AWS 관리형 서비스 공급자(MSP) 프로그램

MSP 검증 체크리스트

2025년 8월 - 7.1

버전(7.1)으로 업데이트된 이 AWS 관리형 서비스 제공업체(MSP) 프로그램 체크리스트는 2025년 8월 29일부터 유효합니다. 파트너는 2026년 2월까지 버전 7.0을 사용할 수 있으며, 이 체크리스트 버전은 해당 시점이 지나면 더 이상 적용되지 않습니다. 2025년 11월 27일 이후에 제출된 모든 신청서는 현재 검증 체크리스트 요구 사항을 준수해야 합니다.

자체 평가 스프레드시트

소개

Amazon Web Services, Inc.(AWS) 관리형 서비스 제공업체('MSP') 파트너 프로그램 검증 체크리스트('체크리스트')는 AWS 관리형 서비스 제공업체 파트너 프로그램('MSP 프로그램')에 지원하려는 AWS 파트너 네트워크 파트너('AWS 파트너')를 대상으로 합니다. MSP 프로그램의 목적은 전체 고객 계약 수명 주기 동안 고객에게 최고 수준의 AWS 클라우드 관리형 서비스 경험을 제공하는 AWS 파트너를 알리는 것입니다. 이 체크리스트는 AWS 파트너가 MSP로 지정되어 AWS MSP 파트너로 불리는 데 필요한 기준을 제공합니다. 고객 참여 수명 주기, 즉 계획/설계, 구축/마이그레이션, 실행, 최적화의 모든 단계에서 고객을 지원하기 위해 '차세대 관리형 서비스 제공업체'가 갖춰야 하는 역량에 대한 AWS의 관점을 기술합니다.

모든 필수 전제 조건 제어를 충족할 경우 AWS 파트너는 역량에 대한 기술 검증을 받게 됩니다. AWS는 기술적 검증을 용이하게 하기 위해 사내 전문가 및 서드 파티를 활용합니다. AWS에는 언제든지 고지 없이 이 문서의 내용을 변경할 권리가 있습니다.

MSP 프로그램 프로세스 개요

MSP 프로그램에 신청하기 위한 상위 절차에는 다음 단계가 포함됩니다.

1. 이 문서에 있는 요구 사항을 확인하여 신청 전제 조건을 이해합니다.
2. 자체 평가 스프레드시트를 작성하여 제출합니다.
3. AWS MSP 팀이 스프레드시트의 전제 조건 항목을 검토하고 필요에 따라 추가 정보를 요청합니다.
4. ISSI가 연락하여 일정을 잡고 최종 기술 검증을 수행할 것입니다.
5. AWS MSP 팀에서 ISSI 감사 결과를 검토하고 나머지 문제를 해결합니다.
6. 파트너가 MSP 프로그램에 참여합니다.

체크리스트 업데이트

이 문서 및 AWS MSP 프로그램은 새로운 모범 사례와 파트너의 피드백, 전문화 프로그램 변경 사항 및 새로운 서비스 역량을 반영하기 위해 정기적으로 업데이트됩니다. 업데이트 과정을 예측할 수 있도록 새로운 제어 또는 상당한 변경 사항이 적용된 제어가 포함된 메이저 업데이트(예: 7.x)는 릴리스 후 90일 이내에 공식적으로 인정된 버전으로 지원됩니다. 기존 제어에 대한 보강 설명 및 마이너 업데이트가 포함된 마이너 업데이트(예: 7.x.y)는 즉시 감사에 사용할 수 있습니다. AWS MSP 프로그램 팀은 사소한 변경 사항과 중대한 변경 사항을 포함하여 예정된 변경 사항을 릴리스하기 전에 항상 파트너에게 알립니다.

검증 체크리스트 버전 7.1은 버전 7.0을 기반으로 작성되었으며, 변경 로그에 기록된 대로 소규모 업데이트가 적용되어 기존의 모든 항목을 유지하면서 여러 항목에 대한 명확성을 높였습니다. 파트너는 이제 검증 체크리스트 버전 7.1을 즉시 사용할 수 있습니다. 이번 버전은 2024년 4분기 AWS MSP 프로그램 평가 기준의 주요 수정 사항으로 도입된 버전 7.0에서 설정된 핵심 프레임워크를 유지합니다. VCL 7.1의 즉각적인 제공을 통해 문서화 및 절차상의 설명을 개선하여 파트너는 특정 제어 기능을 더 잘 이해하고 구현할 수 있습니다.

AWS 관리형 서비스 제공업체(MSP) 감사 프로세스는 이제 특정 제어 항목이 전제 조건 제어 항목으로 지정된 하이브리드 모델로 전환되었습니다. 파트너는 기술 검증 단계로 진행하기 전에 이러한 전제 조건 제어를 충족해야 합니다.

전제 조건 제어: 새로운 하이브리드 감사 모델에서는 파트너가 먼저 특정 전제 조건 제어를 충족해야 합니다. 이러한 전제 조건 제어 항목은 검증 체크리스트 7.1 자체 평가 스프레드시트를 사용하여 오프라인에서 작업할 수 있으며, 파트너는 기술 검증을 원하는 날짜로부터 최소 30일 전에 필요한 증거 자료와 문서를 AWS MSP 프로그램 팀 (aws-msp@amazon.com)에 제출해야 합니다.

전제 조건 제어 항목은 파트너가 보다 포괄적인 기술 검증을 진행하기 전에 먼저 탄탄한 기반을 갖출 수 있도록 설계되었습니다. 이러한 접근 방식을 통해 파트너는 필수 요구 사항을 사전에 해결하는 데 집중하여 전체 감사 프로세스를 간소화할 수 있습니다.

첨부 파일 또는 문서 제출의 경우 PDM과 협력하여 AWS Approved BOX 폴더를 만들고 여기에 문서를 업로드하시기 바랍니다. 자체 평가 워크시트에 링크를 삽입하세요.

또는 선호하는 문서 공유 앱에서 폴더를 만들고 자체 평가 워크시트에서 링크와 자격 증명을 공유하는 방법도 있습니다.

기술 검증: AWS MSP 감사의 기술 검증 단계는 서드 파티 회사에서 수행합니다. 이 기술 검증은 하루 동안 진행되며, 감사자는 파트너의 역량, 프로세스, AWS MSP 체크리스트의 나머지 제어 항목의 규제 준수를 철저하게 평가합니다.

파트너는 지정된 기간 내에 전제 조건 제어 항목을 해결하고 모든 필수 문서 및 증거 자료를 AWS MSP 프로그램 팀에 제공하여 기술 검증에 대해 적절히 준비했는지 확인해야 합니다.

하이브리드 접근 방식으로 AWS MSP 감사 진행 시 목표는 평가 프로세스의 효율성과 효과성을 향상하여 파트너가 가장 중요한 영역에 미리 집중하고 기술 검증 단계를 간소화하도록 하는 데 있습니다.

파트너는 AWS MSP 프로그램 팀(aws-msp@amazon.com) 또는 Partner Development Manager(PDM)에게 문의하여 최신 감사 프로세스 및 전제 조건 제어 항목에 대한 설명이나 지원을 받는 것이 좋습니다.

AWS 관리형 서비스 제공업체(MSP) 프로그램 요구 사항

프로그램에 대한 새로운 신청서 및 전체 감사 갱신을 위한 MSP 프로그램 전체 감사(아래 정의) 일정을 잡기 전에 먼저 다음 항목이 충족되어야 합니다.

1. **APN 프로그램 요구 사항**
    1. **AWS 서비스 파트너 티어**

        Advanced 또는 Premier 티어 AWS 서비스 파트너(요구 사항 보기)

2. **AWS 고객 배포 사례**
    1. **고객 사례 연구**

        AWS 고객 사례 연구 4건 이상(공개 사례 연구 2건 이상 포함)

3. **AWS Partner Central과 AWS 계정의 연결**
    1. **AWS 파트너 계정**

        파트너의 AWS Partner Central 계정은 해당 AWS 계정에 연결되어야 합니다. 이를 통해 파트너는 2025년에 출시된 AWS 채널 파트너의 새로운 기능 및 API에 액세스할 수 있습니다.

4. **AWS Solutions Provider Program(SPP)**
    1. **최종 사용자 보고**

        SPP 프로그램에 등록한 파트너는 최종 사용자 보고 요구 사항을 90%를 초과하여 준수해야 합니다. SPP 프로그램 등록은 MSP 신청의 필수 조건/전제 조건이 아니라는 점을 유의하시기 바랍니다.

5. **자체 평가**
    1. **체크리스트 자체 평가**

        AWS 파트너는 프로그램 신청서를 제출하기 전이나 갱신에 대한 전체 감사 일정을 잡기 전에 먼저 이 페이지 상단에 링크로 연결된 자체 평가 스프레드시트를 작성해야 합니다.

        신규 신청: 완료한 자체 평가를 AWS Partner Central의 신청서에 업로드하세요. 자세한 설명은 AWS 전문화 프로그램 가이드를 참조하세요.

        MSP 갱신 파트너의 경우: 완료한 자체 평가 워크시트를 감사 예정일로부터 최소 30일 전에 aws-msp@amazon.com으로 직접 보내주세요.

        파트너는 모든 관련 문서 및 지원 링크를 비롯해 전제 조건 제어 항목에 대한 포괄적인 응답을 제공해야 합니다. 기술 검증 제어의 경우 파트너는 제어가 '충족'인지 '미충족'인지 여부만 표시하면 됩니다. 그런 다음 감사자는 1일 감사 프로세스를 통해 기술 검증 제어를 철저하게 평가합니다.

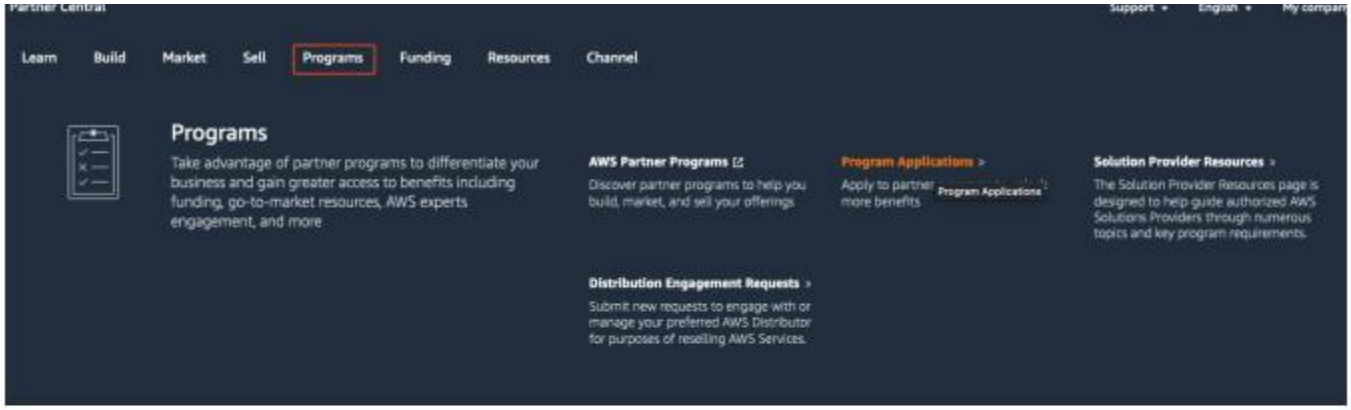
        AWS 파트너는 자체 평가를 작성한 후 Solutions Architect, PDR 및/또는 PDM의 검토를 거친 후 MSP 프로그램 팀에 제출하는 것이 좋습니다. 이는 담당 AWS 팀이 파트너와 업무 협조를 잘해나가고 있는지 확인하고, 감사 전에 파트너에게 필요한 내용을 조언함으로써 감사 결과가 긍정적으로 나올 수 있도록 하기 위함입니다.

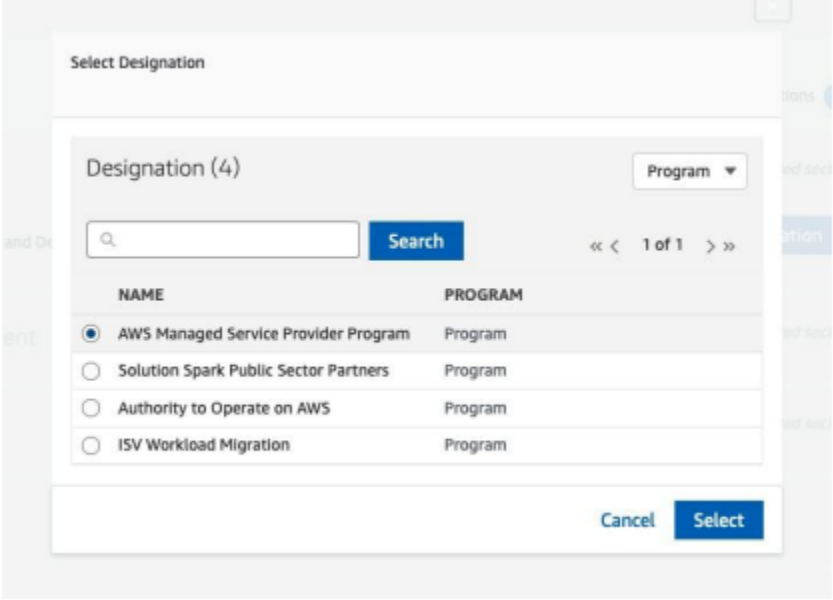
기대 사항

AWS 파트너는 모든 프로그램 요구 사항이 충족되어도 MSP 프로그램에 대한 신청서를 제출하기 전에 먼저 이 문서를 상세히 검토하시기 바랍니다. 문서의 항목이 명확하지 않고 자세한 설명이 필요한 경우 AWS 파트너 개발 담당자(PDR) 또는 파트너 개발 관리자(PDM)에게 문의하세요. 추가 지원이 필요한 경우 PDR/PDM이 MSP 프로그램 팀에 연락할 것입니다.

AWS 파트너가 MSP 프로그램 신청서를 제출할 준비가 되면 AWS 파트너는 이 페이지 상단에 링크로 연결된 '자체 평가 스프레드시트'를 작성해야 합니다. AWS Partner Central에서의 신청 단계는 AWS 컴피턴시, AWS 서비스 제공, AWS Service Ready 또는 AWS MSP 모두 동일합니다. 아래 나열된 신청 단계에 대한 자세한 내용은 프로그램 가이드를 참조하세요.

1. 프로그램으로 이동
2. 프로그램 신청서로 이동
3. 새 신청서를 작성하려면 'Create' 클릭
4. AWS 관리형 서비스 제공업체(MSP) 지정 선택
5. 제품 및 서비스 첨부
6. 사례 연구 첨부
7. 담당자(POC)를 지정하고 문서 첨부
8. 신청서를 제출하고 추적





AWS에서는 영업일 기준 10일 이내에 신청서를 검토하고 질문에 회신하며 프로세스 및 제어 개요와 원하는 경우 전체 감사(아래 정의 참조) 일정을 예약하는 방법에 대한 정보를 제공합니다.

다음 단계로 넘어가도록 신청이 승인된 AWS 파트너는 원하는 경우 전체 감사를 준비하기 위해 ISSI(AWS의 제3자 감사 기관)와 함께 프로세스 및 제어 개요(이전의 '사전 평가') 세션을 거칠 수 있습니다. 이는 선택 사항이며 필수는 아닙니다. 프로세스 및 제어 개요는 선호하는 회의 플랫폼을 사용하여 진행되는 원격 세션으로, 4~6시간이 소요됩니다. 처음 1~2시간은 체크리스트 제어 항목을 충족하기 위한 문서 준비의 모범 사례를 비롯한 감사 프로세스에 중점을 둡니다. 남은 시간은 파트너가 최신 버전의 AWS MSP 파트너 프로그램 검증 체크리스트에 명시된 감사 요구 사항을 논의하고 경험이 풍부한 제3자 MSP 감사 기관과 함께 필수 증거 자료를 이해하는 데 사용됩니다. 준비된 자료를 검토하거나 특정 제어 항목에 대해 자세히 알아보는 시간이 아닙니다.

파트너는 ISSI와 협력하여 AWS MSP 파트너 전제 조건 컨설팅 서비스를 받을 수 있습니다(전체 선택 사항). 이 세션에는 AWS MSP 프로그램 검증 체크리스트의 전제 조건 제어를 위해 파트너가 준비한 증거 자료에 대한 상세한 검토가 포함됩니다. ISSI 컨설턴트는 조사 결과 및 개선 계획(있는 경우)을 요약한 집중 서면 보고서를 제공합니다. 전제 조건 컨설팅 서비스는 원격 세션으로, 원하는 컨퍼런스 플랫폼을 사용하여 수행됩니다. 소요 시간은 4시간 정도입니다.

그런 다음 AWS 파트너는 하루 동안 체크리스트의 기술 검증 섹션에 있는 모든 항목과 관련 역량에 대한 감사를 받게 됩니다. MSP 프로그램 가입이 허가된 AWS 파트너는 이후 36개월마다 전체 감사 갱신을 받아야 합니다. AWS 파트너는 검증 체크리스트를 읽고, 체크리스트를 사용하여 자체 평가를 수행하고, 기술 검증의 '충족' / '미충족' 열과 같은 모든 전제 조건 제어를 해결하고, 감사 당일에 감사자와 공유할 객관적 증거 자료를 수집 및 정리해서 전체 감사에 대비해야 합니다. AWS 파트너는 객관적 증거 자료로 제공되거나 데모에 표시되는 정보를 공유하는 데 필요한 콘텐츠를 보유해야 합니다. AWS는 객관적인 제3자 감사 기관인 ISSI를 활용하여 프로세스 및 제어 개요(선택 사항)와 전체 감사(필수 사항)를 진행합니다. 이러한 감사는 가능한 경우 AWS 파트너가 선호하는 위치에서 AWS 파트너가 선호하는 언어로 진행됩니다. 전체 감사 사이에 12개월마다 AWS 파트너는 이 문서의 감사 프로세스 및 타이밍 섹션에 자세히 설명된 연간 성과 기반 갱신 프로세스를 사용하여 AWS로부터 평가를 받게 됩니다.

각 프로세스 및 제어 개요(선택 사항)에 따라 파트너에게 2,000 USD의 고정 수수료가 부과됩니다. 각 전체 감사(필수 사항)에는 3,000 USD의 감사 수수료와 모든 관련 출장 경비가 실비로 파트너에게 부과됩니다. 타사 감사 기관과의 각 작업은 감사 기관에서 요금을 청구하며 AWS 파트너와 감사자 사이의 별도 계약이 필요할 수 있습니다.

AWS에서는 전체 감사에서 AWS의 요구 사항에 대해 자세히 설명할 수 있는 담당자를 둘 것을 권장합니다(원격 또는 현장). 선임 책임자, AWS 비즈니스 리더, HR/재무/마케팅/영업 부서의 대표, 고급 기술을 보유한 AWS 엔지니어/아키텍트 한 명 이상, 서비스 데스크 및 지원 부분을 담당하는 운영 관리자(또는 관리형 서비스 담당 관리자) 등 여러 명의 전문가가 참여하게 하는 것이 가장 좋습니다.

AWS는 AWS MSP 프로그램 신청에 관심이 있거나 이미 가입한 AWS 파트너를 위해 최근에 모범 사례 가이드(Partner Central 로그인 필요)를 공개했습니다. 이 모범 사례 문서에서는 준수할 경우 좋은 결과를 가져오는 것으로 알려진 MSP 검증 체크리스트의 제어 항목에 대한 지침을 제공합니다.

프로그램 참가 및 혜택: AWS는 재량에 따라 AWS 파트너가 MSP 프로그램의 요구 사항을 충족하지 못하거나 MSP 파트너로서 기대되는 높은 기준을 충족하지 못한다고 판단할 경우 언제든지 AWS 파트너의 MSP 파트너 지위를 철회할 수 있습니다. MSP 파트너로서의 지위가 철회되면 해당 AWS 파트너는 (i) 모든 MSP 프로그램의 혜택을 받지 못하며 사용을 즉시 중단하고, (ii) MSP 프로그램과 관련되어 파트너에게 제공한 모든 자료의 사용을 즉시 중단하고, (iii) 외부에 MSP 파트너임을 알리는 행위를 즉시 중단합니다.

감사 프로세스 및 타이밍

MSP 프로그램에 참여하는 파트너는 연간 감사/갱신 주기를 따릅니다. 파트너 및 담당 AWS 팀(PDM, PMSA)은 MSP 배지의 원래 지정일을 알고 있어야 합니다. 이 날짜가 향후 갱신 기한을 결정하기 때문입니다. 파트너의 원래 지정일은 다음 단계에 따라 Partner Central에서 확인할 수 있습니다.

1. Partner Central에 로그인합니다.
2. 화면 상단에서 '프로그램' 위에 마우스를 올린 다음 '프로그램 애플리케이션'을 선택합니다.
3. '프로그램' 탭을 클릭합니다.
4. 관리형 서비스 제공업체 프로그램을 찾아 선택한 다음 '세부 정보 보기'를 클릭하여 지정일을 확인합니다.

또한 Partner Central에서 얼라이언스 리드 연락처를 최신 상태로 유지하는 것은 파트너의 책임입니다. 아래는 감사 및 갱신에 대해 알아야 할 대략적인 사항입니다.

0년 차: 전체 감사
1년 차(지정일로부터 365일 후): 성과 기반 갱신
2년 차: 성과 기반 갱신
3년 차: 전체 감사(주기 반복)

전체 감사는 MSP 검증 체크리스트에 있는 모든 제어, 전제 조건, 기술 검증에 대한 파트너의 MSP 비즈니스를 평가하는 절차입니다. 파트너는 갱신 기한 3~6개월 전에 현재 체크리스트(Partner Central에 있음) 검토를 시작해야 합니다. 감사자는 파트너 및 담당 PDM에 연락하여 기한 90일 전에 감사 일정을 결정합니다. 전체 감사 진행 후 AWS 파트너와 AWS는 감사로부터 영업일 기준 2일 이내에 강점, 개선 기회 및 조치 항목(필수 사항 및 권장 사항)이 설명된 감사 요약본을 받게 됩니다. 감사자의 예비 합격/불합격 평가가 감사 요약본과 함께 제공됩니다. 파트너는 즉시 감사 요약 보고서를 열고 미해결 필수 조치 항목을 파악하여 AWS와 직접 조정하기 시작해야 합니다(이 시점부터는 ISSI에 추가로 증거를 보내서는 안 됨).

AWS 파트너는 식별된 필수 조치 항목에 대해 영업일 기준 10일 이내에 AWS에 직접 응답하고 조치를 수행해야 합니다. AWS 파트너는 감사 후 미해결 필수 조치 항목에 대한 증거를 ISSI에 추가로 보내서는 안 됩니다. 추가하려는 증거 자료는 aws-msp@amazon.com에 보내야만 AWS에 전달됩니다.

AWS는 영업일 기준 20일 이내에 ISSI로부터 받은 보고서를 검토하고, AWS 파트너로부터 추가 증거를 받은 경우 증거를 검토하여 필수 조치 항목을 수행하고, 최종 합격/불합격 결정을 AWS 파트너에게 전달해야 합니다. 미해결 필수 조치 항목이 있는 KPI 시나리오와 미해결 필수 조치 항목이 없는 KPI 시나리오의 예시가 아래에 요약되어 있습니다.

필수 조치 및 권장 조치 항목 비교: 필수 조치 항목은 MSP 프로그램 가입 승인 전에 처리해야 하는 항목입니다. AWS 파트너가 영업일 기준 10일 이내에 필수 조치 항목을 처리하지 못하는 경우, 언제 어떻게 해당 항목을 처리할 것인지를 설명하는 시행 계획을 MSP 프로그램 관리자에게 제공해야 합니다. 권장 조치 항목은 최종 합격/불합격 평가에 영향을 미치지 않지만 AWS에서 모범 사례로 권장하는 항목입니다. 모든 미해결 권장 항목은 최종 감사 보고서에 포함되며 AWS 파트너는 이를 해결할 수도 해결하지 않을 수도 있습니다.

시나리오 1: 미해결 필수 조치 항목

실행	책임 있는 당사자	이전 조치 이후 주어지는 시간(최대)
감사 발생	파트너, ISSI	-
AWS 및 파트너에게 감사 요약 보고서 제출됨	ISSI	영업일 기준 2일
파트너가 필수 미해결 조치 항목을 처리하려고 추가 증거 자료를 다루고 AWS에만 제공함 이 기간 동안 감사자는 검토를 위해 미해결 필수 항목이 포함된 전체 감사 보고서를 AWS에 제공함	파트너, AWS, ISSI	영업일 기준 10일
파트너의 추가 증거가 검토되고 최종 감사 보고서가 업데이트되며 AWS에서 합격/불합격에 대한 최종 결정을 통지함. 파트너가 AWS로부터 결정에 대한 안내를 받음	파트너, AWS	영업일 기준 20일
전체 KPI: 영업일 기준 32일		

시나리오 2: 미해결 필수 조치 항목 없음

실행	책임 있는 당사자	이전 조치 이후 주어지는 시간(최대)
감사 발생	파트너, ISSI	-
AWS 및 파트너에게 감사 요약 보고서 제출됨	ISSI	영업일 기준 2일
감사자가 검토를 위해 AWS에 전체 감사 보고서를 제공함	ISSI	영업일 기준 7일

AWS에서 합격/불합격에 대한 최종 결정을 통지함. 파트너가 AWS로부터 결정에 대한 안내를 받음	파트너, AWS	영업일 기준 20일
전체 KPI: 영업일 기준 29일		

연간 성과 기반 갱신 프로세스:

MSP 프로그램은 뛰어난 품질과 일관된 고객 경험을 보장하기 위해 연간 성과 기반 갱신 프로세스('갱신 프로세스')를 요구합니다. AWS MSP 파트너는 계속해서 혁신과 뛰어난 고객 경험을 위해 노력함과 더불어 비즈니스 관행을 성장 및 발전시켜야 합니다. 성과 기반 갱신 프로세스의 요구 사항은 다음과 같습니다.

- AWS 파트너가 AWS 파트너 네트워크 이용 약관을 준수하며 해당 티어에서 양호한 상태를 유지
- 가장 최근에 릴리스된 버전의 프로그램 검증 체크리스트에 나열된 모든 현재 MSP 프로그램 요구 사항을 준수
- 파트너 조직의 얼라이언스 리드 연락처가 Partner Central에 최신 상태로 업데이트되어 있음
- 연간 갱신일 직전 12개월 동안 'Managed Services'로 태그된 ACE를 통해 시작된 영업기회 5건

AWS는 언제든지 이 연간 성과 기반 갱신 프로세스를 변경할 수 있는 권리를 보유하며, 변경 사항을 파트너에게 알릴 예정입니다.

AWS는 설정된 요구 사항에 따라 파트너의 성과에 대한 내부 검토를 실시합니다. 이제 모든 성과 기반 갱신은 만기일을 기준으로 분기별로 처리됩니다. 예를 들어 2025년 1월 10일에 만료되는 갱신의 경우, 프로세스는 2025년 3월 31일인 2025년 1분기까지 처리됩니다. AWS가 보내는 성과 기반 갱신에 관한 알림을 받지 못한 경우 갱신이 완료된 것으로 간주할 수 있으며 추가 조치가 필요하지 않습니다. 성과 기반 연간 갱신에 필요한 시작된 영업 기회 수 또는 티어 상태를 충족하지 못할 경우 조치가 필요하다는 알림을 받게 됩니다. 전체 감사 갱신(3년마다)에는 여전히 사례 연구가 필요하다는 점을 알려 드립니다. 세부 사항 및 요구 사항은 최신 체크리스트를 참조하세요.

파트너가 성과 요구 사항을 충족하지 못하는 경우, AWS의 재량에 따라 시행 계획을 완료하고 요구 사항을 달성할 약간의 시간을 주거나 즉시 MSP 프로그램에서 제외할 수 있습니다.

연간 갱신 프로세스 중에는 체크리스트 제어 항목에 대한 감사가 진행되지 않지만, AWS는 이전에 감사를 받은 요구 사항 및 새로 공개된 필수 요구 사항을 계속 준수할 것을 기대하며 AWS 파트너는 자사의 관리형 서비스 비즈니스에 영향을 미치는 정책, 프로세스 및 도구에 중대한 변경 사항이 있는 경우 해당 변경 사항이 적용되는 즉시 이를 공개해야 합니다.

전체 감사(처음 전체 감사로부터 36개월마다 실시):

MSP 프로그램의 또 한 가지 요구 사항은 AWS 파트너의 가장 최근 전체 감사 날짜를 기준으로 36개월마다 전체 감사를 받는 것입니다. 이 전체 감사는 전체 감사가 이루어지는 날짜를 기준으로 현재 버전의 체크리스트를 사용하여 수행됩니다. 자체 평가(이 페이지의 상단에 링크 제공)는 이제 모든 파트너가 첫 전체 감사(프로그램 가입 시), 3년 주기의 전체 감사 갱신 전에 갖춰야 하는 필수 요구 사항입니다. 모든 파트너가 감사를 준비하고 필요한 지원을 받을 수 있도록 원하는 전체 감사일 최소 30일 전에 자체 평가 워크시트를 aws-msp@amazon.com으로 직접 제출해 주세요.

파트너는 모든 관련 문서 및 지원 링크를 비롯해 전제 조건 제어 항목에 대한 포괄적인 응답을 제공해야 합니다. 기술 검증 제어의 경우 파트너는 제어가 '충족'인지 '미충족'인지 여부만 표시하면 됩니다. 그런 다음 감사자는 1일 감사 프로세스를 통해 기술 검증 제어를 철저하게 평가합니다.

자체 평가 워크시트에서 파트너는 AWS MSP 팀의 직접적인 지원이 필요한 영역을 구체적으로 제시해야 합니다. 이를 통해 AWS는 파트너가 감사 전에 체크리스트에 있는 필수 제어 사항을 충족하는 데 도움이 되는 적절한 리소스를 파악합니다. 조직에서 자체 평가를 완료하고 미해결 필수 제어 항목을 발견하지 못했더라도 전체 감사 활동에 앞서 자체 평가를 MSP 프로그램에 제출해야 합니다.

합병, 인수 및 매각의 영향:

MSP 프로그램에는 AWS 파트너의 기술 역량과 비즈니스 및 제공 모델을 검증하기 위한 감사 활동이 포함됩니다. 이러한 비즈니스 및 제공 모델은 합병, 인수, 매각 과정에서 중대한 영향을 받는 경우가 많습니다. 따라서 AWS 파트너는 새로운 전체 감사를 다시 신청하고 완료해야 할 수 있습니다. 아래 지침을 참조하세요.

- 인수/합병:
    - AWS MSP 파트너가 비MSP 파트너를 인수하는 경우: 즉각적 조치가 필요치 않습니다. MSP 파트너는 다음 정기 전체 감사 중에 MSP 비즈니스에 미치는 영향을 보여주어야 합니다.
    - 비MSP 파트너가 AWS MSP 파트너를 인수하는 경우: 인수한 AWS 파트너가 MSP 파트너로 인정받으려면 새로 신청하여 전체 감사를 받아야 합니다. 새로운 비즈니스 및 제공 모델뿐만 아니라 인수한 기술 역량의 통합 내용도 전체 감사 프로세스를 통해 검증받아야 합니다. 인수 합병 이후에도 MSP 프로그램의 지위를 유지할 수 있도록 가능한 한 빨리 이 프로세스를 진행할 것을 권장합니다.
    - AWS MSP 파트너가 다른 AWS MSP 파트너를 인수하는 경우: 즉각적 조치가 필요치 않습니다. 합병된 기업에 대한 평가는 기존 기업 중 한쪽에 대한 다음 정기 전체 감사(둘 중 이른 날짜) 중에 이루어집니다.

- 매각:
    - AWS 파트너가 AWS MSP 비즈니스와 관련된 비즈니스 일부를 매각하는 경우, 매각하는 비즈니스에서는 MSP 파트너로서의 입지에 큰 영향을 미칠 수 있는 MSP 비즈니스에 대한 중대한 변경 사항을 즉시 공개해야 합니다. 영향의 정도에 따라 AWS 파트너는 MSP 프로그램에서 즉시 제외되거나
    - 다음에 예정된 정기 전체 감사에서 비즈니스에 미치는 영향을 명확히 밝혀야 합니다. 매각된 비즈니스는 새로운 AWS 파트너로서 MSP 프로그램에 지원해야 합니다.

필수 및 권장하는 제어 유형 설명

각 요구 사항은 필수 또는 권장으로 지정되어 있습니다. 전체 감사 중에 AWS 파트너는 체크리스트의 모든 요구 사항에 대해 평가됩니다. 다만 파트너는 필수 요구 사항에 대한 세부 증거 자료만 제시하면 됩니다. AWS는 언제든지 신규 필수 요구 사항을 도입할 권리가 있습니다. 대부분의 경우 신규 요구 사항은 먼저 권장 요구 사항으로 게시된 후 검증 체크리스트의 후속 메이저 버전 릴리스에서 필수로 승격됩니다.

다음과 같은 AWS 또는 업계 배지를 보유한 파트너는 전체 감사 기간 동안 특정 MSP 검증 규제 대상에서 면제됩니다.

VCL 7.0의 체크리스트 섹션/컨트롤	**면제**
OPS-009 고객 배포 파이프라인 제어	**AWS DevOps 컴피턴시**를 보유한 AWS 파트너는 이 요구 사항이 면제됩니다.
섹션 5: 전체 보안 섹션	현재 **AWS 레벨 1 MSSP 컴피턴시** 지정을 보유한 AWS 파트너는 이 섹션의 모든 요구 사항이 면제됩니다.
OPS-17 마이그레이션 제어	현재 **AWS 마이그레이션 컴피턴시** 지정을 보유한 AWS 파트너는 이 요구 사항이 면제됩니다.
PLAT-005 AWS 서비스 전문성 제어	현재 **3개 이상의 AWS 컴피턴시 또는 AWS 서비스 제공** 지정을 보유한 AWS 파트너는 이 요구 사항이 면제됩니다.
OPSP-005 서비스 연속성	AWS 파트너의 AWS MSP 비즈니스에 적용된 **ISO 22301** 인증으로도 충분합니다.
SEC-001 보안 정책 및 절차 제어 **PEO-003 직원 오프보딩** **GOVP-001 공급업체 관리**	**SOC 2 / ISO 27001** 인증을 보유한 AWS 파트너는 이러한 요건에서 면제됩니다.

정의

AWS 사례 연구: 사례 연구는 개별 고객 솔루션 및 성과를 상세히 기술한 보고서입니다. 사례 연구에는 고객 소개, 과제 개요, 구현된 솔루션의 세부 정보, 고객이 실현한 성과가 포함되어야 합니다. MSP 프로그램의 목적상, MSP 신청 및 갱신에 사용된 모든 사례 연구는 AWS 파트너와 고객이 최소 6개월 동안 AWS 기반의 관리형 서비스를 제공하기로 합의했음을 입증해야 합니다. AWS 파트너는 고객당 1건의 사례를 사용할 수 있으며 AWS 파트너의 내부 회사 또는 계열사인 고객에 대한 사례는 사용할 수 없습니다. 모든 사례 연구는 '파일럿' 또는 개념 증명 단계가 아닌, 고객과 프로덕션 단계에 있는 프로젝트에 한합니다. 필요한 정보가 모두 명확하게 식별되고 포함되는 한 AWS 파트너는 사례 연구에 특정 문서 형식을 사용할 필요가 없습니다. 예시 사례 연구 템플릿 및 가이드가 제공되므로 필요한 경우 AWS MSP 프로그램: 공개 사례 연구 가이드(Partner Central 로그인 필요)에서 사용할 수 있습니다. 모든 사례 연구는 다음 내용을 포함해야 합니다.

- 고객 이름
- 고객 당면 과제
- 제안된 솔루션
- AWS가 솔루션의 일부로 사용된 방법
- 마이그레이션 또는 솔루션 구현 전후 파트너의 지원 서비스
- 기존 및 신규 솔루션 아키텍처 다이어그램(해당하는 경우)
- 성과/결과
- 성공을 나타내는 지표
- 계약 시작일
- 계약 종료일

위 정보가 없는 사례 연구는 AWS에서 수락하지 않을 수 있습니다. 이러한 사례 연구에 제공되는 정보는 AWS에서 검증 목적으로만 사용됩니다.

공개 사례 연구: 공개 사례 연구는 파트너가 관리 서비스 계약과 관련된 고객의 구체적인 과제를 해결하기 위해 AWS와 지원 서비스를 어떻게 사용했는지 설명하는 예시로, 공개적으로 확인 가능해야 합니다. 이러한 공개 사례는 공식적인 고객 사례 연구, 백서, 동영상 또는 블로그 게시물의 형식이 될 수 있습니다. 파트너는 신청 프로세스 중에는 AWS Partner Central의 '사례 연구 URL' 필드에, 갱신 전체 감사 중에는 외부 감사 기관에, 성과 기반 연간 갱신 프로세스 중에는 성과 기반 갱신 템플릿에 공개 URL(파트너가 게시함)을 제공합니다.

익명화된 공개 사례 연구: 고객과의 계약이 민감한 특성을 지닌 관계로 파트너가 고객의 이름을 공개적으로 밝힐 수 없는 경우 파트너는 공개 사례 연구를 익명화할 수 있습니다. AWS는 익명화된 공개 사례 연구 세부 정보를 게시하지만 고객 이름은 비공개로 유지합니다. 파트너는 검증을 위해 MSP 신청 시 AWS Partner Central 사례 연구의 '회사 이름' 필드에 AWS 고객 이름을 제공해야 하지만 AWS는 이 이름을 공개하지 않습니다.

갱신 전체 감사 및 성과 기반 연간 갱신 프로세스 중에 AWS는 검증 목적으로 고객 이름을 비공개로 파악하기 위해 파트너에게 연락할 수 있습니다. AWS에서 Partner Solutions Finder(PSF)에 게시할 사례 연구 필드에는 '제목', '사례 연구 설명' 및 '사례 연구 URL'이 포함됩니다. 파트너는 AWS Partner Central의 '사례 연구 URL' 필드에 공개 URL(파트너가 게시함)을 제공합니다. 이 URL에는 위에 명시된 사례 연구의 필수 요소가 모두 포함되어야 합니다.

시작된 영업기회: AWS 파트너는 AWS Partner Central에 있는 APN 고객 참여(ACE) 플랫폼을 통해 영업기회를 제출합니다. MSP 프로그램 요구 사항을 충족하는 데 사용되는 영업기회에는 선택한 제공 모델 옵션 중 하나로 '관리형 서비스'가 포함되어야 합니다. 솔루션에 대한 비용 청구가 시작된 후 AWS 파트너는 영업 기회의 상태를 '시작됨'으로 업데이트합니다.

MSP AWS 파트너 전제 조건

ISSI 감사 전에 다음 요건을 충족해야 합니다.

비즈니스

- **BUSP-001 - 웹 보유**

  필수

  AWS 파트너는 기본 웹 사이트에 AWS 관리형 서비스 비즈니스를 설명하고 공개 사례 연구에 대한 링크를 제공하는 공개 랜딩 페이지를 보유합니다. 이 페이지에서는 AWS 기반 워크로드를 설계, 구축 및 관리하는 파트너의 차별화된 전문성을 설명해야 합니다.

  증거 자료는 해당 AWS MSP 비즈니스 랜딩 페이지에 대한 퍼블릭 URL의 형식이어야 합니다.

- **BUSP-002 - 영업 및 마케팅 인증**

  필수

  AWS MSP 비즈니스를 지원하는 AWS 파트너 영업 팀, 마케팅 팀 및/또는 해당 사업부가 모두 AWS 파트너: 영업 인증(비즈니스) 또는 AWS 파트너: 인증(기술)을 보유하고 있습니다.

  증거 자료는 적절한 인증 기록의 형식이어야 합니다. 기록 형식은 PDF, 스프레드시트, 도구 스크린샷 등의 형식일 수 있습니다.

- **BUSP-003 - 고객 사례 연구**

  필수

  AWS 파트너는 4건 이상의 AWS 고객 사례 연구(체크리스트의 정의 섹션에 정의됨)를 보유하고 있습니다. 제공된 사례 연구 중 최소 2건에는 AWS 파트너가 제공한 AWS 관리형 서비스가 고객 문제를 해결하는 데 어떻게 도움이 되었는지 설명하는 공개적으로 사용 가능한 아티팩트가 있어야 합니다.

  이러한 공개 아티팩트는 공식 사례 연구, 백서, 동영상, 블로그 게시물 등의 형식이 될 수 있으며 이전 MSP 감사 및 갱신에 사용된 것이 아니어야 합니다. 비공개 사례 연구의 형식은 PDF나 PowerPoint, Word 형식일 수 있습니다.

직원

- **PEOP-001 - 직원 관리 기술**

  필수

  AWS 파트너는 직원의 기술 전문성을 지속적으로 향상시키기 위한 전략을 정의했습니다. 여기에는 공식적인 교육 및 자격증 및/또는 지속적 학습 문화를 촉진하는 기타 접근 방식이 포함될 수 있습니다.

  증거 자료는 관리형 서비스 운영을 지원하는 직원을 위해 지난 12개월 이내에 수행된 예시 학습 이벤트 또는 활동이 포함된 형식이어야 합니다.

거버넌스

- **GOVP-001 - 공급업체 관리**

  필수

  AWS 파트너는 공급업체의 선정 및 평가를 위한 프로세스를 정의했습니다. 예를 들어 SaaS 공급업체 또는 활동이나 서비스를 하도급받는 다른 서드 파티, 관리형 서비스를 제공하려고 구매한 ISV 도구입니다.

  증거는 공급업체 선정을 위한 상세한 SOP 형식이어야 합니다. 또는 공급업체가 직접 획득한 정보 보안과 관련된 최신 산업 인증(예: ISO 27001, SOC2)의 형식으로 적절한 공급업체 관리 절차를 증명할 수도 있습니다.

- **GOVP-002 - 운영 개선**

  필수

  AWS 파트너는 운영 프로세스(예: 인시던트 관리, 클라우드 비용 관리, 아키텍처 패턴, 성능, 보안 등)를 검토하고, 영업 기회를 식별하고, 작업의 우선순위를 지정하기 위해 정규 케이던스가 포함된 지속적인 개선에 대한 프로세스를 확립했습니다.

  증거 자료는 개선할 수 있는 영업 기회 식별에 초점을 맞춘 거버넌스 프로세스 문서의 형식이어야 합니다.

- **GOVP-003 - 지속 가능성을 향한 노력**

  필수

  AWS 파트너는 장기 전략의 일환으로 지속 가능성 비전을 천명합니다.

  증거 자료는 CxO 담당 리더십의 약속이 포함된 정책 문서/통신문의 형식이어야 합니다.

플랫폼

- **PLATP-001 - 전문가 설계 검토**

  필수

  AWS 파트너는 공인된 AWS Solutions Architect – Associate 또는 Professional이 모든 고객 AWS 프로젝트의 설계 및 구현을 검토할 것을 요구하는 문서화된 정책을 가지고 있습니다. 또한 이 정책은 어떤 경우에 Professional 또는 Specialty 등급 인증을 획득한 개인이 검토를 수행해야 하는지에 대한 구체적인 지침을 포함해야 합니다.

  증거 자료는 문서화된 정책 및 Professional 또는 Specialty 수준 인증을 받은 개인이 문서를 검토 및 승인했음을 보여 주는 고객 프로젝트 문서의 형식이어야 합니다.

보안

- **SECP-001 - 액세스 키 노출 탐지**

  필수

  AWS Trusted Advisor는 자주 사용되는 코드 리포지토리에서 외부에 노출된 액세스 키가 있는지 그리고 노출된 액세스 키로 인해 발생할 수 있는 비정상적인 Amazon EC2(Amazon Elastic Compute Cloud) 사용이 있는지 검사합니다. 액세스 키 노출이 감지되면 서비스에서 AWS CloudWatch Events에 이벤트를 트리거합니다. AWS MSP 파트너가 이 이벤트를 적극 모니터링하고 이에 신속하게 대응할 수 있는 메커니즘을 생성하는 것이 중요합니다.

  AWS 파트너는 모든 관리형 고객 계정에서 서비스 유형이 'RISK'인 모든 AWS Health 이벤트를 처리할 수 있는 자동화된 메커니즘을 구현해야 합니다. 최소한의 요건으로, 노출된 액세스 키에 대한 알림을 수신했을 때 ITSM 또는 보안 티켓팅 시스템에서 가장 높은 심각도로 새 티켓을 생성하는 자동화된 시스템이 구축되어 있어야 합니다. 예시 솔루션을 통해 계정 침해 문제를 탐지하고 완화하는 방법을 확인해 보세요.

  그뿐 아니라 파트너는 노출된 자격 증명의 삭제 또는 교체 등을 포함하는, 노출된 자격 증명에 대한 알림을 처리하는 문서화된 절차를 보유하고 있어야 합니다.

  증거 자료는 노출된 키를 처리하는 방법에 관한 대응 절차를 문서화한 형식이어야 합니다.

- **SECP-002 - 퍼블릭 리소스**

  필수

  AWS 파트너는 고객 리소스를 의도치 않게 또는 불필요하게 공개할 수 있는 구성을 방지 및/또는 탐지하는 도구 및 프로세스를 보유하고 있습니다. 여기에는 최소한 다음 리소스가 포함되어야 합니다.

  - Amazon S3 버킷
  - Amazon RDS 인스턴스
  - Amazon EC2 인스턴스
  - 민감한 포트에 무제한으로 액세스할 수 있는 보안 그룹
  - Amazon EBS 스냅샷
  - Amazon RDS 스냅샷
  - Amazon Machine Image(AMI)

증거 자료는 의도치 않은 퍼블릭 액세스의 위험을 완화하기 위한 절차가 문서화된 형식이어야 합니다.

운영

- **OPSP-001 - 인시던트 관리**

  필수

  AWS 파트너는 다음과 같은 인시던트 관리 프로세스를 문서화했습니다.

  - IT 및 보안 인시던트 식별 방법
  - IT 및 보안 인시던트 로깅 방법
  - IT 및 보안 인시던트 분류 방법
  - IT 및 보안 인시던트 우선순위 지정 방법
  - IT 및 보안 인시던트 조사 및 진단 방법
  - 플레이북 형식의 IT 및 보안 인시던트 대응 계획
  - 고객과 소통하는 방법
  - IT 및 보안 인시던트 해결 방법
  - IT 및 보안 인시던트 종결 방법

  AWS 파트너는 IT 인시던트와 보안 인시던트를 모두 다루는 문서화된 인시던트 관리 프로세스의 증거 자료를 제공해야 합니다.

- **OPSP-002 - 문제 관리**

  필수

  AWS 파트너는 인시던트 후 분석을 수행하고 고객에게 영향을 미치는 이벤트 후 고객에게 커뮤니케이션을 제공합니다. 분석 프로세스는 원인을 식별하고, 완화 조치를 개발하고 재발을 제한 또는 방지하기 위한 시행 계획을 정의해야 합니다. 고객과 원인 및 시행 계획에 대한 맞춤형 커뮤니케이션을 적시에 공유합니다.

  증거 자료는 완료된 시행 계획 및 고객 커뮤니케이션을 포함하여 완료된 인시던트 후 분석 보고서 예시가 포함된 형식이어야 합니다.

- **OPSP-003 - 배포 위험 관리**

  필수

  AWS 파트너는 제한적/카나리 배포, 병렬 환경 배포(예: 블루/그린 배포, 트래픽 이동) 또는 프로덕션 변경 실패의 위험을 제한하기 위한 기타 고급 접근 방식을 구현할 수 있는 역량을 갖추고 있습니다.

  증거 자료는 프로덕션 배포의 위험을 완화하기 위한 절차가 문서화된 형식이어야 합니다.

- **OPSP-004 - 클라우드 재무 관리**

  필수

  AWS 파트너는 정기적으로 고객의 AWS 비용을 평가하고 권장 사항을 제시하여 이를 최적화합니다.

  증거 자료는 고객에게 제공된 권장 사항 문서의 형식이어야 합니다.

- **OPSP-005 - 서비스 연속성**

  필수

  AWS 파트너는 파트너의 고객 서비스 역량에 영향을 미치는 이벤트에 대응하는 프로세스를 정의하고 테스트합니다. 이 절차는 데이터 및 인프라의 완전한 손실, 인력의 상당한 부분에 영향을 미치는 환경적 이벤트(예: 회사 사무실에 대한 물리적 접근을 어렵게 만드는 재해) 및 고객 서비스를 위한 타사 핵심 서비스의 장애(예: 내부 티켓팅 및 헬프데스크 시스템의 장기적 운영 중단)를 다룹니다. 대체/백업 인프라, 도구 및 용량에 대한 비즈니스 연속성 테스트는 매년 실시해야 합니다.

  증거 자료는 지난 12개월 이내에 수행된 비즈니스 연속성 테스트의 결과와 함께 위의 항목을 다루는 프로세스를 문서화한 형식이어야 합니다. 또는 AWS 파트너의 AWS MSP 비즈니스에 적용된 ISO 22301 인증으로도 충분합니다.

MSP AWS 파트너 기술 검증

ISSI 감사에는 다음 요구 사항이 적용됩니다.

비즈니스

- **BUS-001 - 회사 개요**

  필수

  AWS 파트너는 역량을 보여주고 MSP 비즈니스와 관련하여 고객과 대화의 장을 마련하기 위해 회사 개요 프레젠테이션을 제공합니다.

  프레젠테이션은 차세대 클라우드 관리형 서비스에 대한 정보를 포함합니다. 즉, 기존 온프레미스 또는 호스팅되는 관리형 서비스와 비교하여 AWS 환경에서 관리형 서비스의 다른 점이 무엇인지를 DevOps 방식으로 구동되는 자동화를 중심으로 설명합니다.

  개요 프레젠테이션에는 다음 내용이 포함됩니다.

  - 회사 연혁
  - 사무실 위치
  - 직원 수
  - AWS MSP 지원 및 운영 팀의 위치
  - 보유 고객의 수, 규모, 지리적 위치 및 산업/부문을 포함한 고객 프로필
  - 서비스 차별화 요소
  - AWS 파트너 경로, 월별 AWS 청구서 등이 담긴 AWS 관계 개요/세부 정보

  증거 자료는 전체 감사 중에 진행되는 프레젠테이션 형식이어야 하며, 프레젠테이션은 20분으로 제한됩니다.

- **BUS-002 - MSP 비즈니스 성장**

  필수

  AWS 파트너는 AWS 기반 MSP 비즈니스를 적극적으로 성장시키고 있습니다.

  모든 고객 계약은 지난 18개월 이내에 온보딩된 순 신규 고객이거나 기존 고객 계약의 신규 애플리케이션 마이그레이션 또는 기존 아키텍처 리팩터링과 같은 상당한 성장을 입증해야 합니다. 추가 작업 범위 없이는 기존 워크로드에 대한 지속적인 관리형 서비스를 갱신하는 것만으로는 충분하지 않습니다.

증거 자료는 고객 성장을 입증하는 4건 이상의 신규 계약 또는 추가 계약의 형식이어야 합니다. 이러한 모든 신규 계약 또는 추가 계약은 지속적인 관리형 서비스 계약에 해당되어야 합니다.

- **BUS-003 - 재무 계획 및 보고**

  필수

  AWS 파트너는 예측, 예산 편성, 재무 지표 및 보고서 검토를 비롯하여 재무 계획을 위한 프로세스를 갖추고 있습니다.

  증거 자료는 예산, 재무 예측 및 이전 분기 또는 월에 대한 보고서, 또는 재무 계획과 관련된 문서화된 정책 및 프로세스 및 재무 지표에 대한 검토 중 하나의 형식이 될 수 있습니다. 상장 기업의 경우 가장 최근 기간의 공개 증권 서류가 충분한 증거 자료가 됩니다.

- **BUS-004 - 시장 진출**

  필수

  AWS 파트너는 관리형 서비스 영업 기회를 식별하고, 판매자가 이러한 영업 기회를 인지하고 판매하도록 교육하는 방법, AWS 관리형 서비스(MSP) 사례에 대한 수요 및 잠재 고객을 창출하기 위한 구체적인 작업에 대한 프로세스를 보유하고 있어야 합니다.

  증명 자료는 AWS 파트너가 관리형 서비스 제품을 홍보하고 판매하기 위해 고객, 내부 영업 팀, AWS 영업 담당자(해당하는 경우)와 어떻게 소통하는지에 대한 프로세스나 퍼스트 콜 데크를 문서화한 형식이어야 합니다.

직원

- **PEO-001 - 직원 온보딩**

  필수

  AWS 파트너는 AWS 파트너의 AWS 관리형 서비스 사례와 관련된 인력의 온보딩을 위한 프로세스와 체크리스트를 정의했습니다.

  증거 자료는 AWS 파트너의 AWS 관리형 서비스 비즈니스 범위 내에서 완성된 온보딩 기록의 형식이어야 합니다. 예를 들어 완성된 체크리스트, 교육 계획 또는 기타 기록이 포함될 수 있습니다.

- **PEO-002 - 클라우드 혁신 센터(CCoE)**

  필수

  AWS 파트너는 클라우드 혁신 센터(CCoE)를 유지합니다.

  CCoE는 진화하는 기술 운영에 대한 클라우드 모범 사례, 프레임워크, 거버넌스를 만들고, 전파하고, 제도화하는 전담 인원으로 구성된 크로스 기능 팀입니다. 이 팀은 관리형 서비스 제공업체에 엔지니어링 및 비즈니스 부서를 제공하여 이 분야의 고객에게 서비스를 제공하는 방식을 발전시킬 수 있는 중심적인 역할을 합니다.

  이 전담 크로스 기능 팀은 다음 영역에서 MSP 비즈니스 방향을 형성하고 지원합니다.

  1. 클라우드 채택 및 리툴링: 조직 전체에 클라우드 서비스 도입을 촉진하고 재사용 가능한 도구 및 아티팩트를 개발합니다.
  2. 교육 및 변경 사항 관리: 클라우드 학습을 조정하고 변화를 거부감 없이 받아들이는 사고 방식을 수용합니다.
  3. 거버넌스: 워크로드를 클라우드 아키텍처 프레임워크 및 정책에 맞게 유지하는 데 도움이 되는 초기 거버넌스 프로세스 및 모범 사례를 설정합니다.
  4. 전략: 조직의 비즈니스 전략에 맞게 클라우드 제품을 조정합니다.
  5. 운영 및 자동화: 일반적으로 필요한 플랫폼 구성 요소 및 솔루션을 시간이 지남에 따라 표준화하고 자동화합니다.

  CCoE의 증거 자료는 CCoE의 선언문, 조직 구조, 운영 프로세스 및 CCoE가 AWS 파트너 비즈니스에 적용되는 방식에 대한 문서화된 형식이어야 합니다.

- **PEO-003 - 직원 오프보딩**

  필수

  AWS 파트너는 AWS 파트너의 AWS 관리형 서비스 비즈니스와 관련된 인력의 오프보딩을 위한 종료 프로세스와 체크리스트를 정의하여 고객 및 파트너 시스템 및 데이터에 대한 모든 액세스 권한이 취소될 수 있도록 했습니다.

  증거 자료는 AWS 파트너의 AWS 관리형 서비스 비즈니스 범위 내에서 완성된 오프보딩 기록의 형식이어야 합니다. 예에는 AWS 파트너 및 고객 시스템에 대한 직원의 액세스를 종료하는 것이 포함되어야 합니다. 기록은 AWS 파트너의 AWS MSP 비즈니스 범위에 해당하며 정보 보안과 관련된 현행 산업 인증(예: ISO 27001, SOC2)의 형식이 될 수 있습니다.

거버넌스

- **GOV-001 - 위험 및 완화 계획**

  필수

  AWS 비즈니스를 비롯한 비즈니스 위험 영역은 문서화된 완화 계획으로 요약됩니다. 재정적 위험, 비즈니스의 기간 및 성숙도, 빠른 성장을 위한 계획, 대규모 계약/고객에 대한 가정 또는 상실 등이 이에 포함될 수 있습니다.

  증거 자료는 AWS 파트너의 AWS 관리형 서비스 비즈니스와 관련된 문서화된 위험 분석 및 완화 계획의 형식이어야 합니다. 여기에는 파트너가 초기 평가부터 지속적인 모니터링 및 업데이트까지 포괄하여 위험 관리 문서의 전체 수명 주기를 관리하는 방법이 자세히 나와 있습니다.

- **GOV-002 - 고객 만족도**

  필수

  AWS 파트너는 고객 만족도 데이터를 객관적으로 확보할 수 있는 메커니즘을 갖추고 있습니다. 이는 공식적인 설문 조사 프로세스, 고객 상호 작용 후 담당자 기반 설문 조사 또는 고객 리뷰 회의의 일부로 수행됩니다. 목적은 AWS MSP 파트너가 고객 참여의 성공을 측정할 수 있는 반복적인 피드백 메커니즘을 갖추도록 하는 것입니다.

  증거 자료는 피드백이 수집되고 우려 사항이 해소되는 방식(해당하는 경우)을 입증하는 형식으로 구성되어야 합니다. Partner Central을 통해 수집된 AWS 소유 및 운영 고객 만족도(CSAT) 데이터는 허용되지 않습니다. 이 정보는 고객이 명시적으로 권한을 부여하지 않으면 파트너와 공유할 수 없기 때문입니다.

- **GOV-003 - 데이터 소유권 및 고객 오프보딩**

  필수

  고객 계약은 각 당사자가 계약 종료 시 고객 데이터의 처리에 대한 협의를 비롯하여 다음과 같은 데이터에 대한 구체적인 법적 소유권을 정의합니다.

  - 데이터/계정을 고객에게 넘겨주는 시기에 대한 약속
  - 데이터/계정 자격 증명의 전송 형식 및 방법
  - 해당하는 경우, 비고객 IAM 계정, 그룹, 역할 및 연동 제거 프로세스

- 고객이 자신의 데이터 및 AWS 계정에 대한 소유권을 유지할 수 있도록 지원하는 파트너의 관리형 서비스에서 고객 AWS 계정을 오프보딩하는 절차를 정의했습니다.

증거 자료는 위의 요구 사항을 다루며 AWS 파트너의 AWS 관리형 서비스 비즈니스의 범위에 해당하는 계약 템플릿의 형식이어야 합니다.

- **GOV-004 - 운영 준비**

  필수

  AWS 파트너는 운영 시작 후 운영 팀이 고객 환경을 어떻게 지원할 것인지 자세히 설명하는 체크리스트/프로세스 설명 문서 형식으로 운영 준비 상태 프로세스를 보유하고 있습니다.

  증거 자료는 인력, 도구 및 운영 프로세스와 관련된 운영 준비 상태를 판단하기 위한 체크리스트를 포함하여 문서화된 프로세스 형식이어야 합니다.

- **GOV-005 - 공동 책임 모델**

  필수

  AWS 파트너는 파트너가 관리하는 AWS 환경과 관련된 고객의 보안 요구 사항 및 운영 기대 사항을 정의하고 파트너와 고객 간의 역할 및 책임 매트릭스(RACI) 측면에서 이를 공식화합니다.

  증거 자료는 고객에게 제공된 온보딩 문서의 형식이어야 합니다.

- **GOV-006 - 지속 가능성 모범 사례**

  필수

  AWS 파트너는 에너지 효율을 높이기 위해 워크로드 배치를 최적화하고 사용자, 소프트웨어, 데이터, 하드웨어 및 배포 패턴에 맞게 아키텍처를 최적화하는 조치를 취합니다. 이러한 최적화의 예에는 사용자 행동, 아키텍처 설계, 데이터 패턴, 하드웨어 패턴 등을 기반으로 수행된 최적화 단계가 포함될 수 있습니다.

  증거 자료는 AWS 파트너의 AWS 관리형 서비스 비즈니스 범위에서 지난 12개월 이내에 식별, 제안 및/또는 구현된 개선 사항에 대한 설명과 예시가 포함된 형식이어야 합니다.

플랫폼

- **PLAT-001 - 계정 관리**

  필수

  AWS 계정은 여러 고객과 공유되지 않습니다. 이 조건은 AWS 파트너가 소유한 멀티 테넌트 소프트웨어 제품을 SaaS(Software as a Service) 모델로 운영하는 경우에는 적용되지 않습니다. AWS에서 파트너가 고객을 대신하여 관리하는 타사 소프트웨어 제품은 고객별 전용 계정에 배포되어야 합니다.

  증거 자료는 새 AWS 계정을 생성하는 절차 또는 기존 고객 계정의 관리를 수임하는 절차를 포함하는, 고객 환경 분리가 유지되는 방식을 설명하는 문서화된 정책의 형식이어야 합니다.

- **PLAT-002 - 솔루션 역량**

  필수

  AWS 파트너는 대규모 계약의 경우 상세한 설계 문서를 제공합니다. 이 문서는 현행 AWS Solutions Architect 인증을 보유한 AWS 파트너의 AWS 전문가가 검토 및 승인해야 합니다.

  증거 자료는 2명의 독립적이고 관련이 없는 고객을 위해 구현된 시스템에 대한 상세 설계 문서의 형식으로, 최근 18개월 이내에 작성된 것이어야 합니다. 각 문서는 다음 구성 요소를 포함해야 합니다.

  이러한 구성 요소는 시스템이 배포된 후에 기록되는 데 그치지 않고 원래 설계 문서에 정의되어 있어야 합니다.

  1. 기술 솔루션을 통해 해결해야 하는 고객 요구 사항 문서화
  2. 제안된 설계의 아키텍처 세부 정보

- **PLAT-003 - 기능 이외의 요구 사항**

  필수

  AWS 파트너는 다음을 포함하여 기능 이외의 시스템 요구 사항을 충족하기 위한 접근 방식이 포함된 주요 계약에 대한 세부 설계 문서를 고객에게 제공합니다.

  - 성능, 용량 및 가용성에 대한 시스템 요구 사항 또는 목표의 정의
  - 해당하는 경우, SLA(서비스 수준 계약)

- 프로덕션 환경에서 특정 지표를 비롯하여 시스템의 이러한 측면을 모니터링하는 데 사용되는 도구 및 접근 방식
- 프로덕션 환경에 배포하기 전에 설계 사양이 지정된 요구 사항을 충족할 것을 보장하기 위한 테스트 또는 검증 프로세스의 개요

증거 자료는 기능 이외의 요구 사항이 있는 2명의 독립적이고 관련이 없는 고객을 위해 구현된 시스템에 대한 상세 설계 문서의 형식으로, 최근 18개월 이내에 작성된 것이어야 합니다.

- **PLAT-004 - Well- Architected**

  필수

  고객 인프라가 https://aws.amazon.com/architecture/well-architected/에 설명된 대로 AWS Well-Architected Framework에 따라 잘 설계되었음을 보여 주는 상세 설계.

  증거 자료는 2명의 독립적이고 관련이 없는 고객을 위해 구현된 시스템에 대한 상세 설계 문서의 형식으로, 최근 18개월 이내에 작성된 것이어야 합니다. 또는 보안, 운영 우수성, 신뢰성 요소에서 미해결 고위험 문제(HRI)가 전혀 없는 것으로 표시된 고객 예시에 대한 AWS Well-Architected Framework Review(WAFR)를 완료한 경우, 대신 각 고객 예시에 대해 내보낸 WAFR 보고서를 제출할 수 있습니다.

- **PLAT-005 - AWS 서비스 전문성**

  필수

  현재 3개 이상의 AWS 컴피턴시 또는 AWS 서비스 제공 지정을 보유한 AWS 파트너는 이 요구 사항이 면제됩니다.

  AWS 파트너는 광범위한 AWS 서비스를 활용하여 고객을 위해 솔루션을 개선 또는 구현하는 전문성을 입증했습니다.

  증거 자료는 AWS 파트너가 설계 또는 리아키텍팅한 예시 고객 워크로드 2건의 형식으로, 각각 다음을 제외하고 최소 4개 이상의 AWS 서비스를 상당 부분 활용해야 합니다.

  - Amazon Elastic Compute Cloud(Amazon EC2)
  - Amazon Virtual Private Cloud(Amazon VPC)
  - Amazon Relational Database Service(RDS)
  - Amazon Simple Storage Service(Amazon S3)
  - Amazon Elastic Block Storage(Amazon EBS)
  - AWS Identity and Access Management(AWS IAM)

- Amazon CloudWatch
- AWS CloudTrail
- AWS CloudFormation

보안(Level 1 MSSP 컴피턴시를 보유한 AWS 파트너는 이 섹션에서 제외)

- **SEC-001 - 보안 정책 및 절차**

  필수

  AWS 파트너는 공격으로부터 자체 시스템을 보호할 수 있도록 보안 정책 및 절차를 확립했으며, 이러한 정책은 AWS 파트너의 내부 경영진이 검토하고 승인했습니다. 이 시스템에는 고객 관련 PII 정보를 처리하는 고객 관계 관리(CRM) 시스템, 결제 및 인보이스 발행 시스템 등이 포함됩니다.

  보안 정책 및 절차의 증거 자료는 파트너의 MSP 비즈니스 범위 내에서 정보 보안과 관련된 현행 산업 인증(예: ISO 27001, SOC2) 또는 인프라 보안, 데이터 분류를 포함한 정보 보안 관리 프로세스 및 관련 승인에 대한 증명의 형식이 될 수

- **SEC-002 - 보안 인식 교육 및 테스트**

  필수

  AWS 파트너의 MSP 비즈니스 직원은 매년 보안 인식 교육을 이수합니다.

  AWS 파트너는 https://learnsecurity.amazon.com/ 또는 다른 유사한 교육 프로그램을 이용할 수 있습니다.

  증거 자료는 파트너의 MSP 비즈니스를 담당하는 현재 직원에 대한 교육 이수 기록의 형식이어야 합니다.

- **SEC-003 - AWS 계정 구성**

  필수

  AWS 파트너는 모든 관리형 고객 환경에 대해 구현되는 보안 제어의 표준 세트를 정의합니다. 이 표준에는 최소한 부록 A: 최소 AWS 계정 보안 구성에 정의된 모든 항목이 포함됩니다.

  증거 자료는 AWS 파트너가 관리하는 하나 이상의 AWS 조직에 등록된 모든 AWS 계정의 보안 구성 상태를 보여주는 보안 대시보드의 형식이어야 합니다. 심각도가 높음 또는 위험인 모든 결과에는 위험이 완화되는 방법 및/또는 개선 타임라인에 대한 문서가 함께 제공되어야 합니다.

- **SEC-004 - Identity and Access Management**

  필수

  AWS 파트너는 고객 데이터가 포함된 모든 AWS 계정 및 기타 시스템에 대한 액세스를 관리하기 위해 중앙 집중식 자격 증명 제공업체를 사용합니다.

  증거 자료는 고객 계정 및 기타 시스템에 액세스하기 위한 인증 프로세스를 시연하는 형식이어야 합니다.

- **SEC-005 - 정책 관리**

  필수

  AWS 파트너는 권한을 평가 및 제한하는 메커니즘을 구축했습니다. 여기에는 자격 증명의 그룹 및 역할 멤버십에 대한 기준선 설정, 그룹 및 역할에 부여된 특정 권한의 평가가 포함됩니다. 특히, IAM Access Analyzer 또는 유사한 도구를 사용한 AWS IAM 정책 검토가 포함되어야 합니다.

  증거 자료는 그러한 검토(지난 12개월 동안 1회 이상 수행) 및 그 결과의 형식이어야 합니다.

- **SEC-006 - 역할 기반 액세스**

  필수

  AWS 파트너는 소유한 인적 또는 시스템 자격 증명이 AWS 계정에 액세스할 때 모두 임시 자격 증명을 사용하도록 합니다. 특정 AWS 서비스에서 정적 자격 증명(예: Amazon SES SMTP 자격 증명)을 사용해야 하는 사례는 각 IAM 사용자에 대한 정책이 해당 서비스로 제한되는 한 허용됩니다.

  증거 자료는 기능적 역할을 기반으로 권한을 가진 IAM 역할을 보여 주는 형식이어야 하며 파트너 액세스 시나리오를 지원하는 최소 권한 원칙에 부합해야 합니다.

- **SEC-007 - 다중 인증**

  필수

  AWS 파트너의 인적 자격 증명으로 AWS 계정에 액세스하는 데 다중 인증(MFA)이 필요합니다.

증거 자료는 AWS 액세스를 위해 제공된 자격 증명 내에서 MFA를 적용하는 데 사용되는 메커니즘을 시연하는 형식이어야 합니다.

- **SEC-008 - 취약성 관리**

  필수

  AWS 파트너는 AWS 인프라의 보안 및 규정 준수를 평가할 수 있는 취약성 검사 기능을 제공합니다.

  증거 자료는 이 요구 사항을 해결하는 데 사용되는 기술 솔루션을 보여주는 형식이어야 합니다.

- **SEC-009 - 보안 이벤트 로깅**

  필수

  AWS 파트너는 1/ 보존 기간을 포함하여 고객과의 보안 이벤트 로깅 요구 사항을 정의하고, 2/ 필수 보안 이벤트 로깅을 캡처하며, 3/ 보존 기간을 준수하기 위한 제어 조치를 구현합니다.

  증거 자료는 1/ 동의한 요구 사항, 2/ 로그 캡처 방법, 3/ 합의된 기간 동안 보존되었음을 보여주는 고객 사례 형식이어야 합니다.

- **SEC-010 - SaaS 도구 계정 액세스**

  필수

  고객 AWS 계정에 액세스해야 하는 AWS 파트너가 관리하는 모든 타사 SaaS 도구 및 기타 도구는 크로스 계정 액세스를 제공하기 위해 외부 ID가 있는 IAM 역할을 사용해야 합니다.

  증거 자료는 고객 AWS 계정에 액세스할 수 있는 SaaS 도구 목록 및 외부 ID가 필요한 예시 IAM 역할 신뢰 정책의 형식이어야 합니다.

운영

- **OPS-001 - 서비스 수준 관리**

  필수

AWS 파트너는 자문 서비스, 전문 서비스, 운영 서비스와 같이 고객에게 제공하는 서비스와 관련된 SLA를 정의합니다. 이러한 SLA의 예로는 서비스 요청 규정 준수, 인시던트 및 문제 관리, 보안 이벤트, 변경 관리, 배포 품질 등이 포함됩니다(이에 국한되지 않음).

SLA에는 고객이 티켓을 개설하고 요청을 개시할 때 응답 시간, 이벤트 또는 인시던트 트리거에서 개선까지 걸리는 시간, 고객이 시작한 변경/요청에 대한 처리 시간이 포함될 수 있습니다.

증거 자료는 1/ SLA 문서 또는 보고서, 2/ AWS 파트너의 AWS 관리형 서비스 비즈니스에 해당하는 고객과의 검토 프로세스의 형식이어야 합니다.

제공되는 보고서의 예는 다음과 같습니다.

  - 인시던트 관리
  - 서비스에 영향을 주지 않는 인시던트
  - 서비스 수준
  - 성능 분석

- **OPS-002 - 파트너 소유 관리 및 회원 계정을 위한 AWS Support 플랜**

  필수

  AWS 파트너는 모든 AWS Organizations 관리 계정(다른 명칭: 지급자 계정)과 프로덕션 워크로드가 있는 회원 계정을 Business, Enterprise, PLS(파트너 주도) 지원 구독에 등록했습니다.

  증거 자료는 AWS 파트너가 관리하는 AWS Organizations의 목록 및 각 조직의 관리 및 회원 계정에 적용되는 지원 수준이 있는 형식이어야 합니다.

- **OPS-003 - 고객 소유 회원 계정을 위한 AWS Support 플랜**

  필수

  AWS 파트너는 고객에게 AWS Premium Support 플랜의 가치를 명확하게 전달하고 프로덕션 워크로드를 호스트하는 모든 고객 계정에 대해 Business 또는 Enterprise 지원을 권장합니다. AWS Support를 선택하지 않는 고객에게는 관련 위험, 즉 프로덕션에 영향을 미치는 인시던트가 발생할 경우 AWS 파트너에게 기본 AWS 서비스를 검사하고 문제를 해결하기 위한 액세스 권한이 없다는 것을 명확히 설명합니다.

증거 자료는 관리되는 고객 계정 및 연결된 AWS 지원 수준의 목록 및 프로덕션 계정에 AWS Business Support 보장을 사용하지 않는 고객과의 커뮤니케이션이 포함된 형식이어야 합니다.

- **OPS-004 - 서비스 데스크 운영**

  필수

  AWS 파트너는 여러 커뮤니케이션 수단을 통해 24x7 서비스 데스크 기능을 제공합니다. 24x7 직원을 둔 콜 센터 또는 영업시간 이후 지원이 제공되는 8x5 서비스(예: 순환 근무를 기반으로 영업시간 이후 호출기/알림 지원)가 될 수 있습니다.

  AWS 파트너는 서비스 데스크 기능을 제공하는 방식을 설명하거나 보여주어야 합니다. AWS 파트너가 24시간 직원을 둔 서비스 데스크를 유지하지 않는 경우, 영업시간 이후, 주말, 공휴일 지원에 대한 문서화된 절차가 있어야 합니다. AWS 파트너가 영업시간 이후 지원을 위해 타사 서비스를 사용하는 경우 두 제공업체 간에 공통된 도구 및 프로세스 세트가 있어야 합니다.

  증거 자료는 이 요구 사항에 관한 고객과의 계약(공식 또는 기타 문서)의 형식이어야 합니다.

- **OPS-005 - 포괄적인 ITSM 플랫폼 구현**

  필수

  AWS 파트너는 관리형 서비스 고객의 전체 서비스 수명 주기를 효과적으로 관리할 수 있도록 잘 설계된 통합형 ITSM 플랫폼을 보유해야 합니다. ITSM 플랫폼은 최소한 다음과 같은 기능을 제공해야 합니다.

  1. 인시던트 및 문제 관리: 티켓, 에스컬레이션, 근본 원인 분석을 통한 효율적인 인시던트 커뮤니케이션
  2. 변경 사항 관리: 모든 변경 사항을 추적, 승인, 문서화하여 규정 준수를 보장하고 서비스 중단 최소화
  3. 서비스 요청 관리: 간소화된 요청 이행 프로세스 및 보류 중인 요청 표시
  4. 보고 및 분석: 서비스 성능, 보고, 운영 효율성에 대한 인사이트
  5. 통합 및 자동화: 클라우드 모니터링 도구, 자동화 솔루션 등 파트너의 다른 시스템과 원활하게 통합하여 AWS 파트너의 티켓팅/ITSM 시스템에서 항목을 자동으로 만들거나 표준 경고/이벤트에 대한 자동 응답 실행

  AWS 파트너는 위 항목을 다루는 ITSM 플랫폼의 구현 및 효과적인 사용을 보여줘야 합니다.

- **OPS-006 - 릴리스 관리**

  필수

  다음 각 하위 항목에 대한 증거 자료는 프로덕션 변경 사항을 검증 및 관리하기 위한 엔드투엔드 프로세스를 보여주는 고객 사례의 형식이어야 합니다.

  0. AWS 파트너는 버전 제어를 사용하여 코드 및 배포 자산을 관리합니다.
  1. AWS 파트너는 프로덕션에 배포하기 전에 먼저 프로덕션이 아닌 환경에서 변경 사항을 테스트하고 검증하기 위한 표준 절차를 보유하고 있습니다.
  2. AWS 파트너는 프로덕션에 배포하기 전에 변경 승인을 관리하는 시스템을 보유하고 있습니다.
  3. AWS 파트너가 소유하며 배포하는 AWS 리소스의 경우, 파트너는 선언적(예: AWS CloudFormation 또는 HashiCorp Terraform) 또는 명령적(예: AWS Cloud Development Kit) 자동 인프라 배포 도구 중 하나를 사용합니다.

- **OPS-007 - 구성 관리**

  필수

  AWS 파트너는 환경 구성 변경에 대한 기록을 유지합니다. 운영자가 파트너가 수행한 모든 환경 변경 사항을 나열하고 각 변경 사항에 대해 다음과 같은 세부 정보를 추적할 수 있도록 지원하는 시스템이 있어야 합니다.

  - 추가/제거/업데이트된 리소스
  - 변경 날짜 및 시간
  - 현재 상태(예: 배포됨/롤백됨)
  - 변경을 수행한 사용자
  - 변경 사항에 대한 워크플로 승인 또는 경고: 이는 Configuration Management Database(CMDB)를 사용하거나 코드 리포지토리, 코드 서비스로의 인프라, 자동화된 배포 파이프라인 및 문제 추적 또는 워크플로 시스템의 조합을 사용하여 구현할 수 있습니다. 여러 도구가 사용되는 경우, 위에 나열된 모든 세부 정보를 제공하는 단일 통합 보기가 있어야 합니다.

  증거 자료는 고객 사례의 형식이어야 하며 해당 고객 환경의 구성 기록을 보고 최근 승인된 구성 변경 사항의 식별할 수 있는 기능의 시연이 포함되어야 합니다.

- **OPS-008 - 패치 관리**

  필수

  AWS 파트너는 운영 체제, 애플리케이션, 보안 및 규정 준수 관련 패치에 대한 고객 컴퓨팅 리소스 패치 프로세스를 자동화했습니다.

증거 자료는 사용 중인 패치 자동화 도구 및 패치 상태 보고의 기술 시연 형식이어야 합니다.

- **OPS-009 - 고객 배포 파이프라인**

  필수

  AWS DevOps 컴피턴시를 보유한 AWS 파트너는 이 요구 사항이 면제됩니다.

  AWS 파트너는 필요한 경우 자동화된 배포 및 롤백을 지원합니다. 고객 또는 파트너는 수동 개입 없이 새 버전의 애플리케이션 또는 클라우드 인프라를 배포할 수 있어야 합니다. 수동 승인 단계는 허용됩니다.

  증거 자료는 샌드박스 환경에서의 자동 배포를 보여 주거나 지난 6개월 동안 자동 배포를 실행한 고객 예시가 포함된 형식이어야 합니다. AWS 파트너는 고객 또는 파트너가 자동화된 배포를 일관적으로 사용함을 보여 주는 빌드/파이프라인 실행 내역 또는 기타 배포 로그를 제시해야 합니다.

- **OPS-010 - 이벤트 관리 및 동적 모니터링**

  필수

  고객 워크로드 및 인프라 상태 KPI를 정의, 모니터링, 분석: AWS 파트너는 워크로드 및 인프라의 각 구성 요소 상태를 파악하기 위한 지표를 정의했습니다. 다음을 통해 운영 절차를 실행, 모니터링 및 개선할 수 있는 역량을 구축하세요. a. AWS 서비스 또는 서드 파티 도구를 사용하여 워크로드 및 인프라 상태 지표를 정의, 수집, 분석합니다. b: 오류를 캡처하고 운영 이벤트에 대한 문제 해결 및 대응을 지원하는 표준 애플리케이션 로그로 구성되어야 합니다. c. 워크로드 및 인프라 지표의 임곗값을 정의하여 모든 문제에 대한 알림을 생성합니다. d. 태그를 사용하여 리소스를 구성하고 분류합니다.

  증거 자료는 고객 지표, 로그, 추적, 경보, 실시간 대시보드를 통해 인프라 모니터링과 애플리케이션 성능이 어떻게 충족되는지 보여 주는 도구 데모가 포함된 형식이어야 합니다.

- **OPS-011 - 운영 런북**

  필수

  AWS 파트너는 특정 워크로드/인프라/보안 알림에 대응하는 절차를 수행하기 위한 런북을 보유하고 있습니다.

증거 자료는 일상 업무에서 사용되는 런북 형식이어야 합니다.

- **OPS-012 - 이상 탐지**

  필수

  AWS 파트너는 통계 및 기계 학습 이상 탐지 모델(보통 기존의 ISV/오픈 소스 도구 또는 AWS CloudWatch 이상 탐지 기능 사용)을 구현하여 인프라 및 애플리케이션 계층을 비롯한 광범위한 워크로드 지표에 걸쳐 알림을 생성합니다. 이상 탐지는 알림의 오탐지를 줄이고 운영 직원의 경고 피로를 방지하는 데 사용됩니다.

  증거 자료는 이상 탐지 구현을 보여 주는 하나의 고객 예시가 포함된 형식이어야 합니다.

- **OPS-013 - 예측 모니터링 및 IT 운영을 위한 인공 지능(AIOps)**

  권장

  AWS 파트너는 모니터링 및 로깅 데이터의 추세를 식별하고 이상 또는 임곗값 위반이 탐지되기 전에 알림 또는 조치를 트리거할 수 있는 예측 모델(일반적으로 Amazon DevOps Guru 또는 기존의 ISV/오픈 소스 도구 사용)을 구현했습니다.

  증거 자료는 예측 모니터링과 AIOps를 보여 주는 하나의 고객 예시가 포함된 형식이어야 합니다.

- **OPS-014 - 지식 관리**

  필수

  AWS 파트너는 내부 운영 프로세스 및 고객 워크로드 관련 세부 사항에 대한 정보를 구성하기 위한 지식 관리 시스템을 유지 관리합니다. 여기에는 생성할 새 콘텐츠와 업데이트 또는 보관해야 하는 기존 콘텐츠를 식별하는 프로세스가 포함됩니다.

  증거 자료는 지식 관리 시스템을 시연하는 형식이어야 합니다.

- **OPS-015 - 재해 복구**

  필수

  AWS 파트너는 각 워크로드의 사전 정의된 목표 복구 시간(RTO) 및 목표 복구 시점(RPO)에 따라 모든 고객 워크로드 및 인프라에 대해 자동 백업을 구현합니다.

증거 자료는 고객 솔루션의 아키텍처에 사용되는 2개의 AWS 서비스에 대한 예시 백업 작업 및 복구 테스트가 포함된 형식이어야 합니다. 복구 테스트가 각 워크로드의 사전 정의된 Recovery Time Objective(RTO) 및 Recovery Point Objective(RPO)에 대해 평가됩니다.

- **OPS-016 - 클라우드 재무 관리**

  필수

  AWS 파트너는 고객이 다음과 같은 역량을 발휘할 수 있도록 하는 방법론, 프로세스, 관련 도구 경험을 갖추고 있습니다.

  0. 클라우드로 전환하려는 고객을 위한 총 소유 비용(TCO) 유형 분석 작성
  1. 고객이 클라우드 지출을 측정, 모니터링하고 이해할 수 있도록 지원하는 전략/프로세스 작성
  2. 관리형 서비스와 함께 AWS 서비스를 재판매하는 AWS 파트너는 고객과 동의한 요금을 기준으로 AWS 사용 비용을 표시하는 도구 보유

  증거 자료는 위에 나열된 기능을 설명하는 기술 데모가 포함된 형식이어야 합니다.

- **OPS-017 - 마이그레이션**

  필수

  현재 AWS 마이그레이션 컴피턴시 지정을 보유한 AWS 파트너는 이 요구 사항이 면제됩니다.

  AWS 파트너는 다음 작업을 처리하는 표준 방법론 및 자동화 도구를 사용하여 고객 워크로드를 외부에서 AWS로 마이그레이션하거나 현대화할 수 있는 역량을 보유하고 있습니다.

  - 포트폴리오 검색: 사용된 검색 도구와 고객과의 인터뷰를 통해 생성된 보고서, 권장 마이그레이션 및 현대화 전략에 대한 문서(7R - 사용 중지(Retire), 유지(Retain), 리호스팅(Rehost), 재배치(Relocate), 리팩터링(Refactor), 리플랫포밍(Replatform), 재구매(Repurchase))
  - 마이그레이션 또는 현대화 거버넌스: 이해 관계자에게 정보를 제공하기 위한 커뮤니케이션 계획, 가동 중지 시간을 완화하는 전환 계획, 애플리케이션에 대한 테스트 및 롤백 계획
  - 인력 및 기술: RACI 매트릭스, 고객에게 제공되는 전환 계획, 고객을 위해 작성된 역할 기반 교육 계획의 문서화, 고객에게 제공되는 지식 이전 또는 교육 콘텐츠

    - 랜딩 존: 랜딩 존을 만들고 유지 관리하는 데 사용되는 도구의 AWS 다중 계정 구조, 프로세스, 출력이 포함된 다이어그램
    - 운영: 이벤트, 로그, 지표 및 분산 추적을 관찰하고 분석하는 데 사용되는 도구의 클라우드 운영, 대시보드 또는 보고서를 다루기 위해 작성되거나 변경된 런북 또는 표준 운영 절차(SOP)
    - 보안, 위험 및 규정 준수: 고객으로부터 보안, 위험 및 규정 준수 요구 사항을 수집하는 방법과 이러한 요구 사항을 충족하는 데 사용되는 도구에 대한 프로세스 문서화
    - 애플리케이션 마이그레이션 또는 현대화: 파일럿/MVP를 위해 선택한 애플리케이션, 워크로드 또는 솔루션 구성 요소의 문서화된 목록과 파일럿/MVP에서 얻은 지식의 문서화

    증거 자료는 위 항목을 다루는 관련 문서가 포함된 고객 사례 2건의 형식이어야 합니다. 최소 하나 이상의 예시에는 https://docs.aws.amazon.com/prescriptive-guidance/latest/large-migration-guide/migration-strategies.html에 설명된 대로 리팩터링 또는 리플랫포밍이 포함되어야 합니다.

- **OPS-018 - 인공 지능**

    권장

    관리형 서비스 제공업체는 기술과 고객 요구의 교차점에 서 있으며 비즈니스에 혁신적인 AI 솔루션을 제공할 수 있는 독보적인 위치에 있습니다. AI를 사용하여 관리형 서비스 비용을 줄이면서 사용자 경험을 개선합니다. 또한 MSP는 생성형 AI 기술을 활용하여 고객이 사용 사례를 혁신할 수 있도록 지원합니다.

    증거 자료에는 내부 용도로 생성형 AI 기술을 사용하거나 고객 프로젝트에서 파트너의 생성형 AI 제품을 사용하는 것을 보여 주는 문서가 포함될 수 있습니다. 이러한 증거 자료에는 작업 명세서(SOW), 프로젝트 계획, 스프린트 계획, 프로젝트 제안, 기타 관련 결과물이 포함될 수 있습니다.

리소스

- VCL 7.0 및 7.1용 AWS 관리형 서비스 제공업체(MSP) 프로그램 조정 가이드
- AWS 관리형 서비스 제공업체(MSP) 프로그램 모범 사례
- 체크리스트 변경 로그

부록 A - 최소 AWS 계정 보안 구성

신규 계정 생성	
신규 계정 생성	다음 모범 사례가 구현되도록 새 AWS 계정을 만드는 프로세스를 문서화합니다.
	(권장) 계정 생성 프로세스 및 가드레일 구성을 자동화합니다.
계정 연락처	모든 기본 및 대체 계정 연락처를 구성합니다.
	모든 계정 연락처에 이메일 배포 목록을 사용합니다.
	모든 계정 연락처에 직원의 개인 전화번호가 아닌 AWS 파트너 또는 고객이 소유하고 제어하는 전화번호를 사용합니다.
루트 사용자 보안	루트 사용자가 필요한 작업에만 사용되도록 합니다.
	AWS Organizations 관리 계정, 독립 실행형 계정 또는 서비스 제어 정책(SCP)을 사용하여 루트 액세스를 거부하지 않는 모든 계정의 경우 루트 사용자에 강력한 암호를 설정하고 MFA를 활성화합니다. 암호를 안전하게 보관합니다.
	루트 사용자에 대한 액세스 키가 존재하지 않는지 확인합니다.
	(권장) AWS Organization 멤버 계정에서 서비스 제어 정책(SCP)을 사용하여 루트 사용자로부터 액세스를 거부합니다.
이벤트 로깅	AWS Cloud Trail에서 다중 리전 추적을 생성합니다.
	CloudTrail 로그를 별도의 보안 또는 감사 계정의 Amazon Simple Storage Service(S3) 버킷으로 전송합니다. 단일 보안 또는 감사 계정에서 혼잡을 방지하기 위해 대규모 계정 그룹의 경우 예외가 적용될 수 있습니다.
	로그 파일 서버 측(SSE-S3 또는 SSE-KMS) 암호화를 활성화합니다.
	로그 파일 검증을 활성화합니다.
	CloudTrail 로그가 저장되는 S3 버킷을 보호합니다. 버킷 정책이 불필요한 액세스 권한을 제공하지 않는지 확인합니다. - MFA 삭제를 활성화합니다. 서버 측 암호화를 활성화합니다. 수명 주기 구성을 사용하는 S3에서는 MFA 삭제가 불가능하므로 여기서는 MFA를 활성화할 필요가 없습니다.
클라우드 보안 태세 관리	
보안 표준	AWS 기초 보안 모범 사례 또는 CIS AWS Foundations Benchmark와 같은 보안 표준을 채택하고 해당 표준(예: AWS Security Hub) 준수를 지속적으로 평가하도록 도구를 구성합니다.
	채택하는 표준은 최소한 다음 사항을 검증해야 합니다.
	- 루트 사용자에 대해 MFA가 활성화되어 있습니다.
	- 루트 사용자에 대한 액세스 키가 존재하지 않습니다.
	- 모든 리전에서 CloudTrail이 활성화되어 있거나 다중 리전 추적이 존재합니다.
	- S3 버킷에 대한 퍼블릭 액세스가 비활성화되어 있습니다.
	- 보안 그룹이 고위험 포트에 대한 무제한 액세스를 허용하지 않습니다.
	계정의 논리적 그룹(예: 고객 조직별)에서 결과를 집계합니다.
태세 모니터링	새로 식별된 높은 심각도 위험에 대한 알림으로 경보를 생성합니다.
	AWS 계정, 워크로드 및 데이터에서의 악의적 활동을 지속적으로 모니터링하는 위협 탐지 서비스와 통합합니다.
	계획된 개선조치 날짜와 함께 위험 또는 높은 심각도로 분류된 모든 위험에 대한 예외를 문서화합니다.

부록 B - 모범 사례 가이드 및 참조 자료

- Amazon Web Services 백서:
  - http://aws.amazon.com/whitepapers/
- AWS 보안 센터:
  - http://aws.amazon.com/security/
- AWS 보안 모범 사례:
  - https://aws.amazon.com/whitepapers/aws-security-best-practices/
- AWS 규정 준수:
  - https://aws.amazon.com/compliance/
- AWS Cloud Audit Academy:
  - https://www.aws.training/Details/eLearning?id=41556

- AWS 보안 자격 증명 소개:
  - http://docs.aws.amazon.com/general/latest/gr/aws-security-credentials.html
- 시작하기: Amazon Identity and Access Management:
  - http://docs.aws.amazon.com/IAM/latest/UserGuide/getting-started.html
- IAM 모범 사례:
  - http://docs.aws.amazon.com/IAM/latest/UserGuide/IAMBestPractices.html
- Amazon Web Services에 보안 요청 전송:
  - http://aws.amazon.com/articles/1928?_encoding=UTF8&andjiveRedirect=1
- AWS에서 내결함성 애플리케이션 구축:
  - http://d36cz9buwru1tt.cloudfront.net/AWS_Building_Fault_Tolerant_Applications.pdf
- AWS Well-Architected:
  - https://aws.amazon.com/architecture/well-architected/
  - https://wa.aws.amazon.com/wat.pillar.security.en.html
  - https://wa.aws.amazon.com/wat.question.SEC_9.en.html
- AWS 전문화 프로그램 사례 연구 가이드: (Partner Central 로그인 필요)
  - https://partnercentral.awspartner.com/partnercentral2/s/resources?Id=0698W00000wgPO9QAM

변경 사항 요약

버전	날짜	변경 사항 요약
7.1	2025년 8월	신청 절차에 대한 추가 정보 및 설명이 추가되었습니다. GOVP-001 이 업데이트되어 공급업체 선정 과정을 증명하는 실제 문서 제출 요건이 삭제되었으며, 이제 일반 SOP가 허용됩니다.
7.0	2024년 10월	이제 AWS 관리형 서비스 제공업체(MSP) 감사 프로세스는 하이브리드 모델을 준수하며, 이로 인해 파트너가 기술 검증 단계로 진행하기 전에 먼저 지정된 전제 조건 제어 항목을 충족해야 합니다. 오프라인으로 처리할 수 있는 이러한 전제 조건 제어 항목을 사용하려면 기술 검증 최소 30일 전까지 AWS MSP 프로그램 팀에 증거 자료와 문서를 제출하셔야 합니다. 서드 파티 회사에서 실시하는 기술 검증에서는 파트너의 역량, 프로세스, 나머지 제어 항목의 준수 여부를 하루 동안 철저하게 평가합니다.