

전자금융감독규정에 따른

『전자금융기반시설 취약점 분석·평가』

과업내역서

2019. 11.
금융투자협회
Korea Financial Investment Association



목 차

I. 사업 개요	1
1. 사업 명	1
2. 사업 배경	1
3. 사업 목표	1
4. 추진 계획	1
II. 과업 범위	2
1. 기술적 취약점 점검대상	2
2. 관리적·물리적 취약점 점검	2
3. 외부 인력 관리체계 진단 범위	3
III. 요구사항	4
1. 취약점 점검 및 평가 실시	4
2. 취약점 조치 가이드 및 확인 점검	5
3. 외부 인력 관리체계 진단	5
IV. 요구사항 세부내역	6
1. 요구사항 목록	6
2. 요구사항 상세	7

I

사업개요

1

사업명

- '19년 전자금융기반시설 취약점 분석·평가

2

사업배경

- IT컴플라이언스 강화
 - 전자금융거래법 제21조의3, 동 시행령 제11조의5 및 전자금융감독규정 제37조의2의 취약점 분석·평가 준수를 위한 전자금융기반시설에 대한 취약점 분석·평가 실시

3

사업목표

- IT컴플라이언스 보장 및 협회 전자금융기반시설의 취약점 분석·평가를 통한 시스템 안정성 확보 및 고객서비스 신뢰성 증대

4

추진계획

- 사업기간
 - 계약 체결일로부터 6주('19.12월 사업완료, 다만 확인점검은 별도)
- 계약방법
 - 협회 계약업무규정에 의한 「일반경쟁입찰」 방식

II 과업범위

1 기술적 취약점 점검 대상

□ 웹서비스

총 계	응용애플리케이션	시장·공시서비스	개인정보처리	기타
31	2	13	7	9

※ 응용애플리케이션은 메신저시스템과 모바일 앱을 포함하며 점검 대상은 일부 변경 가능(상세 현황은 계약상대자에 한하여 제공)

□ 서버, 네트워크 및 보안장비 등

총 계(식)	서버	네트워크	보안장비	DB
68	22	22	19	5

※ 대상은 일부 변경 가능(상세 현황은 계약상대자에 한하여 제공)

2 관리적·물리적 취약점 점검

□ 관리적·물리적 취약점 점검은 전자금융감독규정에서 규정하고 있는 기준을 따르되 점검항목 및 점검방식에 대해서는 협회와 협의하여 결정

- 법의 규정사항 변경 또는 금융당국 등 상위기관의 기준 및 가이드 변경 시 해당 내용을 반영하되 가능한 협회에서 이전에 실시한 관리적·물리적 취약점 점검항목 및 점검방식을 준용

3 외부 인력 관리체계 진단 범위

□ 외부 인력에 대한 내부통제 대상 전체

구분	영역	협회 관리대상 여부
외부 직원	인력 관리	
	자료 보안관리	
	출입 등 물리적 보안관리	
	단말기 보안관리	
	접근 권한 관리	

* 전자금융감독규정의 전자금융보조업자에 대한 내부통제 대상 참고

□ 외부 인력 및 업체 보안점검 절차와 점검 기준

- **(현황 파악)** 외부 인력 및 업체 현황 파악 상태
- **(중요도 분석)** 외부 인력 및 업체 별 중요도 분석 이행 여부
- **(보안수준 설정)** 외부 인력 및 업체 별 보안요구수준 및 점검 방식 등 관리 현황
- **(점검 기준)** 관리적·물리적·기술적 점검 기준 설정 및 업무 영역별 특이사항 관리 여부

□ 계약 단계별 관리 현황

- **(계약 전 단계)** 사업공고 및 제안요청, 제안서 평가 및 사업자 선정 등 계약 이전 단계의 유의사항 준수 여부
- **(계약 및 수행단계)** 계약서 작성 및 계약, 재위탁 관련 사항 및 사업 수행 시 보안관리 현황 등
- **(완료 단계)** 산출물 관리 및 사후 보안 조치 등 관리 현황

Ⅲ

요구사항

1 취약점 점검 및 평가 실시

- 이전 취약점 조치 결과에 대한 확인점검 수행
 - **(취약점 조치여부 추적)** 전년도 전자금융기반시설 취약점 분석·평가 결과(물리/관리/기술 진단) 및 상반기 홈페이지 취약점 분석·평가 결과(웹 진단)에 대한 조치 이행 확인점검
 - **(체계적인 취약점 관리를 위한 지원)** 취약점 관리 주기(점검 - 개선 - 확인)에 따라 각 취약점 별 사후 추적이 가능하도록 산출물에 반영
- 금융보안원의 신규 취약점 분석·평가 항목에 따른 진단 수행
 - **(정보보호 수준평가)** 관리적·물리적·기술적 현황 분석·평가
 - **(정보시스템 취약점 점검)** 정보시스템 인프라 및 웹서비스의 취약점에 대한 즉시·단기·중기·장기 개선방안 제시
 - 장비별(서버, 네트워크장비, 보안장비, 데이터베이스) 취약점 점검 및 네트워크 구조 진단
 - 모의해킹을 통한 웹사이트 취약점 점검
 - **(위험분석)** 정보자산에 피해를 가할 수 있는 위협의 발생 확률 및 빈도와 자산에 해를 입히는 정도 등의 분석
 - **(취약점 분석·평가 보고서 작성)** 분석·평가 결과를 바탕으로 효과적인 정보보호를 위한 관리적·물리적·기술적 영역별 개선안 마련 및 금융위원회 제출용 보고서 준비

2 취약점 조치 가이드 및 확인점검

□ 취약점 개선방안 제시

- **(조치방법 교육)** 취약점에 대한 조치가이드 제공 및 교육 실시
 - 본회 시스템 운영환경에 맞는 실제적인 조치방법 안내
 - 개선 담당자가 조치방법을 명확하게 이해할 수 있는 샘플 제공

□ 조치 결과 확인점검 실시

- **(조치계획 추진사항 점검)** 취약점의 조치계획에 의한 즉시 조치 사항 등 개선 추진사항에 대한 확인점검
 - ※ 확인점검은 사업기간 이후에 별도의 일정으로 진행

3 외부 인력 관리체계 진단

□ 본회 업무 관련 외부 인력 관리체계 현황 분석·진단을 통한 문제점 도출 및 개선방안 마련

- **(법적 준수사항 분류)** 관련 법령 및 규정*에 따른 외부 인력 관리 준수사항 도출

* 전자금융감독규정, 개인정보 보호법, 정보통신망법, 정보처리위탁규정 등

- **(현황 진단 및 개선사항 도출)** 외부 인력에 대한 내부통제 현황 분석을 실시하고 그 결과에 따라 개선방안 마련

- **(상시 통제활동 제안)** 외부 인력 대상별* 점검목록(체크리스트 등)의 수정·보완 등 상시 통제활동에 대한 효과적인 방안 제시

* 전자금융보조업자, 개인정보처리 수탁자, 본회 상주 외부인력 등

IV

요구사항 세부내역

1 요구사항 목록

□ 목록표

요구사항 분류	요구사항 번호	요구사항 명칭
공통 요구사항	COR-001	사업수행
사업 요구사항	CSR-001	취약점 점검대상 현황분석
	CSR-002	이전 취약점 조치 결과의 확인 점검
	CSR-003	취약점 진단 및 개선 지원
	CSR-004	외부 인력 및 업체 관리 준수사항 도출
	CSR-005	외부 인력 및 업체 내부통제 현황 분석 및 개선방안 마련
보안 요구사항	SER-001	보안관리 계획 수립
	SER-002	보안관리 지침 준수
품질 요구사항	QUR-001	사업수행 방법론 및 적용방안
	QUR-002	산출물 제출 및 관리 방안
사업관리 요구사항	PMR-001	작업 장소 및 수행 환경 구성
	PMR-002	일정, 진척관리 및 보고
사업지원 요구사항	PSR-001	투입인력
	PSR-002	유지관리
	PSR-003	기술지원 및 교육

* 본 과업내역서에서 제시한 사업조건 및 내용을 원칙적으로 준수하여야 하나, 사업 내용이 변경될 경우 과업변경절차는 상호 협의 하에 결정하여야 함

2

요구사항 상세

□ 공통 요구사항(Common Requirement)

요구사항 번호	COR-001
요구사항 분류	공통 요구사항
요구사항 명칭	사업수행
요구사항 세부내용	<ul style="list-style-type: none"> ○ 공통 제약사항은 ‘전자금융기반시설 취약점 분석·평가 용역’ 사업 전반에 관한 일반적인 공통 사항으로서 사업 수행 시 지켜야 할 사항을 규정함. ○ 사업자는 본 사업에 저촉되는 관계 법령, 조약, 행정규칙, 자치법규 등에 위배됨이 없는 최적의 방안을 제시하여야 하며 사업수행기간 중 개정될 경우에는 개정되는 사항에 따라 사업자 책임하에 변경하여야 함. ○ 사업자는 본 과업내역서에 대한 정밀분석을 통해 본 사업이 요구하는 과업을 충족하도록 최적의 방안을 제시하여야 함. ○ 사업자는 과업내역서, 사업수행계획서 등에 명시되지 않은 사항이라도 당연히 필요한 사항 또는 법령규제 사항은 협회의 지시에 따라 보완하여야 하며, 사업수행 과정에서 문제점이 도출되어 해석상의 의견 차이가 있을 경우 상호 협의하되 협회의 해석에 따라야 함. ○ 사업자는 본 사업 범위별 투입인력을 적정하게 산정하여 제시하여야 하고, 협회가 투입인력의 적격성 판단 또는 필요에 의해 투입인력의 교체를 요구할 경우 동급 이상의 인력으로 교체해야 하며, 투입이 확정된 인력의 무단교체는 불허함. ○ 사업자는 총괄수행자(PM)를 현장대리인으로 지정하여 계약종료일까지 현장에 상주하게 하여 협회의 지시에 따라 각종 업무와 보안 등 책임을 담당하게 하여야 함. ○ 사업자는 각 요구사항별 실행계획서 및 결과서 등 산출물을 작성하여 제출 하여야 함.
산출 정보	해당사항 없음
관련 요구사항	해당사항 없음

□ 사업 요구사항(Consulting Requirement)

요구사항 번호	CSR-001
요구사항 분류	사업 요구사항
요구사항 명칭	취약점 점검 대상 현황분석
요구사항 세부내용	○ 취약점 점검 세부계획 수립 ○ 취약점 점검대상 선별
산출 정보	○ 취약점 점검계획
관련 요구사항	해당사항 없음

요구사항 번호	CSR-002
요구사항 분류	사업 요구사항
요구사항 명칭	이전 취약점 조치 결과의 확인 점검
요구사항 세부내용	○ 이전 취약점 항목 확인 및 점검 실시 ○ 취약점 항목별 사후 추적이 가능하도록 문서화
산출 정보	○ 확인 점검 결과서(CSR-003 취약점 분석평가 결과 보고서에 포함할 수 있음)
관련 요구사항	해당사항 없음

요구사항 번호	CSR-003
요구사항 분류	사업 요구사항
요구사항 명칭	취약점 진단 및 개선 지원
요구사항 세부내용	○ 물리·관리·기술적 취약점 분석·평가 및 대책 수립 ○ 각 업무 담당자가 실제적인 취약점 조치가 가능하도록 본회 시스템 운영환경에 맞는 조치가이드 및 샘플 제공 등 개선방안 컨설팅 ○ 취약점 설명 및 조치가이드 교육 ○ 분야별 취약점 개선조치 현황에 대한 확인점검 실시(별도 일정)
산출 정보	○ 취약점 분석평가 결과 보고서(확인점검 결과 보고서) ○ 분야별 취약점 조치 가이드라인 ○ 금융위원회 제출용 보고서
관련 요구사항	○ 금융보안원에서 제시한 취약점 분석·평가 항목을 기준으로 하되, 공인된 기관(OWASP, 국가정보원, KISA, 금융위원회 등)에서 제시하는 취약점 및 최신 동향을 반영하여 진단 및 분석 실시

요구사항 번호	CSR-004
요구사항 분류	사업 요구사항
요구사항 명칭	외부 인력 및 업체 관리 준수사항 도출
요구사항 세부내용	<ul style="list-style-type: none"> ○ 협회가 준수하여야 하는 외부 인력 및 업체 관리 관련 법령 및 규정 정의 ○ 해당 법령 및 규정에 따른 준수사항 목록 마련 <ul style="list-style-type: none"> - 업무 중요도에 따른 유형별 분류
산출 정보	<ul style="list-style-type: none"> ○ 외부 인력 및 업체 관리 관련 법령 및 규정 목록 ○ 외부 인력 및 업체 관리 준수사항 목록
관련 요구사항	해당사항 없음

요구사항 번호	CSR-005
요구사항 분류	사업 요구사항
요구사항 명칭	외부 인력 및 업체 내부통제 현황 분석 및 개선방안 마련
요구사항 세부내용	<ul style="list-style-type: none"> ○ 외부 인력 및 업체 대상 협회의 내부통제 현황 분석 <ul style="list-style-type: none"> - 업무 중요도에 따른 유형별 현황 분석(업체별 분석 아님) ○ 협회 내부통제 현황 분석 결과에 따른 개선방안 마련 ○ 외부 인력 및 업체 유형별 점검표 개발, 점검방식 제안
산출 정보	<ul style="list-style-type: none"> ○ 내부통제 현황 분석 결과서 ○ 외부 인력 및 업체 관리 개선방안 ○ 외부 인력 및 업체 유형별 점검표
관련 요구사항	<ul style="list-style-type: none"> ○ 협회가 일반 금융회사와 다른 특성을 감안하여 내부통제 기준 및 점검표, 점검방식 등 제안

보안 요구사항(Security Requirement)

요구사항 번호	SER-001
요구사항 분류	보안 요구사항
요구사항 명칭	보안관리 계획 수립
요구사항 세부내용	<ul style="list-style-type: none"> ○ 사업수행에 사용되는 인력, 문서 장비 등의 보안관리 계획 수립하여야 하며, 보안상 결격사항이 없도록 조치하여야 함. ○ 사업수행 과정에서 발생하는 각종 산출물에 대한 보안관리 대책을 제시하여야 함.
산출 정보	<ul style="list-style-type: none"> ○ 보안관리 계획서, 보안서약서(협회 제공)
관련 요구사항	해당사항 없음

요구사항 번호	SER-002
요구사항 분류	보안요구사항
요구사항 명칭	보안관리 지침 준수
요구사항 세부내용	<p>가. 보안·개인정보담당자 지정 및 관련 지침 운영</p> <ul style="list-style-type: none"> ○ 보안·개인정보 책임자, 담당자를 지정하여 운영 ○ 용역 수행과정에서 관련 개인정보 등 중요정보가 유출될 경우, 사업자는 개인정보보호법 등에 의한 모든 법적 책임을 짐 <p>나. 유출금지 정보 관리방안</p> <ul style="list-style-type: none"> ○ 사업수행 과정에 중요 유출금지 정보에 대한 관리체계 수립 <p>다. 기밀누설</p> <ul style="list-style-type: none"> ○ 협회의 서면에 의한 승낙 없이 본 계약에 관련하여 알게 된 업무상 기밀은 과업기간 및 본 계약 종료 후에도 제3자에게 누설금지 ○ 본 용역사업을 통하여 취득한 정보는 사업자의 이익을 위하여 이용할 수 없음 <p>라. 보안책임자 및 담당자의 역할</p> <ul style="list-style-type: none"> ○ 사업장 운영 및 과업참여자 자료관리 등 보안관리 계획 수립 ○ 정기적인 보안점검 실시 및 보안관리 대장을 비치하여 운영 ○ 보안상 중요한 정보화문서(공문, 출력물, 책자 등)는 중요도에 따라 분류하여 잠금장치가 있는 곳에 보관처리 ○ 용역사업 시작 전 과업참여자에 대한 비밀유지의무 준수 등의 교육을 실시하고, 협회의 확인을 득해야 하며, 과업 참여자에게 최소 1회 관련 교육(보안관리 지침, 비밀유지 준수 등) 실시 ○ 과업참여자가 교체되는 경우, PC포맷 등 사업관련 자료의 외부 유출을 방지하기 위한 조치 수행 <p>마. 보안관리</p> <ul style="list-style-type: none"> ○ 보호대상 자산을 분류하고, 효과적인 보호수단 적용 및 절차마련 ○ 정기적인 보안점검 시행 <p>바. 성과물 보안관리</p> <ul style="list-style-type: none"> ○ 본 과업에 따른 성과물에 대해서 사업자는 협회의 승인 없이 외부에 제공 또는 공표가 불가함
산출 정보	해당사항 없음
관련 요구사항	해당사항 없음

□ 품질 요구사항(Quality Requirement)

요구사항 번호	QUR-001
요구사항 분류	품질 요구사항
요구사항 명칭	사업수행 방법론 및 적용방안
요구사항 세부내용	○ 사업 수행절차의 체계적 관리를 위한 사업 수행 방법론과 적용 방안을 제시하여야 함. ○ 사업의 공정관리 등 프로젝트 관리방법론에 대한 활용방안을 제시하여야 함.
산출 정보	○ 사업수행계획서
관련 요구사항	해당사항 없음

요구사항 번호	QUR-002
요구사항 분류	품질 요구사항
요구사항 명칭	산출물 제출 및 관리 방안
요구사항 세부내용	○ 사업수행기간 동안 발생하는 각종 산출물을 확인하여 작성 및 제출하여야 하며 제출 부수는 쌍방의 합의 하에 조정 할 수 있음
산출 정보	○ 각 단계별 산출물
관련 요구사항	해당사항 없음

Korea Financial Investment Association

□ 사업관리 요구사항(Project Mng. Requirement)

요구사항 번호	PMR-001
요구사항 분류	사업관리 요구사항
요구사항 명칭	작업 장소 및 수행 환경 구성
요구사항 세부내용	○ 사업수행 장소는 협회가 지정하는 장소에서 수행하여야 함. ○ 사업수행을 위하여 필요한 전산자원(PC, 프린트 등) 및 사무용 비품은 사업자가 보유한 장비를 이용하여야 함. ○ 사업에 필요한 집기, 비품, 관리운영비, 야간·휴일작업 등에 필요한 기타경비 등은 사업자가 부담하여야 함. ○ 작업장 내에서는 보안규정을 준수하여야 함. ○ 반입 PC는 OS 초기 상태이어야 하며, 사업 종료 후 사용하였던 PC는 모두 포맷 처리함.
산출 정보	○ 반출·입 관리대장(협회 제공)
관련 요구사항	해당사항 없음

요구사항 번호	PMR-002
요구사항 분류	사업관리 요구사항
요구사항 명칭	일정, 진척관리 및 보고
요구사항 세부내용	<ul style="list-style-type: none"> ○ 협회가 요청한 추진일정 계획과 사업자가 제시한 일정계획이 다른 경우 사업기간 내 완료를 위한 방안을 제시해야 함. ○ 추진일정은 전체일정과 세부일정으로 구분하여 작성하여야 함. ○ 사업수행 중에 발생하는 주요사항에 대하여는 협회와 상호 협의하여 결정함. ○ 용역기간 중 주 1회 정기회의를 개최함을 원칙으로 하되, 필요시 임시 회의를 개최할 수 있음.
산출 정보	<ul style="list-style-type: none"> ○ 사업수행계획서 ○ 상세일정계획서
관련 요구사항	해당사항 없음

□ 사업지원 요구사항(Project Support Requirement)

요구사항 번호	PSR-001
요구사항 분류	사업지원 요구사항
요구사항 명칭	투입인력
요구사항 세부내용	<ul style="list-style-type: none"> ○ 본 사업에 필요한 인력은 착수함과 동시에 투입되어야 함. ○ 진행 중 참여 인력은 협회의 동의 없이 사업자 임의로 변경할 수 없음. ○ 프로젝트를 수행할 총괄수행자(PM)는 주사업자 소속 직원으로 근속 기간 경력 2년 이상 이어야 하며, 동 사업 관련 PM 수행 경험이 있는 인력을 투입하여야 함. ○ 협회는 참여인력이 사업수행 상 부적당하다고 판단되거나 자격 미달인 경우 사업자에게 교체를 요구할 수 있으며, 사업자는 이에 적극 협조하여야 함.
산출 정보	해당사항 없음
관련 요구사항	해당사항 없음

요구사항 번호	PSR-002
요구사항 분류	사업지원 요구사항
요구사항 명칭	유지관리
요구사항 세부내용	<ul style="list-style-type: none"> ○ 수행 결과물이 활용상 중대한 결함이 발견될 경우 보완해야 함. ○ 효율적인 사업추진을 위한 업무 공유방안을 제시하여야 함.
산출 정보	해당사항 없음
관련 요구사항	해당사항 없음

요구사항 번호	PSR-003
요구사항 분류	사업지원 요구사항
요구사항 명칭	기술지원 및 교육
요구사항 세부내용	<ul style="list-style-type: none"> ○ 본 사업 결과 취약점 조치를 위한 관련 담당자 대상 교육 계획을 수립하여야 함. ○ 사업 완료 후에 취약점 조치에 필요한 사항의 기술지원 요청에 대한 대응 계획을 수립하여야 함.
산출 정보	해당사항 없음
관련 요구사항	해당사항 없음

Korea Financial Investment Association