

『클라우드 기반 표준 랜딩존 구축 업체 선정』

제안 요청서

2026年 7月

본 제안요청서는 관련 법령에 따라 보호의 대상이 되는 기밀정보를 포함하고 있습니다. 본 문서에 포함된 정보의 전부 또는 일부를 무단으로 제3자에게 공개, 배포, 복사 또는 사용하는 것은 엄격히 금지됩니다.

삼성자산운용(주)

1. 사업 개요

항목	내용
사업명	클라우드(AWS)기반 표준 랜딩존 구축 업체 선정
추진 배경	<ul style="list-style-type: none"> - 당사는 데이터 분석, AI 활용, 외부 데이터 연계 등 디지털 업무 수요가 확대됨에 따라 안정적이고 표준화된 클라우드 기반 인프라 필요 - 클라우드 연계 구성이 증가하면서 계정, 네트워크, 보안 권한, 로그 비용 관리 체계를 사전에 표준화 필요성 증대 - 클라우드 자원이 개별 목적에 따라 구성될 경우 보안 정책의 일관성 부족, 운영 책임 불명확, 신규 서비스 도입 지연 문제 발생 가능성으로 인해 이에 AWS기반 랜딩존 구축하여 클라우드 사용의 공통 기반을 마련하고 향후 AI 및 Biz 서비스 확장 시 안정적으로 활용 가능한 표준 운영 체계 확보하고 자 함
사업 범위	<p><input type="checkbox"/> 수동 작업 줄이고 표준화를 보장하기 위해 계층형 가드레일 구현을 통해 보안 확보되고 커스터마이징에 유연한 환경 구축</p> <ul style="list-style-type: none"> - AWS 계정 구조 및 조직 체계 설계 - 네트워크 표준 아키텍처 구축 - 보안 기준 및 접근 통제 체계 구현 - 로그 감사 모니터링 체계 구축 - 암호화 및 데이터 보호 체계 마련 - 비용 관리 및 자원 태깅 표준화 - 인프라 자동화 및 표준 배포 체계 구축 - 운영 거버넌스 및 관리 절차 수립 - 데이터 플랫폼 및 AI 연계 기반 확보
선정 방식	자격 요건 충족 업체 중 견적 총액 기준 선정

2. 주요 제안 요건

구분	세부 요구사항
조직 및 인력 제안 요건	<input type="checkbox"/> 제안사는 AWS 랜딩존 구축 사업의 안정적 수행을 위해 분야별 전문인력을 포함한 전담 수행조직을 구성하여 제시하여야 한

구분	세부 요구사항
	<p>다.</p> <ul style="list-style-type: none"> - 수행조직은 사업관리, 클라우드 아키텍처, 보안, 네트워크, 자동화, 운영 전환 등 역할을 포함하여야 한다 - 사업 수행 중 설계, 구축, 검증, 문서화, 운영 전환 단계 별 담당 인력을 제시하여야 한다 <p>□ 제안사는 투입 인력의 전문성, 유사사업 경험, 자격사항 및 투입계획을 구체적으로 제시하여야 한다</p> <ul style="list-style-type: none"> - 투입 인력은 AWS 랜딩존, 멀티계정 구조, 네트워크 연계, 보안 가드레일, 로그·모니터링, IaC 자동화 구축 경험을 보유하여야 한다. - 금융권 또는 보안 요구 수준이 높은 클라우드 환경에서의 구축 경험을 보유한 인력을 우대한다 <p>□ 제안사는 핵심 인력의 안정적 투입과 변경 관리 방안을 제시하여야 한다</p> <ul style="list-style-type: none"> - 핵심 인력 변경이 필요한 경우 발주사의 사전 승인을 받아야 한다 - 인력 변경으로 인한 일정 지연, 품질 저하, 인수인계 누락이 발생하지 않도록 관리 방안을 제시하여야 한다
표준 기반 및 자동화 영역	<p>AWS 랜딩존의 공통 구성요소를 표준화하고, 신규 계정·서비스 확장 시 반복 적용 가능한 자동화 기반을 마련한다</p> <p>□ 랜딩존 자동화 및 표준 프레임워크 구현</p> <ul style="list-style-type: none"> - AWS 랜딩존 구성과 관련된 계정, 네트워크, 보안, 로그, 권한 등 공통 구성요소를 IaC 템플릿 형태로 구현하여야 한다 - 신규 계정 및 업무 환경 확장 시 재사용 가능한 표준 모듈 형태로 개발하여야 한다 - Naming, IP 대역, 태그, 환경 구분, 계정 정보 등 주요 설정값은 파라미터화하여 변경 및 확장이 가능하도록 구성하여야 한다 <p>□ 자동화 개발 및 형상관리 체계 구성</p> <ul style="list-style-type: none"> - 특정 CSP 콘솔 수작업에 의존하지 않고 코드 기반으로 구축·변경·배포가 가능하도록 구성하여야 한다 - Terraform, GitLab, Packer, Ansible 등 범용 자동화 도구 활용 방안을 제시하여야 한다 - IaC 코드 형상관리, 배포 승인, 변경 이력 관리, 검증 및

구분	세부 요구사항
	롤백 절차를 포함하여야 한다
계정 · 보안 및 접근통제 영역	<p>다중 계정 환경에서 계정 구조, 보안 정책, 권한 체계를 표준화하여 일관된 보안 거버넌스를 확보한다</p> <p>□ 계정 및 조직 구조 관리</p> <ul style="list-style-type: none"> - AWS Organizations 기반의 Multi Account 구조를 설계하고 구축하여야 한다 - 관리, 보안, 로그, 네트워크, 업무 계정 등 계정별 역할과 책임을 구분하여 제시하여야 한다 - OU 구조, 계정 배치 기준, 계정 생성 및 확장 절차를 포함하여야 한다 <p>□ 계층형 가드레일 및 보안 거버넌스 구현</p> <ul style="list-style-type: none"> - 다중 계정 환경에서 보안 정책이 일관되게 적용될 수 있도록 계층형 가드레일을 구현하여야 한다 - 계정, 조직, 업무 환경별 보안 기준과 정책 적용 방안을 제시하여야 한다 - 비인가 설정, 권한 오남용, 보안 정책 위반을 예방 · 탐지할 수 있는 통제 방안을 포함하여야 한다 <p>□ ID 및 접근통제 체계 구축</p> <ul style="list-style-type: none"> - IAM, 관리자 권한 분리, MFA, 최소권한 원칙 등 접근통제 기준을 수립하여야 한다 - 사용자, 관리자, 시스템, 서비스 계정별 권한 부여 및 관리 기준을 제시하여야 한다 - 권한 변경, 권한 회수, 임시 권한 부여, 접근 이력 관리 방안을 포함하여야 한다
네트워크 및 데이터 플랫폼 연계 영역	<p>업무망, 내부 시스템, 외부 서비스, 데이터 · AI 플랫폼과 안정적으로 연계 가능한 클라우드 네트워크 기반을 구성한다</p> <p>□ 네트워크 토폴로지 및 연결 구성</p> <ul style="list-style-type: none"> - VPC, Subnet, Routing, TGW, Direct Connect, PrivateLink 등 AWS 네트워크 표준 아키텍처를 설계하여야 한다 - 업무망, 내부 시스템, 외부 데이터 서비스, Snowflake 등 연계 대상과의 안정적인 연결 구조를 포함하여야 한다. - IP 대역, DNS, 보안그룹, NACL, 라우팅 정책 등 네트워크 구성 기준을 표준화하여야 한다 <p>□ 데이터 및 AI 플랫폼 연계 기반 구성</p> <ul style="list-style-type: none"> - S3, Snowflake, 외부 데이터 수집, 내부 시스템 연계, AI 서

구분	세부 요구사항
	<p>비스 확장을 고려한 클라우드 기반을 구성하여야 한다</p> <ul style="list-style-type: none"> - 데이터 저장, 처리, 연계, 접근통제, 암호화 기준을 반영하여야 한다 - 향후 데이터 분석 및 AI 서비스 도입 시 반복 구축을 최소화할 수 있는 확장 가능한 구조를 제시하여야 한다 (예. Bedrock서비스 등)
<p>운영 안정성 및 관리 체계 영역</p>	<p>랜딩존 구축 이후에도 안정적인 운영, 보안 감사, 비용 관리, 변경 관리가 가능하도록 운영관리 체계를 수립한다</p> <p>□ 로그, 감사 및 모니터링 체계 구축</p> <ul style="list-style-type: none"> - CloudTrail, Config, CloudWatch, VPC Flow Log 등 주요 로그를 중앙 수집할 수 있도록 구성하여야 한다 - 계정별 활동 이력, 설정 변경, 네트워크 흐름, 보안 이벤트에 대한 추적이 가능하여야 한다 - 이상 행위 탐지, 운영 상태 확인, 장애 대응을 위한 모니터링 기준을 수립하여야 한다 <p>□ 암호화 및 데이터 보호 체계 구축</p> <ul style="list-style-type: none"> - KMS 기반 암호화 정책과 키 관리 기준을 수립하여야 한다. - S3, 로그 저장소, 백업 데이터 등 주요 데이터 저장 영역에 대한 보안 설정을 적용하여야 한다 - 중요 데이터 보호를 위한 접근권한, 암호화, 보관, 삭제, 백업 및 복구 기준을 포함하여야 한다 <p>□ 비용 관리 및 태깅 표준화</p> <ul style="list-style-type: none"> - 제안사는 계정, 업무, 프로젝트, 서비스 단위의 비용 식별이 가능하도록 태깅 표준을 수립하여야 한다 - 예산 관리, 사용량 모니터링, 비용 알림 등 비용 통제 방안을 포함하여야 한다 - 리소스 생성 시 필수 태그가 적용될 수 있도록 표준 정책 또는 자동화 방안을 제시하여야 한다 <p>□ 운영 및 변경 관리 절차 수립</p> <ul style="list-style-type: none"> - 랜딩존 구축 이후 운영, 변경, 배포, 점검, 장애 대응을 위한 관리 절차를 수립하여야 한다 - 운영환경과 개발환경의 분리 기준 및 권한 관리 방안을 제시하여야 한다 - 설계 변경, 보안 정책 변경, 리소스 변경 시 승인, 검증, 배포, 기록 관리 절차를 포함하여야 한다

3. 참가 자격 요건

구분	자격 요건
기업 역량	- 제안요청 공고일 기준 국내 금융 클라우드 구축 사업 경험을 보유한 사업자
보유 엔지니어	- 제안사는 AWS 아키텍트, 보안, AI, IaC 자동화 등 분야별 전문 엔지니어 보유 - 핵심 투입 인력은 관련 자격 및 유사 프로젝트 수행 경험 보유 시 우대
구축 실적	- 제안사는 AWS 랜딩존, 멀티 계정, 네트워크 보안 가드레일, 자동화 구축 관련 유사사업 실적을 제시 - 금융권 또는 보안 요구 수준이 높은 기관의 클라우드 구축 실적 우대
구축 역량	- 제안사는 계정 구조, 네트워크, 보안 가드레일, 로그 모니터링, 비용관리 IaC 자동화에 대한 설계 구축 방법론을 제시하여야 한다 - 구축 이후 검증 운영 전환, 문서화 교육 안정화 지원 방안을 제시하여야 한다

4. 견적서 작성 요령

항목	내용
제안 방식	- 투입에 필요한 구축 M/M 총 비용을 제시하며 주요 수행 내역별 세부항목 구분하여 작성

구분	항목	상세내역	M/M	제안가
설계	특급			
	고급			
구축				
안정화				

※사례(Reference): 유관 업종, 규모 또는 유사 보안 요구사항을 해결한 구축

사례가 있을 경우 견적서 제출 시 메일에 기재

5. 제안서 접수 및 유의사항

1. 제출시기 및 방법(제안서, 견적서)

- 제출기한: 2026년 07월 08일(수) 17시까지
- 제출서류: 사업자등록증, 견적서, 구축사업 실적 목록
- 제출방법: 제출기한까지 이메일 제출
- 제출처: asset.bid@samsung.com
- 제안서 크기 및 포맷: “제안서 작성지침” 참조

2. 작성 시 유의사항

- 제안서 작성과 관련하여 발생하는 모든 제반 소요비용은 정보제공 업체가 부담함을 원칙으로 한다.
- 제출되는 제안서의 기재 내용은 당사의 별도 요청이 없는 한 어떠한 사유로도 수정 또는 삭제할 수 없다.
- 제안서 작성 내용중 모호한 표현은 불가능한 것으로 간주한다.
- 제안서 기재사항 누락과 기재내용이 상이 함에 따라 생기는 불이익은 정보제공 업체가 감수해야 한다.
- 문서는 MS-WORD, 파워포인트, PDF 외에는 허용하지 않는다.
- 문서는 한글로 작성한다.
- 우선협상대상자 선정 결과에 대하여 이의를 제기 할 수 없다.

[별첨] 구축 사업 실적

- ※ AWS 또는 Azure 구축 사업 실적을 연도순으로 기재
- ※ 현재 수행 중인 사업 포함, 제안 요청 내역과 관련한 것만 기재

사업명	사업기간	발주처	비고

- 하도급은 발주처가 승인한 경우에 한하여 작성하며 비고란에 원도급 회사를 기재
- 공동도급 계약일 경우 계약금액란에 제출사의 지분만을 기재