let:

26 년 전자금융기반시설 취약점 분석평가 제안요청서

롯데손해보험 2026-01

목 차

I. 사업개요

1. 사업개요

가. 사 업 명 : 26년 전자금융기반시설 취약점 분석평가

나. 사업기간 : 26.01 ~ 12월(약 12개월)

구분		사업기간(예정)	비고
전자금융기반시설 취약점 분석평가	(상반기) 전자금융기반시설 취약점 분석평가	26.02.02(월) ~ 26.06.12(금)	서비스(최초/이행), 인프라(최초)
	(하반기) 전자금융기반시설 취약점 분석평가	26.08.03(월) ~ 26.11.20(금)	서비스(최초/이행), 인프라(이행)
	정보보호관리체계 취약점 분석평가	26.02.02(월) ~ 26.06.12(금), 26.10.26(월) ~ 26.11.20(금)	관리체계(최초/이행)
	시큐어코딩 교육	26 년 내 진행	
정보보호 위험평가	위험평가	26.02.02(월) ~ 26.06.12(금), 26.10.26(월) ~ 26.11.20(금)	ISMS(최초/이행)
	정보보호 사규 제·개정	26.05.04(월) ~ 26.06.30(화)	
금융보안 수준진단 컨설팅		26.07.01(수) ~ 26.10.30(금)	
정보보호 공시 컨설팅		26.03.02(월) ~ 26.05.29(금)	
IT 보안 및 정보보안 감사		26 년 3 분기 내 진행	

- 사업기간은 일부 변동될 수 있으며, 상호 협의 후 진행

2. 사업목적

가. 전자금융감독규정 제37조의 2(전자금융기반시설의 취약점 분석·평가 주기 내용 등) 이행

나. ISMS 인증기준으로 위험평가를 실시하여 국내 기준의 법적 준거성 확보 및 침해유출 사고 방지

다. 정보보호관리체계 검증·개선활동을 통해 대고객 서비스 안전성 확보

라. 금융보안 자율보안 수준진단을 통한 효과적인 디지털 위험대응 체계 마련

마. 정보보호 공시를 통한 대외 신뢰성 확보 및 내부 통제 강화

바. IT보안 및 정보보안 감사를 통해 금융사고 예방 및 규제 준수 강화

3. 제안요청 범위

가. 전자금융기반시설 취약점 분석평가

나. 시큐어코딩 교육

다. 정보보호 위험평가

라. 정보보호 사규 제·개정

마. 금융보안 수준진단 컨설팅

바. 정보보호 공시 컨설팅

사. IT보안 및 정보보안 감사

4. 기대효과

가. 전자금융거래 안전성 및 신뢰성 확보

나. 침해·유출 사고 방지 및 법적 준거성 확보

다. 내부 보안수준 개선 및 조직 보안 성숙도 향상

II. 사업 상세 요건

1. 자산 및 시설현황

가. 자산현황

구분	대상	점검대상		수행주기
관리체계 영역	정보보호관리체계	-		연 1 회
인프라 영역	서버	628 대	· Unix&Linux : 436대 · Windows : 153대 · 기타 : 39대 (Nutanix 11대 포함)	
	네트워크	175 대		
	정보보호시스템	478 대		
	데이터베이스	98 대		
	PC	85 대		
	WEB/WAS	395 대		
	합계	1,859 대		
서비스 영역	웹 애플리케이션	15 개	· 상반기 : 14개 · 하반기 : 15개	반기 1 회
	모바일 애플리케이션	18 개	· 상반기 : 16개 · 하반기 : 18개	
	합계	33 개		

- 자산현황은 사업 투입 이후 대상 적정성 검토 단계에서 수량이 변경될 수 있음

나. 시설현황

구분	위치
롯데손해보험	서울시 중구 소월로 3 에티버스타워
전산센터(IT 인프라 운영)	서울시 금천구
전산센터(재해복구)	용인시 기흥구

2. 전자금융기반시설 취약점 분석평가

가. 점검기준 : 전자금융기반시설 보안 취약점 평가기준 안내서(금융보안원, 제2026-1호)

나. 점검주기

구분		점검주기
관리체계 영역	정보보호관리체계	연 1 회 상반기 실시
인프라 영역	인프라 시스템	
서비스 영역	웹 애플리케이션	연 2 회 상·하반기 실시
	모바일 애플리케이션	

다. 전자금융기반시설 취약점 분석평가 컨설팅

- 취약점 분석평가 컨설팅 방법론 제시
- 취약점 분석평가 대상 별 기술적 진단 방법론 제시
- 당사의 운영 현황을 고려한 진단 수행 및 실 적용 가능한 보완대책 제시
  (하이브리드앱의 경우 웹/앱 각각 기준으로 진단 수행)
- 인프라 영역 NUTANIX 점검 방안 제시(스크립트 또는 인터뷰 등) 및 취약점 분석평가 실시
- 인프라 영역 취약점 자동 진단 도구 또는 스크립트 커스터마이징 지원
- 도출 취약점에 대한 보호대책 제시 및 이행점검 실시
- 지속적인 품질관리를 위해 표준화된 방법론 및 템플릿 제시
- 취약점 진단 결과 리뷰 및 문의 대응 지원
- 취약점 분석평가 보고서 작성(수행사·고객사 양식 별도)
- 취약점 분석평가 보고서 내 직전 점검 결과 대비 특이사항 작성
- 당사에서 요청하는 양식에 지난 3년간(2023~25) 수행한 취약점 점검 결과 입력 지원 (필요시)
- 사내 취약점 관리 시스템에 26년 취약점 점검 결과 입력 및 관리(사내 시스템을 통해 결과 관리 예정)

라. 시큐어코딩 교육

- 시큐어코딩 교육 1회 지원
- 시큐어코딩 교육 수행 및 교육 자료 작성

3. 정보보호 위험평가

가. 평가기준 : 금융권에 적합한 정보보호관리체계 인증기준 점검항목(금융보안원)

나. ISMS 인증기준 기 운영중인 정보보호관리체계 점검 및 미흡사항 개선 컨설팅

- ISMS 인증기준을 바탕으로 당사 현황분석(GAP) 수행
- 인증 범위·전자금융기반시설 진단 대상 자산 및 정보처리시스템 식별·분류, 중요도 평가, 자산관리대장 최신화
- 자산 및 정보처리시스템 중요도 평가 기준 제시
- 위험평가 방법론 제시, 평가 후 도출된 위험에 대하여 조치방안 수립 및 이행점검 실시
- 전자금융거래법, 개인정보보호법 등 관련 법령을 고려하여 정보보호 규정 및 지침, 매뉴얼 현황분석(GAP) 수행 및 제·개정
- 관리적·기술적·물리적 정보보호 정책 및 절차에 대한 적정성 검토 및 미흡 사항 개선
- IDC 실사 점검 및 점검 결과보고서 작성
- 당사에서 요구하는 모든 컨설팅 활동에 대하여 산출물(분석자료, 보고서) 목록 제시 및 산출물 제공
- 퇴직/직무변경 관리 항목(2.2.5)에 대한 중점 점검 및 주요직무자/일반사용자별 권한 회수 관리 프로세스 개선 컨설팅

다. 정보보호 사규(규정/지침/매뉴얼) 제·개정 지원

- 정보보호 규정 및 지침, 매뉴얼 제·개정에 대한 방법론 제시
- 전자금융감독규정, 개인정보보호법 등 관련 법령을 고려하여 현황분석(GAP) 수행 및 제·개정 지원
- 연관부서 지침과의 일관성 및 업무 연관성 검토 지원
- 사규 내 절차서/기준서 작성 및 현행화 지원
- 당사 사규관리 규정에 따른 자구수정 지원
- 네트워크 방화벽 지침 제정 지원
- 사규 담당 부서 검토 및 품의 완료 단계까지 발생하는 수정 건에 대한 지속적인 지원
- 지침 개정 내용을 담당 부서에 공유 및 설명 지원

라. 도입단계 보안 절차 개선 컨설팅

- 서버 보안 하드닝 절차 및 신규 위협 분석 기법을 적용한 자체 보안성 심의 평가 절차 개선
- 자체 보안성 심의 시 서버 계층별(OS, WEB/WAS Application, 어플리케이션용 패키지 등) 보안 강화 방법론(절차/매뉴얼/가이드 등) 및 점검 방안 제시(스크립트 또는 인터뷰 등)
- 자체 보안성 심의 절차 현황 분석 및 개선 필요 사항 제시

4. 금융보안 수준진단

가. 진단기준 : 금융보안 수준진단 프레임워크 가이드 (금융보안원, 26년 발간 예정)

나. 진단범위 : 7개 분야 46개 항목(133개 세부원칙)

다. 금융보안 가이드에 따른 수준진단 및 성숙도 등급 산정

- 거버넌스, 보호 영역별 당사의 현황 분석 및 수준진단
- 항목별 성숙도 등급 산정 및 등급 향상을 위한 가이드 제시
- 수준진단 활동에 대한 산출물(분석자료, 보고서) 목록 제시 및 산출물 제공
- 법무법인을 통한 수준진단 결과 검증(필요시)

5. 정보보호 공시

가. 공시기준 : 정보보호 공시 가이드라인 (한국인터넷진흥원, 2025.02)

나. 공시항목 : 정보보호 투자 현황, 정보보호 인력 현황 등 4개 항목

다. 정보보호 공시자료 작성

- 정보보호 공시 가이드에 따른 정보보호 공시자료 작성
- 정보보호 공시 가이드에 따른 자산/비용, 기술 투자 등 금액 산정

라. 정보보호 공시 사전점검

- 회계법인 또는 정보시스템 감리법인을 통한 사전점검확인서 작성
  (과학기술정보통신부 제출 목적의 공시용, 조서용 2종)

6. IT보안 및 정보보안 감사

가. 감사기준 : 금융감독원 IT자체 감사 가이드라인 (금융감독원, 2025.02)
금융감독원 IT검사업무 안내서 (금융감독원, 2021.01)

나. 당사 환경에 부합한 감사항목 및 범위 선정 (1개월 내 진행 가능한 범위 선정 예정)

다. 금융감독원 가이드라인을 준용하여 IT보안 및 정보보안 감사 실시

- 감사 영역별 당사의 현황 분석 및 감사 실시
- 감사계획(범위), 절차, 기법, 산출물 제공 및 개선사항 가이드 제시
- 감사 증빙자료 수집 및 분석 가능한 Tool 또는 스크립트 제공
- 법무법인을 통한 감사 결과 검증

7. 투입인력 요구사항

가. 본 제안요청서 요구사항을 기준으로 제안사 자체적인 적정 인력을 산정하여 제안

나. 프로젝트 관리자(PM)는 고급 등급 이상으로 하며 단순 사업관리가 아닌, 프로젝트를 직접 수행하고 리딩할 수 있는 인력으로 배정해야 함

다. 정보보호 위험평가 인력이 ISMS 인증심사원 자격을 보유한 경우 평가 시 가점을 부여함

라. 투입 인력이 금융업권 대상 유사 컨설팅 경험(최근 5년)이 있는 경우 평가 시 가점을 부여함

마. 프로젝트 관리자(PM)를 제안사 소속의 정규직원으로 배정하는 경우 평가 시 가점을 부여함

바. 서비스 영역 상/하반기 취약점 분석평가 PL이 최소 3개월 이상 상주할 경우 평가 시 가점을 부여함

사. 인프라 영역 취약점 분석평가 PL이 최소 4개월 이상 상주할 경우 평가 시 가점을 부여함

아. 금융보안 수준진단 수행인력이 ISMS 인증심사원 자격, 10년 이상의 정보보호 컨설팅 경력을 보유한 경우 평가 시 가점을 부여함(심사원 자격, 컨설팅 경력에 별도 가점 부여)

자. 정보보호 공시 수행인력이 정보보호 공시 컨설팅 수행 경험을 보유한 경우 평가 시 가점을 부여함

차. IT보안 및 정보보안 감사 수행인력이 금융감독원 IT검사 수행 경험을 보유한 경우 평가 시 가점을 부여함

8. 정보보호 요구사항

가. 정보보호 관련 공통 요구사항 준수

- 제안사는 사업수행 시 발주처의 보안정책 및 지침을 준수하여야 함
- 제안사는 사업수행으로 알게 된 보안사항에 대해서는 비밀보안을 준수하여야 하며, 이를 위반할 경우 관련 법령 및 계약에 따라 일체 책임을 짐
- 본 사업에 투입되는 인력은 발주처의 보안관련 규정을 준수하여야 함

나. 사업자 및 참여인력 정보보호

- 사업수행에 사용되는 인원, 문서, 장비 등의 보안 관리계획을 수립하여야 하며, 보안상 결격 사항이 없도록 조치해야 함
- 사업자는 본 사업과 관련하여 취득한 업무내용에 대하여 제3자에게 누설하여서는 안되며, 발주처가 요구하는 보안사항을 철저히 준수하여야 함
- 본 제안 및 과업수행 중은 물론 향후에 라도 보안사항 및 기타 System의 내부구성, 네트워크, 보안장비, IP현황, Data 등 일체의 모든 사항에 대해 보안을 유지하여야 함

- 보안유출 등으로 인한 문제발생 시에는 사업자가 모든 책임과 배상의 의무를 지며, 2차로 해당 대표자와 종사자가 민·형사상 책임과 의무를 져야 함
- 사업수행 각 단계별 정보보호 가이드라인을 준수하고, 물리적, 관리적, 기술적인 보안대책 등 안전 및 보안 관리에 대한 운영 규정을 마련하여 비상사태에 대비하여야 함
- 사업 참여 인원에 대해서는 사업 투입 전 보안서약서 작성 제출(의무사항) 및 정보보안 규정, 정보보안지침, 개인정보보호지침을 준수하여야 함
- 기타 사항은 발주처의 보안지침에 따라야 함

9. 사업관리 요구사항

가. 사업추진 성과물 제출

- 사업추진과정에서 생산되는 제반 작업 단위 별 산출물의 종류, 주요내용 작성 및 제출시기, 제출 부수, 제출 매체 등을 제시하고 제출 시기는 사업추진 공정 및 품질보증 계획과 연계되어야 함
- 사업수행과 관련 산출물의 사용권, 소유권 및 저작권은 당사 소유임

III. 제안 요청 사항

1. 제안사 소개

가. 제안사 개요 및 재무 현황

- 제안사의 일반현황 및 주요 연혁
- 최근 3년간 자본금 및 매출 실적 재무구조 등
- 조직 및 인력현황

나. 조직 및 인력현황

- 제안사 조직도 및 업무기능, 인력현황 등 기술
- 자사인력 및 협력업체 인력을 구분하여 기술 (컨소시엄 포함)
- 협력업체가 있는 경우 회사 개요, 연혁, 조직, 경영실태, 사업분야, 사업 수행 실적 등에 대하여 업체별로 기술
- 제안사가 협력업체를 활용하는 경우 반드시 제안서상에 기재하여야 본 사업의 협력업체로 인정함

다. 유사 프로젝트 수행 실적

- 최근 5년간 유사 프로젝트 수행 실적 (별첨7 참조)
- 제안사 또는 협력업체 유사분야 사업실적
- 실적 제출시 주사업자가 아닌 경우 별도 증빙 요청할 수 있음
- 최근 년도 순으로 기재하고, 수행중인 프로젝트 내용 포함

라. 제안사 특징 및 장점

- 타 제안사와 차별화될 수 있는 제안사의 특징 및 장점 기재
- 컨소시엄의 경우, 각 사별 역할과 책임 명시

2. 사업 수행 방안

가. 제안사 특징 및 장점

- 사업 상세 요건의 각 항목을 효과적으로 구현하기 위한 수행 방안을 관리적, 기술적 관점에서 기술
- 방안 기술 시 당사 요건에 포함되지 않은 내용이라도 추가 고려사항이 있는 경우 제시

나. 수행조직 및 추진 일정 계획

- 사업 수행조직, 역할 및 일정에 대한 상세 내용을 제시
- 제안사의 투입인력은 역할별로 구분하여 제시
- 전체 투입인력의 프로파일 제시(별첨 4, 5)

다. 사업 관리 방안

- 사업 관리 방법론에 따른 단계별 관리 방안을 제시해야 하며, 액티비티/태스크/산출물을 상세 제시
- 방법론에 의거 범위관리, 일정관리, 변화관리, 위험관리 등의 방안이 수립되어야 함
- 사업 진척 현황에 대한 업무협의 및 보고 체계를 정립하여 제시해야 하며, 각종보고(정기/부정기) 계획을 상세히 제시
- 사업 수행과정에서 발생하는 의견조정에 관한 절차 제시
- 사업 수행과정에서 발생 가능한 위험요소에 대해 사전에 도출하고 대응방안을 제시

라. 품질 관리 방안

- 사업 산출물 품질확보를 품질보증 계획, 활동절차 및 수행내역, 조직, 검증방법을 제시
- 사업 품질관리 중 예상되는 산출물 및 검증계획을 제시

마. 기타 사항

- 제안사는 당사가 본 제안요청서에서 제시하지 않은 미비점이나 보완해야 할 사항을 추가하여 제안서를 제출해야 하며, 이를 기반으로 추진한 사업의 가용성, 안정성, 운용성에 대한 책임을 질 것
- 정확한 요구분석과 설계로 당사가 지향하는 정보보호관리체계 수립을 완수해야 함

3. 정보보호 관리 방안

가. 단계별 고려해야 할 보안 요건 및 대응 방안 제시

나. 사업 참여 인원에 대한 보안관리 방안

4. 교육 지원 방안

가. 시큐어코딩 교육 등 당사에서 요구하는 교육 및 자문에 대한 계획 및 일정을 제시

나. 제출된 교육계획서는 착수 후 당사의 보완 요청에 따라 제안사와 협의하여 변경 가능해야 함

5. 기술 이전 방안

가. 사업완료 후 원활한 운영을 위해 실무자 및 관련 인원에 대한 기술 및 방법론 이전 계획

나. 기술 및 방법론 이전을 위한 매뉴얼, 산출물 등 제시

6. 제안 가격

가. 별첨6 양식에 준하여 작성하며 가격제안서 제출

나. 항목별 모든 가격은 List Price, 할인율, 공급가 형태로 작성하고, 반드시 VAT포함가에 제출

다. 제시한 가격조건에 대한 유효기간 표시

라. 인건비

- 등급별(특/고/중/초급) 투입 M/M, 등급별 단가를 표시
- 26년 Software 노임단가 기준 (제경비 110%, 기술료 20%)
- 컨설턴트 등급도(특/고/중/초급)으로 분류하고 등급별 기준 및 단가 제시

IV. 제안서 제출

1. 제안서 제출 방법

가. 제출기한 : 2026.01.26(월) 16:00

나. 제출장소 : 서울 중구 소월로 3(에티버스타워) 11층 정보보호팀

다. 제출방법 : 방문제출

라. 제안사 제출서류

- 제안참여공문 1부 (각 사 고유양식)
- 제안 참여업체 서약서 1부 (별첨1 참조)
- 정보보호서약서 1부 (별첨2 참조)
- 재무제표 사본 1부 (별첨3 참조)
- 투입 인력 이력사항 양식 (별첨4 참조)
- 월별 인력 투입계획 양식 (별첨5 참조)
- 가격 제안서 1부 (별첨6 참조 인감날인 후 봉인제출)
- 주요사업실적 양식 1부 (별첨7 참조)
- 제안서 1부 / 요약서 10부 (출력 제출)
- 발표자료 1부 (파일 제출)
- 재무제표 사본 1부
- 제안서는 반드시 공문형식으로 제출해야 하며, 제안서 작성에 소요되는 비용은 제안사의 부담으로 하고, 제출한 제안서는 반환하지 않음

2. 제안서 작성 목차

가. 제안사 소개

- 회사연혁 및 일반사항, 조직 및 인력현황, 유사분야 주요 사업 실적 등

나. 제안 개요

- 제안 배경, 목적, 범위, 전략, 제안의 특징 등을 기술

다. 프로젝트 추진방안

- 과제별 추진방안 기술

라. 프로젝트 관리방안

- 사업수행 방법론, 추진일정·조직, 인력투입계획 및 업무분장, 품질관리 방안 등 기술
- 프로젝트 단계 별 산출물 내용 기술

마. 정보보호 관리계획 방안(투입인력 보안교육 포함)

바. 기타 지원 방안

- 교육지원방안, 기술지원 및 이전방안, 유지보수방안, 기타지원방안 기술

3. 제안 유의사항

가. 해당 사업은 필요 시, 컨소시엄 형태로 진행될 수 있으며 이 경우 각 사의 역할과 책임 및 주사업자(계약대상)에 대하여 명시하여야 함

나. 제안서에 별도의 기재사항이 없을 경우 제안서를 제출함으로써 상기 당사 요구 조건을 모두 수용하는 것으로 간주함. 수용 불가능한 부분이 있을 경우 수용할 수 없는 부분에 대하여 해당 내용을 정식 공문을 통하여 제출하여야 함

다. 제안 발표는 프로젝트 관리자(PM)가 직접 발표하여야 함

라. 본 제안요청서에서 언급하지 않았으나, 본 과업수행에 필요하다고 판단되는 사항이 있을 경우 이를 추가로 제시하여야 함

마. 본 사업의 추진계획이 변경·취소될 경우, 본 사업의 추진은 조정 가능하며 이로 인해 변경·취소되는 경우 제안사는 이의를 제기하지 못함

바. 사업기간 중 제안서에 제출한 참여인력에 대해 당사의 사전 승인 없이 변경할 수 없음. 단, 참여인력 중 당사의 필요에 의해 특정분야 인력의 교체를 요구하는 경우에는 동급 이상의 인력으로 교체하여야 하며, 우선협상대상자로 선정된 이후에도 제시한 추진방안, 인력투입, 협력업체 등이 부적절하다고 판단되는 경우에는 변경을 요청할 수 있음

사. 당사는 제안내용에 대한 확인을 위하여 필요한 경우 투입인력 인터뷰 등을 요구할 수 있으며 제안사는 이에 응하여야 함

아. 사업결과에 따른 산출물 등의 소유권과 지적재산권은 원칙적으로 당사에 귀속되며, 컨소시엄의 경우 구성업체 전체가 해당 권리의 소유를 당사로 인정하여야 함

자. 입찰참가자는 용역입찰 유의사항 등 입찰 및 계약과 관련된 모든 사항을 숙지하고 입찰에 참가하여야 하며, 이를 숙지하지 못한 책임은 입찰참가자에게 있음

차. 제출된 제안서의 내용은 당사가 요청하지 않는 한 변경할 수 없으며, 계약체결 시 계약조건의 일부로 간주함

카. 제출된 제안자료가 부족하거나 확인 등을 위하여 추가자료가 필요하다고 판단되는 경우 제안사는 당사가 지정하는 일시까지 해당자료를 제출하여야 하며, 당사의 별도 요청 및 승낙이 없는 한 일체의 수정, 추가 및 대체를 할 수 없음

타. 기재사항이 누락되거나 제안요청 내용에 대해 언급이 없는 항목은 해당사항이 없는 것으로 간주함

파. 제안서의 내용을 객관적으로 입증할 수 있는 관련자료는 당사에서 요청 시 제출하여야 함

하. 제안서는 허위로 작성되지 않아야 하고 계약된 이후에도 허위로 작성된 사실이 발견되거나 제안된 내용을 충족시키지 못할 경우 제안사는 계약의 무효와 동시에 일체의 손해배상 책임이 있으며 이에 어떠한 이의도 제기할 수 없으며 제안과정에 얻은 정보를 제안 외의 목적으로 사용할 수 없음

4. 제안 자격요건

가. 본 사업의 기간 및 일정, 그 외 요건을 이행할 수 있는 충분한 인력 풀(POOL)을 갖춘 기업

나. 정보보호산업의 진흥에 관한 법률 23조(정보보호 전문서비스 기업의 지정·관리)에 따라 지정된 정보보호 전문서비스 기업

다. 금융사를 대상으로 정보보호 컨설팅 사업을 수행한 경험이 있는 기업

라. 최소 3년 이상 정보보호 컨설팅 사업을 영위하고 있는 기업

마. 정당한 이유 없이 계약을 체결하지 않거나 불이행 또는 이행에 부당한 행위를 한 이력이 없는 기업

바. 경쟁사의 입찰 참가 또는 계약 체결·이행을 방해한 이력이 없는 기업

사. 입찰 참가자격에 관한 서류 또는 계약에 관한 기타 서류를 위조한 이력이 없는 기업

아. 정부/금융기관 등에 부적당 업자로 등재되어 입찰 참가자격이 정지되는 등 제재를 받은 이력이 없는 기업

5. 제안서의 효력

가. 제안서의 내용은 제안사가 수행사업자로 선정된 후 계약서에 명시하지 않더라도 계약서와 동일한 효력을 가짐. 단, 계약서 및 프로젝트 수행계획서에 명시된 경우에는 계약서 및 프로젝트 수행계획서상의 내용이 우선함

나. 당사는 필요 시 제안사에 대하여 추가제안 또는 자료를 요구할 수 있으며 이에 따라 제출된 자료는 제안서와 동일한 효력을 지님

다. 제안서 내용에 대한 해석의 차이가 있을 경우 상호 협의하여 결정하고, 의견이 일치하지 않는 경우 당사의 해석을 우선함

6. 제안서 작성 지침

가. 제안서는 Powerpoint A4지 양식으로 작성하며, 제시된 제안서 목차를 참고하여 작성함

나. 제안문서는 한글로 작성하며 사용된 영문 약어에 대해서는 별도 주석표기 및 설명을 제공하여야 함

다. 제안서의 내용은 명확한 용어를 사용하여야 하며, “~사용가능 하다”, “~할 수 있다”, “~고려하고 있다” 등과 같이 모호한 표현은 평가 시 불가능한 것으로 간주함

라. 제안요건에 명시되지 않은 내용에 대한 추가적인 제안사항이 있는 경우 해당 항목에 포함하거나 또는 별도의 항목을 추가하여 작성할 수 있으며, 또한 작성지침항목 중 해당 사항이 없는 경우는 “해당없음”으로 간략히 기술

마. 제안의 타당성을 수긍할 수 있도록 가급적 계량화, 계수화된 자료를 명기할 것

V. 제안 일반 사항

1. 업체 선정 방식 : 공개입찰 후 협상에 의한 계약

2. 업체 선정 일정

구분	일자	비고
제안요청서 입찰공고	26.01.09(금)	
제안서 제출마감	26.01.26(월)	
제안발표 및 업체 평가	26.01.28(수)	
우선협상대상업체 선정	26.01.29(목)	
협상 및 계약체결	26.01.30(금)	

3. 업체 선정 상세

가. 제안발표는 제안서 제출 순서대로 진행

나. 제안서 검토 후 기술 및 가격을 종합적으로 평가하여 우선협상 대상 및 최종 사업자 선정

다. 제안내용의 검토 및 평가는 당사가 정한 기준에 의하며, 세부 검토 결과는 공개하지 않음

라. 선정결과는 개별통보를 원칙으로 함

4. 문의처

가. 담당자 : 정보보호팀 유수진 책임(02-3455-3469, sujin.yoo@lotteins.co.kr)

나. 문의는 제안서 마감시한 까지만 접수하고 제안사의 영업대표를 통해서만 가능함

다. 모든 질문과 답변은 업체의 영업대표에게 e-mail로 일괄 발송함

별첨1) 제안참여서약서

제안 참여업체 서약서

폐사는 금번 “26 년 전자금융기반시설 취약점 분석평가” 사업자 선정에 대한 적격업체(우선협상대상자, 낙찰자 등) 선정과 관련하여 다음 조건을 준수할 것을 확약하며, 만약 이를 위반 시는 귀사의 어떠한 조치도 감수하겠기에 본 서약서를 제출합니다.

- 다 음 -

가. 귀사의 내외부의 환경변화 등의 사유로 본 제안요청 내용의 일부 또는 전부가 변경되거나 취소되는 경우가 발생하더라도 폐사는 일체의 이의를 제기하지 않겠습니다.

나. 폐사는 적격업체로 선정되지 못한 경우에도 평가결과에 대해 일체의 이의를 제기하지 않겠습니다.

2026 년 월 일

회 사 명 : _____

대표이사 : _____(인)

롯데손해보험㈜ 대표이사 귀하

별첨2) 정보보호 서약서

정보보호 서약서

롯데손해보험㈜ 대표이사 귀하

- 회 사 명 :
- 사업자등록번호 :
- 소 재 지 :
- 대 표 자 성 명 :

상기 법인은 귀사에서 추진 중인 “26년 전자금융기반시설 취약점 분석평가”과 관련하여 제안요청서 1부를 수령하였으며, 본건과 관련하여 취득하게 된 귀사의 사업계획, 전산 System 정보, 기업현황 등 제반 정보나 자료 등을 제안서 작성 목적으로만 사용하며, 다른 목적으로 사용하거나 언론기관을 포함한 제3자에게 공개, 누설 또는 제공하지 않을 것을 서약하는 바이며, 만일 이를 위반할 경우에는 어떠한 민·형사상의 책임도 감수할 것을 서약하고 본 서약서를 제출합니다.

2026 년 월 일

대표이사 (인)

별첨 3) 재무제표

재무적 지표 (최근 3년)

(단위 : 백만원)

구분		2024년	2023년	2022년
총자산				
부문별 매출액	○○부문			
	○○부문			
	계			
당기순이익				
기업신용등급				
금융비용				
부채비율				
차입금의존도				
EBIT				
EBITDA				

별첨4) 투입 인력 이력사항 양식

투입 인력 이력서

1. 인적사항

성명		연령		소속/직급		기술등급	
연락처		E-Mail		총 업무경력	년(년 ~ 년)		
학력사항	*학력 및 학과, 졸업 년도 기재*			자격사항	*취득일자, 만료일자 포함하여 기재*		
				수상이력	*수상기관명, 수상일자 포함하여 기재*		
본 사업 참여임무	[업무]			투입기간		투입개월	
	[역할]					투입공수	

2. 경력사항

소속사	발주처	사업명	참여기간	담당업무	역할

- 경력사항은 본 사업과 연관된 사업을 기재하고, 사업명 구체적으로 작성요청
  참여기간은 실투입기간을 작성하시고, 사업명 및 담당업무로 파악이 불가한 경우 경력 불인정
- 기술등급 : 한국SW협회 기술등급 기준으로 작성

별첨5) 월별 인력 투입계획

역할		성명	등급	ISMS 심사원 자격여부	금융권 컨설팅 횟수 (최근5년)	투입MM												합계
						M1	M2	M3	M4	M5	M6	M7	M8	M9	M10	M11	M12	
컨설팅	PM																	
	취약점 분석평가 (관리체계)																	
	취약점 분석평가 (인프라)																	
	취약점 분석평가 (서비스)																	
	정보보호 위험평가																	
	정보보호 공시																	
	IT 보안 및 정보보안 감사																	

	금융보안 수준진단																	
	소계																	
계																		
등급별	특급																	
	고급																	
	중급																	
	초급																	
계																		

- 인력등급은 별첨4) 에서 정한 기술등급 기재
- 금융권 컨설팅 횟수는 담당 역할에 한하여 작성
- 본 양식의 내용을 기준으로 제안서에 포함

별첨6) 가격제안 양식

1. 인건비

(단위:천원,%,개월)

구분		등급	성명	투입MM	단가	투입기간	금액	공급가	할인율
취약점 분석평가									
정보보호 위험평가									
정보보호 공시									
금융보안 수준진단									
IT보안 및 정보보안 감사									
합계									

2. 시스템

(단위:천원,%,개월)

구분	품목	내역 및 용도		수량	금액	공급가	할인율	유지보수	
								무상유지보수기간	유상유지보수요율
HW									
SW									
솔루션									
합계									

3. 유지보수

(단위:천원)

구분	금액	비고
유지보수비용(1년차)		
유지보수비용(2년차)		
유지보수비용(3년차)		
유지보수비용(4년차)		
합계		

4. TOTAL(1+2)

(단위:천원)

구분	금액	비고
합계		

- 인건비는 별첨5) 월별 인력 투입계획의 등급 및 투입MM와 반드시 일치
- 인건비는 관리체계 취약점 분석평가, 인프라 취약점 분석평가, 모의해킹, 정보보호 위험평가, 사규 제·개정, 공시 컨설팅 등으로 상세 구분하여 기입

별첨7) 주요사업실적 양식

주 요 사 업 실 적

구분 (ISMS/ISMS-P/ 취약점진단/공시/감사) 중 1개만 선택	발주처	업권 (금융권/기타) 중 1개만 선택	사업명	수행년도

- 현재 수행중인 사업도 포함하여 최근 연도순으로 기재하며, 본 사업과 유사한 업무실적을 중심으로 기재함 (기간 : 2021.01월 ~ 2026.01월)
  수행업무 내용으로 판단이 어려운 경우 추가자료 제출 및 불인정
- ISMS, 취약점진단 통합 컨설팅의 경우 각각 분리하여 작성
- 본 양식의 내용을 기준으로 제안서에 포함