공공 부문의 클라우드 서비스 구매

핸드북 - 클라우드 사용 기본 계약을 위한 RFP 예제 포함

버전 2: 2022 년 2 월

고지 사항

본 문서는 정보 제공의 목적으로만 제공됩니다. 특정 지역의 공공 조달 프로세스의 법적 요건에 맞춰 개발되지 않았습니다. 본 문서 내 정보를 판단하고 클라우드 제공업체의 제품과 서비스를 사용하는 데 따르는 책임은 클라우드 고객에게 있습니다. 본 문서는 어떠한 보증, 진술, 계약상 의무 이행 또는 보장을 하거나 조건을 붙이지 않습니다.

예제 문서와 문구는 법적 조언, 지침 또는 자문으로 해석되어서는 안 됩니다. 클라우드 고객은 사업 운영 국가의 법률에 따른 책임과 관련해 법률 자문을 구해야 합니다. CISPE 는 본 문서에서 제공하는 정보와 관련하여 또는 해당 정보로 인해 발생하는 모든 보증, 책임 또는 손해를 책임지지 않습니다.

CISPE 소개

CISPE(**Cloud Infrastructure Services Providers in Europe**, https://cispe.cloud)는 비영리 독립 산업 협회로, 유럽의 클라우드 인프라 서비스 제공업체를 대표하여 업계 및 정책 입안자와 협력하면서 클라우드 서비스와 산업, 공공 생활 및 사회 전반에 있어 클라우드 서비스의 역할에 대해 지침과 교육을 제공합니다.

EU 국가에서 운영되는 기업과 16 개 유럽 국가에 기반을 둔 글로벌 기업들을 비롯해 회원이 꾸준히 증가하고 있습니다. 서비스 중 하나 이상이 CISPE 데이터 보호 행동 강령의 요구 사항을 충족한다고 공표한 기업은 CISPE 에 가입할 수 있습니다. CISPE 는 다음과 같은 활동을 합니다.

- EU 및 EU 회원국 내에서 클라우드 우선 공공 조달 정책의 이점 설파
- 클라우드 인프라 부문과 협력하여 2030 년까지 기후 중립 달성
- EU 차원의 일관된 보안 요구 사항 및 기술 표준 촉진
- 데이터 보호 행동 강령을 통해 포괄적인 개인 정보 보호 요구 사항 지원
- EU 클라우드 인프라 시장의 개방성, 경쟁성 유지 및 종속성 방지
- EU 법률 체계 안에서 부당한 콘텐츠 모니터링 의무 저지

CISPE 의 회원은 정부, 공공 기관 및 기업이 자체 시스템을 구축하고, 수십억 시민들에게 필수 서비스를 제공할 수 있도록 지원하는 필수 'IT 구성 요소'를 제공하고 유지 관리합니다. 이러한 역할의 일환으로 인공 지능(AI), 커넥티드 객체, 자율 주행 차량 및 5G 차세대 셀룰러 연결 기술을 접목한 첨단 기술과 서비스를 개발할 수 있도록 돕고 있습니다.

클라우드 인프라 서비스 행동 강령

2016 년 9 월에 공개한 CISPE 데이터 보호 행동 강령은 EU 일반 데이터 보호 규정(GDPR)보다 먼저 시행되었습니다. CISPE 행동 강령은 엄격한 GDPR 요구 사항에 준거합니다. 따라서 클라우드 인프라 제공업체가 데이터 보호 규정을 준수하는 방식으로 사업을 운영하고 고객이 클라우드 제공업체를 선정하고 그 서비스를 신뢰할 수 있도록 돕는 강력한 기본 계약을 제공하는 데 도움이 됩니다. CISPE 행동 강령은 2021 년 5 월에 유럽 데이터 보호 위원회(EDPB)의 인증을 받았으며, 2021 년 6 월에 관할 기관인 프랑스 CNIL 의 승인을 받았습니다. https://www.codeofconduct.cloud/

기후 중립 데이터 센터 협약

CISPE 는 2019 년 말에 유럽 위원회와 협력하여 2030 년까지 데이터 센터의 기후 중립성을 보장하기 위한 일련의 지표와 자율 규제 이니셔티브를 개발했습니다. 이 이니셔티브는 유럽 데이터 센터

협회(EUDCA), 그리고 다른 무역 협회 및 데이터 센터 시장 관계자들과 함께 개발했으며, 2021 년 1 월 '기후 중립 데이터 센터 협약'(https://www.climateneutraldatacentre.net/)으로 출범되었습니다.

공정 소프트웨어 이니셔티브

CISPE 는 유럽 전역의 CIO 와 제공업체가 소속된 다른 동업 조합의 지원 아래 프랑스 CIO 협회인 CIGREF 와 함께 클라우드 고객을 위한 열 가지 공정 소프트웨어 라이선스 원칙을 제정했습니다. 이 원칙은 성장 혁신과 유연성을 위해 클라우드를 모색하고 소프트웨어 제공업체에 공정한 라이선스 계약 조건을 따르도록 요구하는 기업을 위한 일련의 모범 사례입니다.
https://www.fairsoftware.cloud/

GAIA-X

GAIA-X 는 개방적이고 투명하며 안전한 디지털 생태계를 제공하기 위한 유럽 이니셔티브로 22 개 조직이 창립에 참여했는데 CISPE 가 그중 하나입니다. 따라서 CISPE 는 처음부터 GAIA-X 조직의 비전과 원칙에 전념해 왔으며, 사무총장은 2021 년 6 월 재선에 성공해 이사회에서 활동하고 있습니다. CISPE 데이터 보호 행동 강령 및 SWIPO IaaS 행동 강령 등 핸드북에서 참조한 일부 도구는 GAIA-X 원칙 준수를 입증하는 데 유용합니다. https://www.gaia-x.eu

CISPE 와 공공 부문

CISPE 는 유럽 공공 정책 논의에 기여하고 있으며 유럽 클라우드 인프라 산업의 역할, 기여 및 잠재력을 더 잘 이해할 수 있도록 관련 활동을 펼치고 있습니다.

공공 구매 모델에서는 클라우드 컴퓨팅 도입 및 사용 프로세스를 조건화해야 하는데, 클라우드 서비스 도입은 공공 부문이 알고 있는 기존 기술 도입과는 다릅니다. 따라서 구매 접근 방식을 재고해야 합니다. CISPE 는 EU 정책 입안자들이 '클라우드 우선' 정책 이니셔티브를 기반으로 EU 규모에 맞는 보다 야심 차고 미래 지향적인 접근 방식을 개발하도록 장려하여 유럽의 단일 클라우드 인프라 시장의 성장을 견인하고 디지털 단일 시장(DSM) 성장 목표를 뒷받침하고 있습니다.

이 핸드북은 공공 기관이 클라우드 서비스를 구매할 때 유용한 지침과 지원을 제공하기 위해 제작되었습니다.

추가 정보

CISPE 회원: https://cispe.cloud/members
이사회: https://cispe.cloud/board-of-directors
CISPE 행동 강령에 선언된 클라우드 컴퓨팅 서비스:
https://www.codeofconduct.cloud/public-register/

목차

핸드북 요약 및 목적

이 **클라우드 서비스 구매 핸드북**은 경쟁 조달 프로세스 (**클라우드 서비스 제안 요청서- RFP**) 를 통해 클라우드 서비스를 구매하려고 하나 클라우드 사용 기본 계약서 초안을 작성하는 데 필요한 전문 지식이 부족한 클라우드 고객에게 지침을 제공하기 위해 제작되었습니다.

본 문서는 정보 제공의 목적으로만 제공됩니다. 특정 국가 또는 지역의 공공 조달 프로세스의 법적 요건에 맞춰 개발되지 않았습니다.

이 핸드북은 클라우드 사용 기본 계약에 따라 서비스를 구매할 때 **납품 지시** (Call Off) 또는 **소수 경쟁** (Mini Competition) 에 사용할 수 있는 추가적 선택을 위한 기준 문구이기도 합니다. 이 핸드북의 섹션은 일반적인 IT RFP 와 유사하게 구성되어 있습니다. 클라우드 RFP 가 기존의 IT RFP 와 다른 이유를 이해할 수 있도록 일반적 RFP 및 선정 기준 예제가 주석과 함께 제공됩니다.

유럽 단체 및 기관이 클라우드 우선 접근 방식을 통해 어떻게 IT 인프라를 현대화할 수 있는지 그 방법을 안내하는 EU 위원회 클라우드 전략(EU Commission Cloud Strategy) 출간물에 이어 CISPE 는 2019 년 7 월 '**스마트 클라우드 정책을 통해 정부를 혁신하는 방법**' 행사 기간 동안 유럽 위원회에 이 핸드북을 제공했습니다.

이 핸드북의 **버전 2** 에는 데이터 보호(2.3.1.1 섹션), 클라우드 제공업체 전환 및 데이터 이식(2.3.1.2 섹션), 소프트웨어 계약 조건(2.5.2 섹션), 클라우드 내 지속 가능성(3.6 섹션), 라이브 기술 평가(갱신된 부록 B)에 관한 새로운 지침이 포함되어 있습니다.

'**클라우드 서비스**'란 최종 사용자가 이용할 수 있는 모든 클라우드 기술과 관련 서비스를 의미합니다. 클라우드 인프라뿐 아니라 서비스형 소프트웨어(SaaS) 제품을 구매할 수 있는 클라우드 마켓플레이스 서비스, 클라우드 마이그레이션을 지원, 시행하고 클라우드 워크로드를 지원하는 데 필요한 컨설팅, 전문 또는 관리형 서비스도 클라우드 서비스에 해당합니다.

공공 부문 IT 에서 클라우드 컴퓨팅 도입을 고민하기 시작하면서 기존 조달 전략을 현대화해야 할 필요성이 대두되었습니다. 클라우드 서비스 도입 프로세스를 통해 공공 부문 기관은 최첨단 혁신 기술 활용, 속도와 민첩성 증진, 보안 태세 및 규정 준수 거버넌스 강화 등 클라우드의 이점을 완전히 실현할 수 있으며, 효율성과 비용 절감도 달성할 수 있습니다.

하드웨어, 소프트웨어 및 데이터 센터를 구입하는 기존의 IT 조달 방식은 클라우드 서비스 조달 방식으로 적절하지 않습니다. 요금, 계약 거버넌스, 계약 조건, 보안, 기술 요구 사항, SLA 등에 대한 접근 방식은 클라우드 모델에서 모두 달라지며, 기존 조달 방식을 사용하는 경우 궁극적으로 클라우드 제공업체에서 제공하는 이점이 줄어들거나 사라질 수 있습니다.

공공 부문에서 클라우드 서비스를 도입하는 최상의 방법 중 하나는 **클라우드 사용 기본 계약**을 활용하는 것입니다. 클라우드 사용 기본 계약에서는 복수의 조직이 클라우드 메뉴를 수주하므로 구매 조직에 속하는 적격 구매자는 자신의 요구에 맞춰 클라우드 기술과 관련 서비스를 획득할 수 있습니다. 이러한 기본 계약을 클라우드 계약 수단으로 활용하면 효율적이고 효과적인 방식으로 클라우드 서비스를 구매할 수 있으며, 그 결과 구매 조직과 최종 사용자 주체는 클라우드 서비스를 전면적으로 이용하고 궁극적으로 클라우드의 이점을 완전히 누릴 수 있습니다. 즉, 민첩성을 확보하고, 방대한 규모의 경제에 따른 이점을 실현하고, 확장성을 통해 더 적은 비용으로 가용성을 증진하고, 기능성을 확대하고, 혁신을 가속화하고, 새로운 지역으로 확장할 수 있는 역량을 기를 수 있습니다.

이 백서는 **클라우드 인프라 서비스 제공업체 (CISP) 가 제공하는 서비스형 인프라 (IaaS) 및 서비스형 플랫폼 (PaaS) 클라우드 기술의 구매에 초점을 맞추고 있습니다.** 이러한 클라우드 기술은 CISP 에게 직접 구입하거나 CISP 리셀러를 통해 구입할 수 있습니다. 클라우드 마켓플레이스 서비스(PaaS 및 SaaS) 총판과 클라우드 컨설팅 서비스 총판과 관련해서는 추가적인 RFP 고려 사항이 필요합니다.

또한 이 백서에서는 엔드 투 엔드 (end-to-end) 클라우드 조달 프레임워크 구축의 모든 요소를 다루지는 않습니다. 클라우드 조달 모범 사례, 클라우드 예산 수립 방법, 클라우드 거버넌스 등의 문제를 다루는 다른 업계 문서와 애널리스트 문서도 많습니다. 전반적 클라우드 조달 전략을 개발하는 동안 이러한 자문과 문서를 참고하는 것이 좋습니다. 아래 **표 1** 에서 클라우드 서비스 RFP 핸드북의 개요와 클라우드 서비스 RFP 의 각 구성 요소별 RFP 예제의 위치를 확인할 수 있습니다.

표 1 - 클라우드 서비스 RFP 핸드북 섹션 요약

섹션	개요 및 RFP 예제
1.0 클라우드 사용 기본 계약 개요	클라우드 사용 기본 계약 모델에 대한 개요(상세 분류, 경쟁 방식, 계약 체결)
2.0 클라우드 서비스 RFP 개요	아래 섹션과 관련된 일반적 RFP 예제와 클라우드 서비스 RFP 구조 및 사용 언어에 대한 이론적 근거를 설명하는 주석
2.1 클라우드 서비스 RFP 수립	2.1.1 서론 및 전략적 목표 2.1.2 RFP 응답 일정 2.1.3 정의 2.1.4 기본 계약 내 구매 모델과 경쟁 방식에 대한 상세 설명 2.1.5 입찰자 최소 요구 사항 - 관리
2.2 기술	2.2.1 최소 요구 사항 2.2.2 공급업체 간 비교 2.2.3 계약 체결
2.3 보안	2.3.1 최소 요구 사항 2.3.1.1 데이터 보호 2.3.1.2. 클라우드 제공업체 전환 및 데이터 이식 2.3.2. 공급업체 간 비교 2.3.3 계약 체결
2.4 요금	2.4.1 최소 요구 사항 2.4.2 공급업체 간 비교
2.5 계약 이행 설정/계약 조건	2.5.1 계약 조건 2.5.2 소프트웨어 계약 조건 2.5.3 여러 업체 중 계약할 업체를 선택하는 방법 2.5.4. 온보딩 및 오프보딩
3.0 모범 사례/교훈	3.1 클라우드 거버넌스 3.2 클라우드의 예산 수립 3.3 파트너 비즈니스 모델 이해 3.4 클라우드 브로커 3.5 사전 RFP 소싱/시장 조사 3.6 지속 가능성
부록 A – 입찰자 간 비교를 위한 기술 요구 사항	납품 지시 또는 소수 경쟁 관련 일반적 클라우드 기술 요구 사항 목록

섹션	개요 및 RFP 예제
부록 B – 라이브 기술 평가	클라우드 기술 제품 채점 스크립트 예제(납품 지시 또는 소수 경쟁의 일환으로 실시하는 클라우드 데모)

1.0 클라우드 사용 기본 계약 개요

클라우드 사용 기본 계약을 잘 설계하면 계약에 참여하는 공공 부문 조직과 클라우드 공급업체 모두에게 이익이 되는 방향으로 클라우드 서비스 구매를 이끌 수 있습니다. 클라우드 사용 기본 계약을 잘 설계하면 다음과 같은 이점이 있습니다.

- **협력적 특성:**
    - 유사한 요구 사항에 대해 여러 조직이 연합하여 발주하면 편리성, 효율성, 비용 절감 등의 이점이 있을 뿐만 아니라 주문 프로세스도 단순해집니다. 일반적인 클라우드 기술과 관련 클라우드 서비스(마켓플레이스 솔루션, 컨설팅 등)에 대한 여러 공공 부문 조직의 수요를 효과적으로 집계할 수 있습니다.
- **다양한 클라우드 서비스:**
    - CISP 가 제공하는 클라우드 기술, 마켓플레이스 서비스뿐 아니라 클라우드 마이그레이션을 완전히 지원, 시행하고 클라우드 내 워크로드를 지원하는 데 필요한 모든 컨설팅/전문/관리형 서비스도 클라우드 서비스의 한 부분으로 제공받을 수 있습니다.
    - 클라우드 기술은 CISP 에게 직접 구매하거나 지정된 리셀러를 통해 구매할 수 있습니다.
- **계약 거버넌스:**
    - 조직마다 별도의 계약 조건을 이용하거나 계약을 체결하기보다는 공통의 계약 조건을 이용하고 하나의 마스터 계약을 체결할 수 있습니다.
    - 각 공공 부문 조직에 대해 별도의 도입 프로세스, 계약 조건, 발주 메커니즘을 제공하기보다는 표준 도입 프로세스, 계약 조건, 발주 메커니즘을 제공하므로 공급업체에도 이득입니다.
    - 유연성을 제공합니다. 기존의 정부 정책/규제 안에서 클라우드 계약을 효과적으로 작성, 승인, 이행하려면 여러 실험을 거쳐야 하며, 신속하게 조정할 수 있어야 합니다.

기본 계약을 활용하면 공공 부문과 클라우드 공급업체가 협력하여 계약적, 공학적, 효율적 측면에서 계약을 개선할 수 있으므로 기본 계약을 작성하는 것이 훨씬 더 유익합니다. 효과가 없고 조정할 수 없는 다년 계약은 공공 부문 최종 사용자, 조달 조직, 클라우드 공급업체 등 모두에게 부정적입니다.

- **선택:**
  - 구매자는 자격을 갖춘 여러 CISP 중에서 선택할 수 있으며, 모든 클라우드 서비스와 관련 서비스(클라우드 PaaS/SaaS 마켓플레이스, 클라우드 컨설팅 등)에 대한 기준이 높아집니다.
  - 각 수주자를 적정하게 심사할 수 있어 계약에 참여하는 공급자의 수를 제어할 수 있습니다.

클라우드 서비스 구매를 위한 기본 계약이 효과를 발휘하려면 핵심 CISP 제공 IaaS/PaaS 기술과 PaaS/SaaS 마켓플레이스, 공공 부문 최종 사용자가 클라우드에서 실행되는 워크로드를 계획, 이전, 활용, 유지하는 데 도움을 주는 컨설팅 서비스가 계약에 포함되어야 합니다. 따라서 클라우드 사용 기본 계약을 수립하기 위한 클라우드 서비스 RFP 를 작성할 때는 아래와 같이 상세 분류를 세 가지로 구분하는 것이 좋습니다.

- **상세 분류 1 - 클라우드 기술**
  CISP 에게 직접 구매하거나 지정된 CISP 리셀러를 통해 구매하는 클라우드 기술입니다.
- **상세 분류 2 – 마켓플레이스**
  PaaS 및 SaaS 서비스의 마켓플레이스에 액세스합니다.
- **상세 분류 3 - 클라우드 컨설팅**
  클라우드 관련 컨설팅 서비스(교육, 전문 서비스, 관리형 서비스 등)와 기술 지원입니다.

앞서 언급한 바와 같이 이 문서는 CISP 에서 제공하는 IaaS 및 PaaS 클라우드 기술 (**상세 분류 1**)을 구매하는 경우(CISP 에게 직접 구매하거나 CISP 리셀러를 통해 구매하는 경우)에 초점을 맞춥니다. 클라우드 서비스 RFP 의 상세 분류 2 와 상세 분류 3 에 해당하는 공급업체의 경우 별도의 공급업체 자격 요건이 필요할 수 있습니다.

아래의 **그림 1** 은 클라우드 서비스 RFP 를 잘 구조화할 경우, 즉 상세 분류를 세 가지로 구분할 경우 공공 부문 주체가 민첩성, 지출 및 클라우드 사용에 대한 가시성과 제어성을 갖추고, 필요로 하는

솔루션을 구축하고 유지하는 데 필요한 클라우드 서비스를 보유할 수 있도록 하는 클라우드 사용 기본 계약을 만들 수 있습니다.

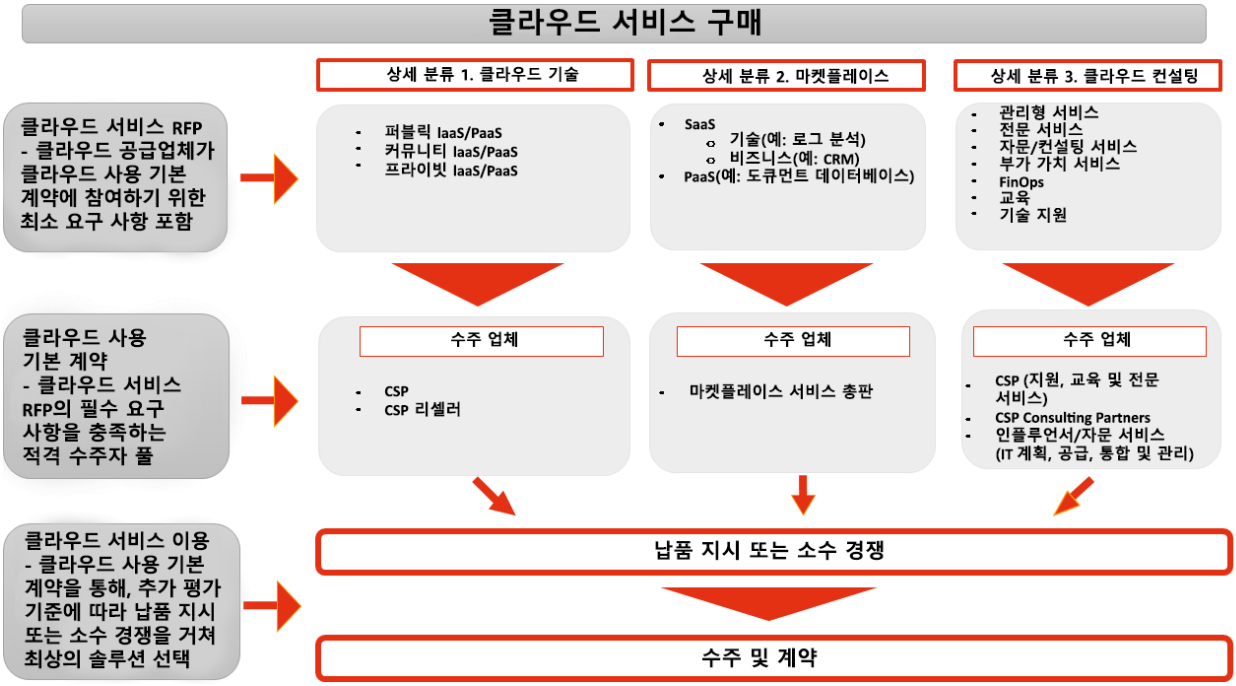

그림 1 - 성공적인 클라우드 서비스 RFP 에서는 상세 분류를 세 가지로 구분합니다. 클라우드 사용 기본 계약에 따라 구매할 때 최종 사용자 요구 사항을 충족하는 기술적, 계약적 적합성을 보장하기 위해 각 상세 분류마다 그 아래에 범주 또는 '오퍼링 유형'을 두고 있습니다.

다음 사항에 유의합니다.

- 각 상세 분류의 수주자는 여럿입니다.
- 상세 분류 3 은 다른 RFP 를 통해 수주하거나 기존 컨설팅 서비스 계약을 통해 수주할 수 있습니다.

상세 분류 1 범주

성공적인 클라우드 사용 기본 계약에서는 CISP 에게 제공 중인 클라우드 모델을 각 상세 분류의 범주대로 구분하여 설명하도록 요청합니다. **퍼블릭** 클라우드, **커뮤니티** 클라우드, **프라이빗** 클라우드에 대한 정의는 클라우드 컴퓨팅 산업 표준[국립표준기술연구소(NIST) 필수 클라우드 특성]을 참조하는 것이 좋습니다. 이러한 방식으로 클라우드 사용 기본 계약을 구성하면 기본 계약을 활용하는 구매 기관과 공공 기관이 다양한 클라우드 모델 중에서 필요에 따라 모델을 선택할 수 있습니다.

상세 분류 1 의 각 클라우드 모델(퍼블릭 IaaS/PaaS, 커뮤니티 IaaS/PaaS, 프라이빗 IaaS/PaaS)에 대한 NIST 의 정의는 2.1.3 정의 **섹션**을 참조하세요.

경쟁 방식 – 납품 지시 또는 소수 경쟁

클라우드 서비스 RFP 의 자격 기준에서는 필수 요소와 최소 기준을 다뤄야 합니다. '있으면 좋은' 기준을 다뤄서는 안 됩니다. 기본 계약의 자격 기준을 충족하는 공급업체에 대해 기준치를 상회하는 추가 기준을 추가할 경우 입찰에 참여하지 못하는 공급업체가 생길 수 있으며, 그로 인해 구매자의 선택의 폭이 좁아질 수 있습니다.

RFP 를 작성하고 클라우드 사용 기본 계약을 수립하면 계약의 적용을 받는 공공 부문 기관은 필요할 때 원하는 클라우드 서비스에 대해 발주를 하거나 '납품 지시'를 내릴 수 있습니다. 기본 계약에 따라 납품 지시 계약을 체결하면 구매자는 기본 계약의 이점은 누리면서 납품 지시 시 기능 사양을 추가하여 요구 사항을 개량할 수 있습니다.

필요하다고 판단될 경우, 특정 워크로드 또는 프로젝트에 가장 적합한 공급자를 선정하기 위해 소수 경쟁을 진행할 수 있습니다. 소수 경쟁은 고객이 기본 계약에 따라 추가 경합을 붙이는 방식으로 상세 분류 안에 있는 모든 공급자를 초청하여 일련의 요구 사항에 응답하도록 합니다. 고객은 상세 분류 안에 있는 모든 가능한 공급자를 입찰에 초청합니다. 따라서 클라우드 서비스 RFP 에서 수주자에 대한 요구 사항을 최소로 설정해야 합니다. 그래야 각 상세 분류에서 선택의 폭이 넓어집니다.

위의 그림 1 에 명시된 각 상세 분류마다 계약과 관련해 **별도의 계약 조건 세트**가 있어야 합니다. 모든 상세 분류의 계약에 대해 '일률적 접근 방식'을 사용하면 기술적 타당성 및 호환성과 관련하여 문제가 발생할 수 있습니다.

2.0 클라우드 서비스 RFP 개요

이 섹션에서는 전략적 목표, 참여자, 정의, 일정, 관리 최소 요구 사항 등 클라우드 서비스 RFP 모델과 범위에 대해 설명합니다. 다시 한번 말하지만, 이 핸드북에서는 **상세 분류 1 - 클라우드 기술**에 초점을 맞춥니다.

2.1 클라우드 서비스 RFP 수립

공공 부문 기관은 클라우드 서비스 RFP 의 서론을 작성할 때 개략적 목표와 요구 사항을 분명하게 명시하는 것이 좋습니다.

2.1.1 서론 및 전략적 목표

전략적 목표를 명확히 하기 위해서는 **(1)** 조직이 클라우드를 사용하여 달성하고자 하는 비즈니스 목표와 이점, **(2)** 기본 계약의 구조(구매 주체, 운영 주체, 예산 수립 주체 등), **(3)** 성공적인 클라우드 구매 및 사용을 위한 핵심 조건인 공공 부문과 클라우드 공급업체 간의 공동 책임 모델에 대한 명확한 이해, **(4)** 클라우드 서비스 제공업체(CISP), 마켓플레이스 서비스의 총판, 컨설팅 파트너, 정부 조달/계약 기관 및 정부 최종 사용자 간에 형성된 관계 유형을 클라우드 서비스 RFP 의 서론에 명시하는 것이 좋습니다. 이러한 네 가지 요점을 명확히 설명하면 고객과 공급업체 모두 RFP 성과물에 대해 명확하게 파악할 수 있을 뿐만 아니라 조직이 자신의 요구를 가장 잘 충족하는 RFP 를 개발할 수 있습니다.

> 클라우드 RFP 는 그 목적부터 기존의 IT RFP 와 다릅니다. 클라우드 기술은 단순히 전통적 컴퓨팅 방식의 대체제가 아닙니다. 클라우드 기술은 기술을 소비하는 방식을 완전히 바꿔 놓았습니다. 클라우드 서비스 RFP 를 잘 설계하면 공공 부문 기관이 클라우드를 신속하게 구매하여 활용하는 데 도움이 됩니다.

클라우드 구매와 관련해서 여러 모범 사례를 언급할 텐데 그중에서 먼저 공동 책임 모델을 명확하게 이해하고 넘어가는 것이 좋습니다. 공동 책임 모델[1]은 클라우드의 보안과 규정 준수에 대해 논의할 때 주로 사용하지만, 클라우드 기술의 모든 요소에 적용됩니다. 클라우드 서비스 RFP 에서는 클라우드 환경에서 CSP 의 소관이 무엇인지와 고객의 책임은 무엇인지를 명확하게 제시해야 합니다. 예를 들어 CISPE 는 클라우드에서 실행되는 리소스와 애플리케이션을 모니터링하는 기능을

[1] **클라우드 인프라 서비스 제공업체를 위한** CISPE **행동 강령** 5 **항 참조**: https://cispe.cloud/website_cispe/wp-content/uploads/2017/06/Code-of-Conduct-27-January-2017-corrected-march-20.pdf

제공합니다. **단**, 이러한 CISP 제공 기능을 실제로 사용하는 데 따르는 책임은 고객에게 있습니다. 방대한 규모로 운영하는 CISP 의 특성상 수백만 고객을 개별적으로 관리하지 않기 때문입니다.

또한 클라우드 고객은 CISP 의 파트너 네트워크가 고객이 클라우드를 활용하고 책임을 관리하는 데 어떻게 도움이 되는지 이해해야 합니다. 예를 들어 클라우드 관리형 서비스 제공업체(MSP)는 고객이 CISP 에서 제공하는 모니터링 기능을 구성하고 사용하여 고유한 규정 준수 및 감사 요구 사항을 충족하도록 지원할 수 있습니다.

간단히 말해 클라우드 모델에서의 책임은 다음과 같습니다.

CISP 는 클라우드 기술 제공

고객은 클라우드 기술 활용

컨설팅 회사(해당하는 경우)는 고객이 클라우드 기술에 액세스하고 활용할 수 있도록 지원

'컨설팅 회사'는 고객이 클라우드를 기반으로 워크로드와 애플리케이션을 설계, 구성, 마이그레이션, 관리하도록 도와주는 컨설팅 및 관리형/전문 서비스 회사입니다. 이러한 회사로는 시스템 통합 사업자, 전략 컨설팅 회사, 대행사, 관리형 서비스 제공업체, 부가 가치 리셀러가 있습니다.

클라우드 서비스 쇼핑은 철물점 쇼핑과 유사합니다. 무언가를 만들고자 할 때 철물점에서 필요한 자재와 공구를 구할 수 있습니다. 캐비닛이나 수영장, 주택 등 원하는 것을 만들 수 있습니다. 자재와 공구를 구매할 때 철물점 직원에게 조언이나 전문 지식을 전해 들을 수는 있지만 철물점 직원이 집을 방문해 대신 만들어 주지는 않습니다. 따라서 몇 가지 방법을 고려할 수 있습니다.

1. 자재와 공구를 직접 구매하고 직접 만듭니다.
2. 자재와 공구는 직접 구매하고 구축 및/또는 운용 작업은 계약을 통해 다른 사람에게 맡깁니다.
3. 계약을 통해 구축/운용 작업을 다른 사람에게 맡기고 자재와 공구 조달도 전체 작업에 포함시킵니다.

클라우드 환경과 솔루션을 직접 구축할 수 있는 자체 기술을 갖춘 조직은 CISP 의 표준 클라우드 기술과 도구를 이용하기만 해도 됩니다(CISP 에게 직접 구매하거나 CISP 리셀러를 통해 구매 - **상세 분류 1** 참조). 필요한 SaaS 및 PaaS 소프트웨어는 클라우드 마켓플레이스를 통해 구매해야

합니다(**상세 분류 2**). 추가적인 컨설팅, 마이그레이션, 구현 및/또는 관리 지원이 필요한 경우 CISP 의 파트너 네트워크에서 해당 서비스를 구매할 수 있습니다(**상세 분류 3**).

RFP 예제: 서론 및 전략적 목표

클라우드 컴퓨팅을 통해 공공 부문 조직은 다양하고 유연하며 경제적인 IT 리소스를 종량제 방식으로 신속하게 이용할 수 있습니다. 새롭고 기발한 아이디어를 구현하거나 IT 부서를 운영하는 데 필요한 적정 유형 및 규모의 리소스를 프로비저닝할 수 있습니다. 하드웨어에 대규모 투자를 하거나 장기 소프트웨어 라이선스 계약을 맺지 않아도 됩니다.

<고객>은 다양한 제휴 조직의 비즈니스 요구를 충족하기 위해 이러한 유형의 상용 클라우드 기술을 이용할 필요가 있습니다.

본 RFP 의 주요 목적은 각기 다른 클라우드 기술과 클라우드 관련 서비스를 대표하는 최대 **<x>**곳의 제공업체와 포괄적인 **<기본 계약>**을 체결하는 것입니다.

1. **상세 분류 1.** 클라우드 기술 구매를 위한 클라우드 서비스 제공업체(CISP) 또는 CISP 리셀러
2. **상세 분류 2.** 마켓플레이스 서비스 제공업체
3. **상세 분류 3.** CISP 오퍼링으로 마이그레이션하고 CISP 오퍼링을 활용할 수 있도록 추가적인 전문 지식을 제공하는 컨설팅 서비스 제공업체

상세 분류 1 과 관련하여, 입찰 조직(CISP 또는 CISP 리셀러)은 오퍼링이 다음과 같은 목표를 어떻게 충족하는지 입증해야 합니다.

- **민첩성 –** 기존의 주 단위나 월 단위가 아닌 몇 분 만에 최종 사용자에게 IT 리소스를 제공합니다.
- **혁신 –** 시장에 출시된 가장 혁신적인 최신 기술을 즉시 이용할 수 있습니다.
- **비용 –** 자본 비용을 가변 비용으로 전환합니다(예: CapEx 를 OpEx 로 전환). 사용하는 만큼만 비용을 지불합니다.
- **예산 수립 –** 청구 정보와 사용량 정보를 세부적, 개략적으로 모두 확인할 수 있습니다. 시간 경과에 따른 지출 패턴을 시각화하고 향후 지출을 예측할 수 있습니다.
- **탄력성 –** 클라우드의 방대한 규모의 경제를 통해 가변 비용을 절감할 수 있습니다.
- **용량 –** 인프라 용량이 얼마나 필요할지 추측할 필요가 없습니다.
- **데이터 센터에 대한 의존 중단** – 랙 설치, 스택 구성, 전원 공급 등 서버와 관련된 과중한 업무에서 벗어나 시민들에게 집중할 수 있습니다.

- **보안 –** 리소스에 대한 우수한 가시성과 감사 용이성을 통해 형식에 맞게 계정을 설계하여 시설과 물리적 하드웨어를 보호하는 데 들어가는 비용을 없앱니다.
- **공동 책임 –** 호스트 운영 체제, 가상화 계층부터 서비스가 운영되는 시설의 물리적 보안에 이르기까지 CISP 가 구성 요소를 운영, 관리, 제어함으로써 운영 부담을 덜어 줍니다.
- **자동화 –** 클라우드 아키텍처에 자동화를 내장하여 더 신속하고 경제적이며 안전하게 확장할 수 있도록 그 능력을 개선합니다.
- **클라우드 거버넌스 –** (1) 모든 IT 자산을 조사하여 목록화하고 (2) 이러한 모든 자산을 중앙에서 관리하고 (3) 사용량/청구/보안 등에 대한 알림을 생성합니다. 그와 동시에 자산 추적, 자산 목록 관리, 변경 관리, 로그 관리 및 분석, 전체적인 가시성 및 클라우드 거버넌스 기능도 제공합니다.
- **제어 –** IT 서비스를 어떻게 소비하는지, 보안, 신뢰성, 성능, 비용을 개선하기 위해 어떤 부분을 조정해야 하는지를 전면적으로 확인할 수 있습니다.
- **가역성 –** CISP 인프라 안팎으로의 마이그레이션을 지원하고 공급업체 종속을 최소화하며 업계 행동 강령을 준수할 수 있도록 이식성 도구 및 서비스를 제공합니다.
- **데이터 보호 –** 클라우드 인프라 서비스 전용 산업 행동 강령인 CISPE 데이터 보호 행동 강령을 통해 일반 데이터 보호 규정(GDPR)의 준수 사실을 입증할 수 있습니다.
- **투명성** – 고객은 자신의 데이터를 처리하고 저장하는 데 사용되는 인프라의 위치를 알 권리가 갖습니다(도시 지역).
- **기후 중립** – 고객은 2030 년까지 기후 중립을 달성하기 위해 입증되고 구체적인 조치를 취하고 있으며 기후 중립 데이터 센터 협약에 서명한 CISP 와 계약을 체결해야 합니다. 이러한 CISP 와 계약을 체결하면 고객이 자체적인 기후 중립 목표를 달성하는 데 도움이 됩니다.

2.1.2 RFP 응답 일정

클라우드 사용 기본 계약과 관련 클라우드 서비스 RFP 를 작성할 때는 입찰자에게 예상 입찰 활동의 일정을 알려주는 것이 좋습니다. 업계와의 연계가 활발할수록 일정을 알리는 것이 좋습니다. 모든 당사자가 RFP 요구 사항을 명확하게 파악하고 실제로 모든 공급업체 서비스가 어떻게 클라우드 서비스 모델에 적합한지 이해하는 데 도움이 되기 때문입니다.

RFP 일정은 현지 법률과 법적 의무의 적용을 받습니다. 아래의 목록은 활동 및 일정에 대한 규범적 목록이 아닌 모범 사례 가이드로 작성되었습니다.

RFP 예제: 응답 일정

클라우드 서비스 RFP 에 관해서는 아래의 RFP 일정을 참조하세요.

클라우드 서비스 RFP 일정
• 정보 요청서(RFI) 발행: • RFI 응답: • 제안 요청서(RFP) 초안 발행: • RFP 응답 초안 기한: • 산업 컨설팅 단계: <일정> • 사전 검증 RFP 발행: • 사전 검증 RFP 응답: • RFP 발행: • 1 차 질문 기한: • 1 차 답변: • 2 차 질문 기한: • 2 차 답변: • RFP 응답 기한: • 제안서 내용 설명 기간: • 협상 기간: • 업체 결정 예정 날짜: • 계약 체결: • 계약 기간(연장 옵션):

RFP 일정은 현지 법률과 법적 의무의 적용을 받습니다. 아래의 목록은 활동 및 일정에 대한 규범적 목록이 아닌 모범 사례 가이드로 작성되었습니다.

2.1.3 정의

클라우드 서비스 RFP 에는 상세한 정의 목록이 있어야 합니다. 정의 목록에는 공급업체 역할(예: 클라우드 서비스 제공업체, 클라우드 리셀러, 공급업체 파트너), 일반 기술 개념(컴퓨팅, 스토리지, IaaS/PaaS, SaaS)을 비롯해 계약 관련 주요 사항이 담겨 있어야 합니다. 다음은 정의 목록 예제입니다.

RFP 예제: 정의

아래의 정의는 국립표준기술연구소(NIST)에서 정한 클라우드 컴퓨팅의 정의입니다.[2]

[2] https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf

- **서비스형 인프라(IaaS).** 소비자는 운영 체제, 애플리케이션 등 임의의 소프트웨어를 배포하고 실행할 수 있는 기본 컴퓨팅 리소스(예: 처리, 스토리지, 네트워크 등)를 프로비저닝할 수 있습니다. 소비자는 네트워크, 서버, 운영 체제, 스토리지 또는 개별 애플리케이션 등의 기반 클라우드 인프라를 관리하거나 제어하지 않습니다. 단, 운영 체제, 스토리지, 배포된 애플리케이션은 소비자가 제어하며, 일부 네트워킹 구성 요소(예: 호스트 방화벽)도 소비자가 제한적으로 제어하는 경우가 있을 수 있습니다.

- **서비스형 플랫폼(PaaS).** 소비자는 제공업체에서 지원하는 프로그래밍 언어, 라이브러리, 서비스, 도구를 사용하여 생성한 소비자 생성형 또는 획득형 애플리케이션을 클라우드 인프라에 배포할 수 있습니다. 소비자는 네트워크, 서버, 운영 체제, 스토리지 또는 개별 애플리케이션 등의 기반 클라우드 인프라를 관리하거나 제어하지 않습니다. 단, 배포된 애플리케이션은 소비자가 제어하며, 애플리케이션 호스팅 환경의 구성 설정도 소비자가 제어하는 경우가 있을 수 있습니다.

- **서비스형 소프트웨어(SaaS).** 소비자는 클라우드 인프라에서 실행되는 제공업체의 애플리케이션을 사용할 수 있습니다. 웹 브라우저(예: 웹 기반 이메일)와 같은 경량 클라이언트 인터페이스나 프로그램 인터페이스를 통해 다양한 클라이언트 디바이스에서 애플리케이션에 액세스할 수 있습니다. 소비자는 네트워크, 서버, 운영 체제, 스토리지 또는 개별 애플리케이션 등의 기반 클라우드 인프라를 관리하거나 제어하지 않습니다. 단, 사용자가 구성을 설정해야 하는 예외적 경우가 있을 수 있습니다.

- **퍼블릭 클라우드.** 일반 대중이 공개적으로 사용할 수 있도록 클라우드 인프라를 프로비저닝합니다. 기업, 학계, 정부 기관 또는 이들 연합이 클라우드 인프라를 소유, 관리, 운영합니다. 클라우드 제공업체의 시설 내에 존재합니다.

- **커뮤니티 클라우드.** 공통의 관심사(예: 미션, 보안 요구 사항, 정책, 규정 준수 고려 사항)를 가진 조직의 특정 소비자 커뮤니티가 독점적으로 사용할 수 있도록 클라우드 인프라를 프로비저닝합니다. 커뮤니티에 속한 하나 이상의 조직, 서드 파티 또는 이들 연합이 클라우드 인프라를 소유, 관리, 운영하며, 클라우드 인프라는 온프레미스나 오프프레미스 방식으로 존재합니다.

- **하이브리드 클라우드.** 두 가지 이상의 서로 다른 클라우드 인프라(프라이빗, 커뮤니티 또는 퍼블릭)를 조합하여 클라우드 인프라를 구성합니다. 각각의 클라우드 인프라를 고유하게 유지하면서도 데이터 이식과 애플리케이션 이식을 지원하는 표준 또는 독점 기술(예: 클라우드 간 로드 밸런싱을 위한 클라우드 버스팅)을 통해 결합됩니다.

- **프라이빗 클라우드.** 다수의 소비자로 구성된 단일 조직(예: 사업부)이 독점적으로 사용할 수 있도록 클라우드 인프라를 프로비저닝합니다. 단일 조직, 서드 파티 또는 이들 연합이 클라우드 인프라를 소유, 관리, 운영하며, 클라우드 인프라는 온프레미스나 오프프레미스 방식으로 존재합니다.

2.1.4 기본 계약 내 구매 모델과 경쟁 방식에 대한 상세 설명

위에서 언급했듯이 공공 부문 조직은 기본 계약이 따르는 클라우드 기술, 관련 구현 및 관리 서비스의 구매 절차에 대해 파악해야 합니다. 그리고 클라우드 기술 공급업체, 관련 컨설팅 서비스 조직, 마켓플레이스 총판, 구매 조직이 각자의 역할을 파악할 수 있도록 클라우드 서비스 RFP 에 이를 명시해야 합니다.

기본 계약의 범위, 납품 지시 또는 소수 경쟁과 관련하여 조직은 다음을 고려해야 합니다.

- 계약에 따르면 클라우드 기술과 관련된 통합 서비스와 관리형 서비스 제공을 책임지는 주체는 누구입니까?
- CISP 리셀러/파트너에 대한 요구 사항에 CISP 와의 계약 관계 유지, 통합 청구 서비스 제공, 클라우드 제공업체 서비스 사용과 관련된 사용량 및 청구 데이터에 대한 적시 및 직접 액세스 가능 이외에 부가 가치 서비스 제공도 있습니까?
- 서비스 부가 가치 리셀러, 시스템 통합 사업자, 관리형 서비스 제공업체 또는 모든 형태의 IT 용역 서비스에 대한 요구 사항이 있습니까?

CISP 는 시스템 통합 사업자(SI) 또는 관리형 서비스 제공업체(MSP)가 아니라는 점에 유의해야 합니다. 많은 공공 부문 고객이 IaaS/PaaS 를 활용하기 위해 CISP 를 필요로 하고 있으며, 컨설팅과 '실천형' 계획 수립, 마이그레이션, 관리 업무는 SI 나 MSP 에 아웃소싱합니다. 클라우드 서비스 모델의 역할과 책임에 대한 설명은 아래 **그림 2** 에서 확인할 수 있습니다.

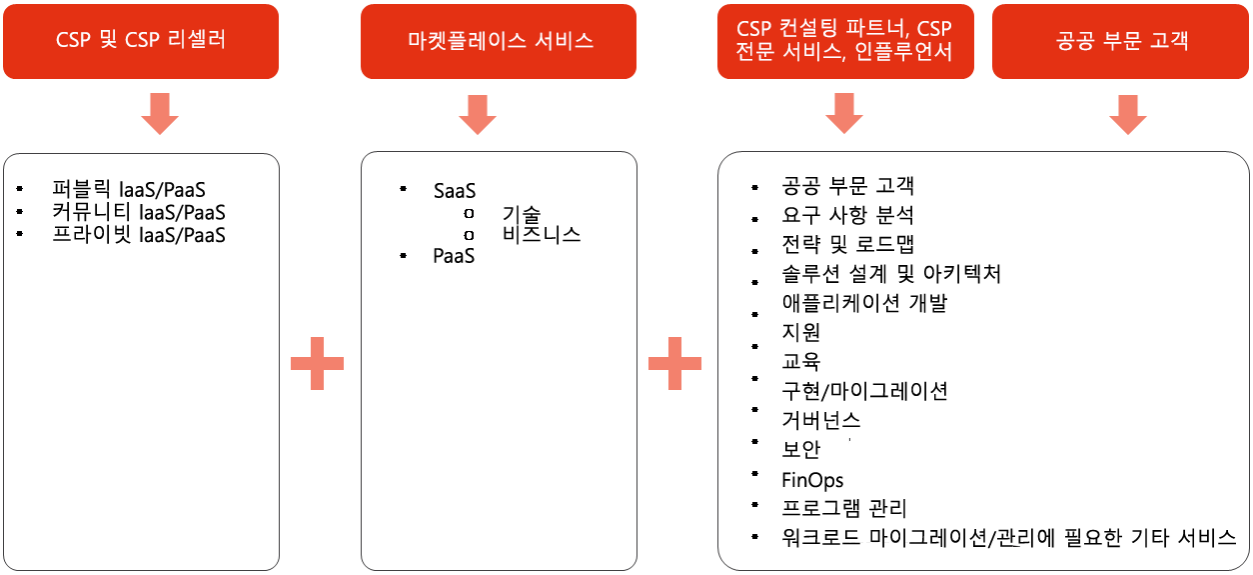

그림 2 – 클라우드 서비스 RFP 는 최종 사용자가 필요로 하는 모든 클라우드 서비스의 메뉴를 제시해야 합니다. 클라우드 기술을 활용하려는 공공 부문 고객은 CISP 를 필요로 합니다. PaaS 제품과 SaaS 제품을 활용하려는 공공 부문 고객의 경우에는 마켓플레이스를 필요로 하기도 합니다. 이들 고객은 클라우드 서비스를 제공하는 데에 자신들이 얼마나 큰 역할을 맡을지 컨설팅 회사/시스템 통합 업체/관리형 서비스 제공업체 등에 얼마나 아웃소싱할 계획인지를 결정할 수 있습니다.

아래의 예제는 위의 그림 2 에 명시된 역할과 책임에 따라 작성되었습니다. 클라우드 사용 기본 계약과 관련 클라우드 서비스 RFP 는 구매자가 각 공급업체의 오퍼링을 적절하게 평가할 수 있도록 보장해야 합니다. 그래야 워크로드/프로젝트에 필요한 서비스를 선정하고 선택할 수 있습니다. 가장 좋은 방법은 앞서 논의한 대로 서비스를 세 가지 상세 분류로 구분하고 기본 계약하에서 납품 지시와 소수 경쟁이 어떻게 실시되는지를 명시하는 것입니다.

RFP 예제: 구매 모델

이 계약은 **기본** 구매 수단으로 사용됩니다. 본 클라우드 사용 기본 계약에서는 클라우드 기술, 관련 마켓플레이스 서비스/제품, 컨설팅 서비스, 전문 서비스/시스템 통합/관리형 서비스/마이그레이션 전문 서비스에 대한 여러 **상세 분류**와 교육 및 지원을 다루며, **<고객>**과 관련이 있는 복수의 적격 구매자가 본 기본 계약을 이용합니다. 이때 상세 분류와 교육 및 지원에 대한 정의는 **<고객>**의 정의를 따릅니다. 이렇게 하면 조달 프로세스를 단순화하는 동시에 규모의 경제를 최적화할 수 있습니다.

기본 계약이 체결되면 조직은 원하는 클라우드 기술과 클라우드 관련 서비스를 필요할 때 구매할 수 있습니다. 별도의 조달을 통해 구매하지 않아도 됩니다. 이러한 접근 방식은 관리 요구 사항을 줄이고 조달 복잡성과 주기 시간을 크게 줄입니다.

기본 계약의 기간은 갱신 기간을 모두 포함해 최대 <X>년입니다. 기본 계약하에서 납품 지시 계약의 최대 기간은 일반적으로 **<x>**개월입니다. 계약 연장에 필요한 경우 적절한 내부 승인을 통해 이 기간을 **<x>**개월 연장하고 다시 **<x>**개월 더 연장할 수 있습니다. 이는 개별 **납품 지시**마다 명시됩니다.

기본 계약은 **세 가지 상세 분류**로 구분됩니다.

1. **상세 분류 1: 클라우드 기술** – 전 범위의 클라우드 제공업체 기술(CISP 가 직접 제공하는 기술, 리셀러가 제공하는 기술, 부가 가치 서비스/지원을 보유한 리셀러가 제공하는 기술).
    i. **IaaS 및 PaaS 서비스** – 클라우드 기술 메뉴[예: 컴퓨팅, 스토리지, 네트워킹, 데이터베이스, 분석, 애플리케이션 서비스, 배포, 관리, 개발자, 사물 인터넷(IoT) 등]. DR/COOP, 아카이브, 빅 데이터 및 분석, DevOps 등의 패키지 클라우드 기술 솔루션을 포함합니다.
2. **상세 분류 2: 마켓플레이스** – 회계, CRM, 디자인, HR, GIS 및 매핑, HPC, BI, 콘텐츠 관리, 로그 분석 등 전 범위의 PaaS 및 SaaS 서비스/제품.
3. **상세 분류 3: 클라우드 컨설팅** – 클라우드 마이그레이션 및 사용과 관련한 포괄적인 컨설팅 서비스(관리형 서비스, 전문 서비스, 자문/컨설팅 서비스, 부가 가치 서비스, FinOps, 기술 지원). 이러한 서비스에는 계획, 설계, 마이그레이션, 관리, 지원, QA, 보안, 교육 등이 포함됩니다.

공급업체는 여러 상세 분류에 오퍼링을 제출할 수 있습니다.

공급업체는 오퍼링과 관련 요금을 임의의 형식으로 제출합니다.

기본 계약 내 경쟁 및 계약 체결

납품 지시

본 기본 계약의 적용을 받는 공공 부문 기관은 필요할 때 원하는 클라우드 서비스에 대해 발주를 하거나 '납품 지시'를 내릴 수 있습니다. 기본 계약에 따라 납품 지시 계약을 체결하면 구매자는 기본 계약의 이점은 누리면서 납품 지시 시 기능 사양을 추가하여 요구 사항을 개량할 수 있습니다.

기본 계약을 통해 체결한 계약에서는 각 상세 분류 내에서 공급자를 선택하는 데 사용되는 요구 사항에 대해 명확한 감사 로그를 제공할 수 있습니다. 최종 구매자는 조기 시장 연계, 내용 증명 질문, 이메일, 대면 대화 등 공급업체와의 커뮤니케이션 기록을 보관해야 합니다.

1. 납품 지시 요구 사항 작성 및 구매에 대한 내부 승인 요구

기본 계약을 이용할 자격이 있는 모든 최종 사용자는 비즈니스 최종 사용자, 구매 전문가, 기술 전문가로 구성된 연합 팀을 조직하여 '필수 항목'과 '선호 항목' 목록을 준비합니다. 이러한 요구 사항은 적합한 상세 분류와 요구 사항을 충족하는 최적의 공급업체를 결정하는 데 도움이 됩니다. 요구 사항 초안을 작성할 때 구매자는 다음을 고려합니다.

- 서비스 이용에 사용할 수 있는 자금
- 프로젝트의 기술 및 조달 요구 사항
- 선택 기준

2. 서비스 검색

기본 계약하에서 구매자는 온라인 카탈로그(기본 계약 적격 수주자 목록과 서비스 목록을 제공하는 포털)을 이용하여 요구에 부합하는 제품/서비스를 찾습니다. 적합한 상세 분류를 선택한 후 서비스를 검색합니다.

3. 서비스 검토 및 평가

기본 계약하에서 구매자는 서비스 설명을 검토하여 요구 사항과 예산 모두를 가장 잘 충족하는 서비스를 찾습니다. 각 서비스 설명에는 다음이 포함됩니다.

- 서비스 정의 문서 또는 서비스 정의 링크
- 계약 조건 문서
- 요금 문서(전체 가격 목록/요금 문서가 요청 시 제공된다는 전제하에 공개 요금 문서 링크 허용)

가격은 가장 일반적인 구성의 서비스에 대한 비용입니다. 반면에 요금은 일반적으로 볼륨을 기반으로 합니다. 따라서 구매자는 항상 공급자의 요금 문서나 공공 요금을 참조하고, 요금 계산기 도구를 사용해 구매할 제품/서비스의 실제 가격을 계산하고, 구매자에게 제공되는 전반적 가치(예: 최적화 서비스를 통한 비용 절감 효과)를 파악해야 합니다.

기본 계약하에서 구매자는 공급자에게 서비스 설명, 계약 조건, 요금 또는 서비스 정의 문서/모델에 대해 설명해 줄 것을 요청해야 될 수 있습니다. 공급자와의 대화 기록은 보관됩니다.

4. 서비스 선택 및 계약 체결

단일 공급업체

한 곳의 공급업체만 요구 사항을 충족하는 경우 해당 공급업체와 계약을 체결할 수 있습니다.

복수의 공급업체

최종 후보 목록에 든 서비스가 여러 개인 경우, 구매자는 '경제적으로 가장 유리한 입찰'에 기반하여 서비스를 선택하게 됩니다. 경제적으로 가장 유리한 입찰 기반 평가는 다음 표의 기준을 참조하세요. 구매자는 어떤 세부 특성을 사용할지, 그리고 그 특성에 어떻게 가중치를 부여할지 결정할 수 있습니다.

구매자는 다음을 수행해야 할 수 있습니다.

- 여러 공급자를 조합하여 검토
- 볼륨 또는 엔터프라이즈 할인과 공급업체 비용 최적화 서비스에 대한 구체적인 정보 확보

공급자에 대한 평가는 항상 공정하고 투명해야 합니다. 최적의 적합성에 따라 선택하며, 프로젝트 요구 사항을 참조하지 않은 채 공급업체/서비스를 배제하지 않습니다.

표 2 - 경제적으로 가장 유리한 입찰 기반 평가

수주 기준
전체 수명 비용: 비용 효율성, 가격 및 운영 비용
기술적 장점과 기능적 적합성: 관련 서비스 수준에 지정된 커버리지, 네트워크 용량 및 성능
사후 서비스 관리: 헬프데스크, 문서, 계정 관리 기능 및 다양한 서비스 제공 보장
비기능적 특성

소수 경쟁

필요하다고 판단될 경우, 특정 워크로드 또는 프로젝트에 가장 적합한 공급자를 선정하기 위해 소수 경쟁을 진행할 수 있습니다. 소수 경쟁은 고객이 기본 계약에 따라 추가 경합을 붙이는 방식으로 상세 분류 안에 있는 모든 공급자를 초청하여 일련의 요구 사항에 응답하도록 합니다. 고객은 상세 분류 안에 있는 모든 가능한 공급자를 입찰에 초대합니다. 기술, 보안 및 요금/가격에 관한 내용은 아래 섹션의 추가 비교 정보를 참조하세요.

계약

구매자와 공급업체는 모두 서비스를 사용하기 전에 계약서 사본에 서명합니다. 기본 계약의 최대 기간은 일반적으로 **<x>**개월입니다. 계약 연장에 필요한 경우 적절한 내부 승인을 통해 이 기간을 **<x>**개월 연장하고 다시 **<x>**개월 더 연장할 수 있습니다.

서비스를 사용하기 전에 모든 이해관계자(구매자 및 공급자)가 계약서 사본에 서명해야 합니다.

2.1.5 입찰자 최소 요구 사항 - 관리

명료한 문구를 사용하여 기본 계약 자격 기준을 수립하면 전통적 솔루션을 '클라우드'로 포장하는 전통적 데이터 센터 또는 하드웨어 제공업체의 제안서 제출을 방지하는 데 도움이 됩니다. RFP 참여 업체는 아래의 최소 입찰자 관리 요구 사항을 어떻게 충족하는지 제시해야 합니다.

다시 한번 말하지만, 이 백서는 **상세 분류 1 - 클라우드 기술**에 초점을 맞추고 있습니다. 단, 요구 사항과 RFP 범위의 관점에서 전반적 맥락을 제공해야 하는 경우를 위해 상세 분류 2 - 마켓플레이스, 상세 분류 3 - 클라우드 컨설팅에 대한 정보도 추가했습니다. 예를 들어 CISP 리셀러/MSP/SI/컨설팅 회사 등에 대한 최소 자격 기준을 포함시켜야 합니다. 이는 해당 업체가 (1) 리셀러 또는 채널 파트너로서 CISP 와 직접 제휴를 맺고 있는지, (2) CISP 오퍼링에 대한 직접 액세스를 서드 파티 주체에게 재판매하는 데에 대해 CISP 의 공인을 받았는지 그리고 (3) 역량과 전문 지식에 대해 CISP 로부터 인증을 취득했는지 확인하는 데 도움이 됩니다.

RFP 예제: 입찰자 최소 요구 사항 - 관리

본 기본 계약에서는 다음 범주에서 복수의 공급업체에 계약을 수여합니다. 공급업체는 상용 CISP, CISP 의 서드 파티 리셀러, 마켓플레이스 서비스 총판 및/또는 CISP 활용을 위한 서비스 제공업체(예: 컨설팅, 마이그레이션 서비스, FinOps 등)여야 합니다. 어떤 역할로 입찰하는지 표시하세요.

상세 분류 1

____ - 퍼블릭 클라우드 서비스(IaaS 및 PaaS)의 직접 제공업체(CISP)

____ - 커뮤니티 클라우드 서비스(IaaS 및 PaaS)의 직접 제공업체(CISP)

____ - 프라이빗 클라우드 서비스(IaaS 및 PaaS)의 직접 제공업체(CISP)

____ - CISP 서드 파티 리셀러(CISP 온라인 클라우드 오퍼링에 대한 직접 액세스 제공 가능)

- 서비스에 대한 직접 액세스를 재판매할 수 있는 CISP 오퍼링 명시: _____
- 해당 오퍼링의 공인 리셀러임을 증명하는 CISP 의 서신 제공: _____

상세 분류 2

____ - CISP 에서 실행되는 마켓플레이스 서비스(PaaS 및/또는 SaaS)의 직접 제공업체

____ - CISP 에서 실행되는 마켓플레이스 서비스(PaaS 및/또는 SaaS)의 총판

상세 분류 3

____ - 전문 서비스를 제공하는 CISP

____ - CISP 기술 지원 제공업체

____- CISP 를 활용하거나 CISP 상에서 운영할 수 있도록 서비스를 제공하는 CISP 파트너

____- CISP 를 활용하거나 CISP 상에서 운영할 수 있도록 서비스를 제공하는 인플루언서/자문가

오퍼링 유형 명시:

- CISP 상의 워크로드를 위한 관리형 서비스(예/아니요): _____
  - 전문성 명시(해당하는 경우): _____
- 전문 서비스: (예/아니요): _____
- 컨설팅 – 교육(예/아니요): _____
- 컨설팅 – 전략(예/아니요): _____
- 컨설팅 – 마이그레이션(예/아니요): _____
- 컨설팅 – 클라우드 거버넌스(예/아니요): _____
- 컨설팅 – FinOps(예/아니요): _____
- 컨설팅 – 기타(구체적으로 명시): _____

어떤 CISP 에 대해 서비스를 제공하는지 명시: _____
해당 CISP 모델에 대해 파트너로 지정받았음을 보여주는 CISP 서신 제공: _____

상세 분류 1 최소 관리 요구 사항

클라우드 서비스 제공업체(CISP)
CISP 자격을 취득하려면 다음 요구 사항을 준수해야 합니다.

CISP 자격 기준 제안 사항	이유
조직 세부 정보(예: 이름, 법적 구조, 등록/DUNS 번호, VAT 등).	
회사 규모, 경제 및 재무 상태[3].	고객이 CISP 의 계약 이행 가능 여부를 판단할 수 있습니다.

[3] 클라우드 서비스 RFP 에서는 직원 수, 내부 직원의 팀 구성 등이 아닌 전반적인 회사 정보에 주목합니다. 클라우드 기술의 경우 서비스 성능과 직원 수 간에 상관 관계가 없습니다. 대신 클라우드 RFP 에서는 요구 사항(적절한 규모)을 충족하기 위한 전반적인 회사 규모와 입증된 경험/성과에 주목합니다.

제외 사유(예: 범죄/사기 행위 등).	
사례 연구/고객 레퍼런스(필수 개수/유형 명시).	고객이 필요한 서비스를 제공하는 데 있어 CISP 의 경험을 산정할 수 있습니다.
기업의 사회적 책임.	CISP 가 수행하는 사회적 책임 중 대중에게 공개된 사회적 책임이어야 합니다.
대중에게 공개된 지속 가능성 약속 및 사례.	고객이 CISP 가 최대한 친환경적인 방식으로 비즈니스를 운영하는 데 전념하고 있음을 알 수 있습니다.
지난 5 년간 혁신을 실현하고 유용한 신규 서비스와 기능을 출시했음을 입증하는 실적을 제공해야 합니다. 특히, PAAS, 기계 학습, 분석, 빅 데이터, 관리형 서비스, 클라우드 사용 최적화 기능과 관련된 실적을 제공해야 합니다. 대중에게 공개된 변경 기록이나 업데이트 피드를 사용하여 실적을 입증할 수 있습니다.	CISP 가 신규 제품을 빠르게 출시하고, 제품에 대해 신속하게 반복 과정을 시행하여 제품을 개선하고 있음을 보여줍니다. 이는 고객이 자본 재편성 투자 없이 최첨단 IT 인프라를 유지하는 데 도움이 됩니다.

CISP와 리셀러/파트너 간 관계

<고객>은 주계약자에 대해 리셀러 또는 채널 파트너로서 CISP 와 직접 제휴를 맺고, CISP 오퍼링에 대한 직접 액세스를 서드 파티 주체에게 재판매하는 데에 대해 CISP 의 공인을 받으며, 역량과 전문 지식에 대해 CISP 로부터 인증을 취득할 것을 요구합니다. 이렇게 하면 **<고객>**은 **기본 계약** 주계약자와 CISP 간에 하도급 계약이라고 하는 추가 계층과 관련된 계약 조건과 서비스를 검토하지 않아도 됩니다. 또한 (1) **<고객>**이 제공되는 서비스와 관련하여 책임 소재를 명확하게 하기 위해 실사를 수행하는 경우 그리고 (2) **<고객>**이 클라우드 서비스 소비를 비롯해 일상적 활동을 수행하는 경우에 리셀러라는 추가 계층으로 인해 발생하는 복잡성이 사라집니다.

2.2 기술

클라우드 서비스 RFP 에서는 고객이 맞춤형 솔루션을 구축하는 데 필요한 표준 클라우드 기술을 제공하도록 요구함으로써 CISP 에 대한 기준을 높여야 합니다. 앞서 언급한 바와 같이 표준 기술과 맞춤형 기술 간 차이는 클라우드 서비스 RFP 에 착수할 때 매우 중요합니다. CISP 는 수백만 고객에게 표준 서비스를 제공하므로 클라우드 서비스 RFP 에서 맞춤화를 논할 때는 솔루션 성과를 달성하는 데 사용되는 클라우드 서비스를 어떤 기반 기법, 인프라, 하드웨어를 사용해 제공하는지보다는 더 높은 가치를 창출하는 솔루션과 성과에 초점을 맞춥니다.

2.2.1 최소 요구 사항

기존의 IT 조달은 조직의 비즈니스 수행 방식을 문서화하는 일련의 작업 세션을 통해 개발한 비즈니스 요구 사항을 기반으로 합니다. 최상의 상황에서도 이들 요구 사항을 완벽하게 도출하는 것은 어려운 과정입니다. 성공한다 하더라도 요구 사항 세션에서 문서화하는 비즈니스 프로세스는 과거의 프로세스에 기반을 두고 있으므로 그 자체로 시대에 뒤떨어지고 비효율적일 수 있습니다. 이러한 요구 사항을 RFP 에 포함해 CISP 에 대해 그대로 사용할 경우 맞춤형 솔루션이 유일한 솔루션이 될 수 있습니다. 이러한 모델은 클라우드 조달에는 적합하지 않습니다.

공공 부문 조직은 자신의 비즈니스 목표와 성능 요구를 파악해야 하지만 시스템 설계와 기능성을 강제하는 바 RFP 에서 규범적으로 다뤄서는 안 됩니다. 대신, 조직은 최상의 비즈니스 적합성을 기준으로 구매해야 합니다. 조직은 성공적인 서비스를 이끌어내지 못할 수 있는 수백 또는 수천 개의 규범적 요구 사항을 바탕으로 제안서를 평가하기보다는 기술과 관련 서비스가 비즈니스 목표를 얼마나 잘 충족하고 강화하는지, 성능 요구를 달성할 수 있는지, 구성을 통해 비즈니스 규칙을 미세 조정할 수 있는지를 바탕으로 평가 기준을 마련해야 합니다.

최상의 솔루션을 얻으려면 클라우드 RFP 에서 질문을 제대로 해야 합니다. 클라우드 모델에서는 물리적 자산을 구입하지 않기 때문에 기존의 데이터 센터 조달 요구 사항 다수가 적용되지 않습니다. **데이터 센터 관련 질문을 재활용하면 필연적으로 데이터 센터 관련 답변으로 이어질 것이며**, 이로 인해 CISP 가 입찰을 할 수 없게 되거나 부적절한 계약으로 이어져서 공공 부문 고객이 클라우드의 모든 기능과 이점을 이끌어내는 데 방해가 될 수 있습니다.

클라우드 서비스 RFP 에서는 CISP 와 클라우드 서비스에 적합한 주요 요구 사항에 초점을 두며, 상세 분류 1 에 대해 자격을 갖춘 공급업체가 높은 기준을 충족할 수 있도록 보장합니다. 또한 요구 사항이 지나치게 규범적이면 안 됩니다. 요구 사항이 지나치게 규범적이면 공공 부문이 다양한 적격 CISP 를 활용할 수 없게 됩니다.

RFP 예제: 클라우드 제공업체 역량

상세 분류 1 에 관해서는 위의 최소 CISP 관리 요구 사항도 참조하세요.

CISP 자격 기준 제안 사항	이유
인프라	
CISP 인프라는 최소 2 개의 데이터 센터 클러스터를 제공해야 합니다. 각 클러스터는 최소 2 개의 데이터 센터로 구성되어야 하며 저지연 링크로 연결되어야 합니다. 그래야 고가용성 액티브-액티브 배포와 DR-BC 시나리오 구현이 가능합니다. 각 클러스터를 구성하는 데이터 센터는 물리적으로 격리되어 있고 서로의 장애로부터 영향을 받지 않아야 합니다.	CISP 는 단일 장애 지점을 피할 수 있는 고가용성 애플리케이션을 구축하는 데 적합한 인프라를 제공할 수 있어야 합니다.
CISP 는 논리적이고 지리적으로 격리된 리전을 제공해야 합니다. CISP 가 고객 데이터를 해당 리전 외부에 복제해서는 안 됩니다.	데이터 레지던시 요구 사항에서는 고객이 데이터 위치를 완전히 제어할 수 있도록 권한을 부여할 것을 지시합니다.
CISP 는 CISP 데이터 센터 간에 직접, 전용, 프라이빗 연결을 제공할 수 있어야 합니다.	프라이빗 연결은 하이브리드 보안 인프라를 구축하기 위한 기본적인 요구 사항입니다.
CISP 는 전송 중 데이터 암호화를 비롯해 충분한 메커니즘을 제공해야 합니다.	고객은 데이터를 비암호화 상태로 전송할 수 없게 하는 기능을 요구할 수 있습니다.
최소 CISP 인증	
CISP 는 ISO 27001 인증을 받아야 합니다.	서드 파티 감사, 인증, 인정을 통해 고객은 서비스(특히 플랫폼)를 벤치마킹하여 품질, 안전 및 신뢰성을 확보할 수 있습니다. 최소 인증 요구 사항을 반드시 충족해야 합니다.
고객이 GDPR 준수 애플리케이션을 구축할 수 있도록, GDPR 을 준수하면서 사용할 수 있는 기능과 서비스를 제공하려면 CISP 는 CISPE 데이터 보호 행동 강령을 준수해야 합니다.	고객은 GDPR 을 준수하면서 애플리케이션을 구축하거나 실행할 수 있어야 합니다.
CISP 는 SOC 1 및 2 보고서(EC 가 사용하는 위치와 서비스 포함)와 같은 서드 파티 감사 보고서를 제공하여 CISP 통제 항목과 절차에 대한 투명성을 보장해야 합니다.	CISP 는 애플리케이션의 작동 및 관리 방법을 투명하게 공개해야 합니다. 신뢰와 투명성을 보장하는 데 중요한 역할을 하는 SOC 보고서.
기후 중립 데이터 센터 협약을 준수해야 하는 CISP.	기후 중립 데이터 센터 협약은 CISP 가 2030 년까지 기후 중립을 달성하여 사용자가 독자적인 지속 가능성 목표를 실현할 수 있게 합니다. FTE(비 SME)가 250 을 초과하는 제공업체의 경우 서드 파티 감사 필수.

CISP 는 SWIPO IaaS 이식성 행동 강령을 준수해야 함.	SWIPO IaaS 이식성 행동 강령은 서비스가 비개인 데이터의 국경 간 이동(Free Flow of non-personal Data) 규정의 제 6 조 '데이터 이식'의 요구 사항을 충족할 수 있도록 보장합니다.
서비스 특성	
CISP 인프라는 프로그래밍 인터페이스(API) 와 웹 기반 관리 콘솔을 통해 액세스할 수 있어야 합니다.	셀프서비스 액세스와 프로그래밍 인터페이스는 CISP 제공업체의 필수 표준으로, 사용자 액세스와 제공업체 간의 중개를 가능한 한 배제합니다.
CISP 는 다음을 비롯한 일련의 서비스를 제공해야 합니다. 객체 스토리지, 관리형 관계형 데이터베이스, 관리형 비관계형 데이터베이스, 관리형 로드 밸런서, 모니터링 및 통합형 오토 스케일링 기능을 제공합니다.	가상 머신을 제공한다고 해서 제공업체를 클라우드 제공업체로 분류할 수는 없습니다. 클라우드 제공업체는 고객의 애플리케이션을 가속화하고 개선하기 위해 일련의 PAAS 및 IAAS 서비스를 제공해야 합니다.
CISP 는 고객이 서비스 사용량과 구성을 자유롭게 변경하거나 CISP(셀프서비스 오퍼링) 안팎으로 데이터를 이동할 수 있도록 허용해야 합니다.	서비스 및 데이터에 대한 셀프서비스 액세스는 고객의 독립성을 완전히 보장하는 엄격한 요구 사항입니다.
CISP 는 서비스 과금 방식으로 '종량제'를 허용해야 합니다.	종량제 방식을 통해 고객은 워크로드의 비용을 최적화하고, 리스크를 최소화하며, 수명이 짧은 애플리케이션 및 PoC 에 CISP 를 활용할 수 있습니다.
데이터 및 시스템 보안	
CISP 는 고객이 데이터를 완전히 제어할 수 있도록 허용해야 하며, 고객이 데이터를 저장할 위치(도시 지역)를 자유롭게 선택할 수 있도록 해야 하고, 고객이 직접 데이터를 이동하지 않는 한 어떠한 고객 데이터도 이동되지 않도록 보장해야 합니다.	고객은 데이터가 저장되는 위치, 콘텐츠에 대한 액세스 관리 방법, 서비스 및 리소스에 대한 사용자 액세스를 제어할 수 있어야 합니다.
CISP 의 특성상 고객은 고객 데이터와 시스템의 기밀성, 무결성, 가용성을 비롯해 보안 정책을 완전히 제어할 수 있어야 합니다.	고객은 워크로드 전반에 걸쳐 보안 표준을 정의하고 구현할 수 있어야 합니다. 제공업체가 고객의 데이터를 '올바르게 처리할 것'이라고 신뢰하는 것만으로는 충분하지 않습니다.
비용 관리	
CISP 는 고객이 시간 경과에 따른 지출을 모니터링할 수 있도록 메커니즘과 도구를 제공해야 합니다. 워크로드, 서비스, 계에 따라 비용을 기본적으로 세분화할 수 있는 도구여야 합니다.	

CISP 는 비용 한도를 초과할 때마다 고객에게 알리는 도구를 제공해야 합니다.	
CISP 는 고객에게 자세한 청구서를 보내야 합니다. 워크로드, 환경, 계정에 따라 비용을 세분화하여 청구서를 구성할 수 있어야 합니다.	

또한 CISP 는 아래의 기술 요구 사항 질문에 대한 답변을 제공해야 합니다.

솔루션

CISP 는 다음 솔루션에 대해 CISP 에서 호스팅되거나 CISP 에 통합되어 있는 사전 구축 템플릿과 소프트웨어 솔루션을 제공하는 방법을 시연해야 합니다.

- 스토리지
- DevOps
- 보안/규정 준수
- 빅 데이터/분석
- 비즈니스 애플리케이션
- 통신 및 네트워킹
- 지리 공간
- IoT
- [기타]

CISP 가 다음 워크로드에 어떻게 사용되었는지 설명하는 개요를 기입하세요.

- 재해 복구
- 개발 및 테스트
- 아카이브
- 백업 및 복구
- 빅 데이터
- 고성능 컴퓨팅(HPC)
- 사물 인터넷(IoT)
- 웹 사이트
- 서버리스 컴퓨팅
- DevOps
- 콘텐츠 전송
- [기타]

2.2.2 공급업체 간 비교

클라우드 서비스 RFP 의 최소 요구 사항 외에도 경쟁 평가 시 CISP 기술을 비교할 수 있는 기준을 제공하는 것이 중요합니다.

클라우드 서비스 RFP 에서는 솔루션 구축을 위해 고객이 사용하는 기능을 이해하고 기업이 필요로 하는 클라우드 기능을 요구해야 합니다. CISP 가 표준적으로 제공하는 기능을 능가하는 기능(CISP 의 사전 구축 솔루션 또는 자동화 기능 등)을 이용하면 클라우드 서비스 RFP 의 '부가 가치 옵션' 또는 '최상의 가치'를 더욱 유의미하게 분석할 수 있습니다.

공공 부문에서는 최상의 가치, 경제적으로 가장 유리한 입찰, 최저 가격 등의 평가 기준을 이용해 입찰자 간에 경쟁을 붙이는 경우가 많습니다. 공공 부문 기관이 클라우드 서비스 RFP 의 이 부분을 계획할 때 클라우드 고유의 기능을 고려한 접근 방식을 확립하는 것이 중요합니다. 예를 들어 단순히 클라우드 제공업체의 오퍼링(예: 컴퓨팅 또는 스토리지) 간에 품목을 비교하는 방식으로는 오퍼링을 효과적으로 비교할 수 없습니다. 그보다는 위의 2.2.1 섹션에 나열된 솔루션과 같은 상위 수준의 솔루션에 중점을 두는 것이 좋습니다. 그러면 공공 부문 기관은부록 A – 입찰자 간 비교를 위한 기술 요구 사항에 나열된 것과 같은 클라우드 고유의 요구 사항에 주목할 수 있습니다.

RFP 에는 클라우드 솔루션을 구축하는 데 필요한 필수 클라우드 특성을 명시해야 합니다. 이를 위해 공공 부문 조직은 국립표준기술연구소(NIST) 필수 클라우드 특성을 활용할 수 있을 뿐만 아니라, 서드 파티 분석가의 보고서를 활용하여 CISP 가 대규모로 운영되는 최적의 '진정한 클라우드' 오퍼링을 보유하고 있는지 확인할 수 있습니다.

RFP 예제 – 공급업체 간 비교

CISP 는 **부록 A** 의 모든 기술 요구 사항 관련 질문에 답변을 제공해야 합니다.

응답자는 다음과 같은 특성을 가지고 있어야 하며 클라우드 서비스 오퍼가 클라우드 컴퓨팅의 다섯 가지 필수 특성을 어떻게 충족하는지 설명해야 합니다[4].

1) **온디맨드 셀프서비스:** 응답자는 서버 시간, 네트워크 스토리지 등의 컴퓨팅 기능을 일방적으로 프로비저닝할 수 있는 역량을 제시해야 합니다. 각 서비스 제공업체와 인적으로 상호 작용할 필요 없이 필요할 때 자동으로 프로비저닝할 수 있어야 합니다. 응답자는 발주 활동과 관련하여 일방적으로(즉, 공급업체 검토 또는 승인 없이) 서비스를 프로비저닝할 수 있는 역량을 제시해야 합니다. 자사의 오퍼링 또는 본인이 제시하는 오퍼에서 이 특성을 어떤 방식으로 충족하는지 설명하세요.

[4] http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf

2) **유비쿼터스 네트워크 액세스:** 응답자는 복수의 네트워크 연결 옵션을 제시해야 하며, 그중 하나는 인터넷 기반이어야 합니다. 자사의 오퍼링 또는 본인이 제시하는 오퍼에서 이 특성을 어떤 방식으로 충족하는지 설명하세요.

3) **리소스 풀링:** 응답자의 CISP 는 멀티 테넌트 모델을 통해 여러 소비자에게 풀링된 컴퓨팅 리소스를 제공해야 하며, 소비자의 수요에 따라 서로 다른 가상 리소스를 동적으로 할당하고 재할당해야 합니다. 사용자는 더 높은 추상화 수준(예: 국가, 지역 또는 데이터 센터 위치)에서 위치를 지정할 수 있습니다. 응답자는 프로비저닝 요청을 받은 후 몇 분 또는 몇 시간 안에 리소스 확장을 지원해야 합니다. 자사의 오퍼링 또는 본인이 제시하는 오퍼에서 이 특성을 어떤 방식으로 충족하는지 설명하세요.

4) **신속한 탄력성:** 응답자의 CISP 는 서비스 프로비저닝 기능과 디프로비저닝 기능(스케일 업 및 다운)을 지원해야 하며, 프로비저닝 요청을 받은 후 정해진 최소 시간(최대 'x'시간) 안에 서비스를 사용할 수 있도록 준비해야 합니다. 응답자는 프로비저닝 요청에 따라 청구를 시간 단위나 일 단위로 매일 조정할 수 있도록 지원해야 합니다.

5) **서비스 측정:** 응답자는 온라인 대시보드 또는 유사한 전자 수단을 통해 서비스 사용에 대한 가시성을 제공해야 합니다.

또한 CISP 는 다음 요구 사항을 충족해야 합니다.

- Gartner 의 IaaS 부문 매직 쿼드런트를 통해 클라우드 서비스 제공에 있어 리더로 인정받았습니다.[5]
- CISP 의 검증된 역량과 신뢰성을 보여주는 업계 공인 서드 파티 분석 보고서를 제공합니다.

마지막으로, CISP 를 비교할 때는 부록 B 에 제시된 시나리오가 사용됩니다.

2.2.2.1 서비스 수준 계약(SLA)

CISP 는 수백만 고객에게 표준화된 상용 SLA 를 제공합니다. 따라서 온프레미스 데이터 센터 모델에서와 같이 맞춤형 SLA 를 제공할 수 없습니다. 대신에 CISP 고객(주로 CISP 파트너의 지원을 받는 고객)은 CISP 의 상용 SLA 를 활용해 클라우드 사용을 설계하여 고객 특유의 요구 사항과 고유의 SLA 를 충족하거나 초과 충족할 수 있습니다.

개별 최종 사용자가 성능 및 가용성 요구 사항을 충족할 수 있도록, 서비스와 상용 SLA 를 활용하는 데 필요한 기능과 지침을 CISP 가 제공하는지 클라우드 서비스 RFP 에서 확인해야 합니다.

[5] https://www.gartner.com/doc/reprints?id=1-2G2O5FC&ct=150519&st=sb

RFP 예제: 서비스 수준 계약

서비스 수준 계약(SLA)에 대한 CISP 의 접근 방식과 관련하여 정보와 링크를 제공하세요.

<고객>은 CISP 에 대해 지속적으로 주시하고 SLA 를 충족하는 않는 상황에서도 계속 작동하도록 중요 워크로드와 애플리케이션을 배포합니다.

<고객>은 **<고객>**이 소유한 장비나 CISP 를 사용해 **<고객>**이 운영하는 서비스와 관련된 SLA 를 적절하게 유지할 책임이 있습니다.

CISP 는 운용 중인 SLA 의 성능을 지속적으로 확인하고 보고할 수 있는 기능과 CISP 인프라를 활용해 성능, 내구성, 신뢰성을 갖춘 서비스를 설계하는 방법을 안내하는 문서화된 모범 사례를 **<고객>**에 제공해야 합니다.

2.2.3 계약 체결

CISP 계약 조건은 클라우드 서비스 모델의 운영 방식(물리적 자산을 구매하지 않으며 CISP 가 표준화된 서비스를 제공하는 환경을 대규모로 운영하는 방식)을 반영하도록 고안되었으므로 CISP 계약 조건을 최대한 반영하고 활용하는 것이 중요합니다. 계약 조건 및 계약 체결에 대한 자세한 내용은 아래의 2.5 섹션을 참조하세요.

2.2.3.1 신규 서비스와 변경 서비스

CISP 는 서비스를 통해 성능을 제공합니다. 유효 기간이 있는 서비스 유지 보수 계약과 업그레이드를 필요로 하는 기존 온프레미스 솔루션과 달리 클라우드 제공업체는 표준화된 서비스를 제공할 뿐입니다. 규모의 경제를 실현하는 클라우드 모델의 경우 기반 인프라에 대한 업그레이드와 변경은 개별 사용자가 아닌 모든 사용자에 대해 전개되므로 고객은 사용할 서비스를 고르고 선택하면 됩니다. 서비스는 과거의 온프레미스 시스템보다 더 원활하며, 클라우드 제공업체가 지속적으로 신규 서비스와 향상된 서비스를 지속적으로 추가하므로 고객은 원하는 대로 사용할 수 있습니다.

RFP 제출 기한 이후에 신규 또는 향상된 CISP 서비스를 추가할 수 없는 경우 공공 부문 조직은 기본 계약의 후속 버전이 발행될 때까지 신규 서비스와 향상된 기능을 활용하지 못합니다. 따라서 제출 기한 이후에 신규 CISP 서비스를 추가할 수 있도록 기본 계약에서 서비스 제공을 광범위하게 서술할 것을 강력히 권장합니다. 기본 계약에 추가할 서비스가 완전히 다른 신규 서비스일 경우 EU 조달법에 따라 도입이 제한될 수 있지만 주요 변경 사항으로 간주되지 않는 업데이트나 신규 버전 서비스는 조달상의 문제없이 추가할 수 있습니다.

RFP 예제: 신규 서비스와 변경 서비스

CISP 는 검증되고 안정적인 가상화 기술과 지속적으로 업데이트되는 최첨단 기술을 모두 활용하는 비용 효율적인 솔루션을 제공해야 합니다. **<고객>**은 클라우드 기술이 **<고객>**과 CISP 의 다른 고객에게 공통 코드 기반 및/또는 공통 환경에서 공동 서비스 기반으로 제공된다는 것을 알고 있으며 이에 동의합니다. CISP 는 때때로 기능, 성능 또는 클라우드 서비스의 다른 특성을 변경, 추가하거나 삭제할 수 있습니다. 변경, 추가, 삭제를 실시하는 경우 그에 따라 클라우드 서비스의 사양이 변경됩니다.

본 납품 주문서의 범위에는 기본 계약의 범위 내에 있는 모든 기존 CISP 서비스와 신규 또는 향상된 CISP 서비스가 포함됩니다. 상용 고객에게 제공되는 CISP 제공 클라우드 서비스를 **<고객>**에게 제공해야 합니다.

2.2.3.2 공급업체 종속/가역성

클라우드 기술의 경우 물리적 자산을 구매하지 않으므로 공급업체 종속이 줄어들며, 고객은 언제든지 클라우드 제공업체 간에 데이터를 이동할 수 있습니다.

그렇다고 하더라도 클라우드 서비스를 구입할 때 어느 정도의 공급업체 종속은 피할 수 없습니다. 모든 클라우드가 동일하지는 않기 때문입니다. 즉, 다른 CISP 에서는 제공하지 못하는 서비스와 기능을 제공하는 CISP 가 있을 수 있기 때문입니다. 따라서 다른 제공업체에서 제공하는 서비스를 사용하지 못하게 될 수 있습니다. 신중한 접근 방식은 클라우드 사용을 종료하는 데 필요한 기능과 서비스를 CISP 가 제공하도록 하는 것입니다. 이때 이들 서비스를 합리적인 '종료 전략'으로 어떻게 사용할 수 있는지도 문서화하여 제공하게 합니다. CISP 는 표준화된 서비스를 고객이 어떤 식으로 구성하여 사용하는지 알 수 없으며 따라서 맞춤형 종료 계획도 제공할 수 없기 때문입니다.

EU '비개인 데이터의 국경 간 이동 규정' 제 6 조'의 요구 사항을 충족하기 위해 '데이터 이식'과 '클라우드 제공업체 전환'을 다루고 있는 산업 행동 강령에 대한 내용은 2.3.1.2 섹션을 참조하세요.

RFP 예제: 온보딩 및 오프보딩

<고객>은 종속을 방지하기 위한 합리적인 종료 전략을 제시하는 제안서를 원합니다. **<고객>**은 물리적 자산을 구입하지 않으며, CISP 는 IT 스택을 위아래로 이동할 수 있는 기능을 제공합니다. CISP 는 이식성 도구 및 서비스를 제공하여 CISP 플랫폼 안팎으로의 마이그레이션을 지원하고 종속을 최소화합니다. CISP 가 제공하는 이식성 도구 및 서비스를 사용하는 방법에 대한 상세 문서는 합리적인 종료 계획으로 사용됩니다.

CISP 는 최소 약정 또는 장기 계약을 **요구**해서는 안됩니다.

서비스 제공업체에 저장된 데이터는 고객이 언제든지 내보낼 수 있습니다. CISP 는 **<고객>**이 필요에 따라 CISP 스토리지 안팎으로 데이터를 이동할 수 있도록 허용해야 합니다. 또한 CISP 는 가상 머신 이미지를 다운로드하여 새 클라우드 제공업체로 이식할 수 있도록 허용해야 합니다. **<고객>**은 머신 이미지를 내보내 온프레미스나 다른 제공업체에서 사용할 수 있습니다(소프트웨어 라이선스 제한이 적용됨).

2.3 보안

보안과 규정 준수 책임은 CISP 와 클라우드 고객의 공동 책임입니다. 공동 책임 모델에서 고객은 인프라에 있는 애플리케이션과 데이터를 설계하고 보호할 방법을 제어합니다. 한편, CISP 에게는 고도의 안전성과 제어성을 갖춘 플랫폼에서 서비스를 제공하고 다양한 추가 보안 기능을 제공할 책임이 있습니다. 공동 책임 모델에서 CISP 와 고객의 책임 수준은 클라우드 배포 모델(IaaS/PaaS/SaaS)에 따라 다르며, 고객은 각 배포 모델에서 어떤 책임을 맡는지 명확히 해야 합니다.

이러한 공동 책임 모델을 이해하는 것은 성공적인 클라우드 서비스 RFP 를 고안하는 데 매우 중요합니다. 공공 부문 조직은 CISP 의 책임과 조직 자신의 책임에 대해 알고 있어야 하며, 컨설팅/ISV 파트너와 솔루션이 어디에 도움이 되는지 알아야 합니다.

2.3.1 최소 요구 사항

클라우드 보안과 관련된 키워드는 **기능**입니다. 공공 부문 조직은 CISP 에 까다롭게 요구해야 하며, CISP 는 고객이 공동 책임 모델에서 책임을 다할 수 있도록 보장하는 데 필요한 보안 기능을 제공해야 합니다. 아래의 대표적인 요구 사항 목록에서 볼 수 있듯이, CISP 는 고객이 이를 활용하여 고유한 클라우드 환경을 안전하게 만들 수 있도록 표준화된 기능을 제공해야 합니다.

- 네트워크 방화벽과 웹 애플리케이션 방화벽 **기능**을 **제공**하여 개인 네트워크를 생성하고 인스턴스 및 애플리케이션에 대한 액세스를 제어합니다.
- 사무실 또는 온프레미스 환경에서 프라이빗 또는 전용 연결을 사용할 수 있는 연결 **옵션**을 **제공**합니다.
- 심층 방어 전략을 구현하고 DDoS 공격을 차단할 수 있는 **기능**을 **제공**합니다.
- 스토리지 및 데이터베이스 서비스에서 사용할 수 있는 데이터 암호화 **기능**을 **제공**합니다.
- 유연한 키 관리 **옵션**을 **제공**하여 CISP 가 암호화 키를 관리할지 선택하도록 하거나 고객이 직접 키를 완벽하게 제어할 수 있도록 합니다.
- 고객이 암호화와 데이터 보호를 CISP 환경에서 개발하거나 배포한 서비스와 통합할 수 있도록 **API** 를 **제공**합니다.
- 조직의 표준에 따라 CISP 리소스의 생성 및 폐기를 관리할 수 있는 배포 **도구**를 **제공**합니다.
- CISP 리소스를 파악한 후 시간 경과에 따른 리소스 변경 사항을 추적하고 관리할 수 있는 인벤토리 및 구성 관리 **도구**를 **제공**합니다.
- 고객이 CISP 환경에서 어떤 일이 일어나고 있는지 정확하게 확인할 수 있는 **도구와 기능**을 **제공**합니다.
- 호출 주체, 대상, 시기, 위치를 비롯한 API 호출에 대한 심층적인 **가시성**을 **지원**합니다.
- 조사 및 규정 준수 보고를 간소화할 수 있는 로그 집계 **옵션**을 **제공**합니다.

- 특정 이벤트가 발생하거나 임계값을 초과할 경우에 알리는 경보 알림을 구성하는 기능을 제공합니다.
- CISP 서비스의 사용자 액세스 정책을 정의, 실시, 관리할 수 있는 **기능**을 **제공**합니다.
- CISP 리소스 전반에서 권한이 부여된 개별 사용자 계정을 정의할 수 있는 **기능**을 **제공**합니다.
- 관리 간접비를 줄이고 최종 사용자 경험을 개선할 수 있도록 기업 디렉터리와 통합 및 연동되는 **기능**을 **제공**합니다.

자세한 요구 사항은 부록 A – 입찰자 간 비교를 위한 기술 요구 사항을 참조하세요.

최소 보안 표준을 능가하는 기능을 이용하면 RFP 의 '부가 가치 옵션' 또는 '최상의 가치'를 더욱 유의미하게 분석할 수 있습니다. 또한 보안과 관련하여 기본 제공되거나 자동화된 기능이 많을수록 더 좋습니다. 입찰자 비교 요구 사항은부록 A – 입찰자 간 비교를 위한 기술 요구 사항을 참조하세요.

공공 부문 조직의 경우 CISP 보안 통제 항목을 제대로 이행하고 있음을 보장하려면 클라우드 인증, 인정, 평가를 활용하는 것이 좋습니다. 예를 들어 ISO 27001 인증 표준에 준거한다는 사실을 보여주려면 독립적 감사 기관의 검증 및 인증을 받은 CISP 를 검토하는 것이 좋습니다. ISO 27001 부록 A 의 14 항에서는 시스템 획득, 개발, 유지 보수에 관한 ISO 요구 사항에 따라 CISP 가 준수하는 구체적 통제 항목에 대해 다루고 있습니다. 이러한 통제 항목은 최소한 IT 관련 RFP 에서 조직이 일반적으로 요구하는 시스템 획득, 개발, 유지 보수에 관한 통제 항목 대부분을 포괄한다고 볼 수 있습니다. 따라서 조직이 시스템 획득, 개발, 유지 보수와 관련하여 중복 활동을 펼치고 클라우드 RFP 에 통제 요구 사항을 나열하기보다는 CISP 에 ISO 27001 인증을 획득하도록 요구하는 것이 합리적입니다.

서드 파티 규정 준수 보고서를 활용하는 이러한 접근 방식은 CISPE GDPR 행동 강령, ISO, SOC 등 대부분의 보안 및 규정 준수 통제 항목에 적용할 수 있습니다.

RFP 예제: 보안

CISP 는 자사의 비독점 보안 프로세스와 기술적 한계를 **<고객>**에 공개하여 **<고객>**과 서비스 제공업체 간에 적절한 보호와 유연성을 확보할 수 있도록 해야 합니다.

CISP 는 보안 및 규정 준수와 관련하여 역할과 책임을 다음과 같이 명시해야 합니다.

- 제안된 오퍼링에 대해 CISP 와 **<고객>**의 보안 관련 역할과 책임을 설명합니다. 책임에 대해 명확하게 설명하고 **<고객>**이 클라우드 환경에서 보안 기능을 구축하고 자동화하는 데 도움이 되는 CISP 서비스의 개요를 서술합니다.
- **<고객>**의 보안 요구 사항과 관련하여 **부록 A** 의 기술 사양에 대한 답변을 제공합니다.

<고객> 콘텐츠의 소유권 및 통제권

CISP 기능이 **<고객>**의 데이터 프라이버시를 어떻게 보호할 수 있는지 설명합니다. **<고객>**의 콘텐츠를 보호하기 위한 적절한 통제 수단을 기입합니다. CISP 는 리전을 엄격하게 격리하여 **<고객>**이 명시적으로 다른 리전으로 객체를 전송하지 않는 한 리전에 저장된 객체가 해당 리전을 벗어나지 않도록 해야 합니다.

- **<고객>**은 콘텐츠, 서비스 및 리소스에 대한 액세스를 관리합니다. CISP 는 **<고객>**이 액세스, 암호화, 로깅 작업을 효율적으로 수행할 수 있도록 향상된 기능을 제공해야 합니다. CISP 는 **<고객>**의 콘텐츠에 액세스하거나 고객 콘텐츠를 사용하지 않습니다. 단, CISP 서비스를 유지 관리하고 **<고객>**과 조직의 최종 사용자에게 서비스를 제공하기 위해 법적으로 요구되는 경우는 예외로 합니다.
- **<고객>**이 콘텐츠를 저장할 리전을 선택합니다. CISP 는 CISP 서비스를 유지 관리하고 **<고객>**과 조직의 최종 사용자에게 제공하기 위해 부득이하게 요구되는 경우를 제외하고, 선택한 리전 외부로 **<고객>**의 콘텐츠를 이동하거나 복제하지 않습니다.
- **<고객>**이 콘텐츠 보호 방법을 선택합니다. CISP 는 전송 중이거나 저장된 **<고객>**의 콘텐츠에 대해 강력한 암호화를 제공해야 하며, **<고객>**이 자체 암호화 키를 관리할 수 있는 옵션을 제공해야 합니다.
- CISP 는글로벌 개인 정보 보호 및 데이터 모범 사례를 활용하는 보안 보증 프로그램을 갖추고 있어야 합니다. **<고객>**은 이 프로그램을 통해 CISP 의 보안 제어 환경을 구축, 운영, 활용할 수 있습니다. 보안 보호 조치와 제어 프로세스는 여러 서드 파티의 독자적인 평가를 통해 독립적으로 검증된 것이어야 합니다.

클라우드 인정 인증과 평가를 통해 공공 부문 조직은 CISP 가 효과적인 물리적 및 논리적 보안 통제 수단을 갖추고 있다는 확신을 가질 수 있습니다. RFP 에서 이러한 인정을 활용하면 조달 프로세스를 간소화하고 클라우드 환경에 필요하지 않을 수 있는 중복되고 지나치게 부담이 큰 프로세스 또는 승인 워크플로를 피할 수 있습니다.

클라우드 RFP 에서는 CISP 가 규정 준수 인증과 평가에 준거하고 있음을 입증할 수 있도록 그 기회를 제공해야 합니다. 위에서 언급한 바와 같이, 위험 시나리오와 위험 관리 방식은 인정 체계 전반에서 상당 부분 중복되어 있습니다. 통제 항목과 요구 사항은 이들 인정에서 함께 묶여 제공되므로 RFP 에서 규정 준수를 다루는 데 있어 개별 통제 항목(**대부분 온프레미스 데이터 센터에 맞춘 이전 RFP 에서 가져온 것이므로 클라우드 컴퓨팅에는 적용되지 않을 수 있음**)을 중복하여 나열하는 것보다 CISP 가 인증을 준수하도록 요구하는 것이 더 빠른 방법입니다

참고: 아래에 나열된 보고서에 액세스할 수 있는 방법을 이해하는 것도 매우 중요합니다. 예를 들어 SOC 1 및 SOC 2 보고서는 일반적으로 중요한 문서입니다. 이러한 문서에 액세스하는 데 필요한

계약(예: 기밀 유지 계약 – NDA)을 파악하고 RFP 응답의 일환으로 해당 문서를 제출하도록 요청하지 마세요(이러한 문서는 정보 공개에 관한 법률이나 클라우드 보안을 저해하는 유사 법률을 통해 공개될 수 있음).

RFP 예제: 규정 준수

데이터 처리, 데이터 보안, 기밀성, 가용성 등 클라우드 서비스 운영 모범 사례에서 도출된 공신력 있는 보안, 규정 준수 및 운영 표준을 활용하면 클라우드 기술 조달을 간소화할 수 있습니다.

<고객>은 아래 및 **부록 A** 에 설명된 대로 승인된 보안, 규정 준수 및 운영 표준을 기준으로 고유한 제안 오퍼링을 평가합니다. 각 표준의 규정 준수와 관련해 공급업체가 획득한 인증에 의존함으로써 **<고객>**은 표준을 충족하는 최소 규정 준수를 제안서 평가의 기준으로 사용할 수 있습니다.

CISP 가 계약 기간 동안 최소 표준을 계속 준수하도록 요구하는 것으로 서비스 규정 준수를 최신 상태로 유지할 수 있는 이점이 있습니다.

직접 또는 리셀러를 통해 입찰 중인 CISP 는 다음과 같은 독립적인 서드 파티 증명, 보고서 및 인증을 획득할 수 있음을 입증할 수 있어야 합니다(참고 – 이러한 증명, 보고서 및 인증 중 일부가 보안 문제로 인해 공개 제한 대상이 되는 경우, **<고객>**은 CISP 와 협력하여 양측의 합의하에 액세스 권한을 획득해야 함).

인증/증명	**법, 규정 및 개인 정보 보호**	**조율/프레임워크**
☐ C5(독일)		☐ CDSA
☐ CISPE 데이터 보호 행동 강령(GDPR)		
☐ CNDCP(기후 중립 데이터 센터 협약)		
☐ DIACAP	☐ EU 데이터 보호 지침	☐ CIS
☐ DoD SRG 레벨 2 및 4	☐ EU 모델 조항	☐ 형사 사법 정보국(CJIS)
☐ HDS(프랑스, 의료)		
☐ FedRAMP	☐ FERPA	☐ CSA
☐ FIPS 140-2	☐ GDPR	☐ EU-US 프라이버시 실드
☐ ISO 9001	☐ GLBA	☐ EU 세이프 하버
☐ ISO 27001	☐ HIPAA	☐ FISC

☐ ISO 27017	☐ HITECH	☐ FISMA
☐ ISO 27018	☐ IRS 1075	☐ G-Cloud(영국)
☐ IRAP(호주)	☐ ITAR	☐ GxP(FDA CFR 21 Part 11)
☐ MTCS 티어 3(싱가포르)	☐ PDPA – 2010(말레이시아)	☐ ICREA
☐ PCI DSS 레벨 1	☐ PDPA – 2012(싱가포르)	☐ IT Grundschutz(독일)
☐ SEC 규칙 17-a-4(f)	☐ PIPEDA(캐나다)	☐ MARS – E
☐ SecNumCloud(프랑스)		
☐ SOC1/ISAE 3402	☐ 개인 정보 보호법(호주)	☐ MITA 3.0
☐ SOC2/SOC3	☐ 개인 정보 보호법(뉴질랜드)	☐ MPAA
☐ SWIPO IaaS 행동 강령		
	☐ 스페인 DPA 승인	☐ NIST
	☐ 영국 DPA - 1988	☐ 업타임 인스티튜트 티어
	☐ VPAT/제 508 호	☐ 영국 클라우드 보안 원칙

위의 목록은 설명 목적으로만 제공되었으며 클라우드 서비스에 적용될 수 있는 인증 및 표준을 모두 포함하는 것으로 간주해서는 안 됩니다.

2.3.1.1 데이터 보호

클라우드 서비스를 사용할 때 고려해야 할 중요한 고려 사항 중 하나는 일반 데이터 보호 규정(GDPR)을 비롯한 관련 EU 데이터 보호법에 따라 개인 데이터를 처리해야 한다는 것입니다. GDPR 은 원칙 기반 규제이므로 규정 준수를 보장하는 데 도움이 되는 부문별 지침을 제공하지 않습니다. 다만 행동 강령과 같은 규정 준수 도구를 도입하여 부문별 지침을 제공할 것을 권장합니다. CISPE 는 프랑스 데이터 보호 기구(CNIL)와 협력하여 유럽 데이터 보호 위원회의 지원 아래 데이터 보호 행동 강령(CISPE 강령[6])을 개발했으며, 이 강령은 유럽에서 일반적으로 적용되고 있습니다. 이 강령의 목적은 CISP 가 GDPR 을 준수하고 고객이 수행하고자 하는 개인 데이터 처리에 CISP 가 적합한지 여부를 평가할 수 있도록 돕는 것입니다.

- 이 강령은 IaaS 부문에만 초점을 맞추고 있으며 IaaS 제공업체의 구체적인 역할과 책임을 다루고 있습니다.

[6] https://cispe.cloud/code-of-conduct/

- 이 강령은 클라우드 인프라 서비스와 관련하여 공정하고 투명한 처리와 적절한 보안 조치의 측면을 명확히 하는 데 도움이 됩니다(GDPR, 제 40 조 [2]).
- 데이터가 EU 를 벗어나지 않도록 보장함으로써 고객이 데이터에 대한 주권을 유지할 수 있는 방법을 이해하는 데 도움이 됩니다.
- 유럽 클라우드 데이터 서비스 개발을 위한 EU 의 GAIA-X 이니셔티브를 지원하는 데이터 보호 모범 사례를 촉진합니다.

CISPE 강령과 같은 데이터 보호 행동 강령을 준수함으로써 CISP 는 GDPR 를 엄격하게 준수하면서 개인 데이터를 처리한다고 보장할 수 있습니다.

RFP 예제: 데이터 보호

직접 또는 리셀러를 통해 입찰 중인 CISP 는 CISPE 강령과 같은 데이터 보호 행동 강령을 준수할 수 있음을 입증할 수 있어야 합니다. 데이터 보호 강령은 GDPR 프레임워크에 명시된 요구 사항에 준거해야 합니다. 데이터 보호 강령에는 적어도 (1) CISP 의 역할과 책임에 대한 명확한 정의, (2) CISP 는 마케팅이나 홍보의 목적으로 고객 데이터를 사용하지 않는다는 요건, (3) 유럽 경제 지역 내에서만 데이터를 처리할 수 있는 CISP 서비스를 고객이 선택할 수 있다는 내용이 포함되어 있어야 합니다. 유럽 데이터 보호 기구의 인가를 받은 외부 독립 감사 기간이 인정한 외부 독립 감사 기관(감시 기관)에게 강령 준수 여부를 검증받아야 합니다.

2.3.1.2 클라우드 제공업체 전환 및 데이터 이식

고객은 CISP 또는 PaaS/SaaS 제공업체에 '종속'되지 않고 원하는 클라우드 서비스를 자유롭게 선택할 수 있어야 합니다.

CISP 가 제공하는 클라우드 서비스는 '일대다' 기준으로 표준화 및 제공되며, 서비스 구성, 프로비저닝, 제어는 고객이 수행합니다. 클라우드 컴퓨팅의 이점은 고객이 고유한 애플리케이션 및 솔루션을 개발하는 데 필요한 표준화된 서비스를 선택할 수 있다는 것입니다. 이외에도 언제든지 고객 요구를 가장 잘 충족하는 신규 서비스나 다른 서비스로 전환할 수 있다는 이점도 있습니다.

행동 강령을 통해 데이터를 보호할 수 있을 뿐 아니라 온프레미스 인프라에서 클라우드로 전환할 때나 CISP 간에 전환할 때 고객에게 자신감과 확신을 줄 수 있습니다. CISPE 는 유럽 CIO 협회(EuroCIO)와 함께 공동 의장을 맡고 IaaS 클라우드 서비스의 데이터 이동 및 클라우드 서비스

전환을 위한 행동 강령(SWIPO IaaS 강령[7,8])을 개발했습니다. 행동 강령 초판은 EU 의 '데이터의 국경 간 이동 규정'에 따라 개발되었으며, 2019 년 11 월 EU 핀란드 대통령직 아래 유럽 위원회에 제공되었습니다. 그리고 2020 년 5 월 SWIPO AISBL 협회가 행동 강령 초판을 발행했습니다. 2021 년 4 월 SWIPO AISBL 은 강령을 준수하는 첫 번째 서비스를 공표했으며, 2021 년 5 월 강령을 준수하는 첫 번째 CISPE 회원 서비스를 공표했습니다.

RFP 예제: 클라우드 제공업체 전환 및 데이터 이식

직접 또는 리셀러를 통해 입찰 중인 CISP 는 SWIPO IaaS 강령과 같은 '전환 및 데이터 이식' 행동 강령을 준수할 수 있음을 입증할 수 있어야 합니다. 행동 강령에서는 고객이 CISP 를 전환하기로 결정한 경우 고객이 자신의 비즈니스 데이터를 안전하게 전송하기 위해 어떤 조치를 취해야 하는지 자세히 설명해야 합니다.

2.3.2 공급업체 간 비교

위 섹션의 기술 기준과 마찬가지로 클라우드 서비스 RFP 의 최소 보안 요구 사항 이외에도 경쟁 평가 시 CISP 보안 기능과 서비스를 비교할 수 있는 기준도 제공해야 합니다.

CISP 보안 요구 사항 예제는 부록 A – 입찰자 간 비교를 위한 기술 요구 사항을 참조하세요. CISP 를 평가하는 공공 부문 기관의 주요 보안 고려 사항은 다음과 같습니다.

RFP 예제: 주요 보안 고려 사항

- 공동 책임 모델에 대한 CISP 의 이해 및 고객이 CISP 기능과 서비스에 대한 보안 책임 조항을 이해하는 데 도움이 되는 문서(예: GDPR 의 맥락에서 설명)
- CISP 보안 태세와 물리적/논리적 제어 수단에 대한 비독점 공개 문서 등 CISP 인프라 보안과 관련된 입증된 기록
- 클라우드 보안과 관련한 CISP 지원
- 고객이 계정 설계를 정형화하고 보안 및 클라우드 거버넌스 제어를 자동화하고, 감사를 간소화하는 데에 사용할 수 있는 서비스
- 템플릿과 같은 방식(CISP/CISP 파트너가 구축한 보안 템플릿 표본 포함)으로 리소스 모음을 생성, 프로비저닝, 관리할 수 있는 역량
- 통제 항목을 신뢰하고 반복 가능한 방식으로 구축할 수 있는 역량
- 지속적, 실시간 감사를 위한 기능
- 클라우드 거버넌스 정책의 기술 스크립팅 역량

[7] https://ec.europa.eu/digital-single-market/en/news/cloud-stakeholder-working-groups-start-their-work-cloud-switching-and-cloud-security
[8] https://swipo.eu/

- 변경 권한이 없는 사용자는 중단할 수 없는 강제 실행 기능을 생성할 수 있는 역량
- 정책, 표준, 규정에 기입된 사항을 안정적으로 구현하고 시행 가능한 보안 및 규정 준수를 확립하여 IT 환경에 대해 기능성과 신뢰성을 갖춘 클라우드 거버넌스 모델을 만들어 내는 능력
- 일반적으로 빈번하게 발생하는 네트워크 및 전송 계층의 DDoS(분산 서비스 거부) 공격을 방어하는 서비스 및 정교한 애플리케이션 계층 공격을 완화하는 사용자 지정 규칙을 작성하는 능력
- 관리형 위협 탐지 서비스

2.3.3 계약 체결

위에서 언급했듯이, CISP 계약 조건은 클라우드 서비스 모델의 운영 방식(물리적 자산을 구매하지 않으며 CISP 가 표준화된 서비스를 제공하는 환경을 대규모로 운영하는 방식)을 반영하도록 고안되었으므로 CISP 계약 조건을 최대한 반영하고 활용하는 것이 중요합니다. 계약 조건 및 계약 체결에 대한 자세한 내용은 아래의 2.5 섹션을 참조하세요.

보안에 관해서는 RFP 의 원래 항목과 일치하는 한 CISP 가 오퍼링을 지속적으로 업데이트하거나 공급자가 제출 기한 이후라도 제품을 추가하도록 허용할 것을 강력히 권장합니다. 여기에는 보안 기능과 서비스가 빠르게 발전하고 CISP 가 대다수의 경우 무료로 사용할 수 있는 보안 중심 서비스를 자주 출시한다는 점이 반영되어 있습니다. 보안 오퍼링 변경이 부정적 영향을 미치지 않도록 기준 보안 수준(위의 최소 요구 사항 참조)을 설정하는 것이 중요합니다.

물론 공동 책임 모델은 클라우드 서비스 RFP 에서 보안의 핵심입니다. 각 당사자는 보안 책임을 명확히 해야 하며, CISP 는 CISP 제공 클라우드 기술에 대한 CISP/고객의 보안 책임을 문서화해야 합니다. 또한 고객이 보안 모범 사례를 내재화하고 자동화할 수 있도록 관련 문서도 제공해야 합니다.

클라우드 사용 기본 계약에서는 공급업체가 클라우드 서비스 RFP 에 명시된 최소 보안 및 규정 준수 요구 사항을 더 이상 충족하지 않을 경우 해당 공급업체를 배제할 수 있도록 유연성을 제공해야 합니다.

2.4 요금

수요 변동을 고려하여 클라우드 기술 구매 계약을 체결하려면 공공 부문 조직은 사용한 서비스에 대해서만 비용을 지불하고 사용량과 지출에 대해 클라우드 거버넌스와 가시성을 제공하는 계약을 체결해야 합니다.

중요한 것은 클라우드 서비스 RFP 에서는 단가를 단순하게 비교하는 것이 아니라, 가치와 총 소유 비용(TCO)을 고려해야 한다는 점입니다. 최저 단가를 고려하는 전통적 관행은 클라우드 모델에 적합하지 않으며, '경제적으로 가장 유리한 입찰'이나 종합적으로 볼 때 최저 가격으로 귀결되지 않습니다.

CISP 요금 평가를 지원하려면 유사한 역량을 갖춘 CISP 가 기본 계약의 자격을 얻을 수 있도록 먼저 요금 관련 최소 요구 사항을 활용해 CISP 사전 검증을 실시하거나 후보 목록을 작성하는 것이 좋습니다. 그런 다음 납품 지시와 소수 경쟁의 평가 프로세스에서 일반적인 공공 부문 워크로드에 맞는 대표적 클라우드 아키텍처 예제와 요금 시나리오를 선택하고 CISP 에게 요금 책정을 요구합니다. 또한 라이브 테스트 데모를 실시하여 CISP 가 제공하는 클라우드 기술 서비스의 성능과 탄력성을 비교해 보는 것도 좋습니다. 클라우드 기술 데모 테스트 스크립트 예제에 대한 내용은 부록 B 를 참조하세요.

2.4.1 최소 요구 사항

클라우드 서비스 RFP 의 요금 섹션에는 네 가지 주요 요소가 있습니다.

1. **종량제 요금:** 클라우드 고객은 종량제 요금 모델을 채택하고 있습니다. 즉, 매월 말 사용한 만큼에 대해서만 비용을 지불하면 되며, 활용률과 리소스 지표를 최적화할 수 있습니다.
2. **투명성:** CISP 요금은 투명하게 공개되어야 합니다.
3. **유연성:** 시장 요금에 따라 클라우드 가격이 변하는 등의 유연성이 있습니다. 이 접근 방식에서는 클라우드 요금의 동적이고 경쟁적인 특성을 활용하여 혁신과 가격 인하를 실현합니다.
4. **지출 제어:** CISP 는 고객이 (1) 사용량과 지출을 세부적, 개략적으로 모두 모니터링하고 (2) 사용량과 지출이 사용자가 지정한 한도에 도달하면 알림을 보내고 (3) 사용량과 지출을 예측하여 향후 클라우드 예산을 편성할 수 있도록 보고, 모니터링 및 예측 도구를 제공해야 합니다.

RFP 예제: 요금

<고객>은 제안 요청에 응한 CISP 에게 상용 클라우드 기능으로 각 서비스를 제공하는 데 있어 어떤 방식과 요금 모델을 제안하는지 명시할 것을 요청합니다.

CISP 는 다음을 제공해야 합니다.

- 서비스 정의 문서 또는 서비스 정의 링크
- 계약 조건 문서
- 요금 문서(전체 가격 목록/요금 문서가 요청 시 제공된다는 전제하에 공개 요금 문서 링크 허용)

가격은 가장 일반적인 구성의 서비스에 대한 비용입니다. CISP 는 볼륨 기반 할인 옵션과 구매할 제품의 실제 가격과 구매자에게 제공되는 전반적 가치(예: 최적화 서비스를 통한 비용 절감 효과)를 산출할 수 있는 가격 계산기 도구를 제공해야 합니다.

기본 계약하에서 구매자는 공급자에게 서비스 설명, 계약 조건, 요금 또는 서비스 정의 문서/모델에 대해 설명해 줄 것을 요청해야 될 수 있습니다. 공급자와의 대화 기록은 보관됩니다.

추가적인 요금 요구 사항

- 비즈니스 유연성을 극대화하고 확장성과 성장을 지원하는 동적 요금 모델을 클라우드 기술에 제공합니다.
- 요금 속성에는 다음이 포함되어야 합니다.
  - 요금이 주문형, 공과금 방식의 종량제로 제공됩니까? 요금 모델을 설명하세요.
  - 사용 및/또는 대량 구매를 약정하면 추가 할인을 받을 수 있습니까? 방법에 대한 세부 정보를 제공하세요.
  - 요금이 공개되어 있고 투명합니까? 요금 공개 링크를 기입하세요.
  - 요금이 동적이고 시장 경쟁에 신속하고 효율적으로 대응합니까?
  - 지출 추적을 위한 모범 사례 및 리소스를 제공하고 있습니까?
  - 비용 최적화를 위한 모범 사례 및 리소스를 제공하고 있습니까?

요금 투명성

혁신과 경쟁에 따라 상용 클라우드 기술의 요금이 지속적으로 인하되는 추세이므로 기본 계약하에 **<고객>**이 계측에 따라 지불하는 CISP 서비스 단가는 클라우드 제공업체 웹 사이트에 게시된 클라우드 제공업체의 단가(고객이 서비스 단위를 소비하는 시점의 단가)를 초과해서는 안 됩니다.

예산 수립 및 청구 알림/보고서

클라우드 기술의 제공 내용과 사용 현황을 입증하기 위해 CISP 는 **<고객>**에 시간, 일 또는 월, 조직의 각 계정, 제품 또는 제품 리소스, 사용자 정의 태그에 따라 비용을 세분화한 상세 청구 보고서를 생성할 수 있는 도구를 제공해야 합니다. **<고객>**은 클라우드 공동 책임 모델의 당사자 중 하나로서 CISP 가 제공하는 예산 수립 및 청구 기능과 도구를 사용하여 고유의 예측 요구 사항과 보고 요구 사항을 충족할 책임이 있음을 인식하고 있습니다.

- **<고객>**이 청구 정보를 세부적, 개략적으로 모두 확인할 수 있는 방법에 관한 정보를 제공하고, 시간 경과에 따른 지출 패턴을 시각화하고 향후 지출을 예측할 수 있도록 지원합니다.
- **<고객>**이 서비스, 연결 계정 또는 리소스에 적용된 사용자 지정 태그로 사용량/청구 보기를 필터링하는 방법과 **<고객>**이 정의한 한도/예산에 도달하거나 한도/예산을 초과하는 경우 알림을 전송하는 청구 경보를 생성하는 방법에 관한 정보를 제공합니다.

- **<고객>**이 과거 사용량에 기반해, 정해진 예측 기간 동안 클라우드 사용량을 얼마나 사용할지 예측하는 방법에 관한 정보를 제공합니다. 비용과 지출에 대한 거버넌스를 강화하기 위해 CISP 는 **<고객>**의 CISP 청구서 **견적**을 제공하고 **<고객>**이 예상 사용량에 대해 경보와 예산을 사용할 수 있게 해야 합니다.

2.4.2 공급업체 간 비교

공공 부문 조직은 최상의 가치, 경제적으로 가장 유리한 입찰 또는 최저 가격과 같은 평가 기준을 사용하여 입찰자 간의 경쟁을 요구하는 경우가 많습니다. 기본 계약 납품 지시 또는 소수 경쟁의 요금 책정을 계획하고 있는 경우 클라우드 고유의 기능을 고려한 접근 방식을 구축하는 것이 중요합니다. 예를 들어 단순히 클라우드 제공업체의 오퍼링(예: 컴퓨팅 또는 스토리지) 간에 품목을 비교하는 방식은 성능, 클라우드 네이티브 서비스와 CISP 모니터링 도구를 통한 비용 최적화, CISP 가 무료로 제공할 수 있는 차별화 서비스 등의 기능을 고려하지 않는다는 점에서 효과적인 비교 방식이 아닙니다. 또한 CISP 의 정가는 품목이 매우 많을 수 있으며, 요금 모델은 서비스마다, 제공업체마다 다를 수 있습니다.

TCO 분석

정의된 사용 사례의 총 소유 비용(TCO)에 초점을 맞추는 것이 좋습니다. 총 소유 비용에서는 클라우드 솔루션의 모든 측면(파트너 서비스, 표준 CISP 할인, 성능 향상, 비용 절감/최적화를 이끌어내는 기술 기능 등)을 고려합니다.

시나리오별 비교

평가 프로세스에서는 일반 시스템이나 애플리케이션에 맞는 대표 시나리오도 고려합니다. 이러한 시나리오(웹 호스팅 또는 사용자가 x 명인 HR 시스템 구현 등)에는 리소스의 속도와 규모, 애플리케이션 또는 솔루션의 성능, 스토리지 액세스 시간, 소량의 복잡한 데이터와 대량의 단순 컴퓨팅 작업 비교가 포함될 수 있습니다. 또한 애플리케이션이나 시스템에는 세금 신고 기간 동안의 대량 처리, 홍수 경보 등의 긴급 재난 알림과 같은 대표 시나리오가 있을 수 있습니다. 시나리오는 고객이 프로젝트 동안 사용할 수 있는 기술과 서비스의 범위를 포괄해야 합니다. 이렇게 하면 고객은 프로젝트의 총 예상 비용을 비교할 수 있습니다.

재무 및 기술 측면에서 시나리오 비교

CISP 제품 간에 요금을 비교할 때 기술적 이점을 고려하는 것도 중요합니다. 예를 들어 지리적 리전에 있는 클러스터에 데이터 센터를 두는 모델을 채택한 CISP 의 경우 해당 CISP 의 고객은 액티브-액티브 재해 복구(DR) 토폴로지를 구축할 수 있습니다. 이러한 이중화와 데이터 센터 구성을 갖추지 못한 CISP 라면 재해 복구 요구를 고려할 경우 비용이 x% 더 비싸질 수 있습니다.

CISP 를 평가할 때 요금에 대해 왜 부가적인 기술 기능을 망라하는 전체론적 접근 방식을 취해야 하는지에 대한 예시로서, 아래의 '단순 1 대 1' 비교를 생각해 보세요.

예: 고객은 기본 계약의 자격을 충족하는 CISP 가 제공하는 객체 스토리지의 가격을 비교하려고 합니다. CISP 1 의 스토리지 '단위' 항목의 가격은 0.023 EUR/GB 입니다. CISP 2 의 동일한 '단위'의 가격은 0.01 EUR/GB 입니다. 단순하게 단위끼리 비교하는 경우 고객은 다음과 같은 중요한 질문을 던지지 않을 것입니다.

1. 장애 발생 시 사용할 수 있는 객체의 중복 복사본은 몇 개입니까? 위의 예에서 CISP 1 은 서로 다른 두 개의 시설에 데이터를 저장하여 데이터가 동시에 손실되지 않도록 방지하며, 데이터 복사본을 여러 개 유지합니다. CISP 2 의 경우 중복 복사본이 생성되지 않습니다.
2. 저장된 객체의 지속 가능성은 어느 정도입니까? CISP 1 은 99.999999999%, CISP 2 는 99%입니다.
3. 전체 프로젝트 또는 워크로드의 소유 기간 동안 발생하는 비용을 고려하고, 데이터 저장 및 사용 방법과 관련하여 비용 최적화 기능을 통해 비용을 어떻게 절감할 수 있는지 고려합니다. 예를 들어 CISP 의 서버리스 기능을 더 많이 사용하면 비용을 x% 줄일 수 있습니다.

이는 요금, 특히 보안과 규정 준수와 관련된 기술적 고려 사항 중 일부에 불과합니다.

요금 시나리오 관련 고려 사항

기본 요금 – 이는 본질적으로 CISP 의 공개 가격입니다. CISP 는 기본 요금을 공개해야 하지만 CISP 를 효과적으로 비교하기 위해 위에서 언급했듯이 고객은 구체적 시나리오를 3~5 개 요청할 수 있습니다. 시나리오는 고객이 프로젝트를 진행하면서 사용할 법한 서비스와 기술을 광범위하게 포괄해야 합니다. 이렇게 하면 고객은 프로젝트의 총 예상 비용을 비교할 수 있습니다. 품목/SKU 수준에서 비교를 하는 것은 고객과 공급업체에게 도움이 되기 보다는 문제가 될 소지가 많습니다. 고객은 모든 CISP 의 수많은 품목을 비교해야 하는 반면, 서비스 사용량만으로 실제 가격을 결정하는 경우 공급업체는 이 수준에서 세부 정보를 제공하고 관리하기 때문입니다.

최상의 가치를 모색하는 클라우드 고객이라면 필수적으로 CISP 의 중요 기능을 평가해야 합니다. 예를 들어 CISP 의 경우 무료 또는 사실상 무료인 서비스를 다수 보유하고 있을 수 있는데, 요금 평가 시 이러한 서비스가 고려 대상이 되며, 유사한 기능을 유료로 제공하는 다른 CISP 가 있을 수 있습니다.

CISP 가 '기본 제공 기능 개수'와 기본 제공 서비스가 전체 영향 비용(impact cost)에서 차지하는 비중을 제시하도록 평가 기준을 작성할 수 있습니다. CISP 볼륨 기반/차등 요금 책정과 예약형 인스턴스/스팟 인스턴스 등의 구매 할인도 평가 기준에서 고려될 수 있습니다. 예를 들면 다음과 같습니다.

- 고객이 예약형 컴퓨팅 용량(1 년, 3 년 등) 구매 시 x% 절감
- 차등/볼륨 요금 책정에 따라 x% 할인
- 아키텍처 검토 및 인프라 최적화(예: 최적의 컴퓨팅 옵션으로 전환)를 기반으로 x% 절감
- 위에서 언급한 대로 전체 수명 비용 및 비용 최적화 기능을 통한 비용 절감 방법 고려

요금 시나리오

입찰자는 평가 목적으로만 아래 시나리오에 대한 요금을 제공해야 합니다. 실제 가격은 온디맨드 종량제 모델의 서비스 소비량을 기준으로 합니다.

다음은 가격 발견을 위한 대표적 요구 사항으로, 이러한 명목상 요구 사항은 계약 기간 동안 변경될 수 있다는 사실을 명시적으로 이해하고 있다는 조건하에 제공됩니다. 12 개월, 36 개월 온디맨드 요금과 12 개월, 36 개월 예약 용량 요금을 모두 기입하세요.

제공 정보:

- 제안된 솔루션의 이름:
- 입찰자의 최저 요금:
- 서비스 시간: 24x7x365
- 서비스 가용성: 99.95%

또한 워크로드가 유사하고 1/2/3 년 동안 CISP 모니터링 및 최적화 도구, 최적형 클라우드 네이티브 솔루션, CISP 가격 인하를 통해 지출을 최적화한 경험이 있는 기존 고객의 사례도 요금 시나리오에 포함될 수 있습니다.

2.5 계약 이행 설정/계약 조건

CISP 가 제공하는 클라우드 기술과 운영 작업은 그 특성상 표준화되어 있으므로 계약 조건도 표준화되어 있습니다. 다만 현지 법률과 규정에 맞춰 이들 계약을 약간 조정할 수는 있습니다.

기존의 IT 조달 방식에서는 엄격한 규칙을 적용하여 입찰자로 하여금 조달의 모든 또는 대다수 요구 사항을 준수하도록 요구하고 그렇지 않을 경우 입찰을 거부하는 경우가 많습니다. 또는 필수 요구 사항에 엄격한 하위 요구 사항을 넣어 이를 준수하도록 하는 경우도 있습니다. 클라우드 기술은

맞춤형 솔루션을 설계하는 데 유용하게 이용할 수 있는 일련의 표준 구성 요소, 도구이므로 클라우드 기술에 기존의 공급 방식을 사용하면 조달에 실패할 수 있습니다.

2.5.1 계약 조건

클라우드 서비스 RFP 에서 계약 체결 부문을 작성할 때는 기존 CISP 거래 조건(commercial terms)을 확인하고 이해하는 일이 선행되어야 합니다. 이들 거래 조건은 CISP 웹 사이트에서 쉽게 찾아볼 수 있습니다. 공공 부문 기관들은 점차 CISP 의 거래 조건을 편하게 받아들이고 있습니다. 거래 조건을 이해하기 위해 취할 수 있는 활동 중 하나는 CISP 와 CISP 의 파트너를 만나 접근 방식을 심층적으로 분석하는 것입니다. 이때 물어볼 주요 질문은 CISP 가 특정 거래 조건을 운용하는 '이유'입니다. 이들 거래 조건 중 일부는 기존 IT 조건과 다를 수 있는데, 이들 조건이 클라우드 계약에 포함되는 데에는 매우 구체적인 '이유'가 있습니다. 공개되어 있는 조건을 수용할 수 없는 경우 CISP 는 종종 다소 수정 가능한 계약을 제시하기도 합니다.

CISP 의 계약 조건을 검토하는 것만큼 기존의 정책, 규정 및/또는 법률(예: 기술, 데이터 기밀 등급, 개인 정보 보호, 인력 관련 정책, 규정 및/또는 법률)을 이해하는 것도 중요합니다. 기존의 IT 오퍼링을 구매하고 활용하는 데에 맞춰 고안된 정책/규정/법률은 CISP 의 모델과 상충하는 경우가 많습니다. 클라우드 서비스 RFP 를 통해 원래의 기본 계약 입찰에 포함되어 있던 클라우드 기술만 이용하도록 하는 것이 그 예입니다. CISP 는 끊임없이 신규 서비스와 신규 기능을 추가하고 있습니다. 기존의 IT 제품 갱신 접근 방식을 따른다는 이유로 신규 서비스에 대한 이용을 막는 것은 최종 고객에게 불합리하게 작용합니다. 이런 경우 CISP 와의 심층적 논의를 통해 정책/규정 및/또는 법률을 살펴보는 것이 중요합니다.

사전 RFP 논의 활용

위에서 언급한 것처럼 RFP 초안을 작성하기 전에 CISP, 관련 공급업체와 만나 업체의 계약 조건을 파악하고 조직의 접근 방식, 정책, 규정, 법률을 업체에게 알려주는 시간을 가져야 합니다. 이러한 논의를 할 때 가장 중요한 것은 양측 모두가 관련 조건이 '왜' 그렇게 만들어졌는지 이해하는 것입니다. 예를 들어 클라우드 계약 조건은 기존 데이터 센터, 관리형 서비스, 하드웨어, 수축 포장 소프트웨어, 시스템 통합 계약 조건과 다릅니다. 단일 모델이고 지속적인 혁신을 수반하기 때문에, 해당 비즈니스 모델에서는 RFP 프로세스가 충분히 유연해야 협상과 논의를 통해 계약 조건을 명료화할 수 있습니다.

논의 또는 협상 과정에서 계약 조건을 명료화함으로써 공공 부문 조직은 클라우드 모델을 더 잘 이해할 수 있고 조직의 요구를 충족하는 제공업체를 잘못해서 거절하는 사태를 예방할 수 있습니다. 대표적 프로세스 중 하나는 조직이 논의하고자 하는 조건을 수주 결정을 내리기 전에 미리

파악하는 것입니다. 조직은 입찰자와 수용 가능한 조건을 사전에 협상함으로써 수주 결정에 가장 적합한 조건을 확보할 수 있으며, 좋은 제안을 거절하는 결과를 초래할 수 있는 의견 차이를 해결할 수 있습니다. 공공 부문 기관도 자신의 정책, 규정, 법률을 검토할 수 있으며, 양측 모두 클라우드 사용이 이들 모델에 어떻게 적합한지 이해할 수 있습니다. 기존의 조항을 활용할 방법이 있는 경우가 많습니다. 문제의 소지가 있는 부분은 양측이 협력하여 해결 방안을 찾을 수 있습니다. 따라서 RFP 및 후속 계약 협상을 진행하기 전에 이러한 논의를 가지는 것이 좋습니다.

협상 유연성

CISP 의 표준 계약 조건을 따르면서도 현지 법률을 준수하여 계약을 체결하려면, (1) 입찰자에게 표준 계약을 체결할 것을 요구하고, (2) 클라우드 서비스 RFP 를 위한 기본 계약을 수립할 때 부적합한 계약 조건은 제정하지 않으며, (3) 기본 계약으로 이어지는 자문 및 제안의 모든 조항(법으로 강제하는 의무 조항 제외)에 대해 협상의 여지를 두는 것이 좋습니다.

참고: 공동 책임의 범위는 클라우드 모델에 따라 다르며, 계약 조건에 반영되어야 합니다. 예를 들어 CISP 는 데이터를 소유하고 데이터 상주 위치를 결정하는 것은 고객이라는 사실을 공식화하고 데이터 위치 선택을 제한하는 도구를 제공합니다. **단**, 이들 도구를 사용하는 데에 따르는 책임은 고객 또는 파트너에게 있습니다.

클라우드 사용 기본 계약의 각 상세 분류마다 계약과 관련해 별도의 계약 조건 세트가 있어야 합니다. 모든 상세 분류의 계약에 대해 '일률적 접근 방식'을 사용하면 기술 타당성 미 호환성과 관련하여 문제가 발생할 수 있습니다.

이미 언급한 바와 같이, 협상의 여지가 없는 의무 조건을 포함하는 RFP 는 제공업체에게 '싫으면 말고'식의 제의로 좋은 제안도 거절하는 결과를 야기할 수 있습니다. 공공 부문 조직은 **법률상 요구되지 않는 한** 의무 조건을 사용하는 데에 따른 결과를 신중하게 고려해야 합니다. 조직은 의무 요구 사항 또는 조건이 필요한지에 대해 확실히 해야 합니다. 의무 사항으로 분류하는지에 따라 향후 협상이 달라지기 때문입니다. 최상의 기술과 솔루션을 확보하는 데 필요한 유연성을 조직에 제공하려면 의무 요구 사항 또는 조건 사용을 최소한으로 유지해야 합니다.

CISP 클라우드 기술은 완벽히 표준화되고 완전히 자동화된 방식으로 제공됩니다. 그러므로 CISP 는 기반 서비스를 맞춤화할 목적으로 계약 조건을 변경할 수 없습니다. 또한, 일반적으로 서비스의 가격은 모든 사용자에게 공개되며, 모든 사용자가 표준 가격으로 서비스를 이용합니다. 즉, CISP 는 특정 고객을 대신해 더 많은 위험을 감수하기 위해 가격을 조정할 수 없습니다.

간접 구매

CISP 에게 클라우드 기술을 직접 구매하는 대신 CISP 리셀러에게 구매할 수도 있습니다. CISP 리셀러에 대한 자세한 내용은 위의 2.1.3 섹션을 참조하세요.

RFP 예제: 계약 조건

CISP 또는 대리 공급업체는 공개된 계약 조건을 제공해야 하며, **<고객>**이 제공하는 주요 계약 조건에 대해 피드백을 제공해야 합니다.

<고객>은 낙찰자의 계약 조건에 따라 낙찰자와 서면 계약을 체결할 계획입니다. 입찰자는 **<고객>**이 검토할 수 있도록 일련의 계약 조건 제안을 제공해야 합니다. 여기서 계약 조건 제안은 최상의 상업적, 법적 제안을 나타냅니다. 제안자와 <고객>은 <협상/논의> 단계에서 양측의 계약 조건을 모두 논의할 수 있습니다.

- 기본 계약의 주요 조건에는 최대한 다음 요소를 포함합니다.
  - 기본 계약 기간
  - 기본 계약 거버넌스
  - 기본 계약 성과
  - 기본 계약 만료
  - 기본 계약 범위
  - 발주 프로세스
  - 기밀 조항
  - 범주별 IP 및 정보
  - CISP 가 충족해야 하는 최소 기술 요구 사항(예: 품질 표준, 인증, 보안 및 데이터 보호)
- **기본 계약 상세 분류마다 조건이 다를 수 있습니다.**
- CISP 서비스 세부 사항은 납품 지시에서 고려될 수 있으며, 납품 지시에서 다룹니다.
- 계약 변경 허용 – 고객과 공급자가 계약 변경에 동의하지 못하게 제한하거나 신규 서비스 또는 개선 기능을 사용하지 못하게 제한해서는 안 됩니다. 클라우드 서비스는 진화하는 특성을 보입니다. 즉, 서비스 개선이 끊임없이 이루어지며, 고객의 효율성을 증진하는 방향으로 개선이 전개됩니다.
- 고객이 서비스 수준 계약(SLA)을 지정해서는 안 됩니다. 고객 계약 조건에서 CISP 표준 서비스 제공 모델과 다른 주문 맞춤형 SLA 를 정의해서는 안 됩니다. CISP 표준 SLA 를 허용하면 CISP 는 원가를 낮추고 그에 따른 혜택을 고객에게 되돌려 줄 수 있으며 고객은 CISP 가 SLA 를 달성한다는 확신을 가질 수 있습니다.
- 책임 상한은 비례해야 합니다. 책임은 구매한 서비스에 비례해야 하며, 책임 상한이 불균형적으로 높아서는 안 됩니다. 상한이 불균형적으로 높으면 CISP 는 저가치 프로젝트를 수락하는 것을 주저하게 됩니다. 저가치 프로젝트는 고객이 특정 클라우드 솔루션이 자신의 조직에 적합한지 결정하는 데에 유용한 도입부이자 '테스트' 사례의 역할을 하는 경우가 많습니다.

- 고객 데이터는 고객이 소유해야 합니다. 고객은 데이터를 제어하고 소유해야 하며 데이터가 보관되는 지리적 위치를 결정할 수 있어야 합니다. 그래야 고객이 공급업체에 종속되지 않고 데이터를 새 공급업체로 자유롭게 이동할 수 있습니다.

2.5.2 소프트웨어 계약 조건

이 핸드북에서는 CISP 가 제공하는 IaaS 및 PaaS 클라우드 기술 구매에 초점을 맞추고 있지만, 공공 부문 조직이 공급업체로부터 소프트웨어를 구입할 때 고려할 수 있는 소프트웨어 계약 조건에 주목하는 것도 중요합니다. 잘 구성된 클라우드 서비스 RFP 의 일환으로 소프트웨어를 구매하는 방법에 대해 알아보려면 그림 1(5 페이지)을 참조하세요.

소프트웨어는 공공 부문을 포함한 거의 모든 비즈니스에서 중요한 역할을 합니다. 클라우드 서비스 RFP 에 소프트웨어 라이선스 계약 조건과 같은 의무를 포함하면 공공 부문 기관이 소프트웨어를 구입할 때 최상의 가치를 얻고 공급업체를 자유롭게 선택할 수 있게 됩니다.

자세한 내용은 클라우드 고객을 위한 열 가지 공정 소프트웨어 라이선스 원칙[9]을 참조하세요. 이 원칙은 CIGREF[10](디지털 기술 사용자를 대표하는 프랑스 대기업과 공공 행정 기관이 소속된 협회)가 유럽의 다른 CIO 및 제공업체 협회의 지원 아래 CISPE 와 함께 제정한 것으로, 규모에 관계없이 조직이 클라우드로 전환할 때 조직의 디지털 트랜스포메이션을 방해하는 요소로 양 협회가 꼽은 관행을 타파하는 데에 그 목적을 두고 있습니다.

RFP 예제: 소프트웨어

<고객>은 낙찰자의 계약 조건에 따라 낙찰자와 서면 계약을 체결할 계획입니다. 입찰자는 **<고객>**이 검토할 수 있도록 일련의 계약 조건 제안을 제공해야 합니다. 여기서 계약 조건 제안은 최상의 상업적, 법적 제안을 나타냅니다. 소프트웨어 공급업체와 <고객>은 <논의/협상> 단계에서 양측의 계약 조건을 모두 논의할 수 있습니다.

요구 사항 1.0. 소프트웨어 공급업체는 세부적 수준의 비용 명세서, 개략적 수준의 비용 명세서를 비롯해 명확한 라이선스 계약 조건을 제시해야 합니다.

요구 사항 1.1. 라이선스 조건을 준수하지 못하는 데 따른 모든 청구 내역은 세부적 형태와 개략적 형태로 제공되어야 합니다.

[9] https://www.fairsoftware.cloud/principles/
[10] https://www.cigref.fr/

요구 사항 2.0. 소프트웨어 라이선스는 <고객>이 라이선스 소프트웨어를 온프레미스에서 자신이 선택한 클라우드로 마이그레이션할 수 있게 해야 합니다. 이때 동일한 소프트웨어를 따로 다시 구매할 필요가 없어야 합니다.

요구 사항 2.1. 소프트웨어 라이선스는 라이선스를 부여하는 데에 제한이 있거나 비용 증가를 야기해서는 안 됩니다. 그렇지 않으면 <고객>이 자신이 선택한 클라우드에서 라이선스 소프트웨어를 실행하는 데에 제한이 있을 있습니다.

요구 사항 3.0. 소프트웨어 라이선스는 <고객>이 라이선스 소프트웨어를 조직이 선택한 클라우드뿐 아니라 자체 하드웨어에서도 실행할 수 있도록 허용해야 합니다. 자체 하드웨어에서만 실행할 수 있는 소프트웨어를 일반적으로 '온프레미스 소프트웨어'라고 부릅니다.

요구 사항 4.0. 소프트웨어 라이선스는 라이선스 소프트웨어를 <고객> 전용 하드웨어에서만 실행하도록 요구해서는 안 됩니다.

요구 사항 5.0. 소프트웨어 공급업체는 공급업체의 라이선스 소프트웨어가 다른 공급자의 클라우드 오퍼링에 사용되는 경우, 소프트웨어 감사를 더 자주 실시하거나 방해 목적으로 실시하거나 소프트웨어 라이선스 수수료를 더 많이 부과하는 등의 불이익을 <고객>에 가해서는 안 됩니다.

요구 사항 6.0. 디렉터리 소프트웨어는 다른 아이덴티티 서비스와 다르지 않은 방식으로 사용자 아이텐티티를 동기화하고 인증하기 위한 개방형 표준을 지원해야 합니다.

요구 사항 7.0. 소프트웨어 공급업체는 소프트웨어 설치 하드웨어 소유자만을 기준으로 동일한 소프트웨어에 대해 요금을 다르게 부과해서는 안 됩니다.

요구 사항 7.1. <고객> 소유의 데이터 센터에 설치된 소프트웨어, 제 3 자가 관리하는 데이터 센터에 설치된 소프트웨어, 제 3 자에게 임대한 컴퓨터에 설치된 소프트웨어 또는 <고객>이 선택한 클라우드 제공업체의 클라우드에 설치된 소프트웨어의 가격 사이에 차별을 두어서는 안 됩니다.

요구 사항 8.0. 법률상 요구되거나 보안 문제로 인해 부득이한 경우가 아닌 한, 소프트웨어 공급업체는 계약 기간 동안 <고객>이 이전에 받은 사용 허가를 제한하는 식으로 라이선스 조건을 중대하게 변경해서는 안 됩니다.

요구 사항 9.0. 소프트웨어 공급업체는 소프트웨어 라이선스가 <조직의 요구 사항>에 명시된 대로 <고객>의 계획된 소프트웨어 사용을 모두 망라한다고 기술함으로써 <고객>에게 오해를 불러일으키면 안 됩니다. 그러한 사용을 망라하려면 추가 라이선스를 구매해야 할 수 있습니다.

요구 사항 10.0. <고객>이 소프트웨어 라이선스를 재판매 및 양도할 수 있는 권한을 가지고 있는 경우, 소프트웨어 공급업체는 재판매 라이선스를 합법적으로 취득한 <고객>에 공정한 조건에 따라 지속적으로 지원 및 패치를 제공해야 합니다.

2.5.3 프로젝트별로 수주자를 선택하는 방법

본 기본 계약의 적용을 받는 공공 부문 기관은 필요할 때 원하는 클라우드 서비스에 대해 발주를 하거나 '납품 지시'를 내릴 수 있습니다. 기본 계약에 따라 납품 지시 계약을 체결하면 구매자는 기본 계약의 이점은 누리면서 납품 지시 시 기능 사양을 추가하여 요구 사항을 개량할 수 있습니다.

필요하다고 판단될 경우, 특정 워크로드 또는 프로젝트에 가장 적합한 공급자를 선정하기 위해 소수 경쟁을 진행할 수 있습니다. 소수 경쟁은 고객이 기본 계약에 따라 추가 경합을 붙이는 방식으로 상세 분류 안에 있는 모든 공급자를 초청하여 일련의 요구 사항에 응답하도록 합니다. 고객은 상세 분류 안에 있는 모든 가능한 공급자를 입찰에 초청합니다. 따라서 클라우드 서비스 RFP 에서 수주자에 대한 요구 사항을 최소로 설정해야 합니다. 그래야 각 상세 분류에서 선택의 폭이 넓어집니다.

오퍼링 유형(예: 퍼블릭 IaaS/PaaS, 커뮤니티 IaaS/PaaS, 프라이빗 IaaS/PaaS)의 각 상세 분류 범주마다 계약과 관련해 별도의 계약 조건 세트가 있어야 합니다. 각 상세 분류의 계약에 대해 '일률적 접근 방식'을 사용하면 기술 타당성 미 호환성과 관련하여 문제가 발생할 수 있기 때문입니다.

수주자 선택과 관련한 RFP 예제는 2.1.4 섹션을 참조하세요.

2.5.4 온보딩 및 오프보딩

클라우드 사용 기본 계약을 설정할 때 고려해야 할 사항 중 하나는 동적 구매 시스템(DPS) 옵션입니다. DPS 모델을 사용하면 기본 계약의 최소 요구 사항을 충족하는 모든 공급업체가 기본 계약에 참여할 수 있습니다. 기본 계약에 참여할 수 있는 공급업체 수를 엄격하게 제한하지 않습니다. 기존의 계약 모델과 달리 공급업체는 계약이 존속하는 한 언제든 'DPS 기본 계약' 참여를 신청할 수 있습니다.

적격 공급업체의 서비스 품질과 보증을 보장하려면 공공 부문 기관은 표준을 높게 설정하는 것이 좋습니다. 단, 표준을 지나치게 구체적으로 설정해서는 안 됩니다. 지나치게 구체적일 경우 공정 경쟁을 저해하는 방식으로 CISP 의 실격을 야기할 수 있습니다. 궁극적인 목표는 최종 사용자에게 많은 옵션을 제공하지 않으면서도 클라우드 기술의 표준을 가능한 한 높게 유지하는 것입니다.

3.0 모범 사례/교훈

아래에서는 잘 작성된 클라우드 서비스 RFP 를 통해 성공적인 클라우드 사용 기본 계약을 실현하는 방법에 대해 몇 가지 교훈을 소개합니다.

3.1 클라우드 거버넌스

클라우드 거버넌스는 공동의 책임입니다. CISP 는 클라우드 환경의 모든 측면에 클라우드 거버넌스를 내재화할 수 있는 기능과 서비스를 제공하는 한편, 고객은 기존 클라우드 거버넌스 표준을 가져와 클라우드가 클라우드 거버넌스를 어떻게 지원하는지 학습합니다.

클라우드에서 고객은 단순히 보유한 IT 환경을 관리하는 것이 아니라 원하는 IT 환경을 구축할 수 있는 기회를 얻게 됩니다. 클라우드를 통해 고객은 (1) 모든 IT 자산을 조사하여 목록화하고 (2) 이러한 모든 자산을 중앙에서 관리하고 (3) 사용량/청구/보안 등에 대한 알림을 생성할 수 있습니다. 클라우드의 이러한 주요 이점 덕분에 고객은 지속적으로 새 하드웨어를 구매하여 설치하지 않고도 아키텍처를 최적화하고 최대로는 자동화할 수 있습니다. 아키텍처를 최적화하고 자동화하는 일은 CISP 가 수행하므로 고객은 인프라 관리라는 획일적 업무에서 벗어나 미션 크리티컬 운영 업무에 집중할 수 있습니다.

CISP 클라우드를 사실상 하나의 큰 API 로 생각하면 이해하는 데 도움이 됩니다. 새 서버를 가동하거나 보안 설정을 변경하려는 경우 API 를 호출하기만 하면 됩니다. 환경에 적용된 변경 사항이 모두 로깅되고 기록됩니다. 각 변경 사항에 대해 변경자, 변경 항목, 변경 위치, 변경 시간이 기록됩니다. 기록을 통해 클라우드 거버넌스, 제어, 가시성을 확보할 수 있습니다. 이는 클라우드 환경에서만 가능합니다. 이를 통해 고객은 기존 IT 거버넌스 모델을 재고하고 클라우드가 제공하는 이점을 고려하여 기존 IT 거버넌스 모델을 간소화하고 개선할 수 있는 방법을 결정할 수 있습니다.

클라우드 거버넌스는 클라우드에 수반되는 긍정적인 프로세스 변화와 신규 기술 세트를 전달하고 통합하는 것을 의미하기도 합니다. 예를 들어 프로젝트 관리자는 IT 환경이 구축될 때까지 몇 개월을 기다리는 상황에 익숙하므로, 클라우드에서 개발 또는 테스트 환경을 구축하는 일정을 지나치게 길게 잡을 수 있습니다(클라우드를 사용하는 경우 몇 분만에 구축할 수 있음). 이처럼 새롭게 발견한 민첩성에 적응하는 일은 하나의 진화 과정이며 프로그램마다 일어납니다. 이러한 교훈을 공유하여 클라우드 사용 기본 계약이 새로운 프로세스와 민첩성에 적합한 방식으로 계속 발전할 수 있도록 해야 합니다.

3.2 클라우드의 예산 수립

공공 부문 구매 및 예산 요구 사항에 맞게 종량제 클라우드 요금을 체계화하는 데 있어서는 CISP 서비스를 **클라우드 기술** 품목 아래에 단일 품목(컴퓨팅, 스토리지, 네트워킹, 데이터베이스, IoT 등)으로 묶는 방법이 효과적입니다. 이 접근 방식은 사용자에게 기존 기술과 신규 기술을 비롯해 모든 CISP 기술을 실시간으로 제공할 수 있는 유연성을 제공하며, 사용자가 필요할 때 필요한 리소스에 빠르게 액세스할 수 있도록 합니다. 또한 변동하는 수요에 대응하여 사용률을 최적화하고 비용을 절감할 수 있게 합니다.

공공 부문 조직은 컨설팅/전문 또는 관리형 서비스, 마켓플레이스의 소프트웨어, 클라우드 지원 서비스, CISP 오퍼링 교육이 필요한 경우 클라우드 사용 기본 계약 내에 있는 다른 상세 분류의 주문에 대해 품목을 새로 추가할 수 있습니다.

적절한 리소스 범주에 선택적 계약 품목을 도입함으로써 계약 유연성을 확장하여 미래 성장에 대응할 수 있습니다. 또는 클라우드 기술을 컨설팅/전문/관리형 서비스와 함께 하나의 품목으로 묶고자 하는 조직은 '클라우드 기술 및 보조 인력' 등의 품목으로 묶을 수 있습니다.

다음은 이 접근 방식의 대표적인 예입니다. 아래 예제에서 '#1001 - 클라우드 기술' 품목의 각 단위는 사용한 '클라우드 기술'의 1.00 EUR 에 상응합니다. 매달, 현재의 사용량 예측치와 예상 사용량 예측치를 토대로 추가 주문에 대해 자금을 조달할 수 있습니다.

표 3 - 단일 품목 요금 구조의 예.

품목 번호	제품/서비스	수량	단위	단가	금액
1001	클라우드 기술	1,000	각	1 EUR	1000 EUR
1002	컨설팅 서비스	1	주간	3000 EUR	3000 EUR
1003	클라우드 지원	1	월간	1000 EUR	1000 EUR
1004	클라우드 교육	1	일간	300 EUR	3000 EUR
1005	클라우드 마켓플레이스	10	각	10 EUR	100 EUR

이 구조가 작동하는 방식의 예는 다음과 같습니다. 공공 부문 조직은 CISP 와 협력하여 조직이 사용할 클라우드 기술 서비스의 양을 추정합니다. 조직이 공급업체와의 계약 조건(예: 5 년간 1000 만 EUR, 즉 연간 200 만 EUR)에 동의합니다. 조직이 연간 200 만 EUR 의 초기 금액을 거치합니다. 매달 청구서가 발행되고 해당 자금으로 요금을 결제합니다. 해당 계좌에서 요금이 인출됩니다. CISP 모니터링 및 예측 도구를 사용하여 나머지 자금의 소진 속도를 모니터링합니다. 나머지 자금이 부족해질 경우 조직은 서비스를 유지하기 위해 투입할 수 있는 추가 자금을 CFO 에게 요청합니다.

RFP 예제: 요금 - 계약 체결

지불 조건

다음과 같이 **<고객>**에서 사용하는 리소스에 대해서만 지불하도록 지불 조건을 구성해야 합니다.

1. 월별 지불은 실제 서비스 사용량/소비량에 기반하며, CISP 의 공개 요금을 따릅니다.

최소 사용량 보장 및 최대 지출

일정 기간 동안 특정 클라우드 서비스 제공업체의 리소스가 얼마나 소비될지 **<고객>**이 정확하게 판단하기가 불가능하므로, 주문은 '클라우드 기술'이라는 단일 주문 품목의 고정 가격 단위 수량으로 지정됩니다.

주문한 품목의 각 단위는 주문한 클라우드 기술의 **<1.00 EUR>**의 가치에 해당합니다. 이 주문의 수량을 수정하는 방식으로 추가 주문을 주기적으로 넣을 수 있으므로 **<고객>**은 변동하는 기간의 요구에 대해 예상 사용량을 기반으로 CISP 클라우드 기술의 'EUR 금액' 수량을 자유롭게 선주문하는 유연성을 확보하게 됩니다. 다양한 요구 사항을 충족하는 데 사용되는 클라우드 기술의 예상 비용을 충분히 감당하는 금액 안에서 **<고객>**은 수량을 주기적으로 선주문할 수 있습니다.

품목 번호	설명	수량	단위	가격
01	CISP 클라우드 기술	1,000	각	1,000.00 EUR

최소 주문/추가 주문

<고객>의 예상 클라우드 기술 사용량을 기반으로 수량을 <10,000> 단위로 발주합니다. 이러한 방식을 사용하면 **<고객>**은 유연성을 확보함으로써 운영을 지원하는 데 필요한 만큼 '클라우드 기술'을 **<10,000>** 단위로 선주문하고 클라우드 컴퓨팅의 '종량제' 방식을 계속 따를 수 있게 됩니다.

납품 지시를 요청하면 처음에는 **<100,000>** 단위가 추가분으로 주문되며 이때 비용은 **<100,000 EUR>**입니다. 품목을 하나 이상 사용해 단일 추가 주문을 할 때 발주할 수 있는 최소 품목 단위는 **<x>**입니다. 납품 주문서에 따라 발주할 수 있는 최대 단위 수는 **<x>**를 초과할 수 없으며, 이전에 납품 지시로 주문한 단위를 모두 합친 값보다 많으면 안 됩니다. **<고객>**은 이 섹션에서 명시한 한도 내에서 발주해야 할 책임이 있습니다.

최대 주문

총 최대 주문량은 **<x>**입니다. 여기에는 단위당 가격이 **<x>**인 단일 품목을 최대 **<x>** 단위 포함되어 있습니다. 이 값은 수행 기간 동안의 **<고객>** 요구 사항에 대한 추정치를 기반으로 하지만 보장되지는 않습니다.

3.3 파트너 비즈니스 모델 이해

공공 부문 기관은 CISP 의 서비스 제공 모델을 이해하고, 컨설팅, 관리형 서비스, 재판매 등을 제공하는 파트너가 프로세스에서 얼마나 중요한지 인식해야 합니다. 많은 고객이 인프라 활용을 위해 클라우드 제공업체를 필요로 하고 있으며, '실천형' 계획 수립, 마이그레이션, 관리 업무는 시스템 통합 업체나 관리형 서비스 제공업체에 아웃소싱합니다. 이처럼 '서비스'가 혼재되어 있는 상황으로 볼 때 하도급 업체에 대한 의무 전가 조항(flow-down clause) 등 클라우드 제공업체에 적용되지 않는 요구 사항이 있을 수 있습니다.

의무 전가 조항을 이용해 왜 CISP 와 파트너, 리셀러 간의 관계를 이해해야 하는지에 대해 설명해 보겠습니다. 일부 조달 유형에는 주계약자로 하여금 일부 의무 조항을 파트너/하도급 업체에 전가하게 하는 조항이 있습니다. 일반적으로 CISP 는 표준 서비스를 대규모로 제공하므로, 즉 특정 최종 고객의 고유 요구 사항(공공 부문 계약에 따른 공공 부문 고객의 요구 포함)에 맞춤화된 서비스를 제공하지 않으므로 정식 하도급 파트너로서 대응하거나 입찰에 응하지 않습니다. 간접 조달 모델(CISP 리셀러를 통해 클라우드 서비스 조달)에서 CISP 는 상용 서비스의 '2 티어' 공급자에게는 적용되지 않는 조항이라는 이유를 들어 리셀러에 대해 이러한 조항을 거부할 수 있습니다. 이런 경우 CISP 는 계약에 따른 작업 범위를 직접 수행하지 않습니다. 대신에 CISP 파트너가 CISP 인프라를 사용하여 해당 작업을 수행합니다. 따라서 CISP 는 (하도급 업체가 아닌) 파트너 작업에 대한 상용 공급자가 됩니다. 직접 조달 모델(CISP 에게 직접 클라우드 서비스 구매)에서 CISP 는 계약 서비스의 상업적 특성상 그리고 대다수 CISP 의 경우 상용 서비스를 제공하는 데에 있어 하도급 업체를 필요로 하지 않는다는 점을 들어, 전형적 상품 하도급 업체에 적용되는 이러한 '의무' 조항을 일반적으로 거부합니다.

3.4 클라우드 브로커

클라우드 브로커를 공급업체 종속 가능성을 줄이기 위한 수단으로 이해할 경우 문제가 될 수 있습니다. 클라우드 브로커는 이론상 건전한 발상일지 모르지만 실제로는 실현되는 가치보다 야기되는 복잡성과 혼란이 더 클 수 있습니다.

여러 클라우드에서 동시에 또는 상호적으로 동작하도록 애플리케이션을 설계하려고 시도하면 필연적으로 기능 상쇄가 일어납니다. **클라우드에 로제타 스톤(문제 해결을 위한 핵심 열쇠)은 없습니다.** 이러한 접근 방식은 궁극적으로 공공 부문 고객과 클라우드 서비스 사이에 불필요한 복잡성을 더해 본래 추구하던 확보하고자 한 효율성과 보안상 이점이 훼손되고 그 결과 확장성 및 민첩성 저하, 비용 증가, 혁신 감속이 야기될 수 있습니다.

3.5 사전 RFP 소싱/시장 조사

공공 부문 기관은 클라우드 서비스 RFP 를 계획할 때 프로세스의 시작부터 고위 경영진, 비즈니스 이해관계자, 기술, 금융, 조달, 법률 및 계약 등 전 조직의 이해관계자를 포함시켜야 합니다. 이러한 접근 방식을 통해 모든 이해관계자가 클라우드 모델을 이해하고, 결과적으로 기존의 IT 조달 방법을 재평가할 수 있게 됩니다.

업계와의 대화와 관련해서는 공공 부문 기관이 심층 대화를 통해 CISP, CISP 파트너, PaaS/SaaS 마켓플레이스 공급업체, 업계 전문가 등 업계의 의견을 수렴하는 시간을 갖기를 적극 권장합니다. 예를 들어 업계와의 대화는 산업의 날, 보안 및 조달 워크숍과 같은 형태일 수 있습니다. 클라우드 조달에 대한 이해도를 높일 수 있는 또 다른 효과적인 방법은 RFI 를 발행하거나 이상적으로는 RFP 문서 초안을 발행하는 것입니다. 많은 경우 클라우드 서비스 RFP 최종본을 발행하기 전에 잠재적 문제를 식별, 논의, 조정할 수 있습니다.

3.6 지속 가능성

지속 가능성은 클라우드 컴퓨팅에 내재되어 있으며, 클라우드로 전환하면 온프레미스 서버나 엔터프라이즈 데이터 센터에 비해 에너지 효율성이 향상됩니다. 지속 가능성을 우선시하고 지속 가능성 목표 달성의 의지를 천명한 CISP 를 파악하면 클라우드가 지속 가능성을 더 확고히 할 수 있습니다. 데이터 센터 산업이 따라야 할 명료하고 간단하며 영향력 있는 지속 가능성 기준을 확립하고 데이터 센터 운영업체와 클라우드 서비스 제공업체가 2030 년까지 기후 중립을 달성하도록 보장하기 위해 유럽 CISP 와 데이터 센터 운영업체는 유럽 위원회의 지원 아래 자율 규제 이니셔티브인 기후 중립 데이터 센터 협약[11]을 제정했습니다. 기후 중립 데이터 센터 협약에서는 데이터 센터 에너지 효율성, 용수 보전, 서버 재사용 및 수리, 무탄소 에너지를 이용한 데이터 센터 전원 공급에 대해 명확한 목표를 제시합니다. 기후 중립 데이터 센터 협약에 참여하는 CISP 는 이러한 목표를 달성하고 기후 중립 운영업체 간주 기준 따라 인증을 받는 데에 동의합니다.

클라우드 서비스 RFP 에서는 CISP 에 기준 이행 여부, 특히 CISP 의 자율 규제 참여 여부와 약정 이행 시기에 대한 질문을 해야 합니다.

RFP 예제: 지속 가능성

기후 중립 데이터 센터 자율 규제 이니셔티브에 서명하여 기후 중립 데이터 센터를 운영하기로 약속했습니까? 그렇다면 언제 서명했습니까?

사용을 위해 기후 중립 데이터 센터 협약 인장을 획득했다는 증거를 제시할 수 있습니까?

[11] https://www.climateneutraldatacentre.net/self-regulatory-initiative/

부록 A – 입찰자 간 비교를 위한 기술 요구 사항

다음은 기본 계약에 따라 납품 지시 또는 소수 경쟁을 시행하는 동안 CISP 를 비교하는 데에 사용할 수 있는 일반적인 클라우드 기술 요구 사항입니다.

1. 클라우드 제공업체 프로필

	요구 사항
1.	**시장 경험:** 클라우드 시장 부문에서 비즈니스를 운영한지 얼마나 되었습니까?
2.	**개방성 및 데이터 보호:** 데이터 보호 산업 행동 강령 또는 가역성 산업 행동 강령을 준수합니까? 오픈 소스 및 오픈 API 개발 원칙을 준수합니까?

2. 글로벌 인프라

	요구 사항
1.	**글로벌 기반:** 사용자의 지연 시간은 줄이면서 스루풋은 늘릴 수 있는 글로벌 인프라를 제공합니까?
2.	**리전:** 원하는 지역에 리전을 보유하고 있습니까?
3.	**도메인/영역:** 도메인 또는 영역의 개념을 구현하고 있습니까? 즉, 복수의 데이터 센터를 저지연 네트워크를 통해 그룹화하여 고가용성과 고내결함성을 제공하고 있습니까? • 구현하고 있는 경우, 원하는 지역에 있는 도메인 또는 영역의 수와 데이터 센터의 수를 기입하세요.
4.	**도메인/영역 거리:** 이중화, 고가용성, 저지연성을 지원하기 위해 물리적으로 분리되어 있는 데이터 센터를 통해 도메인 또는 영역을 구축하고 있습니까?
5.	**데이터 센터 구축:** 다른 데이터 센터에 장애가 발생해도 영향이 없도록 이중 전력, 냉각, 네트워크 설비를 갖춘 데이터 센터를 제공합니까?

6.	**데이터 센터 복제:** 자동 장애 조치 기능을 갖춘 도메인 또는 영역의 데이터 센터에서 데이터 복제를 제공합니까?
7.	**도메인/영역 복제:** 리전 내 도메인 또는 영역에서 데이터 복제를 제공합니까?

3. 인프라

3.1 컴퓨팅

	요구 사항
1.	**컴퓨팅 – 일반 인스턴스 – 범용:** 다음 인스턴스 유형을 제공합니까? • 범용 - 일반 애플리케이션에 최적화되어 있으며, 컴퓨팅, 메모리, 네트워크 리소스를 균형 있게 제공합니다. ○ 제공하는 경우, 가장 큰 인스턴스는 무엇입니까?
2.	**컴퓨팅 – 일반 인스턴스 – 메모리 최적형:** 다음 인스턴스 유형을 제공합니까? • 메모리 최적형 - 메모리 집약적 애플리케이션에 최적화되었습니다. ○ 제공하는 경우, 가장 큰 인스턴스는 무엇입니까?
3.	**컴퓨팅 – 일반 인스턴스 – 컴퓨팅 최적형:** 다음 인스턴스 유형을 제공합니까? • 컴퓨팅 최적형 - 컴퓨팅 집약적 애플리케이션에 최적화되었습니다. ○ 제공하는 경우, 가장 큰 인스턴스는 무엇입니까?
4.	**컴퓨팅 – 일반 인스턴스 – 스토리지 최적형:** 다음 인스턴스 유형을 제공합니까? • 스토리지 최적형 - 대용량의 로컬 스토리지를 제공합니다. ○ 제공하는 경우, 스토리지 용량(5, 10, 20, 50TB)을 최대 얼마까지 프로비저닝하고 디스크(HDD/SSD)를 최대 몇 개까지 인스턴스에 연결할 수 있습니까?

5.	**컴퓨팅 – 일반 인스턴스 – 그래픽 최적형:** 다음 인스턴스 유형을 제공합니까? • 저비용 그래픽 - 컴퓨팅 인스턴스에 저비용 그래픽 가속화를 제공합니다. o 제공하는 경우, 가장 큰 인스턴스는 무엇입니까?
6.	**컴퓨팅 – 일반 인스턴스 – GPU 최적형:** 다음 인스턴스 유형을 제공합니까? • GPU - 그래픽 집약적 애플리케이션을 위한 하드웨어 그래픽 처리 장치(GPU)를 제공합니다. o 제공하는 경우, 클라우드 제공업체는 GPU 를 인스턴스당 몇 개 제공할 수 있으며, 어떤 GPU 모델을 제공할 수 있습니까?
7.	**컴퓨팅 – 일반 인스턴스 – FPGA 최적형:** 다음 인스턴스 유형을 제공합니까? • FPGA - 애플리케이션에 맞는 맞춤형 하드웨어 가속화를 개발하고 배포할 수 있도록 FPGA(필드 프로그래머블 게이트 어레이)를 제공합니다. o 제공하는 경우, 클라우드 제공업체는 FPGA 를 인스턴스당 몇 개까지 제공할 수 있습니까?
8.	**컴퓨팅 – 성능 순간 확장 가능 인스턴스:** 기준치의 CPU(중앙 처리 장치) 성능을 제공하다가 기준치 이상으로 성능을 확장할 수 있는 성능 순간 확장 가능 인스턴스를 제공합니까? • 제공하는 경우, 가장 큰 성능 순간 확장 가능 인스턴스는 무엇입니까?
9.	**컴퓨팅 – IO 집약적 인스턴스:** 저지연, 초고도의 임의 I/O 성능, 고도의 순차 읽기 스루풋을 실현하는 데에 최적화된 NVMe SSD 를 사용하는 인스턴스를 제공합니까? • 제공하는 경우 가장 큰 인스턴스의 IOPS(초당 입출력 작업 처리량) 용량은 최대 얼마입니까?
10.	**컴퓨팅 – 임시 로컬 스토리지:** 변경이 잦은 정보를 저장할 임시 스토리지로 사용할 수 있도록 컴퓨팅 인스턴스에서 로컬 스토리지를 지원합니까?
11.	**컴퓨팅 – 다중 NIC 지원:** 인스턴스에 NIC(네트워크 인터페이스 카드)를 여러 개(기본 및 보조) 할당할 수 있도록 지원합니까? • 지원하는 경우, NIC 는 인스턴스당 최대 몇 개까지 할당할 수 있습니까?
12.	**컴퓨팅 – 인스턴스 친화도:** 사용자에게 같은 데이터 센터에 있는 인스턴스끼리 논리적으로 그룹화할 수 있는 기능을 제공합니까?

13.	**컴퓨팅 – 인스턴스 반친화도:** 사용자에게 인스턴스를 논리적으로 그룹화하고 이를 리전의 다른 데이터 센터에 배치할 수 있는 기능을 제공합니까?
14.	**컴퓨팅 – 셀프서비스 프로비저닝:** 프로그래밍 방식의 인터페이스, 관리 콘솔 또는 웹 포털을 통해 인스턴스 여러 개를 동시에 프로비저닝할 수 있는 셀프서비스 기능을 제공합니까?
15.	**컴퓨팅 – 사용자 지정:** 사용자 지정 가능한 인스턴스를 제공합니까? 즉, vCPU(가상 중앙 처리 장치), RAM 등의 구성 설정을 변경할 수 있는 기능을 제공합니까?
16.	**컴퓨팅 - 테넌시** 단일 사용자 전용 하드웨어에서 실행되는 단일 테넌트 인스턴스를 제공합니까? • 제공하는 경우, 사용 가능한 가장 큰 단일 테넌트 인스턴스는 무엇입니까?
17.	**컴퓨팅 – 호스트 친화도:** 인스턴스를 가동하고 해당 인스턴스가 항상 같은 물리적 호스트에서 재가동되도록 지정하는 기능을 제공합니까?
18.	**컴퓨팅 – 호스트 반친화도:** 특정 인스턴스를 다른 물리적 호스트에서 분리하여 호스팅할 수 있는 기능을 제공합니까?
19.	**컴퓨팅 – 오토 스케일링:** 수요가 급격하게 증가할 경우 성능을 유지하기 위해 인스턴스의 수를 자동으로 늘릴 수 있는 기능(즉, '스케일 아웃')을 제공합니까?
20.	**컴퓨팅 – 이미지 가져오기 메커니즘:** 사용자에게 기존 이미지를 가져와서 향후 인스턴스 프로비저닝에 사용할 수 있는 새 비공개 이미지로 저장하는 기능을 제공합니까? • 제공하는 경우, 어떤 형식이 지원됩니까?
21.	**컴퓨팅 – 이미지 내보내기 메커니즘:** 실행 중인 기존 인스턴스 또는 인스턴스 사본을 가져와서 인스턴스를 가상 머신 형식으로 내보내는 기능을 지원합니까? • 제공하는 경우, 어떤 형식이 지원됩니까?
22.	**컴퓨팅 – 서비스 중단:** 호스트 수준에서 하드웨어 또는 서비스 유지 보수 작업을 진행하는 동안 인스턴스 가동 중단을 방지하는 메커니즘을 제공합니까?

23.	**컴퓨팅 – 인스턴스 재가동:** 물리적 호스트에서 장애가 발생하는 경우 정상 작동 중인 호스트에서 인스턴스를 자동으로 재가동하는 메커니즘을 제공합니까?
24.	**컴퓨팅 – 알림:** 컴퓨팅 복원 이벤트가 발생하는 경우 해당 이벤트에 대해 알리는 기능을 보유하고 있습니까? 또한 사용자가 셀프서비스 수단을 사용해 알림을 활성화하거나 비활성화할 수 있습니까?
25.	**컴퓨팅 – 이벤트 예약:** 사용자의 인스턴스에 대해 인스턴스 재가동, 중지, 가동, 폐지 등의 이벤트를 예약할 수 있는 기능을 제공합니까?
26.	**컴퓨팅 – 메커니즘 백업 및 복원:** 통합 백업 및 복원 메커니즘을 제공합니까?
27.	**컴퓨팅 – 스냅샷 메커니즘:** 수동 온디맨드 스냅샷 메커니즘을 제공합니까?
28.	**컴퓨팅 – 메타데이터:** 사용자에게 인스턴스에 대해 임의의 키-값 페어를 설정할 수 있는 인스턴스 메타데이터 서비스를 제공합니까?
29.	**컴퓨팅 – 메타데이터 호출:** 인스턴스가 자체 정보를 찾기 위해 호출할 수 있는 API(애플리케이션 프로그래밍 인터페이스)를 제공하는 인스턴스 메타데이터 서비스를 제공합니까?
30.	**컴퓨팅 – 입찰 메커니즘:** 비미션 크리티컬 워크로드를 호스팅하기 위해 즉시 인스턴스화할 수 있는 저비용 인스턴스 입찰에 대한 입찰 메커니즘을 제공합니까?
31.	**컴퓨팅 – 정기 예약 메커니즘:** 주기적(매일, 매주, 매월)으로 추가 컴퓨팅 용량을 예약하여 확보할 수 있는 방법을 제공합니까?
32.	**컴퓨팅 – 사전 확보 메커니즘:** 차후(1 년, 2 년, 3 년 등)를 위해 추가 컴퓨팅 용량을 확보할 수 있는 방법을 제공합니까?
33.	**컴퓨팅 – LINUX 운영 체제:** 엔터프라이즈 Linux 배포판(Red Hat, SUSE 등)나 일반 무료 Linux 배포판(Ubuntu, CentOS, Debian 등)의 최신 두 개 장기 지원 버전을 지원합니까? 엔터프라이즈 Linux 배포판과 일반 무료 Linux 배포판 중 적어도 하나는 지원해야 합니다.
34.	**컴퓨팅 – WINDOWS 운영 체제:** Windows Server 의 최신 두 개 주요 버전(Windows Server 2017 및 Windows Server 2016)을 지원합니까?

35.	**컴퓨팅 – 라이선스 이식성:** 라이선스 이식성과 지원을 제공합니까? • 제공하는 경우, 소프트웨어 공급업체, 소프트웨어 이름, 버전 및 해당 버전을 기입하세요.
36.	**컴퓨팅 – 서비스 한도:** 위의 컴퓨팅 섹션과 관련해 제한(서비스 한도)을 두고 있습니까? 예: 계정당 최대 인스턴스 개수 계정당 최대 전용 호스트 개수 예약된 IP 주소의 최대 개수

3.2 네트워킹

	요구 사항
1.	**네트워킹 – 가상 네트워크:** 클라우드 내 기업의 자체 네트워크를 나타내는 논리적으로 격리된 가상 네트워크를 생성할 수 있는 기능을 지원합니까?
2.	**네트워킹 – 같은 리전 연결:** 같은 리전에 있는 두 개의 가상 네트워크를 연결해 프라이빗 IP 주소로 해당 네트워크 간에 트래픽을 라우팅하는 기능을 지원합니까?
3.	**네트워킹 – 다른 리전 연결:** 서로 다른 리전에 있는 두 개의 가상 네트워크를 연결해 프라이빗 IP 주소로 해당 네트워크 간에 트래픽을 라우팅하는 기능을 지원합니까?
4.	**네트워킹 – 프라이빗 서브넷:** 퍼블릭 IP 주소나 인터넷 라우팅 없이 인스턴스를 프로비저닝할 수 있는 완전히 격리된(프라이빗) 가상 네트워크 및 서브넷을 생성하는 기능을 제공합니까?
5.	**네트워킹 – 가상 네트워크 주소 범위:** RFC(Request For Comments) 1918 에 정의된 IP 주소 범위와 공개 라우팅이 가능한 CIDR(Classless Inter-Domain Routing) 블록을 지원합니까?
6.	**네트워킹 – 다중 프로토콜:** TCP(전송 제어 프로토콜), UDP(사용자 데이터그램 프로토콜), ICMP(인터넷 제어 메시지 프로토콜)를 포함한 다중 프로토콜을 지원합니까?

7.	**네트워킹 – IP 주소 자동 할당:** 퍼블릭 IP 주소를 인스턴스에 자동으로 할당하는 기능을 지원합니까?
8.	**네트워킹 – 고정 IP 주소 예약:** 특정 인스턴스가 아닌 사용자 계정에 연결된 IP 주소를 지원합니까? IP 주소는 명시적으로 해제하기 전까지 연결된 채로 유지되어야 합니다.
9.	**네트워킹 – IPV6 지원:** 클라우드 제공업체가 게이트웨이 또는 인스턴스 수준에서 IPv6 을 지원하고 이 기능을 사용자에게 공개합니까?
10.	**네트워킹 – NIC 당 다중 IP 주소:** 특정 인스턴스에 연결된 NIC(네트워크 인터페이스 카드)에 기본 IP 주소와 보조 IP 주소를 할당할 수 있는 기능을 지원합니까?
11.	**네트워킹 – 다중 NIC:** 특정 인스턴스에 복수의 NIC(네트워크 인터페이스 카드)를 할당하는 기능을 제공합니까?
12.	**네트워킹 – NIC 및 IP 이동성:** 인스턴스 간에 NIC(네트워크 인터페이스 카드)와 IP 주소를 이동하는 기능을 지원합니까?
13.	**네트워킹 – SR-IOV 지원:** 성능, 지연성, 지터 개선을 위해 SR-IOV(단일 루트 I/O 가상화) 등의 기능을 지원합니까?
14.	**네트워킹 – 입구 필터링:** 인스턴스로 들어오는 인바운드 트래픽(유입)에 적용되는 규칙을 추가하거나 제거할 수 있도록 지원합니까?
15.	**네트워킹 – 출구 필터링:** 인스턴스에서 나가는 아웃바운드 트래픽(유출)에 적용되는 규칙을 추가하거나 제거할 수 있도록 지원합니까?
16.	**네트워킹 – ACL:** 서브넷의 인바운드 트래픽과 아웃바운드 트래픽을 제어할 수 있도록 ACL(액세스 제어 목록)을 제공합니까?
17.	**네트워킹 – 흐름 로그 지원:** 네트워크 트래픽 흐름 로그를 캡처할 수 있는 기능을 제공합니까?
18.	**네트워킹 – NAT:** 이 클라우드 네트워크는 프라이빗 네트워크에 있는 인스턴스에서는 인터넷이나 다른 클라우드 서비스에 접속할 수 있지만 인터넷에서는 인스턴스에 접속하지 못하게 하는 NAT(네트워크 주소 변환) 게이트웨이 관리형 서비스를 제공합니까?

19.	**네트워킹 - 출발지/목적지 확인:** NIC(네트워크 인터페이스 카드)에서 출발지/목적지 확인을 비활성화하는 기능을 보유하고 있습니까?
20.	**네트워킹 – VPN 지원:** 클라우드 제공업체와 사용자 데이터 센터 간의 VPN(가상 프라이빗 네트워크) 연결을 지원합니까?
21.	**네트워킹 – VPN 터널:** 가상 네트워크에 VPN(가상 프라이빗 네트워크) 연결을 여러 개 구축할 수 있도록 지원합니까?
22.	**네트워킹 – IPsec VPN 지원:** 사용자가 퍼블릭 인터넷에서 IPsec VPN 터널이나 SSL VPN 터널을 통해 클라우드 서비스에 액세스할 수 있도록 허용합니까?
23.	**네트워킹 – BGP 지원:** IPsec VPN 터널에서 장애 조치를 개선하기 위해 BGP(경계 경로 프로토콜)를 사용합니까?
24.	**네트워킹 – 프라이빗 전용 연결:** 대량의 데이터를 빠르게 전송할 수 있도록 클라우드 제공업체의 위치와 사용자의 데이터 센터, 사무실 또는 콜로케이션 환경 간에 프라이빗 직접 연결 서비스를 제공합니까?
25.	**네트워킹 – 프런트엔드 로드 밸런서:** 인터넷을 통해 클라이언트로부터 요청을 받아 이들 요청을 로드 밸런서에 등록된 인스턴스에 배포하는 프런트엔드(인터넷 연결) 로드 밸런싱 서비스를 제공합니까?
26.	**네트워킹 – 백엔드 로드 밸런서:** 트래픽을 프라이빗 서브 넷에서 호스팅되는 인스턴스로 라우팅하는 백엔드(프라이빗) 로드 밸런싱 서비스를 제공합니까?
27.	**네트워킹 – 7 계층 로드 밸런서:** 여러 인스턴스에 네트워크 트래픽을 분산할 수 있는 7 계층(하이퍼텍스트 전송 프로토콜, HTTP) 로드 밸런서 서비스를 제공합니까?
28.	**네트워킹 – 4 계층 로드 밸런서:** 여러 인스턴스에 네트워크 트래픽을 분산할 수 있는 4 계층(전송 제어 프로토콜, TCP) 로드 밸런서 서비스를 제공합니까?
29.	**네트워킹 – 로드 밸런서의 세션 친화도:** 세션 친화도를 지원하는 로드 밸런싱 서비스를 제공합니까?
30.	**네트워킹 – DNS 기반 로드 밸런싱:** 단일 도메인에 속한 여러 호스트에서 호스팅되는 인스턴스에 대해 트래픽의 로드 밸런싱을 지원하는 로드 밸런싱 서비스를 제공합니까?

31.	**네트워킹 – 로드 밸런서 로그:** 로드 밸런서로 보낸 모든 요청에 대한 상세 정보를 담고 있는 로그를 제공합니까?
32.	**네트워킹 – DNS:** 가용성과 확장성이 뛰어난 도메인 이름 시스템(DNS) 서비스를 제공합니까?
33.	**네트워킹 – 지연 시간 기반 DNS 라우팅:** 지연 시간 기반 라우팅을 지원하는 DNS(도메인 이름 시스템) 서비스, 즉 최상의 지연성을 제공하는 리소스를 사용해 DNS 쿼리에 응답하는 DNS 서비스를 제공합니까?
34.	**네트워킹 – 지역 기반 DNS 라우팅:** 지역 기반 라우팅을 지원하는 DNS(도메인 이름 시스템) 서비스, 즉 사용자의 지리적 위치를 기반으로 DNS 쿼리에 응답하는 DNS 서비스를 제공합니까?
35.	**네트워킹 – 장애 조치 기반 DNS 라우팅:** 장애 조치 기반 라우팅을 지원하는 DNS(도메인 이름 시스템) 서비스를 제공합니까? 즉, 해당 시점에 활성 상태인 리소스로 DNS 쿼리를 라우팅하는 DNS 서비스를 제공하고 기본 리소스에 장애가 발생하면 평소 대기 상태로 있던 보조 리소스가 활성 상태로 전환됩니까?
36.	**네트워킹 – 도메인 등록 서비스:** 도메인 이름 등록 서비스를 제공합니까? 즉, 사용자가 사용 가능한 도메인 이름을 검색하고 등록할 수 있습니까?
37.	**네트워킹 – DNS 건전성 점검:** 건전성 점검을 사용해 리소스의 건전성과 성능을 모니터링하는 DNS(도메인 이름 시스템) 서비스를 제공합니까?
38.	**네트워킹 – DNS 및 로드 밸런서 통합:** 클라우드 제공업체의 로드 밸런서와 통합되는 DNS(도메인 이름 시스템) 서비스를 제공합니까?
39.	**네트워킹 – 가상 편집기:** 트래픽 관리 정책을 구축할 수 있는 도구를 사용자에게 제공합니까?
40.	**콘텐츠 전송 네트워크(CDN):** 짧은 지연 시간과 높은 데이터 전송 속도로 콘텐츠를 배포할 수 있는 CDN(콘텐츠 전송 네트워크) 서비스를 제공합니까?
41.	**네트워킹 – CDN 캐시 만료:** 객체 비활성화, 객체 버전 관리 기능 등을 비롯해 엣지 캐시가 만료되기 전에 엣지 캐시에서 객체를 제거할 수 있는 CDN(콘텐츠 전송 네트워크) 서비스를 제공합니까?

42.	**네트워킹 – CDN 외부 오리진:** 사용자 지정 오리진, 즉 HTTP 서버를 지원하는 CDN(콘텐츠 전송 네트워크) 서비스를 제공합니까?
43.	**네트워킹 – CDN 최적화:** 여러 오리진 서버의 구성과 서로 다른 URL 의 캐시 속성을 세세하게 제어할 수 있는 CDN(콘텐츠 전송 네트워크) 서비스를 제공합니까?
44.	**네트워킹 – CDN 지리 제한:** 지리적 제한을 지원하는 콘텐츠 전송 네트워크(CDN) 서비스를 제공합니까? 즉, 특정 지역의 사용자는 콘텐츠에 액세스하지 못하게 제한합니까?
45.	**네트워킹 – CDN 토큰:** 사용자가 콘텐츠에 대한 액세스 제어를 강화할 수 있도록 일반적으로 만료 날짜/시간 등의 부가 정보가 담긴 서명 URL 을 지원하는 CDN(콘텐츠 전송 네트워크) 서비스를 제공합니까?
46.	**네트워킹 – CDN 인증서:** 엣지 로케이션에서 HTTPS 를 통해 콘텐츠를 안전하게 전송하기 위해 사용자 지정 SSL 인증서를 지원하는 CDN(콘텐츠 전송 네트워크) 서비스를 제공합니까?
47.	**네트워킹 – CDN 멀티 티어 캐시:** 지연 시간을 줄이기 위해 리전 엣지 캐시를 사용하여 다중 티어 캐시 접근 방식을 사용하는 콘텐츠 전송 네트워크(CDN) 서비스를 제공합니까?
48.	**네트워킹 – CDN 압축:** 파일 압축을 지원하는 CDN(콘텐츠 전송 네트워크) 서비스를 제공합니까?
49.	**네트워킹 – CDN 암호화 업로드:** 사용자의 오리진 인프라에 있는 특정 구성 요소 및 서비스에서만 정보를 볼 수 있는 방식으로 사용자가 민감한 데이터를 안전하게 업로드할 수 있게 하는 CDN(콘텐츠 전송 네트워크) 서비스를 제공합니까?
50.	**네트워킹 – 엔드포인트:** 통신 비용을 줄이고 트래픽 보안을 개선하기 위해 클라우드 제공업체의 네트워킹 서비스에서 사용자에게 제공업체의 내부 네트워크 연결(즉, 프라이빗 연결)을 통해 트래픽을 라우팅할 수 있는 엔드포인트를 제공합니까?
51.	**네트워킹 – 서비스 한도:** 위의 네트워킹 섹션과 관련해 제한(서비스 한도)을 두고 있습니까? 예: 계정당 최대 가상 네트워크 개수 가상 네트워크의 최대 크기

	계정당 최대 서브넷 개수 계정당 최대 로드 밸런서 개수 최대 액세스 제어 목록(ACL) 항목 개수 최대 가상 프라이빗 네트워크(VPN) 터널 개수 배포당 최대 오리진 개수 로드 밸런서당 최대 인증서 개수

3.3 스토리지

	요구 사항
1.	**블록 스토리지 서비스:** 컴퓨팅 인스턴스에서 사용할 수 있는 블록 수준의 스토리지 볼륨을 제공합니까?
2.	**블록 스토리지 – IOPS:** 블록 스토리지의 구매 옵션을 제공할 때 성능 측정 단위인 IOPS 나 MB/S 등을 이용해 성능 목표나 성능 등급을 명확하게 제시합니까?
3.	**블록 스토리지 – SSD:** 지연 시간이 10 밀리초 미만인 SSD 지원 스토리지 미디어를 지원합니까? • 지원하는 경우, 인스턴스당 SSD 를 최대 몇 개까지 연결할 수 있습니까?
4.	**블록 스토리지 - 확장:** 사용자에게 새 볼륨을 프로비저닝하여 데이터를 복사/이동하는 대신 기존 블록 스토리지 볼륨의 크기를 늘릴 수 있는 기능을 제공합니까?
5.	**블록 스토리지 - 스냅샷:** 블록 스토리지 서비스를 위한 스냅샷 기능을 보유하고 있습니까?
6.	**블록 스토리지 – 데이터 폐기:** 권한이 없는 사용자 및/또는 제 3 자가 더 이상 데이터를 읽거나 액세스하지 못하도록 데이터를 영구 폐기하는 기능을 지원합니까?
7.	**블록 스토리지 – 저장 데이터 암호화:** 볼륨 및 스냅샷에 저장된 데이터에 대해 서버 측 저장 데이터 암호화 기능을 제공합니까? • 해당하는 경우, 어떤 암호화 알고리즘이 사용됩니까?
8.	**객체 스토리지 서비스:**

	웹상의 데이터를 그 양에 관계없이 저장하고 불러올 수 있도록 보안, 내구성, 고확장성을 갖춘 객체 스토리지를 제공합니까?
9.	**객체 스토리지 – 저빈도 액세스:** 액세스 빈도가 적은 객체와 파일을 위한 저비용 스토리지 서비스 티어를 지원합니까?
10.	**객체 스토리지 – 낮은 내구성:** 사용자가 중요도가 떨어지고 쉽게 재현 가능한 객체를 저렴하게 저장할 수 있도록 이중화 정도를 낮춘 티어를 제공합니까?
11.	**객체 스토리지 – 저빈도 액세스:** 액세스 빈도는 적지만 액세스 속도는 빨라야 하는 데이터를 위한 티어를 제공합니까?
12.	**객체 스토리지 – 객체 계층화:** 객체 스토리지 계층화 기능(액세스 빈도에 따라 객체 스토리지 클래스 또는 계층 간에 객체를 전환할 것을 권장할 수 있는 기능)을 제공합니까?
13.	**객체 스토리지 – 수명 주기 관리:** 객체를 생성해서 삭제하기까지, 즉 객체의 생애 동안 객체를 어떻게 관리할지 정의하는 수명 주기 구성을 사용해 객체의 수명 주기 관리를 지원합니까?
14.	**객체 스토리지 – 정책 기반 관리:** 저장 데이터, 데이터 수명 주기, 데이터 등급 설정을 관리하는 정책을 생성하고 관리할 수 있는 기능을 제공합니까?
15.	**객체 스토리지 - 위치 및 시간 기반 정책:** 사용자에게 사용자의 위치와 요청 시간에 기반하여 데이터에 대한 액세스를 제한하는 정책을 생성할 수 있는 기능을 제공합니까?
16.	**객체 스토리지 – 웹사이트 호스팅:** 객체 스토리지 서비스에서 정적 웹 사이트 호스팅을 지원합니까?
17.	**객체 스토리지 – 저장 데이터 암호화:** 제공업체가 관리하는 암호화 키를 사용해 저장 데이터에 대해 서버 측 암호화(SSE)를 지원합니까? • 해당하는 경우, 어떤 암호화 알고리즘이 사용됩니까?
18.	**객체 스토리지 – 사용자 키로 암호화:** 고객 제공 암호화 키를 사용하는 서버 측 암호화(SSE) 기능을 제공합니까?
19.	**객체 스토리지 - 키 관리 서비스:** 암호화 키를 생성하고 키 사용을 제어하는 정책을 정의하고, 키가 제대로 사용되고 있는지 입증하기 위해 키 사용을 감사하는 키 관리 서비스를 사용해 서버 측 암호화(SSE)를 지원합니까?

20.	**객체 스토리지 – 클라이언트 측 마스터 키:** 사용자에게 암호화 키를 제어하고 클라이언트 측 객체의 암호화/복호화를 완료할 수 있는 기능을 제공합니까?
21.	**객체 스토리지 – 강력한 일관성:** 새 객체의 PUT 작업에 대해 쓰기 후 읽기 일관성을 지원합니까?
22.	**객체 스토리지 - 데이터 지역성:** 엄격한 리전 격리를 제공합니까? 즉, 리전에 저장된 객체는 사용자가 명시적으로 객체를 다른 리전으로 전송하지 않는 한 해당 리전을 벗어나지 않습니까?
23.	**객체 스토리지 - 복제:** 사용자가 선택한 리전들에 객체를 자동으로 복제하는 교차 리전 복제 기능을 제공합니까?
24.	**객체 스토리지 - 버전 관리:** 이 클라우드 공급자는 버전 관리, 즉 객체의 여러 버전을 저장하고 관리하는 기능을 지원합니까?
25.	**객체 스토리지 - 삭제 불가 표시:** 사용자가 항목을 삭제 불가로 표시할 수 있도록 허용합니까?
26.	**객체 스토리지 - MFA 삭제:** 추가 보안 옵션으로 작업 삭제에 대해 다중 인증(MFA)을 지원합니까?
27.	**객체 스토리지 – 멀티파트 업로드:** 객체를 부분의 합으로 업로드하도록 허용합니까? 즉, 객체 데이터를 쪼개서 이를 임의의 순서로 따로 업로드할 수 있도록 허용합니까?
28.	**객체 스토리지 - 태그:** 변경 가능한 동적 태그를 객체 수준에서 생성하고 결부하는 기능을 제공합니까?
29.	**객체 스토리지 - 알림:** 객체 수준에서 특정 이벤트, 즉 추가/삭제 작업이 발생하면 알림을 전송하는 기능을 제공합니까?
30.	**객체 스토리지 - 로그:** 요청자, 요청 시간, 요청 작업, 응답 상태, 오류 코드 등 단일 액세스 요청에 관한 세부 정보가 담긴 감사 로그를 생성하는 기능을 제공합니까?
31.	**객체 스토리지 – 객체 인벤토리:** 사용자가 빠르게 객체와 객체 상태를 시각화하고 퍼블릭 액세스를 통해 객체를 빠르게 찾을 수 있도록 지원하는 객체 인벤토리 기능을 제공합니까?

32.	**객체 스토리지 – 메타데이터 인벤토리:** 사용자가 빠르게 객체의 메타데이터를 시각화할 수 있도록 지원하는 객체 인벤토리 기능을 제공합니까?
33.	**객체 스토리지 – 업로드 최적화:** 최적화된 네트워크 경로를 사용해 엣지 로케이션에서 스토리지 서비스로 데이터를 라우팅하는 기능을 보유하고 있습니까?
34.	**객체 스토리지 – 쿼리 기능:** 사용자에게 SQL(구조화 질의 언어) 문을 사용해 객체 스토리지 서비스에 쿼리할 수 있는 기능을 제공합니까?
35.	**객체 스토리지 – 하위 집합 검색:** 사용자에게 SQL(구조화 질의 언어) 표현식을 사용해 객체에서 데이터의 하위 집합만 검색할 수 있는 기능을 제공합니까?
36.	**파일 스토리지 서비스:** 클라우드의 컴퓨팅 인스턴스에서 사용할 수 있는 간단하고 확장 가능한 파일 스토리지 서비스를 제공합니까?
37.	**파일 스토리지 – 이중화:** 고도의 가용성과 내구성을 실현할 수 있도록 여러 데이터 센터 또는 시설에 파일 시스템 객체(즉, 디렉터리, 파일, 링크)를 저장합니까?
38.	**파일 스토리지 – 데이터 폐기:** 권한이 없는 사용자 및/또는 제 3 자가 더 이상 파일 스토리지 데이터를 읽거나 액세스하지 못하도록 데이터를 영구 폐기하는 기능을 지원합니까?
39.	**파일 스토리지 – 고가용성:** 클라우드 제공업체의 관리형 파일 시스템에서 고도의 고가용성을 제공합니까?
40.	**파일 스토리지 – NFS:** NFS(네트워크 파일 시스템) 프로토콜을 지원합니까?
41.	**파일 스토리지 – SMB:** SMB(서버 메시지 블록) 프로토콜을 지원합니까?
42.	**파일 스토리지 – 저장 데이터 암호화:** 클라우드 제공업체의 파일 스토리지 서비스에서 저장 데이터 암호화 기능을 지원합니까?
43.	**파일 스토리지 – 전송 중 암호화:** 클라우드 제공업체의 파일 스토리지 서비스에서 전송 중 데이터 암호화 기능을 지원합니까?

44.	**파일 스토리지 – 데이터 마이그레이션 도구:** 사용자가 온프레미스 시스템에서 클라우드 기반 파일 시스템으로 데이터를 이전하는 데 사용할 수 있는 데이터 마이그레이션 도구를 제공합니까?
45.	**아카이브 스토리지 서비스:** 액세스 빈도가 적고 거의 변경 불가능한 객체와 파일을 보관하기 위한 저비용 스토리지 서비스를 제공합니까?
46.	**아카이브 스토리지 - 내결함성:** 클라우드 제공업체의 아키텍처에서 아카이브 스토리지 서비스에 대해 내결함성을 제공합니까?
47.	**아카이브 스토리지 - 불변성:** 보관된 객체와 파일의 불변성을 지원합니까?
48.	**아카이브 스토리지 – WORM:** WORM(Write Once Read Many) 기능을 제공합니까?
49.	**아카이브 스토리지 – 하위 집합 검색:** 사용자에게 SQL(구조화 질의 언어) 표현식을 사용해 보관된 객체에서 데이터의 하위 집합만 검색할 수 있는 기능을 제공합니까?
50.	**아카이브 스토리지 – 검색 속도:** 비용과 검색 시간을 다양하게 조합해 만든 데이터 검색 옵션을 사용자에게 제공합니까?
51.	**아카이브 스토리지 – 저장 데이터 암호화:** 클라우드 제공업체의 아카이브 스토리지 서비스에서 저장 데이터 암호화 기능을 지원합니까?
52.	**스토리지 – 서비스 한도:** 위의 스토리지 섹션과 관련해 제한(서비스 한도)을 두고 있습니까? 예: 최대 볼륨 크기 인스턴스에 연결된 드라이브의 최대 개수 최대 IOPS(초당 입출력 작업 처리량) 최대 객체 크기 스토리지 계정당 최대 객체 개수 최대 스냅샷 개수

4. 행정적 관리

	요구 사항
1.	**행정적 관리 – 사용자 및 그룹:** 인프라 및 리소스의 사용자와 사용자 그룹을 생성하고 관리할 수 있는 서비스를 제공합니까?
2.	**행정적 관리 – 암호 재설정:** 사용자가 셀프서비스 방식으로 사용자의 암호를 재설정할 수 있도록 허용합니까?
3.	**행정적 관리 – 권한:** 리소스 수준에서 사용자와 그룹에 권한을 추가하는 기능을 제공합니까?
4.	**행정적 관리 – 임시 권한:** 일정 기간 동안에만 유효한 권한을 생성하는 기능을 제공합니까?
5.	**행정 – 임시 보안 인증:** 사용자에게 몇 분에서 몇 시간 동안 지속되는 임시 보안 인증을 생성하여 신뢰할 수 있는 사용자에게 제공하는 기능을 제공합니까?
6.	**행정 – 액세스 제어:** 인프라 리소스에 대한 세분화된 액세스 제어 기능을 제공합니까? • 제공하는 경우, 이 제어 기능에서는 어떤 조건(즉, 시간, 발신 IP 주소 등)이 사용될 수 있습니까?
7.	**행정 – 기본 제공 정책:** 클라우드 제공업체의 인프라에 사용자 및 그룹에 적용할 수 있는 액세스 제어 정책이 포함되어 있습니까?
8.	**행정 – 사용자 지정 정책:** 클라우드 제공업체의 인프라에서 사용자 및 그룹에 적용할 수 있는 액세스 제어 정책을 생성하고 사용자 지정하도록 허용합니까?
9.	**행정 – 정책 시뮬레이터:** 액세스 제어 정책을 프로덕션 환경에 반영하기 전에 해당 정책을 테스트할 수 있는 메커니즘을 제공합니까?
10.	**행정 – 클라우드 MFA:** 인프라에 대한 액세스 제어 및 인증의 추가 계층으로 다중 인증(MFA)을 사용할 수 있도록 지원합니까?
11.	**행정 – 서비스 한도:** 위의 행정적 관리 섹션과 관련해 제한(서비스 한도)을 두고 있습니까? 예: 최대 사용자 수

	최대 그룹 수 최대 관리형 정책 수

5. 보안

	요구 사항
1.	**보안 – 신원 조회:** 서비스 인프라(물리적 여부에 관계없음)에 액세스할 수 있는 클라우드 제공업체의 모든 직원은 신원 조회를 받습니까?
2.	**보안 – 물리적 액세스:** 특정 문제 티켓, 변경 요청, 유사한 형태의 공식 승인 없이는 직원이 서비스 인프라에 액세스하지 못하게 제한합니까?
3.	**보안 – 액세스 로그:** 인프라에 대한 직원 액세스를 로깅합니까? 즉, 직원의 액세스를 항상 로깅하고 최소 90 일 동안 로그를 보존합니까?
4.	**보안 – 호스트 로그인:** 직원이 컴퓨팅 호스트에 로그인하지 못하게 제한하고, 그 대신 컴퓨팅 호스트에서 수행되는 모든 작업을 자동화하여 이러한 자동 작업의 내용을 로깅한 후 최소 90 일 동안 보존합니까?
5.	**보안 – 암호 키:** 사용자 데이터를 암호화하는 데 사용되는 암호화 키를 생성하고 제어하는 서비스를 제공합니까?
6.	**보안 – 액세스 키 관리:** 마지막으로 액세스 키를 사용한 시기를 파악하고 오래된 키를 교체하고 비활성 사용자를 제거하는 기능을 제공합니까?
7.	**보안 – 고객 제공 키:** 사용자가 자체 키 관리 인프라에서 클라우드 서비스 제공업체의 키 관리 서비스로 키를 가져올 수 있도록 허용합니까?
8.	**보안 – 암호 키 서비스 통합:** 데이터 전송 중 암호화 기능을 제공하기 위해 클라우드 제공업체의 키 관리 서비스를 다른 클라우드 서비스에 통합할 수 있습니까?
9.	**보안 – HSM:** 전용 하드웨어 보안 모듈(HSM)을 제공합니까? 즉, 변조 방지 하드웨어 모듈 내에서 보안 키 스토리지를 제공하고 암호화 작업을 처리하는 하드웨어 기기를 제공합니까?

10.	**보안 – 암호 키 내구성:** 필요할 때 키를 사용할 수 있도록 복사본을 여러 개 보관하는 등 키의 내구성을 유지하기 위한 지원을 제공합니까?
11.	**보안 – SSO:** 사용자가 여러 계정과 비즈니스 애플리케이션에 대한 액세스를 중앙에서 관리할 수 있도록 관리형 SSO(싱글 사인온) 서비스를 제공합니까?
12.	**보안 – 인증서:** SSL(보안 소켓 계층)/TSL(전송 계층 보안) 인증서를 프로비저닝, 관리, 배포하기 위한 관리형 서비스를 제공합니까?
13.	**보안 – 인증서 갱신:** 클라우드 제공업체의 인증서 관리 서비스에서 인증서 갱신을 지원합니까?
14.	**보안 – 와일드카드 인증서:** 클라우드 제공업체의 인증서 관리 서비스에서 와일드카드 인증서 사용을 지원합니까?
15.	**보안 - 인증 기관** 클라우드 제공업체의 인증서 관리 서비스가 인증 기관(CA)의 역할을 합니까?
16.	**보안 – Active Directory:** 클라우드에서 관리형 Microsoft Active Directory(AD)를 제공합니까?
17.	**보안 – 온프레미스 Active Directory:** 클라우드 제공업체의 관리형 Microsoft Active Directory(AD) 서비스를 온프레미스 Microsoft Active Directory(AD)와 통합할 수 있습니까?
18.	**보안 – LDAP:** 클라우드 제공업체의 관리형 Microsoft Active Directory(AD) 서비스에서 LDAP(라이트웨이트 디렉터리 액세스 프로토콜)를 지원합니까?
19.	**보안 – Active Directory:** 클라우드 제공업체의 관리형 Microsoft Active Directory(AD) 서비스에서 SAML(보안 보장 마크업 언어)을 지원합니까?
20.	**보안 – 보안 인증 관리:** 사용자가 API(애플리케이션 프로그래밍 인터페이스) 키, 데이터베이스 보안 인증 정보, 기타 보안 암호와 같은 보안 인증 정보를 손쉽게 교체, 관리, 검색하는 데 도움이 되는 관리형 서비스를 제공합니까?
21.	**보안 – WAF:**

	애플리케이션 가용성을 저해하거나 보안을 위협하거나 과도한 리소스 소비를 야기하는 일반적인 웹 익스플로잇으로부터 웹 애플리케이션을 보호하는 데 도움이 되는 웹 애플리케이션 방화벽(WAF)을 제공합니까?
22.	**보안 – DDoS:** 흔히 자주 발생하는 네트워크 및 전송 계층의 DDoS(분산 서비스 거부) 공격을 방어하는 서비스와 정교한 애플리케이션 계층 공격을 완화하는 사용자 지정 규칙을 작성하는 기능을 제공합니까?
23.	**보안 – 보안 권장 사항:** 애플리케이션과 리소스의 잠재적 취약성을 자동으로 평가하는 서비스를 제공합니까?
24.	**보안 – 위협 탐지:** 관리형 위협 탐지 서비스를 제공합니까?
25.	**보안 – 서비스 한도:** 위의 보안 섹션과 관련해 제한(서비스 한도)을 두고 있습니까? 예: 최대 고객 마스터 키 수 최대 하드웨어 보안 모듈(HSM) 수

6. 규정 준수

아래 목록은 설명 목적으로만 제공되었으며 클라우드 서비스에 적용될 수 있는 인증 및 표준을 모두 포함하는 것으로 간주해서는 안 됩니다.

클라우드 제공업체가 충족한 산업별 국제 규정 준수 표준을 명시하세요.

인증/증명	**법, 규정 및 개인 정보 보호**	**조율/프레임워크**
☐ C5(독일)	☐ EU 데이터 보호 지침	☐ CDSA
☐ CISPE 데이터 보호 행동 강령	☐ EU 모델 조항	
☐ CNDCP(기후 중립 데이터 센터 협약)		
☐ DIACAP	☐ FERPA	☐ CIS
☐ DoD SRG 레벨 2 및 4	☐ GDPR	☐ 형사 사법 정보국(CJIS)

☐ FedRAMP
☐ FIPS 140-2
☐ HDS(프랑스, 의료)
☐ ISO 9001
☐ ISO 27001
☐ ISO 27017
☐ ISO 27018
☐ IRAP(호주)
☐ MTCS 티어 3(싱가포르)
☐ PCI DSS 레벨 1
☐ SEC 규칙 17-a-4(f)
☐ SOC1/ISAE 3402
☐ SOC2/SOC3
☐ SWIPO IaaS 행동 강령

☐ GLBA
☐ HIPAA
☐ HITECH
☐ IRS 1075
☐ ITAR
☐ PDPA – 2010(말레이시아)
☐ PDPA – 2012(싱가포르)
☐ PIPEDA(캐나다)
☐ 개인 정보 보호법(호주)
☐ 개인 정보 보호법(뉴질랜드)
☐ 스페인 DPA 승인
☐ 영국 DPA - 1988
☐ VPAT/제 508 호

☐ CSA
☐ EU-US 프라이버시 실드
☐ EU 세이프 하버
☐ FISC
☐ FISMA
☐ G-Cloud(영국)
☐ GxP(FDA CFR 21 Part 11)
☐ ICREA
☐ IT Grundschutz(독일)
☐ MARS – E
☐ MITA 3.0
☐ MPAA
☐ NIST
☐ 업타임 인스티튜트 티어
☐ 영국 클라우드 보안 원칙

공공 부문 조직은 위의 규정 준수 보고서를 활용하여 인증을 획득한 보안, 규정 준수 및 운영 표준을 기준으로 고유한 제품을 평가할 수 있습니다. 이러한 보고서는 CISP 가 해당 보고서에서 요구하는 규정을 준수함으로써 아래의 데이터 센터 운영 통제 항목을 이행하고 있다는 사실을 보여줍니다. 공공 부문 조직은 이러한 보고서를 획득하도록 요구함으로써 아래의 통제 항목이 제대로 이행되고 있다는 확신을 얻을 수 있습니다.

- **면밀한 검토에 따른 접근 권한 부여:** CISP 는 정당한 사업상의 이유로 현장에 있어야 하는 사람들에 한해 물리적 접근을 허용해야 합니다. 접근 권한을 부여했더라도 필요한 작업이 완료되면 접근 권한을 바로 철회해야 합니다.
- **출입 통제 및 모니터링:** 데이터 센터 외곽 계층에 대한 출입은 통제된 프로세스를 통해 이루어져야 합니다. CISP 는 출입구에 경비 담당자를 배치하고 감독자를 고용하여 보안 카메라를 통해 담당자와 방문객을 감시해야 합니다. 승인을 받은 직원이 현장에 있는 경우 해당 직원에게 다중 인증을 요구하고 사전 승인 구역으로 액세스를 제한하는 배지를 배부해야 합니다.

- **CISP 데이터 센터 직원:** 데이터 센터에 정기적으로 출입해야 하는 CISP 직원은 직무에 기반하여 관련 시설 구역에 대한 접근 권한을 부여받아야 하며, 접근에 대한 조사를 정기적으로 받습니다. 각 직원의 접근 승인이 유효한지 확인하기 위해 구역 접근 관리자가 직원 명단을 정기적으로 검토해야 합니다. 데이터 센터에 상주해야 하는 지속적인 비즈니스 요구가 없는 경우 해당 직원은 방문자 프로세스를 거쳐야 합니다.

- **부정 출입 모니터링:** CISP 는 비디오 감시, 침입 탐지, 액세스 로그 모니터링 시스템을 사용해 데이터 센터 자산에 대한 부정 출입을 끊임없이 모니터링해야 합니다. 출입문을 열어 두거나 강제로 열면 경보를 울리는 장치를 사용해 출입문의 보안을 유지해야 합니다.

- **CISP 보안 운영 센터를 통한 글로벌 보안 모니터링:** CISP 보안 운영 센터는 전 세계에 위치해야 하며 CISP 데이터 센터의 보안 프로그램을 모니터링, 분류, 시행할 책임이 있습니다. 물리적 액세스 관리 및 침입 탐지 대응을 감독하는 동시에 현장 데이터 센터 보안 팀에 연중무휴 글로벌 지원을 제공해야 합니다. 즉, 액세스 활동을 추적하고, 액세스 권한을 철회하고, 잠재적 보안 사고에 대응하고 분석할 수 있도록 준비하는 등의 모니터링 활동을 지속적으로 수행해야 합니다.

- **계층별 액세스 검토:** 인프라 계층에 대한 액세스는 비즈니스 요구에 따라 제한해야 합니다. 계층별 액세스 검토를 시행하는 경우 모든 계층에 대한 접근 권한은 기본적으로 부여되지 않습니다. 특정 계층에 대한 액세스는 특정 계층에 액세스해야 하는 경우에만 허용되어야 합니다.

- **정기적인 작업의 일환으로 장비 유지 관리 수행:** CISP 팀은 시스템, 네트워크 및 백업 장비에 대한 진단을 시행하여 현재 및 비상 상황에서 제대로 작동하는지 확인해야 합니다. 데이터 센터 장비와 유틸리티에 대한 정기적인 유지 보수 점검은 CISP 데이터 센터 운영의 일부여야 합니다.

- **비상 시에 대비한 백업 장비:** 용수, 전력, 통신 및 인터넷 연결은 CISP 가 비상 상황에서도 운영을 지속할 수 있도록 이중화를 적용해 설계해야 합니다. 전력 공급 시스템은 완전히 이중화되어야 합니다. 그래야 중단이 발생하더라도 발전기로 전체 시설에 예비 전력을 제공하면서도 무정전 전원 장치를 특정 기능에 사용할 수 있습니다. 과열을 방지하고 나아가 서비스 중단 가능성을 줄이기 위해 인력과 시스템을 통해 온도와 습도를 모니터링하고 제어해야 합니다.

- **기술과 사람이 유기적으로 서로 보완하여 보안 강화:** 데이터 계층에 대한 접근 권한을 얻으려면 필수 절차를 거쳐야 합니다. 필수 절차에는 권한이 있는 개인이 애플리케이션에 대한 사람의 액세스를 검토하고 승인하는 과정이 포함됩니다. 한편, 위협 및 전자 침입 탐지 시스템을 통해 식별된 위협 또는 수상한 활동에 대해 모니터링하고 자동으로 경보를 발동해야 합니다. 예를 들어 문을 열어 두거나 강제로 열면 경보가 울립니다. CISP 는 보안 카메라를 배치하고 법적 및 규정 준수 요구 사항에 따라 영상을 보관해야 합니다.

- **물리적/기술적 침입 방지:** 다중 인증을 요구하는 전자 제어 장치로 서버실에 대한 액세스 지점을 강화해야 합니다. 또한 CISP 는 기술적 침입에 대해서도 대비해야 합니다. 데이터를 삭제하려고 하면 CISP 서버는 이를 직원에게 알릴 수 있어야 합니다. 예기치 않게 위반 행위가 발생하면 CISP 서버는 자동으로 비활성화되어야 합니다.

- **공격자의 주요 목표가 되는 서버와 미디어:** CISP 는 고객 데이터를 저장하는 데 사용되는 미디어 스토리지 디바이스의 보안 등급을 '치명(Critical)'으로 분류하고 수명 주기 내내 그에 맞게 즉, '고영향(High Impact)'으로 취급해야 합니다. CISP 는 디바이스를 설치하고, 디바이스에서 서비스를 제공하고, 디바이스를 더 이상 사용할 수 없게 될 경우 완전히 폐기하는 방법에 대한 표준을 명확하게 확립해야 합니다. 스토리지 디바이스의 수명이

다하면 CISP 는 NIST 800-88 에 명시된 기술을 사용해 미디어를 폐기합니다. 고객 데이터가 저장된 미디어의 경우 데이터를 안전하게 폐기할 때까지 CISP 의 통제를 계속 받습니다.

- **서드 파티 감사자가 CISP 절차 및 시스템 검증:** CISP 는 외부 감사자의 감사 아래 데이터 센터 조사를 받아야 합니다. 심층 조사를 실시하여 CISP 가 보안 인증을 획득하는 데 필요한 규칙을 따르고 있다는 확인을 받아야 합니다. 규정 준수 프로그램 및 요구 사항에 따라 외부 감사자는 CISP 직원이 미디어를 처리하고 폐기하는 방법에 대해 인터뷰할 수 있습니다. 감사자는 또한 보안 카메라 피드를 보고 데이터 센터의 모든 출입구와 복도를 관찰할 수 있습니다. 그리고 CISP 전자 액세스 제어 디바이스, 보안 카메라와 같은 장비를 검사할 수도 있습니다.

- **예상치 못한 상황에 대비:** CISP 는 자연 재해, 화재와 같은 잠재적 환경 위협에 능동적으로 대비해야 합니다. 자동 센서 설치와 대응 장비 설치는 CISP 가 데이터 센터를 안전하게 보호하는 두 가지 방법입니다. 누수 감지기를 설치하여 직원에게 문제를 알리고 자동 펌프로 누수를 제거하여 손상을 막아야 합니다. 마찬가지로 자동 화재 감지 장비와 진압 장비로 위험을 줄이고 CISP 직원과 소방관에게 문제를 알릴 수 있습니다.

- **여러 가용 영역을 이용한 고가용성 지원:** CISP 는 내결함성을 높이기 위해 가용 영역을 여러 개 제공해야 합니다. 각 가용 영역은 하나 이상의 데이터 센터로 구성되어야 하며, 서로 물리적으로 분리되어 있어야 합니다. 또한 이중 전력과 네트워크를 갖추고 있어야 합니다. 고속의 프라이빗 광섬유 네트워킹을 사용해 가용 영역을 서로 연결해야 합니다. 그래야 중단 없이 가용 영역 간에 장애 조치를 자동으로 취하도록 애플리케이션을 설계할 수 있습니다.

- **장애 시뮬레이션 및 대응 성과 측정:** CISP 는 비즈니스 연속성 계획을 가지고 있어야 합니다. 비즈니스 연속성 계획은 운영 프로세스 안내서로서 자연 재해 때문에 발생하는 장애를 방지하고 줄이는 방법과 장애 발생 이전, 도중, 이후에 취해야 할 세부 조치를 개략적으로 보여줘야 합니다. 예상치 못한 상황을 완화하고 이에 대비하기 위해 CISP 는 양한 시나리오를 시뮬레이션하는 훈련을 실시하여 비즈니스 연속성 계획을 정기적으로 테스트해야 합니다. CISP 는 인력과 프로세스가 어떻게 기능하는지에 대해 문서화하고 교훈과 응답률을 개선하는 데 필요하다고 생각되는 시정 조치에 대해 보고받아야 합니다. CISP 오류로 인한 추가적 가동 중단을 최소화하는 체계적인 복구 프로세스에 대해 교육을 받고 이를 활용해 장애를 신속하게 회복할 수 있도록 대비해야 합니다.

- **효율성 목표를 충족하도록 지원:** CISP 는 환경 위험을 해결하는 것 외에도 지속 가능성 고려 사항을 데이터 센터 설계에 통합해야 합니다. CISP 는 데이터 센터에 재생 가능 에너지를 사용하겠다는 약속에 대해 세부 정보를 제공해야 하며, 고객이 자체 데이터 센터를 사용할 때와 비교해 어떻게 탄소 배출을 줄일 수 있는지에 대한 정보도 제공해야 합니다.

- **부지 선정:** 위치를 선정하기 전에 먼저 CISP 는 초기 환경 및 지리 평가를 실시해야 합니다. 데이터 센터 위치는 홍수, 기상 이변, 지진 활동과 같은 환경 위험을 완화할 수 있도록 신중하게 선택해야 합니다. CISP 가용 영역은 서로 독립적이며 물리적으로 분리되도록 구축되어야 합니다.

- **이중화:** 데이터 센터는 서비스 수준을 유지하면서 장애를 예측하고 견딜 수 있게끔 설계되어야 합니다. 장애 발생 시 자동 프로세스에 따라 트래픽이 장애 지역에서 다른 곳으로 이전되어야 합니다. 핵심 애플리케이션을 N+1 표준으로 배포해야 합니다. 그래야 데이터 센터에 장애가 발생했을 때 나머지 사이트로 트래픽을 분산할 수 있을 만큼 용량을 충분히 확보할 수 있습니다.

- **가용성:** CISP 는 시스템의 가용성을 유지하고 운영 중단 시 서비스를 복구하는 데 필요한 중요 시스템 구성 요소를 식별해야 합니다. 중요 시스템 구성 요소는 격리된 여러 위치에 백업해 놓아야 합니다. 고도의 신뢰성을 갖추고 독립적으로 운영되게끔 각 위치와 가용 영역을 설계해야 합니다. 애플리케이션에서 중단 없이 가용 영역 간에 장애 조치를 자동으로 취할 수 있도록 가용 영역을 서로 연결해야 합니다. 복원력이 뛰어난 시스템, 즉 서비스 가용성이 시스템 설계 기능 중 하나가 되어야 합니다. 가용 영역과 데이터 복제를 활용해 데이터 센터를 설계하면 CISP 고객은 복구 시간을 극단적으로 단축하고, 복구 지점 목표를 달성하고, 초고도의 서비스 가용성을 실현할 수 있습니다.

- **용량 계획**: CISP 는 가용성 약정과 요구 사항을 지원하기 위해 서비스 사용량을 지속적으로 모니터링하여 인프라를 배포해야 합니다. CISP 는 CISP 인프라 사용량과 수요를 최소 매달 평가하는 용량 계획 모델을 유지해야 합니다. 이 모델은 향후 수요 계획을 지원해야 하며 정보 처리, 통신, 감사 로그 보관 등의 고려 사항을 포함해야 합니다.

비즈니스 연속성 및 재해 복구

- **비즈니스 연속성 계획:** CISP 비즈니스 연속성 계획은 환경 장애를 방지하고 줄이기 위한 조치를 개략적으로 보여줘야 합니다. 장애 발생 이전, 도중, 이후에 취해야 할 조치에 대한 운영 세부 정보가 포함되어야 합니다. 다양한 시나리오의 시뮬레이션을 진행하는 테스트를 통해 비즈니스 연속성 계획을 뒷받침해야 합니다. 테스트 도중, 테스트 이후에 CISP 는 지속적 개선을 목표로 인력 및 프로세스 성과, 시정 조치, 교훈을 문서화해야 합니다.

- **팬데믹 대응:** CISP 는 감염병 발생 위협에 신속하게 대응할 수 있도록 재해 복구 계획에 팬데믹 대응 정책과 절차를 통합해야 합니다. 완화 전략에는 주요 프로세스를 지역 밖 리소스로 이전하는 대체 인력 모델과 주요 비즈니스 운영을 지원하기 위한 위기 관리 계획 가동이 포함되어야 합니다. 감염병 계획은 국제 기구의 연락 창구를 비롯해 국제 보건 기관과 국제 보건 규정을 참조해야 합니다.

모니터링 및 로깅

- **데이터 센터 액세스 검토:** 데이터 센터에 대한 액세스를 정기적으로 검토해야 합니다. CISP 의 HR 시스템에서 직원의 기록이 만료되면 액세스 권한이 자동으로 철회되어야 합니다. 승인된 요청 기간이 지나 직원 또는 계약직 직원의 액세스 권한이 만료된 경우 계속 CISP 의 직원으로 남아 있더라도 해당 직원의 액세스 권한을 철회해야 합니다.

- **데이터 센터 액세스 로그:** CISP 데이터 센터에 대한 물리적 액세스는 로깅, 모니터링, 유지되어야 합니다. CISP 는 논리적 및 물리적 모니터링 시스템에서 얻은 정보를 상호 연관시켜 필요에 따라 보안을 강화해야 합니다.

- **데이터 센터 액세스 모니터링:** CISP 는 보안 프로그램 모니터링, 분류, 시행을 담당하는 글로벌 보안 운영 센터를 통해 데이터 센터를 모니터링해야 합니다. 데이터 센터 액세스 활동을 관리 및 모니터링하여 연중무휴 글로벌 지원을 제공하고, 대응을 분류, 자문, 분석, 전달하여 현지 팀 및 기타 지원 팀이 보안 사고에 대응하도록 지원해야 합니다.

감시 및 탐지:

- **CCTV:** 서버실에 대한 물리적 액세스 지점을 CCTV(폐쇄 회로 텔레비전 카메라)로 녹화해야 합니다. 이미지는 법적 및 규정 준수 요구 사항에 따라 보관해야 합니다.

- **데이터 센터 진입 지점:** 물리적 접근은 전문 보안 직원이 보안 감시, 탐지 시스템 및 기타 전자 수단을 사용해 건물 입구에서 제어해야 합니다. 승인받은 직원은 다중 인증 메커니즘을 사용하여 데이터 센터에 접근해야 합니다. 서버실 입구는 문을 열어 두거나 강제로 열면 경보가 울리며 사고 대응이 시작됩니다.

- **침입 탐지:** 데이터 계층 내에 전자 침입 탐지 시스템을 설치하여 보안 사고를 모니터링, 탐지하고 담당자에게 자동으로 알려야 합니다. 입실 또는 퇴실 시 다중 인증을 하도록 요구하는 장치를 설치하여 서버실 출입구의 보안을 유지해야 합니다. 이러한 장치는 문을 열어 두거나 인증 없이 문을 강제로 열면 경보를 울립니다. 다중 인증 없이 데이터 계층에 진입하거나 데이터 계층을 이탈하려고 하면 이를 감지하도록 문 경보 시스템을 구성해야 합니다. 경보는 즉각적 로깅, 분석, 대응을 위해 연중무휴 CISP 보안 운영 센터로 바로 전달되어야 합니다.

디바이스 관리

- **자산 관리:** CISP 자산은 인벤토리 관리 시스템을 통해 중앙에서 관리해야 합니다. 인벤토리 관리 시스템에서는 CISP 소유 자산의 소유자, 위치, 상태, 유지 보수, 설명 정보를 보관하고 추적합니다. 조달 후에는 자산을 스캔하고 추적해야 하며, 유지 보수 중인 자산은 소유권, 상태 및 해결 여부를 확인하고 모니터링해야 합니다.

- **미디어 폐기:** CISP 는 고객 데이터를 저장하는 데 사용되는 미디어 스토리지 디바이스의 보안 등급을 '치명(Critical)'으로 분류하고 수명 주기 내내 그에 맞게 즉, '고영향(High Impact)'으로 취급해야 합니다. CISP 는 디바이스를 설치하고, 디바이스에서 서비스를 제공하고, 디바이스를 더 이상 사용할 수 없게 될 경우 완전히 폐기하는 방법에 대한 표준을 명확하게 확립해야 합니다. 스토리지 디바이스의 수명이 다하면 CISP 는 NIST 800-88 에 명시된 기술을 사용해 미디어를 폐기해야 합니다. 고객 데이터가 저장된 미디어의 경우 데이터를 안전하게 폐기할 때까지 CISP 의 통제를 계속 받아야 합니다.

운영 지원 시스템

- **전력:** CISP 데이터 센터의 전력 시스템은 완전히 이중화되어야 하며 운영에 대한 영향 없이 연중무휴 유지 보수가 이루어져야 합니다. CISP 는 데이터 센터에 예비 전력 공급 장치를 설치하여 시설의 필수 부하에 전력 장애가 발생하더라도 운영을 유지할 수 있게 해야 합니다.

- **기후 및 온도:** 과열을 방지하고 서비스 중단의 가능성을 줄이기 위해 CISP 데이터 센터는 기후 제어 메커니즘을 사용하고 서버와 기타 하드웨어를 적정 작동 온도로 유지해야 합니다. 인력과 시스템을 통해 온도와 습도를 모니터링하고 적정 수준으로 제어해야 합니다.

- **화재 감지 및 진압**: CISP 데이터 센터에는 자동 화재 감지 및 진압 장비가 설치되어 있어야 합니다. 화재 감지 시스템의 연기 감지 센서를 네트워킹 공간, 기계 공간, 인프라 공간에서 사용해야 합니다. 또한 진압 시스템을 사용해 해당 공간을 보호해야 합니다.

- **누수 감지:** 누수 여부를 감지할 수 있도록 CISP 는 데이터 센터에 누수 여부를 감지하는 기능을 설치해야 합니다. 물로 인한 추가 손상을 막기 위해 물이 감지되면 물을 제거하는 메커니즘을 갖춰야 합니다.

인프라 유지 보수

- **장비 유지 보수:** CISP 는 전기 장비와 기계 장비를 모니터링하고 예방적 차원에서 유지 보수를 수행하여 CISP 데이터 센터 내 시스템의 운영성을 지속적으로 유지해야 합니다. 장비 유지 보수 절차는 유자격자가 수행하고 문서화된 유지 보수 일정에 따라 완료해야 합니다.

- **환경 관리:** CISP 는 문제를 즉시 식별할 수 있도록 전기 및 기계 시스템과 장비를 모니터링해야 합니다. CISP 건물 관리 시스템과 전자 모니터링 시스템을 통해 획득한 정보와 지속적 감사 도구를 활용해 이 작업을 수행해야 합니다. 장비의 운영성을 지속적으로 유지하기 위해 예방적 유지 보수를 실시해야 합니다.

거버넌스 및 위험

- **지속적으로 데이터 센터 위험 관리:** CISP 보안 운영 센터는 데이터 센터에 대해 위협 및 취약성 검토를 정기적으로 실시해야 합니다. 데이터 센터 위험 평가 활동을 통해 잠재적 취약성을 지속적으로 평가하고 완화해야 합니다. 비즈니스 전체에 존재하는 위험을 식별하고 관리하는 데 사용되는 전사적 차원의 위험 평가 프로세스와 더불어 이 평가를 실시해야 합니다. 또한 이 과정에서 지역적 규제와 환경 위험도 고려해야 합니다.
- **서드 파티 보안 인정:** CISP 데이터 센터에 대한 서드 파티 테스트에서는 서드 파티 보고서에 기록된 대로, CISP 가 보안 인증을 획득하는 데 필요한 규칙을 따라 적절하게 보안 조치를 구현했는지 확인해야 합니다. 규정 준수 프로그램 및 해당 요구 사항에 따라 외부 감사자는 미디어 폐기 테스트, 보안 카메라 영상 검토, 데이터 센터의 출입구 및 복도 관찰, 전자 액세스 제어 디바이스 테스트, 데이터 센터 장비 검사를 수행할 수 있습니다.

7. 마이그레이션

	요구 사항
1.	**마이그레이션 서비스:** 클라우드 제공업체가 제공하는 데이터 마이그레이션 서비스는 몇 개입니까?
2.	**마이그레이션 – 중앙 집중식 모니터링:** 서버 및 애플리케이션 마이그레이션 상태를 추적하고 모니터링할 수 있는 중앙 집중식(단일 창) 서비스를 조직에 제공합니까?
3.	**마이그레이션 - 대시보드:** 클라우드 제공업체의 마이그레이션 도구에서 마이그레이션 상태, 관련 지표 및 마이그레이션 이력을 신속하게 시각화할 수 있는 대시보드를 제공합니까?
4.	**마이그레이션 - 클라우드 제공업체 도구:** 클라우드 제공업체의 마이그레이션 도구를 서버와 애플리케이션 마이그레이션을 수행할 수 있는 클라우드 제공업체의 다른 마이그레이션 도구와 통합할 수 있습니까?
5.	**마이그레이션 - 서드 파티 도구:** 클라우드 제공업체의 마이그레이션 도구를 서드 파티 마이그레이션 도구와 통합할 수 있습니까? • 통합할 수 있는 경우, 지원되는 서드 파티 마이그레이션 도구는 무엇입니까?
6.	**마이그레이션 – 멀티 리전 마이그레이션:** 다른 리전에서 진행 중인 서버 마이그레이션과 애플리케이션 마이그레이션을 추적하고 모니터링할 수 있는 기능을 클라우드 제공업체의 마이그레이션 도구에서 제공합니까?

7.	**마이그레이션 – 서버 마이그레이션:** 온프레미스 가상 서버를 클라우드로 마이그레이션하는 방법을 클라우드 제공업체의 마이그레이션 도구에서 제공합니까? • 제공하는 경우, 현재 지원되는 가상 환경은 무엇입니까?
8.	**마이그레이션 – 서버 발견:** 클라우드로 마이그레이션할 온프레미스 가상 서버를 자동으로 찾는 발견 기능이 클라우드 제공업체의 마이그레이션 도구에 있습니까?
9.	**마이그레이션 – 서버 성능 데이터:** CPU(중앙 처리 장치) 활용률, RAM(랜덤 액세스 메모리) 활용률과 같은 서버 및/또는 가상 머신의 성능을 수집하고 표시하는 기능이 클라우드 제공업체의 마이그레이션 도구에 있습니까?
10.	**마이그레이션 – 검색 데이터베이스:** 수집된 모든 데이터를 중앙 데이터베이스에 저장하는 기능이 클라우드 제공업체의 마이그레이션 도구에 있습니까? • 도구가 있는 경우 조직에 이러한 데이터를 내보낼 수 있는 기능이 있습니까? 어떤 형식으로 내보냅니까?
11.	**마이그레이션 – 저장 데이터 암호화:** 수집하여 검색 데이터베이스에 저장한 모든 정보를 암호화합니까?
12.	**마이그레이션 – 증분 서버 복제:** 클라우드 제공업체의 마이그레이션 도구에서는 서버 또는 가상 머신에 대해 수행된 모든 변경 사항이 최종 마이그레이션 이미지에 포함되도록 지원하는 방식으로서 서버 또는 가장 머신 마이그레이션 동안 실시간 자동 증분 서버 복제를 제공합니까? • 제공하는 경우, 해당 서비스를 얼마나 오래 실행할 수 있습니까?
13.	**마이그레이션 - VMware:** 클라우드 제공업체의 마이그레이션 도구에서 온프레미스에서 클라우드로 VMware 가상 머신을 마이그레이션하는 기능을 지원합니까?
14.	**마이그레이션 – Hyper-V:** 클라우드 제공업체의 마이그레이션 도구에서 온프레미스에서 클라우드로 Hyper-V 가상 머신을 마이그레이션하는 기능을 지원합니까?
15.	**마이그레이션 – 애플리케이션 발견:** 클라우드 제공업체의 마이그레이션 도구에 애플리케이션을 마이그레이션하기 전에 해당 애플리케이션을 발견해서 그룹화하는 기능이 있습니까?

16.	**마이그레이션 – 종속성 매핑:** 클라우드 제공업체의 마이그레이션 도구에 서버와 애플리케이션을 마이그레이션하기 전에 서버와 애플리케이션 간에 종속성을 발견하는 기능이 있습니까?
17.	**마이그레이션 – 데이터베이스 마이그레이션:** 클라우드 제공업체의 마이그레이션 도구에 온프레미스 데이터베이스를 클라우드로 마이그레이션하는 기능이 있습니까?
18.	**마이그레이션 – 데이터베이스 마이그레이션 가동 중단:** 클라우드 제공업체의 마이그레이션 도구에 가동 중단을 최소화하면서 클라우드에 데이터베이스 마이그레이션을 수행하는 기능이 있습니까? 즉, 마이그레이션 프로세스 중에도 원천 데이터베이스가 온전하게 운영됩니까?
19.	**마이그레이션 – 원천 데이터베이스:** 클라우드 제공업체의 마이그레이션 도구에서 Oracle, SQL Server 등 다양한 데이터베이스 원천의 마이그레이션을 지원합니까? • 제공하는 경우, 클라우드 마이그레이션이 지원되는 원천 데이터베이스를 모두 기입하세요.
20.	**마이그레이션 – 이기종 마이그레이션:** 클라우드 제공업체의 마이그레이션 도구에 이기종 데이터베이스 마이그레이션을 수행할 수 있는 기능이 있습니까? 즉, Oracle 에서 SQL Server 로 마이그레이션하는 경우와 같이 원천 데이터베이스와 다른 유형의 대상 데이터베이스로 마이그레이션할 수 있습니까? • 기능이 있는 경우, 가능한 이기종 마이그레이션의 조합을 모두 기입하세요.
21.	**마이그레이션 – 페타바이트 규모의 데이터 마이그레이션:** 안전한 기기를 사용해 대규모 데이터를 클라우드 안팎으로 전송하는 페타바이트 규모의 데이터 전송 솔루션을 제공합니까?
22.	**마이그레이션 – 엑사바이트 규모의 데이터 마이그레이션:** 초대규모 데이터를 클라우드로 이전하는 엑사바이트 규모의 데이터 전송 솔루션을 제공합니까?
23.	**마이그레이션 – 엔터프라이즈 백업:** 고객의 데이터 센터를 클라우드 스토리지 서비스, 즉 클라우드 제공업체의 스토리지 서비스로 데이터를 전송하여 저장하는 서비스와 원활하게 통합하는 서비스를 제공합니까?
24.	**마이그레이션 – 엔터프라이즈 백업 - 객체 스토리지:** 클라우드 제공업체의 엔터프라이즈 백업 서비스를 클라우드 객체 스토리지 서비스와 통합할 수 있습니까?
25.	**마이그레이션 – 엔터프라이즈 백업 - 파일 액세스:** 클라우드 제공업체의 엔터프라이즈 백업 서비스를 사용하면 사용자가 NFS(네트워크 파일 시스템) 프로토콜과 같은 파일 프로토콜을 통해 객체를 저장하고 검색할 수 있습니까?

26.	**마이그레이션 – 엔터프라이즈 백업 - 블록 액세스:** 클라우드 제공업체의 엔터프라이즈 백업 서비스를 사용하면 사용자가 iSCSI(Internet Small Computer System Interface) 프로토콜과 같은 블록 프로토콜을 통해 객체를 저장하고 검색할 수 있습니까?
27.	**마이그레이션 – 엔터프라이즈 백업 - 테이프 액세스:** 클라우드 제공업체의 엔터프라이즈 백업 서비스를 사용하면 사용자가 가상 테이프 라이브러리를 통해 데이터를 백업하고 테이프 백업본을 제공업체의 클라우드에 저장할 수 있습니까?
28.	**마이그레이션 – 엔터프라이즈 백업 - 암호화:** 클라우드 제공업체의 엔터프라이즈 백업 서비스에서 저장 데이터 암호화 기능과 전송 중 데이터 암호화 기능을 제공합니까?
29.	**마이그레이션 – 엔터프라이즈 백업 - 서드 파티 소프트웨어 통합:** 클라우드 제공업체의 엔터프라이즈 백업 서비스를 일반적으로 사용되는 서드 파티 백업 소프트웨어와 통합할 수 있습니까?
30.	**마이그레이션 - 서비스 한도:** 위의 마이그레이션 섹션과 관련해 제한(서비스 한도)을 두고 있습니까? 예: 동시 가상 머신 마이그레이션 최대 수 주문 가능한 데이터 전송 솔루션 최대 수

8. 청구

	요구 사항
1.	**청구 – 추적 및 보고:** 사용자가 클라우드 오퍼링 사용량을 관리하고 모니터링할 수 있도록 청구 추적 및 보고 서비스를 제공합니까?
2.	**청구 – 알림:** 사용자의 지출이 한도에 초과하면 사용자에게 알림을 보내 경고하는 메커니즘을 사용자에게 제공합니까?
3.	**청구 – 원가 관리:** 비용과 지출을 요약한 그래픽을 만들고 표시하는 메커니즘을 제공합니까?
4.	**청구 – 예산:** 예산을 표시, 관리하고 추정 비용을 예측하는 메커니즘을 제공합니까?
5.	**청구 – 통합 보기:** 기본 청구 계정 하나에 여러 계정의 청구를 통합하는 메커니즘을 제공합니까?
6.	**청구 – 서비스 한도:** 클라우드 제공업체가 위의 청구 섹션과 관련해 제한(서비스 한도)을 두고 있습니까? 예: 그룹화할 수 있는 최대 계정 수 생성할 수 있는 최대 경보 수 관리할 수 있는 최대 예산 수

9. 관리

	요구 사항
1.	**관리 – 모니터링 서비스:** 클라우드 리소스와 애플리케이션을 관리하기 위해 미리 정의한 지표를 사용해 수집, 모니터링, 보고하는 모니터링 서비스를 제공합니까?
2.	**관리 - 경보:** 클라우드 제공업체의 모니터링 서비스를 사용하면 사용자가 경보를 설정할 수 있습니까?
3.	**관리 - 사용자 지정 지표:** 클라우드 제공업체의 모니터링 서비스를 사용하면 사용자가 사용자 지정 지표를 생성하고 모니터링할 수 있습니까?

4.	**관리 – 모니터링 정밀도:** 클라우드 제공업체의 모니터링 서비스에서는 1 분 수준 등 다양한 수준의 모니터링 정밀도를 제공합니까?
5.	**관리 – API 추적 서비스:** 가시성 향상을 위해 콘솔과 API(애플리케이션 프로그래밍 인터페이스) 수준에서 클라우드 리소스의 활동을 로깅, 모니터링 및 저장하는 서비스를 제공합니까? • 제공하는 경우, 이 추적 서비스와 통합되는 클라우드 제공업체의 서비스는 무엇입니까?
6.	**관리 – 알림:** API(애플리케이션 프로그래밍 인터페이스) 활동 수준을 기반으로 알림을 전송할 수 있습니까?
7.	**관리 – 압축:** API(애플리케이션 프로그래밍 인터페이스) 추적 시스템과 관련된 스토리지 비용을 줄일 수 있도록 API 추적 시스템에서 생성한 로그를 압축하는 메커니즘을 제공합니까?
8.	**관리 – 리전 집계:** 모든 리전에서 계정의 API(애플리케이션 프로그래밍 인터페이스) 활동을 기록하는 기능을 제공하고 이 정보를 사용하기 편하게 합산하여 전달합니까?
9.	**관리 - 리소스 인벤토리:** 사용자가 배포한 리소스 구성을 평가, 감사, 감정하는 서비스를 제공합니까?
10.	**관리 – 구성 변경:** 리소스 구성 변경 사항이 자동으로 기록됩니까?
11.	**관리 – 구성 이력:** 과거 어느 시점에서든 리소스 구성을 검사할 수 있는 기능을 제공합니까?
12.	**관리 – 구성 규칙:** 규정 준수를 준비, 구성하고 지속적으로 모니터링하기 위한 지침과 권장 사항을 제공합니까?
13.	**관리 - 리소스 템플릿:** 사용자에게 템플릿과 같은 방식으로 리소스 모음을 생성, 프로비저닝, 관리할 수 있는 기능을 제공합니까?
14.	**관리 - 리소스 템플릿 복제:** 재해 복구(DR) 상황에서 잠재적으로 사용될 다양한 리전에 이러한 리소스 템플릿을 신속하게 복제할 수 있는 기능을 제공합니까?
15.	**관리 - 템플릿 디자이너:** 끌어다 놓기 기능이 있는 사용하기 쉬운 그래픽 도구를 제공합니까? 끌어다 놓기 기능이 있는 경우 리소스 템플릿 작성 프로세스를 가속화할 수 있습니다.

16.	**관리 – 서비스 카탈로그:** 서버, 가상 머신, 소프트웨어, 데이터베이스 등과 같은 서비스의 카탈로그를 생성하고 관리하는 서비스를 제공합니까?
17.	**관리 – 콘솔 액세스:** 클라우드 서비스를 손쉽게 관리하고 모니터링할 수 있는 웹 기반 사용자 인터페이스를 제공합니까?
18.	**관리 – CLI 액세스:** 명령줄 인터페이스(CLI)를 통해 여러 클라우드 서비스를 관리, 구성하고 스크립트를 사용해 관리 작업을 자동화할 수 있는 통합 도구를 제공합니까?
19.	**관리 – 모바일 액세스:** 사용자가 클라우드에 접속해 리소스를 관리할 수 있도록 스마트폰 애플리케이션을 제공합니까? • 제공하는 경우 이 애플리케이션을 iOS 와 Android 에서 모두 사용할 수 있습니까?
20.	**관리 – 모범 사례:** 사용자가 클라우드 사용 방법을 모범 사례와 비교하는 데 도움이 되는 서비스를 제공합니까?
21.	**관리 – 서비스 한도:** 클라우드 제공업체가 위의 관리 섹션과 관련해 제한(서비스 한도)을 두고 있습니까? 예: 계정당 구성 규칙의 최대 개수 생성할 수 있는 최대 경보 수 저장할 수 있는 최대 로그 수

10. 지원

	요구 사항
1.	**지원 - 서비스:** 전화, 채팅, 이메일을 통해 연중무휴 언제든지 지원을 제공합니까?
2.	**지원 – 지원 티어:** 다양한 지원 티어를 제공합니까?
3.	**지원 – 티어 할당:** 소비한 리소스/서비스를 사용자 스스로 세부 분류에 따라 각기 다른 지원 수준에 할당하도록 허용합니까? 또 각기 다른 수준의 지원을 획득하거나 받기 위해 별도의 클라우드 계정을 유지하도록 사용자를 강제하지 않습니까?

4.	**지원 – 포럼:** 고객이 문제를 논의할 수 있는 공개 지원 포럼을 제공합니까?
5.	**지원 - 서비스 상태 대시보드:** 여러 리전의 서비스 가용성에 대한 최신 정보가 표시되는 서비스 상태 대시보드를 제공합니까?
6.	**지원 - 맞춤형 대시보드:** 사용자의 특정 리소스를 지원하는 서비스의 성능과 가용성을 맞춤형으로 보여주는 대시보드를 제공합니까?
7.	**지원 - 대시보드 이력:** 1 년치 서비스 건전성 대시보드 기록을 제공합니까?
8.	**지원 – 클라우드 자문가:** 맞춤형 클라우드 전문가의 역할을 하며 모범 사례에 비춰 리소스 사용량을 비교하는 서비스를 제공합니까?
9.	**지원 – TAM:** 전 범위의 클라우드 서비스에 대해 전문 기술을 제공하는 기술 계정 관리자(TAM)를 제공합니까?
10.	**지원 – 서드 파티 애플리케이션 지원:** 일반적인 운영 체제와 일반적인 애플리케이션 스택 구성 요소를 지원합니까?
11.	**지원 – 퍼블릭 API:** 지원 사례를 작성, 편집, 종료하기 위해 지원 사례와 프로그래밍 방식으로 상호 작용하는 퍼블릭 API(애플리케이션 프로그래밍 인터페이스)를 제공합니까?
12.	**지원– 서비스 설명서:** 사용자 안내서, 자습서, FAQ. 릴리스 정보 등 모든 서비스에 관한 양질의 기술 문서를 공개적으로 제공합니까?
13.	**지원– CLI 서비스 설명서:** 명령줄 인터페이스(CLI)에 관한 양질의 기술 문서를 공개적으로 제공합니까?
14.	**지원– 참조 아키텍처:** 클라우드 제공업체의 다양한 클라우드 서비스를 결합하여 솔루션을 구축하는 데 도움이 되는 무료 온라인 참조 아키텍처 문서 모음을 제공합니까?
15.	**지원– 참조 배포:** 일반적인 솔루션(예: DevOps, 빅 데이터, 데이터 웨어하우스, Microsoft 워크로드, SAP 워크로드 등)을 구현할 때 참조할 수 있는 검증받은 상세 단계별 절차(모범 사례 포함) 문서를 온라인에서 무료로 제공합니까?

부록 B – 라이브 기술 평가

CISP 를 선택할 때는 CISP 의 공개 서비스와 인프라를 사용하여 클라우드 플랫폼 기능을 '라이브'로 평가하는 것이 중요합니다. 기술 평가는 최종 후보에 오른 CISP 마다 최소 하루 이상 진행하는 것이 좋습니다. 평가 중에는 다음을 수행할 수 있습니다. 1) 심층 평가를 실시하여 입증된 역량이 귀사의 RFP 요구 사항 및 CISP 의 서면 답변과 일치하는지 여부를 평가하고, 2) 귀사의 전문가가 CISP 를 조사하여 CISP 가 귀사의 특정 기술 및 조직 요구 사항에 적합하고 일치하는지 확인하며, 3) CISP 서비스는 물론, 미래의 요구를 충족하기 위해 확장하고, 복원력을 발휘하여 안전하게 운영하고, 혁신을 지속하는 CISP 의 능력에 대해서도 확신을 얻습니다.

클라우드 서비스 RFP 의 요구 사항에 응답할 때 CISP 는 요구 사항을 개략적으로 해석하여 부합 여부를 기술하는 경우가 있습니다. 이 경우 조직의 운영 환경/애플리케이션 요구를 충분히 반영하지 못하는 결과가 생깁니다. 업계 최고의 기술, 운영, 보안, 애플리케이션 전문가로 라이브 기술 평가 패널을 구성하는 것이 좋습니다. 평가자는 평가 내내 CISP 에 이의를 제기해야 하며, 모범 사례로서 CISP 를 독립적으로 채점해야 하고, 0~4(0=불량, 1=다소 불량, 2=수용 가능, 3=양호, 4=우수)와 같이 정해진 척도로 채점해야 합니다. 이후 데모 점수를 통합하여 각 평가 시나리오의 평균 점수를 전체 CISP 평가로 합산할 수 있습니다 표준 편차가 큰 시나리오는 확정하기 전에 평가 팀에서 논의되어야 합니다. 점수를 합산한 후 시나리오의 중요도에 따른 가중치를 적용할 수 있습니다.

데모 범위와 관련하여 CISP 의 플랫폼을 전체적으로 살펴본 다음, 플랫폼에서 실행되는 특정 워크로드를 보다 심층적으로 평가하는 것이 좋습니다. 아래는 플랫폼 및 워크로드 평가의 개요 예제입니다. 조직은 이 개요 예제를 기준선으로 삼아 시작하거나 개요 예제를 조직의 상황에 맞게 수정하여 선택한 CISP 가 조직의 특정 기능 요구 사항과 비기능 요구 사항을 충족하는지 확신할 수 있습니다. 모범 사례로서, 시나리오 및 요구 사항 목록을 제시한 공급자는 평가 범위를 극대화하고 20%의 Q&A 시간을 포함하는 라이브 평가 의제를 제안할 수 있습니다.

플랫폼 평가: 다수의 CISP 가 최적의 가치를 제공하고 위험을 최소화하는 클라우드 접근 방식을 지칭하기 위해 'Well Architected'라는 용어를 채택했습니다. 라이브 기술 데모의 Well Architected 시나리오에는 다음이 포함될 수 있습니다.

1. **보안:** 아이덴티티, 중앙 집중식 거버넌스, 자동 위협 감지, 데이터 보호, 이벤트 준비 상태
2. **성능 효율성:** 적정 규모로 조정, 확장성/탄력성, 서버리스
3. **신뢰성:** 고가용성(장애에 대한 탄력성), 변경에 따른 위험 최소화, 재해 복구, 백업
4. **비용 관리:** 재무 운영, 상업적 최적화, 예산 및 비용 할당
5. **운영 우수성:** 클라우드 마이그레이션과 클라우드 내 운영에 필요한 자동화, 모니터링, 지원, 관리 및 기능

워크로드 평가: 데모를 실시할 수 있는 일반적인 애플리케이션 유형은 다음과 같습니다.

- **웹 애플리케이션:** 백엔드 데이터베이스, 정적 객체 스토리지를 포함해 동적 웹 사이트를 공개적으로 호스팅
- **데이터 분석:** 여러 데이터 제공업체의 데이터를 통합하고 대량(TB/PB 크기의 데이터)의 다양한(정형, 비정형 등의 다양한 형식) 데이터를 빠른 속도(생성, 변경 및 쿼리 패턴의 속도)로 처리할 수 있는 데이터 레이크 또는 레이크 하우스
- **데이터 과학 플랫폼:** 조직 전반에 걸쳐 AI/ML 기반 기능을 개발, 배포 및 사용할 수 있는 플랫폼
- **IoT 애플리케이션:** 클라우드, 네트워크 기능, 디바이스를 포괄하는 IoT 플랫폼/기능

조직에 중요한 각각의 대표 워크로드별로, CISP 가 시연할 시나리오를 정의할 수 있습니다. 시나리오에서는 워크로드를 Well Architected 방식으로 배포하는 전반적인 능력을 입증해야 합니다. 다음 페이지에는 1) CISP 의 플랫폼 및 2) 웹 애플리케이션 워크로드 예제에 대한 라이브 기술 평가 기준 예제가 나와 있습니다.

플랫폼 – 라이브 기술 평가 예제

시나리오 ID	시나리오 이름	중요도 (1=낮음, 4=매우 높음)	데모 요구 사항	채점 고려 사항
Plat.Sec.1	아이덴티티 페더레이션	4	기존 아이덴티티 스토어에서 클라우드 서비스로 페더레이션하는 기능을 시연합니다.	• SAML 등의 표준 프로토콜 지원 • SCIM 기반 아이덴티티 복제 지원 • 기업 아이덴티티 스토어 내에서 각종 액세스 수준을 정의하고 클라우드 제공업체 내에서 적용할 수 있음 • 특정 팀/개인을 특정 계정/프로젝트/워크로드만 사용하도록 제한할 수 있음 • 속성 기반 액세스 제어(ABAC)를 지원하며, 클라우드 제공업체의 아이덴티티 및 관리(IAM) 시스템 내에서 이러한 속성을 사용하여 클라우드 리소스에 대한 액세스를 제어할 수 있음
Plat.Sec.2	중앙 거버넌스	4	정책과 요구 사항을 조직(글로벌 정책), 사업부, 프로젝트 수준에서 일원적으로 정의하는 기능을 시연합니다.	• 정책에는 다음이 포함되어야 합니다. 서비스 활성화/비활성화, 지리적 제한(지역 제한) 적용 • 관리자를 포함한 사용자가 감사/거버넌스 제어 수단을 비활성화하지 못하도록 제한
Plat.Sec.3	사용자 권한 제한	3	사용자 권한 강화를 위한 자동 권장 사항을 시연합니다.	• 현재의 사용 권한을 요구되는 사용 권한과 비교할 수 있음 • 최소 권한을 촉진하는 정책 자동 생성
Plat.Sec.4	감사 로깅	4	허용된 작업과 허용되지 않은 작업을 모두 포함하여 클라우드 활동에 대한 감사 기록을 시연합니다.	• 전체 조직에 대한 일원적 로그 • 낮은 수준의 추적과 책임을 지원하는 계정/프로젝트 고유 로그 • 로그를 쿼리할 수 있는 도구

시나리오 ID	시나리오 이름	중요도 (1=낮음, 4=매우 높음)	데모 요구 사항	채점 고려 사항
				• 특정 이벤트/로그 항목을 기준으로 트리거 작업을 활성화하는 도구 • 공급자 지원 활동을 확인할 수 있음 • 관리자도 로그를 삭제하지 못하도록 방지할 수 있음
Plat.Sec.5	네트워크 격리	4	가능한 경우 클라우드 내에서 서로 다른 테넌트를 격리하는 방법을 시연하고 입증합니다. 격리된(연결성 없음) 프라이빗(인터넷 없음) 서브넷과 퍼블릭(인터넷 액세스 있음) 서브넷의 구성을 시연합니다	• 테넌트(VPC 과 교차 연결 서비스에 있는 테넌트 포함) 분리 • 클라우드 인프라 외부(온프레미스)와 내부, 인터넷으로의 트래픽 흐름을 제어할 수 있음 • 컨테이너 호스팅 또는 서비스형 함수(FaaS)와 같은 공유 서비스를 사용할 때 분리를 적용하는 방법
Plat.Sec.6	저장 암호화	4	BYOK, 클라이언트 측 암호화 옵션을 포함하여 저장 데이터를 암호화하는 기능을 시연합니다	• 민감한 데이터에 대해 암호화를 요구할 수 있음 • 제공업체 관리형 키 또는 고객 관리형 키를 사용할 수 있음 • FIPS 140-2 준수 • 암호화 요구 사항을 준수하는 않는 경우에 경고하고 로깅할 수 있음 • 추가 비용에 미치는 영향 • 성능에 미치는 영향 • 양자 증명 알고리즘 및 키 크기 지원
Plat.Sec.7	전송 중 암호화	4	전송 중 데이터를 암호화하는 기능을 시연합니다	• 기본적으로 서비스 API 암호화 • 로드 밸런서, 관리형 API 에서 전송 중 암호화(TLS)를 활성화할 수 있음

시나리오 ID	시나리오 이름	중요도 (1=낮음, 4=매우 높음)	데모 요구 사항	채점 고려 사항
				• 상호(클라이언트 및 서버) 인증 지원
Plat.Sec.8	키 관리	4	키 관리 기능을 시연합니다. 전체 키 수명 주기 포함 클라우드 서비스와의 통합 포함	• 키 생성, 사용, 교체, 폐기에 대해 로깅
Plat.Sec.9	구성 관리	3	클라우드 플랫폼의 구성 관리 기능을 시연합니다	• 정확한 CMBD 유지 • 규정 준수 확인 • 비준수 상태를 기준으로 조치 자동 트리거 • 모범 사례 또는 사용자 지정 규칙에 따라 구성 변경 사항을 평가할 수 있음
Plat.Sec.10	네트워크 보안	3	서드 파티 규칙 세트/방화벽 및 볼륨 공격 보호와의 통합을 포함하여 웹 애플리케이션 방화벽과 방화벽 기능을 시연합니다	• WAF(웹 애플리케이션 방화벽) 기능: 확장성 • 프라이빗 및 퍼블릭 네트워크 지원 • 규칙 세트에 대한 산업/공급업체 피드를 구독할 수 있음 • WAF 의 이벤트를 기준으로 인프라 내에서 작업 자동 트리거 • 방화벽 기능, 확장성 • 호스트 기반 및 네트워크 기반 방화벽 • CIDR IP 블록을 지정하는 기능 외에 논리적 그룹 또는 객체를 참조할 수 있음 • 각 수준/구성 요소에서 지원되는 규칙 수 • 정책 및 네트워크 구성을 통해 분산 운영 모델(네트워크 팀 + 개발 팀)을 지원할 수 있음

시나리오 ID	시나리오 이름	중요도 (1=낮음, 4=매우 높음)	데모 요구 사항	채점 고려 사항
Plat.Sec.11	네트워크 연결	3	온프레미스 네트워크에 연결하는 기능과 엔드포인트/클라이언트를 클라우드 내 프라이빗 네트워크에 연결하는 기능을 시연합니다	• 프라이빗 연결(10Gbs 이상의 고대역폭) • 조직 전체의 라우팅 및 방화벽 정책을 제어할 수 있음 • VPN 연결(사이트 간 및 클라이언트 기반) • IPV6 지원
Plat.Sec.12	인스턴스 관리	3	인스턴스 관리 기능을 시연합니다.	• 대규모 인스턴스의 패치 상태를 모니터링하고 관리할 수 있음 • Linux 및 Windows 운영 체제의 패치 관리 지원 • SSH 를 사용하지 않고 전체 서버 플릿에서 명령을 실행할 수 있음 • 가상 머신에 대한 원격 액세스를 중앙에서 제어하고 감사할 수 있음 • 콘솔, CLI, API 를 통해 인스턴스 크기 변경, 추가 볼륨 연결, 네트워크 구성 변경 등을 수행할 수 있음
Plat.Sec.13	정책 적용	3	퍼블릭 인터넷에서 액세스하지 못하도록 서비스를 구성하는 기능을 시연합니다	• 중요/기밀 데이터를 담고 있을 가능성이 높은 서비스에 대해 트래픽을 프라이빗 네트워킹으로 격리할 수 있음 • 소스 네트워크를 기반으로 데이터에 대한 액세스를 제어하는 정책을 정의할 수 있음 • 높은 수준의 보안 인증 정보를 가진 사용자를 포함하여 모든 사용자에게 이러한 액세스 제한을 적용하는 기능

시나리오 ID	시나리오 이름	중요도 (1=낮음, 4=매우 높음)	데모 요구 사항	채점 고려 사항
Plat.Sec.14	취약성 검사	2	이미지(컨테이너 및 VM)의 취약성을 검사하는 기능을 시연합니다	• 레지스트리에서 컨테이너를 자동으로 검사할 수 있음 • 가상 머신에서 알려진 취약성을 검사할 수 있음 • 네트워크 검사를 수행할 수 있음
Plat.Sec.15	네트워크 검사	2	고객 환경 내에서 네트워크 트래픽(NetFlow 및 전체 패킷)을 캡처/미러링하는 기능을 시연합니다	• 전체 패킷 캡처를 포함해 클라우드 제공업체 인프라 내의 트래픽 일부/전부를 미러링할 수 있음 • 캡처할 트래픽을 간단하게 선택할 수 있음 • 초대규모 트래픽 볼륨(50Gbps 이상)으로 확장할 수 있음
Plat.Sec.16	위협 탐지	3	네트워크의 위협, 보안 인증 사용 및 사용 패턴 분석을 비롯해 플랫폼의 침입 탐지 기능을 시연합니다.	• 마이닝과 같은 의심스러운 활동을 탐지할 수 있음 • SSH 로그인 등 인증 공격에서 무차별 암호 대입 행위를 탐지할 수 있음 • 보안 인증 정보 유출 또는 남용을 탐지할 수 있음 • ML 을 적용하여 다수의 이벤트를 분석하고 우선순위가 높은 이벤트 표면화 • 활성화/구성 활동(간단할수록 좋음) • 외부 서비스와 통합하고 알림을 트리거할 수 있음 • 모든 프로젝트/계정에 대해 글로벌 수준에서 IDS 를 구성할 수 있음
Plat.Perf.1	컴퓨팅 최적화	2	가상 머신 비용과 서비스형 함수의 비용을 최적화하기 위한 자동 권장 사항을 시연합니다	• 실제 활용률 및 워크로드 패턴을 기반으로 한 권장 사항 • 추정 절감액과 예상되는 부하 수준/기술 영향에 대한 인사이트가 권장 사항에 포함됨

시나리오 ID	시나리오 이름	중요도 (1=낮음, 4=매우 높음)	데모 요구 사항	채점 고려 사항
				• 절감액과 가상 머신이 너무 작게 구성되는 등의 '성능 위험'이 모두 최적화에 포함되어야 함
Plat.Perf.2	환경 최적화	2	로드 밸런서, 네트워킹, 데이터베이스, 스토리지 등, 다른 클라우드 구성 요소에 대한 자동 권장 사항을 시연합니다	• 권장 사항에서 핵심 컴퓨팅 이외의 구성 요소에서 기대되는 절감액과 잠재적 성능 효율 개선 기회를 특정함
Plat.Perf.3	컴퓨팅 오토 스케일링	4	가상 컴퓨팅 환경에서 로드 밸런서 배후에 배포되는 애플리케이션의 오토 스케일링 기능을 시연합니다. 사용 가능한 각종 옵션/접근 방식과 스케일링 이벤트 전후에 알림 등의 다른(선택 사항) 조치를 트리거할 수 있는 기능을 시연합니다	• 스케일링의 다양한 옵션(트리거 기반, 시간 기반, 수동 또는 기계 학습을 적용해 필요한 용량을 예측하는 지능형 접근 방식) • 로드 밸런서 및 건전성 점검 등록 등 스케일링 완전 자동화 • 스케일링 수명 주기의 특정 시점에서 임의의 코드 조각을 실행할 수 있음
Plat.Perf.4	스토리지의 온라인 확장	3	워크로드를 중단하지 않고 블록 스토리지의 용량과 스루풋을 모두 확장할 수 있는 기능을 시연합니다	• 서비스를 완전히 재구성할 필요 없이 서로 다른 스토리지 유형 간에 블록 스토리지를 전환하는 기능 • VM 에 제공되는 볼륨 크기를 늘리는 기능
Plat.Perf.5	관리형 서비스의 오토 스케일링	3	소수(수십 명)에서 다수의(수천 명) 동시 사용자를 지원하도록 객체 스토어, API 게이트웨이, FaaS 플랫폼, NoSQL 데이터베이스를 확장하는 기능을 시연합니다	• 관리자의 개입 없이 원활하게 오토 스케일링 • 스케일 업 활성 기간 동안 프로덕션 스케일링 요구 사항에 맞게 일관된 성능 제공 • FaaS 와 같은 일부 구성 요소의 경우 필요에 따라 사전 예열, 동시 실행 제한 관리 등의 옵션도 모색해야 함

시나리오 ID	시나리오 이름	중요도 (1=낮음, 4=매우 높음)	데모 요구 사항	채점 고려 사항
Plat.Perf.6	컨테이너 기반 워크로드	3	컨테이너 기반 워크로드를 호스팅하는 기능을 시연합니다	• 컨테이너 호스팅 플랫폼을 위한 옵션 • 로드 밸런서와 같은 다른 IaaS 구성 요소와 통합 • 서비스 메시 솔루션의 가용성 • Kubernetes 등 컨테이너 호스팅을 위한 비독점 옵션 • 컨테이너 제어 평면 내에서 고가용성 기본 지원 • 온프레미스 컨테이너 호스트를 관리할 수 있음
Plat.Rel.1	리전 복원력	4	국지적인 장애(예: 정전)가 발생한 상황을 가정해 리전 내 관계형 데이터베이스 인스턴스의 자동 장애 조치를 시연합니다	• 자동 장애 조치 • 클라우드 리전 내에서 장애 영역 격리 • 명확하게 경계를 나눠 간단하게 설계함으로써 고가용성 실현
Plat.Rel.2	인스턴스 자동 복구	2	건전성 점검 실패에 따른 단일 인스턴스/인스턴스 세트의 자동 복구를 시연합니다	• 건전성 점검 구성 가능 • 인스턴스 복구/리프로비저닝 완전 자동화
Plat.Rel.3	로드 밸런서 건전성 인식	3	로드 밸런서가 장애가 있는 인스턴스를 자동으로 감지하고 트래픽을 다른 정상 호스트로 리라우팅하는 방법을 시연합니다	• 건전성 점검 구성 가능 • 정상 호스트로 트래픽 자동 라우팅

시나리오 ID	시나리오 이름	중요도 (1=낮음, 4=매우 높음)	데모 요구 사항	채점 고려 사항
Plat.Rel.4	리전 장애 조치	3	보조 리전으로 트래픽 자동 이전 등 다중 리전 아키텍처를 시연합니다	• 전역적 건전성 점검 • 자동 라우팅 옵션: 지연 시간, 가중치 및 장애 조치 • 가상 머신 워크로드와 객체 스토어 /NoSQL 데이터베이스 서비스 등의 관리형 서비스 지원
Plat.Rel.5	백업 및 복구	4	가상 머신, 데이터베이스, 관리형 서비스에 대해 백업 및 복구 옵션을 시연합니다	• 자동화 수준 • 같은/다른 클라우드 리전에 복원할 수 있음 • 다른 클라우드 리전에 백업본을 복사할 수 있음
Plat.Cost.1	예산	3	하위 계정, 프로젝트에 맞게 구조화하는 방법 등 예산 관리 기능을 시연합니다	• 조직의 다양한 수준에서 예산 관리 및 모니터링을 적용하는 기능을 고려해야 함 • 태깅을 통해 구성 요소를 그룹화하는 기능, 특정 클라우드 서비스에 대해 예산을 설정하는 기능, 경보/모니터링에 대해 임계값을 구성하는 기능 등 유연성을 확인해야 함
Plat.Cost.2	예산 할당	1	프로젝트에 대한 예산 할당 프로세스 등 새로운 프로젝트 환경(계정)을 제공하는 방법을 시연합니다. 1) 기술적 검토/IT, 2) 상업적 검토/재무에 대한 수동 승인 단계가 프로비저닝에 포함되어야 합니다	• 적절한 승인을 받아 자체 프로비저닝을 수행할 수 있음 • 조직에 맞게 적절한 예산 설정, 알림 또는 예산 정책의 구성 자동화
Plat.Cost.3	예산 보고	2	조직 전체의 예산에 대해 보고할 수 있는 기능을 시연합니다. 특정 부서와 조직 전체(필수 정보로 제한)에 대해	• 조직의 다양한 수준에서 가시성을 제공하여 인식과 투명성을 확보할 수 있음. 단, 필수 정보만 제공하는 방식으로 제공함

시나리오 ID	시나리오 이름	중요도 (1=낮음, 4=매우 높음)	데모 요구 사항	채점 고려 사항
			보고서를 작성합니다. '실제' 지출액뿐 아니라 예상/추정 지출액도 보고서에 포함되어야 합니다	• 예측은 현재와 과거의 소비 동향을 기반으로 하며, 예산 초과 가능성이 있을 경우 조기 경고를 제공해야 함
Plat.Cost.4	예산 관리	1	예산 임계값에 도달했을 때 조치를 취할 수 있는 능력을 시연합니다. 조치에는 알림, 제한 적용 또는 예산 초과 지출을 방지하기 위한 적극적 개입이 포함될 수 있습니다	• 여러 프로젝트에 대해 간단히 조치를 정의할 수 있음 • 프로젝트마다 다르게 조치를 수행하는 기능. 예를 들어 개발 환경과 프로덕션 환경에 대해 다른 조치를 수행할 수 있음 • 같은 예산/프로젝트에 대해 여러 개의 조치와 임계값을 정의할 수 있음 • 표준 기능 외에 사용자 지정 조치를 정의할 수 있음
Plat.Cost.5	예산 주기성	1	일간/월간/연간 등 기간에 따라 예산을 적용하는 기능을 시연합니다. 연간 예산의 경우 연간 예상 지출의 변동 분포를 적용하는 기능을 시연합니다	• 다양한 기간에 대한 예산을 정의할 수 있음 • 연간 예산의 경우 1 년에 걸친 지출 분배를 구성할 수 있음. 세금 신고 등의 계절적/고탄력적 워크로드에 특히 중요함
Plat.Cost.6	서드 파티 마켓플레이스	3	서드 파티 제품을 구입하고 배포할 수 있는 기능을 시연합니다. 마켓플레이스를 통해 제공되는 서드 파티 제품 세트에 대한 예산을 설정하는 방법과 사용 가능한 제품을 제한하는 기능을 시연합니다	• 특정 제품에 대한 예산(글로벌 예산, 프로젝트/계정 세트 예산)을 설정할 수 있음 • 광범위한 마켓플레이스의 일부만 클라우드 사용자에게 제시할 수 있음
Plat.Cost.7	컴퓨팅 요금 모델	3	가상 머신에 적용할 수 있는 다양한 요금/상용 모델을 시연합니다	• 장기 약정, 세분화된(분/시간당) 요금이 필요 없는 온디맨드 모델이 있어야 함

시나리오 ID	시나리오 이름	중요도 (1=낮음, 4=매우 높음)	데모 요구 사항	채점 고려 사항
				• 장기 약정을 선택하는 대가로 할인을 받을 수 있음 • 중단 가능성이 있는 인스턴스를 구입하는 대가로 할인을 받을 수 있음 • 같은 프로젝트/계정에서 이들 모델을 혼용할 수 있어야 하며, 이점을 다른 계정과 공유할 수 있어야 함
Plat.Cost.8	상업적 최적화 권장 사항	3	상업적 최적화 권장 사항을 받아 지출을 (기술적 변경 없이) 최적화하는 기능을 시연합니다	• 가상 머신 및 관리형 데이터베이스를 비롯한 여러 서비스에 대한 전반적인 권장 사항 • 권장 사항을 간단히 수행하고 예상 절감액/이점을 파악할 수 있음
Plat.Cost.9	전용 호스트	4	전용 호스트를 프로비저닝하여 특정 호스트에 연결된 온프레미스 라이선스를 사용할 수 있도록 지원하는 기능을 시연합니다	• 프로비저닝 용이 • 호스트 활용률을 관리할 수 있음 • 여러 프로젝트/테넌시 간에 호스트를 공유할 수 있음
Plat.Ops.1	가상 머신 마이그레이션	3	가상 머신을 온프레미스에서 클라우드 기반 VM 서비스로 가져오는 방법을 시연합니다	• Windows 및 Linux 기반 운영 체제를 모두 가져올 수 있음 • 여러 머신을 한 번에 가져올 수 있음 • 복제 세션을 유지 관리하여 클라우드에 대한 신속한 '장애 조치'를 지원할 수 있음
Plat.Ops.2	DevOps 및 자동화 기능	4	환경을 코드로 정의하는 방법, 완전 자동 배포를 통한 지원, 자동 테스트 및 롤백 등 DevOps/자동화 기능을 시연합니다	• 네트워크, 가상 머신, 스토리지, 데이터베이스 등 모든 시스템 구성 요소를 코드로 정의할 수 있음 • 파이프라인을 만들 수 있음 • 코드 리포지토리를 만들 수 있음

시나리오 ID	시나리오 이름	중요도 (1=낮음, 4=매우 높음)	데모 요구 사항	채점 고려 사항
				• 빌드를 자동화할 수 있음 • 블루/그린 배포를 수행할 수 있음 • 환경을 여러 개 생성하고 여러 단계에 걸쳐 배포할 수 있음 • 실패한 배포 자동 롤백
Plat.Ops.3	애플리케이션 호스팅	2	로우 코드/플랫폼 서비스에서 단순한 2 계층 애플리케이션을 호스팅하는 방법을 시연합니다. 애플리케이션/웹 계층을 위한 관계형 데이터베이스 및 오토 스케일링 기능 포함	• UI 를 통한 간편한 구성 • 건전성 점검, 스케일링, 고가용성 포함 플랫폼 지원, Windows 및 Linux
Plat.Ops.4	보안 통합	2	보안 인시던트 및 이벤트 관리의 관점에서 플랫폼의 통합 기능을 시연합니다	• 통합을 위해 클라우드 제공업체와 API 의 보안 관련 로그를 손쉽게 통합하여 사용할 수 있음
Plat.Ops.5	ITSM 통합	3	ITSM(IT 서비스 관리) 관점에서 플랫폼의 통합 기능을 시연합니다	• API 를 통해 지원 사례를 제기, 모니터링, 업데이트할 수 있음 • API 를 통해 서비스 또는 서비스 세트를 '제품'으로서 프로비저닝할 수 있음
Plat.Ops.6	지원	4	지원 오퍼링을 시연합니다	• 워크로드 유형별로 지원 수준이 다름 • 특정 서비스에 적합한 운영 체제/데이터베이스 엔진 등도 지원할 수 있음 • 중요 워크로드에 대해 전담 지원 리더를 통해 고급 오퍼링을 제공할 수 있음

시나리오 ID	시나리오 이름	중요도 (1=낮음, 4=매우 높음)	데모 요구 사항	채점 고려 사항
				• 체계적인 이벤트 준비 및 아키텍처 검토 프로세스를 제공할 수 있음 • 제공업체 로드맵에 대한 인사이트
Plat.Ops.7	감사 용이성	4	규정 준수 감사를 지원하는 데 필요한 도구를 시연합니다	• 콘솔을 통해 규정 준수 감사 세부 정보를 얻을 수 있음 • 환경 감사를 관리하고 자동화할 수 있음
Plat.Ops.8	VM 에서 컨테이너로	1	가상 머신의 애플리케이션을 컨테이너로 변환하고 클라우드 제공업체의 컨테이너 플랫폼을 사용해 서비스를 제공하는 방법을 시연합니다	• 변환 용이 • 변환 시간 • 플랫폼 지원, .Net 및 Java

워크로드: 웹 애플리케이션 - 라이브 기술 평가 예제

다음 섹션에서는 특정 '웹 애플리케이션' 워크로드에 대한 워크로드 평가 시트 예제를 제공합니다. 특정 애플리케이션에 대한 평가 시트를 개발할 때는 요구 사항, 당면 과제, 제약 사항을 잘 아는 애플리케이션 사용자, 개발자, 관리자를 참여시키는 것이 좋습니다.

시나리오 ID	시나리오 이름	중요도 (1=낮음, 4=매우 높음)	데모 요구 사항	채점 고려 사항
Web.Sec.1	보안 - 애플리케이션 보호	3	SQL 명령어 삽입, XSS 스크립팅 공격 및 기타 공격을 통해 애플리케이션을 악용하려는 악의적인 시도를 차단하는 기능을 시연합니다	• '즉시 사용 가능한' 표준 규칙/기능으로 일반적인 공격을 방어할 수 있음 • 사용자 지정 검사/규칙/함수를 생성할 수 있음
Web.Sec.2	보안 - 속도 기반 보호	3	단시간에 많은 요청을 애플리케이션으로 보내거나 대량의 데이터를 애플리케이션으로 보내는 등의 공격을 차단/방어하는 기능을 시연합니다	• 특정 IP 주소 또는 주소 목록에서 한도를 구성하고 요청 속도를 제한할 수 있음
Web.Sec.3	보안 - 소스 기반 보호	3	네트워크/지리적 소스에 따라 액세스를 제한하는 기능을 시연합니다	• 네트워크 블록 또는 네트워크 블록 목록으로 제한할 수 있음 • IP 목록을 관리할 필요 없이 오리진 국가별로 제한할 수 있음
Web.Sec.4	보안 - 네트워크 세분화	4	인프라를 통해 남북 트래픽 흐름과 동서 트래픽 흐름이 발생하는 것을 막기 위해 구성 요소(웹 서버, 앱 서버/DB 서버)를 격리/보호하는 기능을 시연합니다	• 구성 요소를 서로 다른 서브넷에 배치하고 여러 서브넷 간의 트래픽 흐름을 제어할 수 있음 • 네트워크 인터페이스 수준에서 트래픽 흐름을 제어할 수 있음 • 논리 그룹 및 CIDR 블록을 참조할 수 있음
Web.Sec.5	보안 - TLS 지원 및 인증서 관리	4	TLS 보안 엔드포인트를 제공하고, 인증서 자동 교체 등을 비롯하여 TLS 보안 엔드포인트를 제공하도록	• 최신 TLS 프로토콜 지원(필요한 경우 기존 버전 비활성화 가능) • 간단한 인증서 생성, 관리 및 교체(완전 자동화하는 것이 이상적)

시나리오 ID	시나리오 이름	중요도 (1=낮음, 4=매우 높음)	데모 요구 사항	채점 고려 사항
			지원하는 구성 요소를 자동으로 관리하는 기능을 시연합니다	
Web.Perf.1	성능 - 확장성	4	동적 오토 스케일링을 통해 웹 애플리케이션의 동시 사용자를 10 명에서 10 만 명으로 확장하는 능력을 시연합니다	• 시간 기반 및 트리거 기반 스케일링 규칙을 정의할 수 있음 • 최종 사용자, 관리자를 위한 원활한 스케일링 로드가 증가하면 자동으로 스케일 아웃하고 로드가 감소하면 자동으로 스케일 인 • 웹 애플리케이션의 각 계층(로드 밸런서, 웹 계층, 데이터 계층 등)에 확장성이 있는지 확인 • 필요에 따라 애플리케이션의 여러 계층에서 서비스를 캐싱할 수 있음
Web.Perf.2	성능 - 글로벌 제공	3	호주, 아시아, 아프리카, 중동, 북아메리카, 남아메리카, 유럽을 비롯한 전 세계 여러 지역에서 지연 시간을 시연하는 등, CDN 기능을 시연합니다	• CISP 콘솔/API 를 통해 CDN 을 만들고 구성할 수 있음 • 여러 지역에 대해 배포 규칙 구성 가능 • 다양한 사용 사례/애플리케이션에 대해 캐싱 구성 가능
Web.Rel.1	신뢰성 - 단일 리전 복원력	4	CISP 데이터 센터 네트워크 연결 손실과 같은 국지적 이벤트에 대한 내결함성을 시연합니다	• 클라우드 리전(도시)의 자동 장애 조치 및 고가용성
Web.Rel.2	신뢰성 - 다중 리전 배포	3	전역적으로 복제된 데이터베이스를 포함하여 웹 애플리케이션의 다중 리전 배포를 시연합니다	• 다중 리전 애플리케이션을 프로그래밍 방식으로 배포할 수 있음 • 데이터 스토어의 리전 간의 복제 • 최적의 리전으로 사용자 자동 라우팅

시나리오 ID	시나리오 이름	중요도 (1=낮음, 4=매우 높음)	데모 요구 사항	채점 고려 사항
Web.Rel.3	신뢰성 - 다중 리전 장애 조치	3	리전에 영향을 미치는 서비스 문제가 발생한 상황에서 웹 애플리케이션의 자동 장애 조치를 시연합니다	• 여러 클라우드 리전의 자동 장애 조치 및 고가용성
Web.Cost.1	비용 - 가시성	2	애플리케이션당 비용을 추적하는 기능을 시연합니다	• 스케일 업/스케일 다운되는 때를 비롯하여 특정 애플리케이션의 과거 비용을 확인할 수 있음
Web.Cost.2	비용 - 예산	2	애플리케이션별로 예산과 관련 알림을 설정하는 기능을 시연합니다	• 애플리케이션별로 예산을 구성할 수 있으며, 구성한 임계값을 기반으로 조치/경고를 트리거할 수 있음
Web.Ops.1	운영 - 유지 보수 간격	3	특히 유지 보수가 애플리케이션 가용성에 영향을 미칠 수 있는 경우에 비즈니스 요구 사항에 맞게 유지 보수 기간을 구성하는 기능을 시연합니다	• 관계형 데이터베이스 서비스와 같은 구성 요소에 대해 유지 보수 기간 구성 가능
Web.Ops.2	운영 - 로깅	3	가상 머신 종료/장애 발생 시 로그를 보존하는 기능을 비롯해, 여러 구성 요소에서 애플리케이션에 대한 로깅을 중앙 집중화하는 기능을 시연합니다	• 애플리케이션 요구 사항에 따라 크기를 조정할 수 있는 중앙 집중식 로깅 서비스를 구성할 수 있음 • 특정 로그 이벤트를 기준으로 경고 또는 조치를 트리거하는 규칙/필터를 정의할 수 있음
Web.Ops.3	운영 - 모니터링	3	성능, 가용성, 응답 시간, 오류 수 등에 대한 애플리케이션 모니터링 기능과 다양한 지표 임계값을 기준으로 조치를 취하거나 알림을 트리거하는 기능을 시연합니다	• 디스크 IO, CPU, 데이터베이스 지표, 네트워크, 로드 밸런서 등, 사용 가능한 표준 지표의 모음 • 사용자 지정 지표와 임계값을 정의할 수 있음 • 가장 중요한 지표를 나타내는 사용자 지정 대시보드를 만들고 그러한 대시보드를 관련 사용자와 공유할 수 있음