채권과 파생상품(선물, 옵션 등)은 운용대상에서 제외

2. [세부심사내용] 어떤 사항에 대해, 어떻게 테스트 하는가?

1 **(심사 프로세스) 사전심사, 본심사**(포트폴리오 운용심사, 시스템심사), **최종심의**를 거쳐 테스트베드 **통과여부를 결정**

2 **(1단계 : 사전심사) 참여요건**(신청 업체, 알고리즘) **충족 여부를 확인**하고, **가상의 투자자 정보**를 바탕으로 **알고리즘의 투자자 성향별 포트폴리오 산출역량**을 심사(1개월 이내)

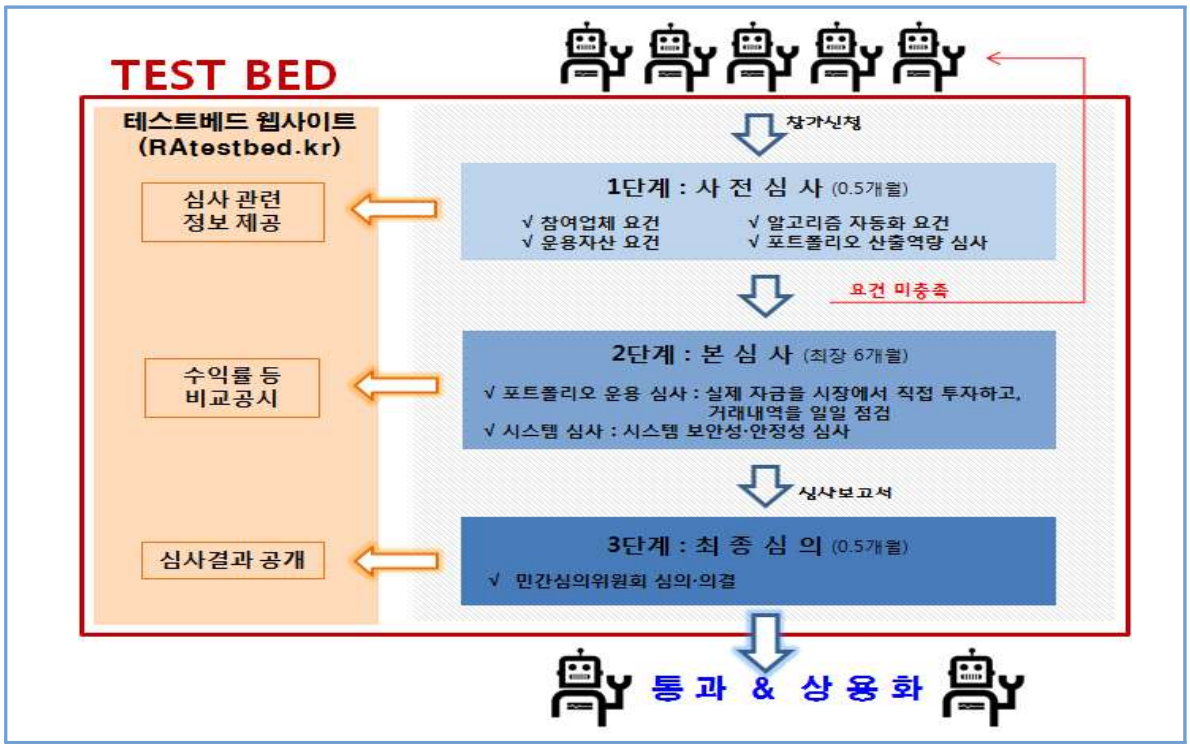
3 **(2단계 : 본심사)** 사전심사에서 **도출된 포트폴리오에 대해 일정기간**(6개월 이내) **동안 실제 자금***을 **운용**토록 하여 **알고리즘의 안정성** 심사

* 원칙적으로 업체 고유자금을 운용하되, RA 기술보유 핀테크업체(자문·일임 未등록)가 단독으로 참여하는 경우에는 임원자금으로 운용하는 것을 허용

○ 또한, **단기간 내에 상용화**를 하려는 업체에 대해서는 해킹·재해방지 체계 등 **서비스 전달체계의 안정성·보안성** 심사를 동시 진행

4 **(3단계 : 최종심의) 민간심의위원회**에서 테스트베드 **통과여부 결정**

< 로보어드바이저 테스트베드 전체 프로세스 >



3. [테스트베드 통과효과] 테스트베드 통과시 어떤 혜택이 있는가?

1 **(대고객 서비스 허용)** 전문인력의 개입 없이 **RA가 자문을 수행**하거나 **고객자산을 직접 운용하는 것을 허용**(자본시장법 시행령 개정중)

2 **(마케팅 허용) 테스트베드 통과사실 및 성과**를 투자광고 등에 활용할 수 있도록 허용하되, 테스트베드에 불참한 RA알고리즘은 **테스트베드 미참여 사실을 투자광고·투자설명서에 드러나도록 명시**

※ 다만, "로보어드바이저" 명칭사용은 테스트베드 통과여부와 상관없이 허용

3 **(온라인 보고서의 원칙적 제공 허용)** 테스트베드 통과 RA는 일임보고서를 **원칙적으로 온라인 매체를 통해 교부할 수 있도록 개선**

4. [사후관리] 테스트베드 통과 이후에 알고리즘은 어떻게 관리되는지?

1 **(포트폴리오 운용)** 테스트베드를 통과한 RA는 심사가 종료된 후에도 본심사시 **등록한 포트폴리오를** 계속 **운용***하여야 함

* 다만, 테스트베드 통과 직후 상용화되지 않는 RA 알고리즘의 경우에는 추후 상용화시 포트폴리오 운용 재개시(상용화 이전까지는 운용의무 면제)

2 **(재심사)** 테스트베드를 통과한 RA와 동일성을 인정하기 곤란한 정도로 **중대한 변경***이 발생한 경우, 새로운 RA로 간주하여 **재심사 진행**

* (예) 투자자성향 분석로직의 변경, 포트폴리오구성 원칙의 변경, 리밸런싱 원칙의 변경, 운용대상 자산종류의 변경 등

5. [정보제공] 투자자가 테스트베드 웹사이트*에서 얻을 수 있는 정보는?

* www.RAtestbed.kr, 9월 중 오픈 예정

1 **(심사관련 정보)** 심사가이드라인, 참여업체 현황 등 **심사 관련 일반정보** 뿐만 아니라, RA 알고리즘별 **일일 포트폴리오 운용정보**를 데이터 검증 후 **매일 제공**

○ 추후, 제1차 테스트베드 결과 발표 시 **테스트베드를 통과한 RA의 투자전략 소개, 심사결과 등도 공개할 예정**

2 **(RA 위험조정수익률 등 비교공시)** **투자위험과 투자성과에 대한 균형잡힌 정보**를 제공하기 위해 단순 수익률 뿐만 아니라 위험조정수익률, 변동성 등 **다양한 지표를 게시**

3 **(투자자 유의사항)** **테스트베드의 취지·한계**, RA 투자의 **위험요인** 등 투자자가 RA 투자시 유의해야할 사항들에 대해 **안내**

6. [테스트베드 운영주체] 테스트베드는 어느 기관에서 운영하는가?

□ **(의사결정 : 민간심의위원회)** **심사의 전문성·객관성을 확보**하기 위해 다양한 분야의 민간전문가를 중심으로 **민간심의위원회 구성·운영***

* 컴퓨터 알고리즘, 인공지능 등 IT, 금융보안, 금융시장, 금융관련 법률 분야의 전문가(10인 이내)로 구성할 예정이며, 심사의 공정성을 위해 심의위원은 비공개

○ 테스트베드 상세심사지침, 테스트베드 심사보고서 심의 및 **최종통과 여부 결정** 등 테스트베드 운영에 필요한 **중요 의사결정업무 수행**

□ **(사무국 : 코스콤 內 독립부서)** 코스콤* 내 테스트베드 운영 사무국을 설치하여 **민간심의위원회의 원활한 업무수행을 지원**

* IT 기술 및 자본시장 관련 인프라에 대한 전문성을 감안하여 코스콤으로 선정

○ 심사지침에 따른 심사 실무, 심사보고서 작성, 테스트베드 웹사이트 및 데이터 관리 등의 업무를 수행

Ⅲ. 향후 추진일정

□ **로보어드바이저 테스트베드 설명회 개최**

○ 일시 / 장소 : 9.1일(목), 10:00 / 금융투자협회 불스홀

□ **제1차 테스트베드 신청서 접수** (9월초~ 9월 하순)

* **(신청방법)** 테스트베드 웹사이트를 통해 참여신청서와 제출서류를 온라인으로 제출(단, 접수 초기에는 전자(화)문서 형태로 작성하여 e-mail로 제출)
(참가비) 알고리즘당 50만원 수준(민간심의위원회 결정 예정)

□ **테스트베드 웹사이트 1차 오픈** (9월 중순)

□ **제1차 테스트베드 진행** (9월 하순 ~ '17.4월, 최장 6개월 가정시)

* 제2차 테스트베드는 내년 상반기에 진행(1분기 중 신청서 접수)할 계획이며, 테스트베드는 향후 연 2~3회 주기로 개최될 예정

※ 자세한 내용은 별첨을 참조하시기 바랍니다.

[별첨 1] 로보어드바이저 테스트베드 참여 기본 요건
[별첨 2] 로보어드바이저 테스트베드 세부 심사 내용
[별첨 3] 로보어드바이저 테스트베드 주요 심사 항목
[별첨 4] 로보어드바이저 테스트베드 통과 효과

OPEN 출처표시 공공누리 공공저작물 자유이용허락
☞ 본 자료를 인용 보도할 경우 출처를 표기해 주십시오.
http://www.fsc.go.kr
금융위원회 대 변 인
prfsc@korea.kr
넓게 듣겠습니다 바르게 알리겠습니다

별첨 1 로보어드바이저 테스트베드 참여 기본 요건

1 참여 가능 업체 유형

◇ RA와 기존 금융서비스의 융복합, 순수 기술업체의 서비스 상용화 등을 통한 **시장의 혁신과 역동성 지원**하기 위해 **다양한 형태의 참가유형을 폭넓게 허용**

1 **RA 기술보유 업체**(자문·일임업 未등록자)

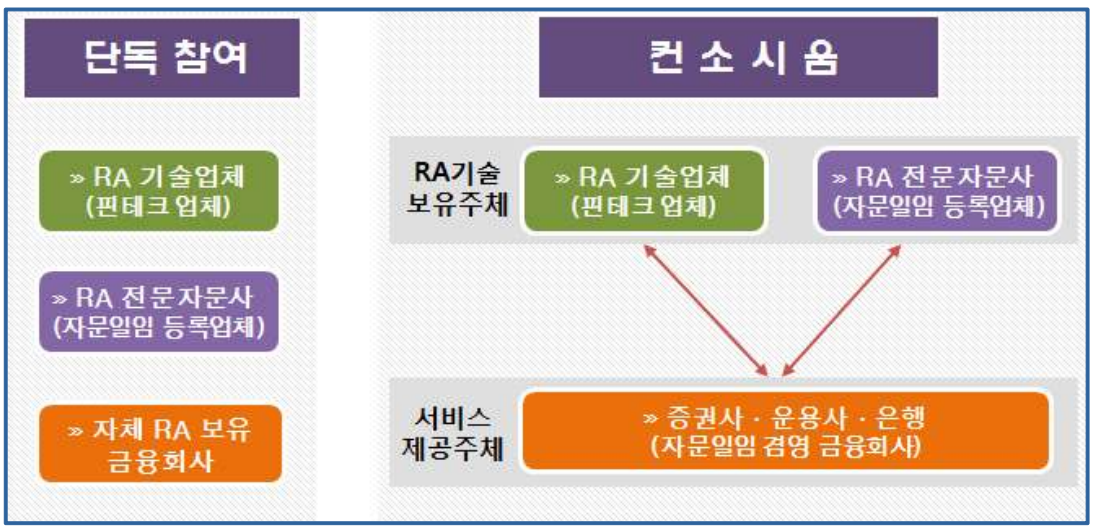
* 단, 서비스 상용화를 전제로 참여하는 만큼 '법인'으로 한정

2 **자체 개발한 RA 기술**을 이용하여 직접 자문·일임서비스를 제공하고자 하는 **자문·일임업자**(겸영 은행·증권사 포함)

3 **RA 기술보유 주체**(RA 전문자문사, RA 기술업체 등)와 **서비스제공 주체**(자문·일임 겸영 은행·증권사 등)로 구성된 **컨소시움**

※ 금융업이 아닌 무료 자산관리서비스 제공 목적의 RA의 경우, 테스트베드 시행초기에 집중되는 심사수요, 제한된 심사인력 등을 고려하여 테스트베드 참가 허용 여부를 추후 검토

< 테스트베드 참여 유형 >



2 신청을 위한 RA 알고리즘의 최소 요건

◇ 심사대상 알고리즘(법상 용어 : 전자적 투자조언 장치)은 **자동화 요건, 운용자산 요건**을 기본적으로 **충족하여야 함**

1 **(자동화 요건) 원칙적으로** 투자자 성향분석(프로파일링), 자산배분, 리밸런싱 등의 과정에서 **사람의 개입없이 전산시스템**만으로 서비스 제공이 가능해야 함

○ 다만, **주문집행**의 경우 **국내 RA업체 기술수준**(주문집행 자동화 기술 보유 업체는 소수)과 **RA의 핵심역량**이 투자자 성향에 따른 맞춤형 자산배분인 점을 감안하여 **자동화의 예외를 인정**



○ **(필수적 자동화)** 테스트베드에 참여하기 위해서 **포트폴리오 구성**(① ~ ③), **리밸런싱***(⑤) **단계는 반드시 자동화가 필요**

* 리밸런싱 규칙에 따라 자동적으로 자산배분 및 포트폴리오 셀렉션 재조정이 이루어져야 하나, 리밸런싱 시점까지 자동으로 인식할 필요는 없음

○ **(선택적 자동화) 주문집행단계**(④)의 경우, 참여 업체의 선택에 따라 **자동화 시스템 구축 여부에 대한 심사** 가능

2 **(운용자산 요건) 펀드**(ETF 포함), **파생결합증권**(ELS, ETN, DLS 등), **주식**으로 운용하여야 하며, **하나 또는 복수의 자산군**으로 포트폴리오 구성 가능

○ 대기성 자금인 경우, **예금, RP 등의 포트폴리오 편입 허용***

* 일반투자자의 소액자금에 대한 맞춤형 자산관리라는 RA 특성 및 국·내외 사례 등을 고려하여, 거래단위가 큰 채권과 원본초과 손실가능성이 있는 파생상품(선물, 옵션등)은 운용대상에서 제외

※ 한 업체가 복수의 알고리즘을 대상으로 테스트베드에 신청할 수 있음

별첨 2 로보어드바이저 테스트베드 세부 심사 내용

1 심사 프로세스

□ 사전심사, 본심사, 최종심의를 거쳐 테스트베드 **통과여부 결정**

단계	사전 심사	본심사		최종 심의
소요기간	0.5개월	6개월 이내		0.5개월
처리 흐름	(참여신청) ↓ 테스트베드 개시 ↓ 서면/구술/현장 심사 및 보완	[운용심사] 포트폴리오 운용 개시 ↓ 주문입력 ↓ 매매종료 ↓ 체결내역 제출 잔고내역 제출 ↓ 변경내역 제출 ↓ 일일운용 종료 ↓ 포트폴리오 운용 종료	[시스템심사] 시스템심사 및 보완 ↓ 심사 종료	심의위원회 최종 심의 ↓ 테스트베드 종료

2 1단계 : 사전심사

□ **(참가신청)** 테스트베드 웹사이트를 통해 **참가신청서와 필요서류***를 **온라인으로 제출****

* 법인등기, 알고리즘 설명서, 투자자 성향분석 설명자료, 과거 시황의 가정 하에 자체 운용역량을 테스트한 결과자료, 리밸런싱 설명자료 등

** 1차 테스트베드는 전자(화)문서 형태로 작성하여 e-mail로 제출

□ **(심사항목)** 테스트베드 **참여요건**(업체·알고리즘) 및 **알고리즘의 투자자 성향별 포트폴리오 산출역량**을 심사

○ **(참여요건) 참여 업체 유형*에 따른 요건 및 알고리즘의 자동화 요건 및 운용자산 요건**에 대해 서류를 중심으로 심사

* ① RA기술보유 업체(자문·일임업 미등록 법인), ② RA기술보유 자문·일임업자, ③ 금융회사 컨소시움

○ **(포트폴리오 산출역량) 가상의 투자자 정보**를 RA에 입력 후 실제 **맞춤형 포트폴리오가 산출**되는지 여부를 심사

i) 다양한 투자성향을 가진 **복수의 가상 투자자 정보를 입력**

ii) 투자자별로 **리스크 수준이 다른 복수의 포트폴리오가 유의미하게 구분되어 산출**되는지 여부 심사

iii) 한 개의 포트폴리오가 **최소 5개 이상의 투자대상자산으로 분산되어 구성**되는지 여부 심사

□ **(요건 미충족 업체)** 심사 과정에서 **보완을 요구**하고, 운용개시 전까지 보완이 이루어지지 못한 경우 **신청접수 반려**

2 2단계 : 본심사

□ 사전심사 과정에서 **도출된 포트폴리오에 대해 일정기간* 동안 실제 자금을 운용**하도록 하여 **알고리즘의 안정성**을 심사

* 최소 3개월 이상으로서 안정성을 모니터링하기에 충분한 기간(심의위 확정 예정)

① **(포트폴리오 유형) 안정추구·위험중립·적극투자형** 등 3유형

② **(운용계좌 수) 3가지 유형별 포트폴리오**를 각각 **3개의 계좌에서 동시에 운용**하여 다계좌 운용역량 심사(총 9개 계좌 운용)

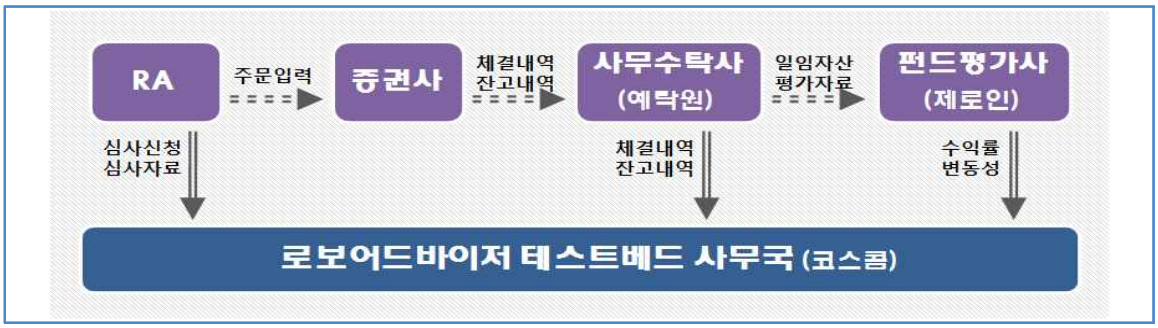
③ **(운용규모)** 계좌별로 참여 업체가 **해당 알고리즘에 대해 제시하는 최소 가입금액 이상의** 자금을 운용

* 예) A 알고리즘 제시 최소가입금액 100만원 × 9계좌 = 최소 운용 규모 900만원

④ **(운용자금)** **원칙적으로 업체 고유자금**을 운용하되, **RA 기술보유업체**(자문·일임 未등록업체)가 단독으로 참여하는 경우에는 **임원자금으로 운용하**는 것을 허용

⑤ **(심사주기)** 일일 거래내역정보를 바탕으로 알고리즘의 **오류발생 및 유효한 리밸런싱 발생 여부** 등을 사무국이 일일 점검·확인

* 일일 운용종료 후 거래내역과 최종 잔고내역을 테스트베드 사무국에 제출



⑥ **(시스템 심사)** 테스트베드 종료 후 **단기간 내에 상용화**를 하려는 업체에 대해서는 **로보어드바이저 서비스의 대고객 전달체계**에 대한 **안정성·보안성** 심사를 동시 진행

- **(보안성)** **알고리즘, 주문내역, 투자자 개인정보** 등 RA의 핵심정보에 대한 **해킹 방지 역량** 심사(금융보안원)

- **(안정성)** **자연재해, 해킹** 등의 사고 발생시 **체계적인 대응을** 위한 **비상조치 매뉴얼, 복구시스템** 등 보유 여부 심사(코스콤)

별첨 3 로보어드바이저 테스트베드 주요 심사 항목

심사 항목	심사항목의 주요 내용
테스트베드 참여요건	테스트베드 참여 업체 요건, 알고리즘의 자동화, 운용자산 요건을 충족해야 함
알고리즘의 합리성	알고리즘의 운용목표, 주요전제 등에 대해 설명이 가능하고, 알고리즘 테스트 결과가 신뢰가능한 수준이어야 함
개인 맞춤성	투자자성향 분석 도구가 투자자의 투자목적, 위험감수능력 등 다양한 측면을 고려하여야 하며, 투자자성향 분석에 따라 유의미하게 구분되는 복수의 포트폴리오 산출되어야 함
분산투자	최소 5개 이상의 상품·종목으로 구성된 포트폴리오가 산출되어야 함
합리적인 리밸런싱	리밸런싱 발생기준·원칙이 수립되어 있고, 이에 기반하여 리밸런싱이 유효하게 발생하여야 함
다계좌 동시 관리	복수 계좌를 동시에 운용하더라도 알고리즘이 오류없이 정상적으로 작동하여야 함
법규 준수성	알고리즘이 법령에서 금지하는 투자(예: 투자자 동의 없는 계열회사 증권 투자)를 자체적으로 제한할 수 있어야 함
유지·보수 전문인력	알고리즘, 시스템을 시의 적절하게 업그레이드하고 지속적으로 관리할 수 있는 IT 전문 인력을 1인 이상 보유하여야 함
시스템 보안성	알고리즘, 주문내역, 투자자 개인정보 등 RA의 핵심 정보에 대한 해킹 방지 시스템을 보유해야함
시스템 안정성	알고리즘, 시스템 장애 발생시 체계적으로 대응할 수 있는 비상조치매뉴얼·시스템 등 보유해야 함

별첨 4 로보어드바이저 테스트베드 통과효과

1. 로보어드바이저에게 직접 자문·일임서비스를 제공받을 수 있습니다.

테스트베드 불참/미참여 RA

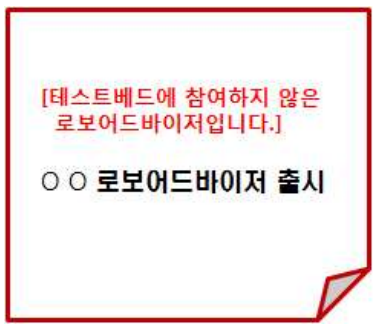


테스트베드 통과 RA



2. 테스트베드의 성과를 투자광고에 활용할 수 있습니다.

테스트베드 불참/미참여 RA



테스트베드 통과 RA



3. 일임보고서를 이메일을 통해 낮은 비용으로 제공할 수 있습니다.

테스트베드 불참/미참여 RA



테스트베드 통과 RA

