

SMB Copilot in-a-Box

 D:MOA

SMB Copilot in-a-box

Microsoft 365 Copilot 도입 및 배포를 위한 추진 단계별 요구되는 핵심 개념을 미리 파악하고, Microsoft 365 Copilot 도입 전 필수 준비 항목 및 의사결정이 필요한 사항을 사전에 검증하고 지원 함.

- 주요 고려사항



신규 업무 프로세스

기업의 성장을 위한
업무 프로세스 구축 필요



생산성/보안 구성

조직 내/외부 사용자에게 대한
생산성 환경과 보안 설정 통합



통일된 업무 솔루션

주요 프로젝트 관리
기존 업무프로세스 단일화
문서 공유 및 공동작업 환경 구성



보안관리 체계

외부 네트워크에서 제한된 접속
문서 암호화 및 권한 관리

SMB Copilot in-a-box

Microsoft 365 Copilot 도입 및 배포를 위한 추진 단계별 요구되는 핵심 개념을 미리 파악하고, Microsoft 365 Copilot 도입 전 필수 준비 항목 및 의사결정이 필요한 사항을 사전에 검증하고 지원 함.

- 필수 항목인 Microsoft 365 도입으로 무엇을 할 수 있을까요?

통합된 사내 협업체계 구축



- 데스크톱과 웹 환경 그리고 모바일과 태블릿까지의 상시 업무 수행을 할 수 있는 환경과 도구 배포
- 현재 조직 내에서 진행 중 또는 예정인 프로젝트 관리와 프로젝트 수행을 위한 협업공간 제공

조직 외부와의 협업



- 업무영역이 조직 외부로 확장됨에 따라 조직 데이터 접근 관리 체계 확립
- 조직 내부 사용자와 외부 사용자를 구분하여 서비스 접근을 제어하고 유연한 협업을 위해 각각의 권한 설정

보안관리체계 구축



- 조직 내 데이터 관리와 유출 위험을 최소화하며 문서 암호/복호화를 통해 보안 유지
- 보안 설정의 권한관리를 통해 데이터 접근레벨 관리

SMB Copilot in-a-box

Microsoft 365 Copilot 도입 및 배포를 위한 추진 단계별 요구되는 핵심 개념을 미리 파악하고, Microsoft 365 Copilot 도입 전 필수 준비 항목 및 의사결정이 필요한 사항을 사전에 검증하고 지원 함.

- 필수 항목인 Microsoft 365 도입은 왜 필요할까요?

기존의 업무 프로세스 및 현황

단일화 되지 않은 소통도구(카카오톡, Teams 등)
사업부서 별 서로 다른 협업 도구 사용

기존에 사용하던 프로젝트 관리 도구의 기능 미흡으로
부서 성향 별 서로 다른 협업 도구 사용

서로 다른 협업도구를 사용하기 때문에 별도의
보안체계 구성이 어려운 상황

단일화된 소통도구 및 협업 도구와
공동작업 환경, 문서 유출방지 및 데이터 보안 필요



업무 방식 변경에 따른 변화관리 중요성

- 시간과 장소 제약이 없는 신속한 커뮤니케이션과 협업이 필수
- 조직 내부 사용자 뿐만이 아니라 외부 사용자와의 업무 중요성 증대

Microsoft 365 도입을 통한 새로운 업무 프로세스

사내 메신저를 Teams로 통합관리
사업부별로 사용하던 협업도구를 SharePoint
Online으로 단일화

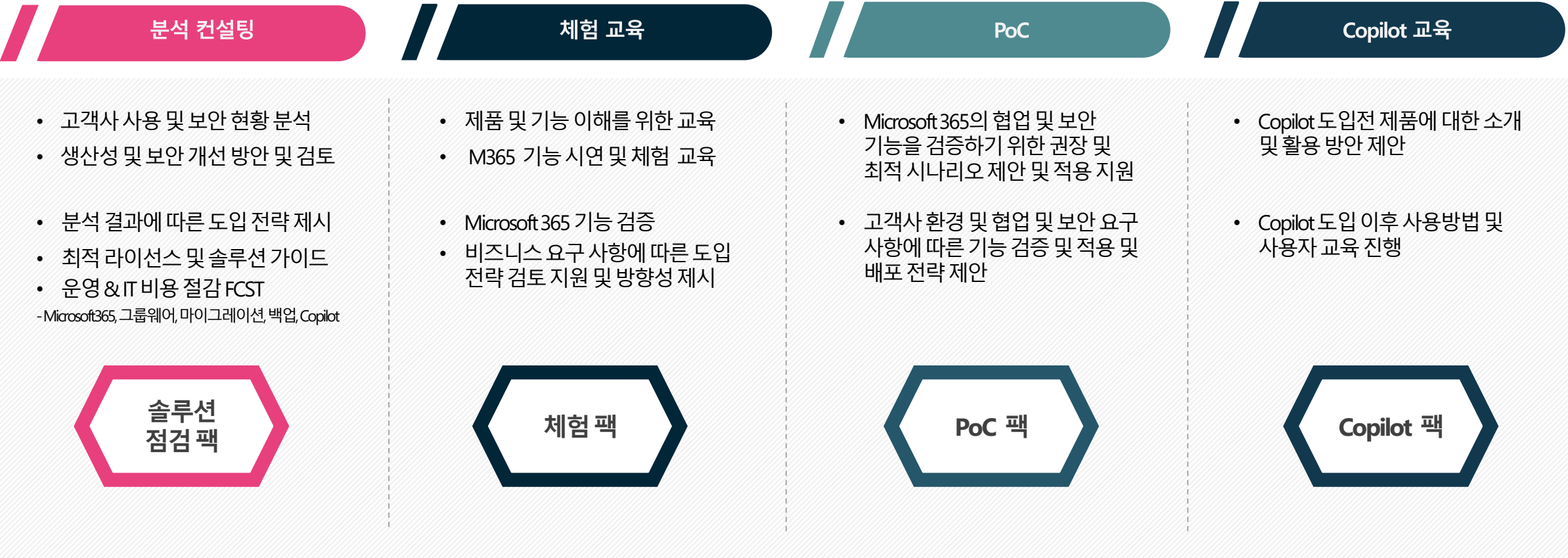
Teams를 활용한 협업공간 제공
프로젝트 관리를 위해 Planner 및 To-Do 기능과 3rd Party 솔루션을
In-App 형태로 활용

문서 중앙관리화를 위한 민감도 레이블 정책 구성으로 문서 보안
및 권한관리
조직의 데이터 유출 방지를 위한 DLP 정책 구성

모바일 환경에서의 보안을 위해 MAM 앱 보호 정책 구성
Azure AD의 조건부 액세스 정책을 통해 외부 네트워크의 제한적
접속 또는 차단

Microsoft 365의 원활한 도입을 위한 디모아 주요 제공 프로그램

기업에 요구되는 스마트 워크 업무 환경과 진보된 보안을 위해 Microsoft 365 을 도입하기 위한
분석 컨설팅, 체험 교육, 검증 프로그램을 제공 합니다.
이는 AI기반 도구인 Copilot을 업무에 활용하기 위해 필수로 요구됩니다.



디모아 고객/파트너사에 제공되는 기타 서비스

Microsoft 365 비즈니스에 필요한 고객 및 파트너사 교육 서비스 및 기술/구축 지원 서비스를 제공 합니다.

교육 서비스

- 고객사: 현업 요구 사항에 따른 사용자 교육 및 세미나
- 고객/파트너: 제품 및 기능 교육 및 체험 세미나
- 고객사/파트너사: M365 도입한 고객사를 위한 IT 관리자 운영 교육 (유료)

기술 지원 및 구축 지원

- Microsoft 365 구매 고객 1차 기술 지원 (고객사)
- Microsoft 365 도입 및 사용에 필요한 가이드 지원 (고객/파트너)
- Microsoft 365도입 미팅에 방문 지원 (고객/파트너)
- Microsoft 도입을 위한 구축 지원 (유상 및 별도 협의)

유지 보수

- Microsoft 365 도입한 기업의 운영 및 유지보수 지원
(유상 구축 고객에 한하며, 별도 협의)
- 1차, 2차 기술 지원 (협의 기간에 따라 상이)
- 서비스 정기 점검 (연 4회)
- 관리자 교육 (연 1회, 별도 협의 필요)
- 사용자 교육 (연 1회, 별도 협의 필요)

고객/파트너사를 위한 디모아 지원 인력 및 역량

Microsoft 전문 기술지원 인력 현황

Microsoft 제품군에 따라 분야별로 전문화된 전문 컨설턴트와 엔지니어를 운영하고 있습니다.
전체 인원 총 5명이 기술 역량을 확보하며, 관련 업무를 수행 중 입니다.



MP Team (Modern Workplace & Presales)

역할	주요 기술 분야	등급	인원
Consultant	Microsoft Solution Architect & Design	특급	1명
System Engineer	Application Server Exchange, SharePoint, Teams, Defender, Purview Information Protection	중급	3명
System Engineer	Platform Windows, Client O/S, Office Exchange, sharepoint, Teams	초급	1명
총			5명

보유 역량

Microsoft Certifications	
특급	Microsoft 365 Certified: Enterprise Administrator Expert
	Microsoft® Certified Solutions Expert: Productivity Charter Member
	Microsoft® Certified Solutions Associate: Office 365
	Microsoft® Certified Solutions Expert: Messaging
	Microsoft® Certified Technology Specialist: Windows 7 and Office 2010, Deployment
	Microsoft® Certified Solutions Expert: Messaging
	Microsoft® Certified Solutions Expert: Communication
	Microsoft® Certified Solutions Expert: SharePoint (Inactive)
	Microsoft® Certified Solutions Associate: Windows Server 2012
	Microsoft® Certified Solutions Expert: Data Platform (Inactive)
	Microsoft® Certified Solutions Associate: SQL Server 2012/2014
	Microsoft® Certified Technology Specialist: Windows Server 2008 Active Directory, Configuration
	Microsoft® Certified IT Professional: Database Administrator 2008
	Microsoft® Certified Technology Specialist: SQL Server 2008, Implementation and Maintenance
중급	Microsoft 365 Certified: Modern Desktop Administrator Associate
	Microsoft 365 Certified: Enterprise Administrator Expert
	Microsoft® Certified Solutions Associate: Windows 10
	Microsoft® Certified Solutions Associate: Office 365
초급	Microsoft Certified Professional
	Microsoft 365 Certified : Fundamentals
	Microsoft 365 Certified: Messaging Administrator Associate
	Microsoft 365 Certified: Enterprise Administrator Expert
	Microsoft 365 Certified: Teams Administrator Associate
	Microsoft Certified: Azure Fundamentals

유료 지원 프로그램 서비스 (예정)

유료 기술 지원 계약 고객에게는 아래와 같은 기술 지원 서비스를 제공할 예정 입니다. (FY25 예정)

서비스 구성		서비스 적용 방안	Basic	Standard	Premium
디모아 Microsoft 365 지원 서비스	Microsoft 기술 자문	고객의 단순 기술 문의 요청 서비스 진행(근무시간 내)	●	●	●
	AD 및 AAD 관리	사내AD 및 Azure AD 변화 관리	●	●	●
	M365 구독 관리	M365 사용자 구독 관리	●	●	●
	장애 지원(일반)	일반 지원 : 1차, 2차 기술지원으로 디모아 기술 인력 지원	●	●	●
	장애 지원(프리미엄)	프리미엄 지원 : MS Premium 기술 지원		●	●
	전담 기술지원 인력 배정	고객별 담당 엔지니어 전담하여 서비스		●	●
	요청응답시간	장애 접수 후 최초 응답시간 보장	6시간	4시간	2시간
	사내 서버 관리	MS 기반 서버 운영 및 변경		●	●
	8 x 5 기술지원	8시간 x 5일(업무 5일) 기술지원 및 긴급 장애 처리 서비스	●	●	●
	8 x 7 기술지원	8시간 x 7일(업무 5일 + 휴일 2일) 기술 지원 및 긴급 장애 처리 서비스		●	●
	24 x 7 기술지원	365일 상시 장애 처리 서비스			●
	서비스 상태 모니터링	서비스 상태 모니터링		●	●
	Alert 관리	서비스 이상에 대한 Alert 관리		●	●
	월별 리포트 제공	월별 서비스 통계 및 점검 사항 리포트		●	●

Microsoft 365 도입을 위한 사전점검 리스트

Area	Sub Area	Questionnaire	Answer		참고사항
			예	아니오	
★아래 모든 질문에서 사용하고 계시는 메신저, 메일, 그 외 모든 솔루션의 경우 공유가능하시다면 참고사항에 솔루션 이름을 적어주시기 바랍니다.★					
Communication	Mail	메일 시스템을 사용중이신가요? 사용중이시라면 참고사항에 메일 시스템 이름을 기입 부탁드립니다.			예 : 자체 메일서버 / 하이웍스 / 비즈메카 / 카페 24 등
		메일 사용이 회사 업무의 어느정도 비율을 차지하고 있습니까? (50%이상 예 / 50%이하 아니오)			
		sales, help, tax 등 회사 공용 메일계정 또는 그룹메일계정을 사용중이십니까?			
		임직원들에게 필요한 사서함 공간이 50GB 이상 입니까?			
		대용량 첨부파일을 사용 중입니까?			
	Message	사내에서 업무적으로 사용중인 메신저가 있으십니까?			
		쪽지 보내기 기능 이외에 사용하시는 기능이 있으십니까?			
		메신저에서 사용자의 상태정보를 확인할 수 있습니까?			
		메세지 데이터 저장 및 관리가 필요하십니까?			
		고객 또는 협력사와 커뮤니케이션 하기위해 메시저를 이용 중입니까?			
	Call/Video/Conference	비대면 업무 시스템이 구축되어 있습니까?			
		화상회의 솔루션을 사용중이십니까?			
		화상 회의 솔루션의 성능에 어느정도 만족 하십니까?			
		화상 회의 장비를 갖추고 계십니까?			
		다중 화상회의 시스템이 구축되어 있습니까?			
		사용중인 솔루션에서 IP/Telephone 기능을 사용 가능합니까? (전화걸기, Call-fwding 등)			
		회의 중에 회의 내용을 녹음하고 녹화할 수 있는 솔루션을 사용하고 있습니까?			
		회사 외부에서 회사 내의 공유 공간에 있는 문서에 대한 접근이 가능합니까?			
Collaboration	Mobility	회사 내의 문서 접근 과정에 모바일 또는 메일 등의 2차 인증을 사용하고 있습니까?			
		회사내 PC에서 작성한 자료를 외부에서 태블릿 및 스마트폰으로 빠르게 접근 가능한 시스템이 구축되어 있으신가요?			
		회사 외부에서 개인의 업무 정보(메일과 일정, 작업 등)를 확인할 수 있습니까?			
		회사 외부에서 팀 업무 정보(일정, 작업 등)를 확인할 수 있습니까?			
		사내 전용 메신저를 스마트폰에서도 동일하게 사용중이신가요?			
		조직에서 임직원들에게 제공하는 클라우드 저장소 또는 중앙 저장소가 있습니까?			
		외부 유출 걱정 없이 안전한 위치에 문서 중앙화 시스템이 구축되어 있으신가요?			
		문서의 공유가 어떤 방식으로 이루어지고 있습니까? 있으시다면 참고사항에 간략히 기입 부탁드립니다.			
	Sharing	외부인에게 문서파일을 공유할때 특정 인원만 보거나 수정 가능한 시스템이 구축되어 있습니까?			
		공동으로 작성되는 문서의 변동 사항이 실시간으로 모두에게 반영될 수 있나요?			
		회사 내 공지사항 등 전달이 잘 이뤄지고 있습니까? 있다면 전달 방법을 참고사항에 기입 부탁드립니다.			
		사내 일정 공유가 원활하게 이루어지고 있습니까?			
		예 : 전체 메일 / 사내 메신저 / 카카오톡 등			
	Resource	회의실 및 장비 리소스 관리 및 공유가 이루어지고 있습니까?			
		차량 등 자원 관리 및 예약 현황 공유가 이루어지고 있습니까?			

Microsoft 365 도입을 위한 사전점검 리스트

Area	Sub Area	Questionnaire	Answer		참고사항
			예	아니오	
★아래 모든 질문에서 사용하고 계시는 메신저, 메일, 그 외 모든 솔루션의 경우 공유가능하시다면 참고사항에 솔루션 이름을 적어주시기 바랍니다.★					
Security	Identity	사용되는 계정들의 경우 보안이 강화되어 있습니까? (예 : 다중보안)			
		중요 시스템에 대한 임직원들의 권한이 세분화 되어 있습니까?			
		통합 디렉토리 서비스 기반의 SSO가 구현되어 있습니까?			
		사용자 정보가 디렉토리 서비스와 연동되어 있습니까?			
		조직의 업무시스템에 접근하는 조직 외부 사용자가 있습니까?			
		업무 시스템에 접근하는 외부 사용자가 있다면 이에 대한 허용, 차단 등의 관리가이루어 지고 있습니까?			
	Information	외부 사용자를 허용 하기 위한 관리가 되어 있다면, 외부 사용자 허용 리스트가 있습니까?			
		회사 중요 파일의 내용을 보호 (복사, 회신, 전달 등의 금지) 할 수 없게 조치하셨습니까?			
		입사 혹은 퇴사 시 메일, 계정, 자료에 대한 관리가 이루어지고 있습니까?			
		사용자가 삭제한 자료를 되돌리기 용이한 시스템을 구축하셨습니까?			
		문서별로 접근 권한을 부여하고 계십니까?			
		수신 메일에 첨부되어있는 파일의 보안 검사를 진행하고 계십니까?			
		내외부 메일에 대한 Spam/Virus/Phishing/ATP 방지 장비 또는 솔루션을 사용중이십니까?			
		내외부 네트워크로 접근할 때 URL 등을 제한하는 장비 또는 솔루션을 사용 중입니까?			
		VPN없이 외부에서 내부 데이터에 접근이 가능합니까?			
		보안 메일(전달 금지/인쇄 금지/복사 금지 등)을 작성할 수 있습니까?			
		메일 데이터 백업이 이루어지고 있습니까?			
		조직 외 사용자를 협업을 제한하기 위한 솔루션 또는 프로세스를 운영하고 있습니까?			
		재택 근무자 또는 출장자를 위한 별도의 보안 솔루션이 있습니까?			
	Dashboard	현재 회사 내 업무 상황을 쉽게 파악할 수 있는 대시보드를 보유하고 계신가요?			
		회사 내 시스템 사용현황을 쉽게 파악할 수 있는 대시보드를 보유하고 계신가요? (ex 메일 저장 공간)			
		현재 사내 보안 현황에 관련된 레포트를 받고 계십니까?			
	Device	회사 내에서 물리적인 네트워크 보안 솔루션이 적용되고 있습니까?			
		사내 데이터에 인증 받은 디바이스만 접속 가능한 구성이 되어있습니까?			
		접근 가능한 디바이스에 대한 관리가 이루어 지고 있습니까?			
		접근 디바이스에 대한 보안 준수 규정 또는 정책이 운영 중입니까?			
Audit	정책을 기준으로 관리되는 기록에 대해 이메일 발송, 로컬 저장 등 정책을 기반으로 하는 행위 발생시, 관련 사실이 담당자들에게 보고되고 있습니까?				
	감사(Audit)를 위한 대비가 필요한 상황입니까?				
	인스턴트 메시징 인프라(메신저 등)를 통해 주고 받는 메시지는 모니터링이 가능합니까?				
	데이터 중요도에 따른 권한 및 정책 관리 프로세스가 운영되고 있습니까?				
	현재 시스템 및 사용자의 활동 및 데이터에 대한 활동 로그가 감사되고 있습니까?				
	감사가 되고 있다면 보존해야 하는 로그의 최소 기간도 있습니까?				