금융권 클라우드 가이드라인을 위한 Azure 보안 전략

신용녀
National Technology Officer
한국마이크로소프트

Microsoft

금융권 클라우드 이용 확대 방안(18.9), 금융권 클라우드 개정('19.1)

규제 개혁 장관 회의	개인정보 비식별화 가이드 라인	클라우드 보안 워크숍 개최	클라우드 서비스 이용가이드 발간	금융권 클라우드 이용 확대 방안
❑ 민감한 정보를 제외한 업무는 원칙적으로 물리적 망 분리의 예외를 허용한다는 방침 처음 발표 ❑ 9월 금융 당국의 전자금융감독 규정 수정 방침 발표	❑ 금융보안원, 한국신용정보원은 비식별 빅데이터 활용 활성화를 위해 "비식별화 가이드라인 발표" ❑ 9월 "금융권 대상 비식별 조치 세미나" 개최 ❑ 비식별화된 정보에 대해서는 개인정보로 취급하지 않고 다양한 빅데이터 분석이 가능	❑ 9/28일 금융감독원 IT검사 실장은 "금융 사업자가 자체적으로 수립한 자산 중요도에 따라 비중요 정보 시스템으로 지정" 가능하다고 함 ❑ 이 경우 망분리 및 원격 관리 규정이 예외 처리 됨	❑ 금보원, 금감원에서는 클라우드 서비스 이용가이드라인 발간 ❑ 비중요 정보시스템 정의 절차 명시 ❑ 고유식별정보 및 개인신용정보 처리(송신, 수신, 전달) 하는 경우 비중요로 정의 불가	❑ 현재 전자금융감독규정에만 존재하는 클라우드 제한 규정을 정비해 이용범위를 확대 ❑ 사고 발생 시 법적분쟁, 소비자 보호·감독 관할의 문제로 국내 소재 클라우드에 한해 우선 허용 ❑ 금융당국의 감독방안 보완 필요

금융권 클라우드 제도 개선 TF 구성(7월) -> 금융권 클라우드 서비스 가이드라인 개정(8~12월)

클라우드 이용범위에 따른 금융권 적용사례(Before)

- **고유식별정보 또는 개인신용정보를 처리하는 정보처리시스템**

AI활용 대고객 서비스 (챗봇 등) | 빅데이터 분석 | 인터넷 뱅킹, HTS등 | 재해복구센터 구축 | 콜센터 /CRM(고객관리) | 오픈 API 제공 | 혁신 서비스 테스트

- **고성능 컴퓨팅**

파생상품 개발 | 보험 손해액 산정 | 회계 시스템

- **대고객 신규 서비스 구축**

신규 모바일 앱 템 | 뱅킹 서비스 | 홈페이지

전자금융감독규정 개정 ('19. 1.1.)

금융위원회

보 도 자 료

보도	2018.12.7.(금) 11:00	배포	2018.12.7.(금)

책 임 자	금융위 전자금융과장 주 홍 민(02-2100-2970)	담 당 자	김 영 진 사무관 (02-2100-2973)
	금감원 IT.핀테크전략국장 전 길 수(02-3145-7420)		정 기 영 팀장 (02-3145-7415)

제 목 : 「전자금융감독규정」 개정·시행(2019년 1월 1일)

- 금융회사가 클라우드를 자율적으로 안전하게 활용할 수 있게 됩니다.

1. 개정 배경

□ 금융위원회는 '18.12.5(水) 제21차 정례회의를 개최하여, 「**전자금융감독규정 개정안**」을 **심의·의결**하고 '19.1.1일 시행할 예정

○ 지난 '16년부터 금융권은 개인신용정보가 아닌 '비중요 정보'에 한해 클라우드를 허용하였으나,

- 최근 **금융분야 디지털화(digitalization)가 폭넓게 확산**됨에 따라 클라우드 이용 확대와 관련한 추가 규제완화 필요성이 지속 제기

* 클라우드 규제완화 건의, 전문가 의견 수렴(핀테크 간담회(4.11), 클라우드 간담회(4.17))

○ 이에 금번 개정안은 클라우드 활용 범위를 **개인신용정보까지 확대**하되, **금융권 보안수준 및 관리·감독체계를 강화**하도록 함

2. 주요 내용

1 금융권 클라우드 이용범위 확대 (§14조의2 제1항·제8항)

○ **(현행)** 금융회사·전자금융업자는 중요정보(개인신용정보·고유식별정보)를 포함하지 않은 **非중요정보만 클라우드**에서 이용 가능

○ **(개선) 개인신용정보·고유식별정보도 클라우드에서 이용** 가능

2 금융권 클라우드서비스 안전성 기준 제시 (§14조의2 제1항, 별표2의2)

○ **(현행)** 금융회사 등이 비중요정보만을 이용할 수 있고, **별도의 클라우드 서비스의 안전성 기준이 없음**

○ **(개선) 금융분야 특수성을 반영한 안전성 확보조치** 등 금융권 클라우드 이용·제공 기준을 제시

< 금융 클라우드 안전성 기준 >

데이터 보호	금융권 통합보안관제 지원, **전산자료 접근통제, 정보시스템 가동기록 보존**, 중요정보 **암호화 등 데이터 보호**, 개인(신용)정보법 등 금융관련 법령 준수
서비스장애 예방/대응	클라우드 이용시에도 주요 전산장비 **이중화 및 백업체계를 구축**, 서비스 **연속성 보장, 장애 발생시 비상 대응조치통지 의무**

3 클라우드에 대한 내부통제 강화 (§14조의2 제1항·제2항 등)

○ **(현행)** 개인신용정보·고유식별정보를 포함하지 않은 **비중요 정보시스템**에 대해서 **별도의 안전성 평가없이**도 지정·운영

○ **(개선)** 금융회사가 클라우드 서비스의 **안전성을 평가**하고, **자체 정보보호위원회 심의·의결**을 거치도록 함

4 클라우드 이용 관련 보고의무 등 감독 강화 (§14조의2 제3항~제6항)

○ **(현행)** 비중요정보 처리시스템 운영현황에 대해서만 보고

○ **(개선)** 정보의 중요도에 따라 클라우드 이용 현황을 **감독당국에 보고**하고, **법적책임, 감독·검사 의무** 등을 계약서에 명확화

5 국내 소재 클라우드 운영 (§14조의2 제8항)

○ 사고 발생시 법적 분쟁, 소비자 보호, 감독 관할 등을 고려해 **개인신용정보 처리는 국내 소재 클라우드**에 한해 **우선 허용**

6 기타 : 허가·등록의 물적요건 정비 등

금융분야
클라우드컴퓨팅서비스
이용 가이드

금융미래를 열어가는 금융보안파트너

금융보안원
FINANCIAL SECURITY INSTITUTE

2019. 1.

금융분야 클라우드서비스 이용 관련 기본 방향

□ 금융회사의 클라우드서비스 이용은 「금융회사의 정보처리 업무 위탁에 관한 규정」 제5항 및 제6항에 따라 **정보처리 위탁**에 해당

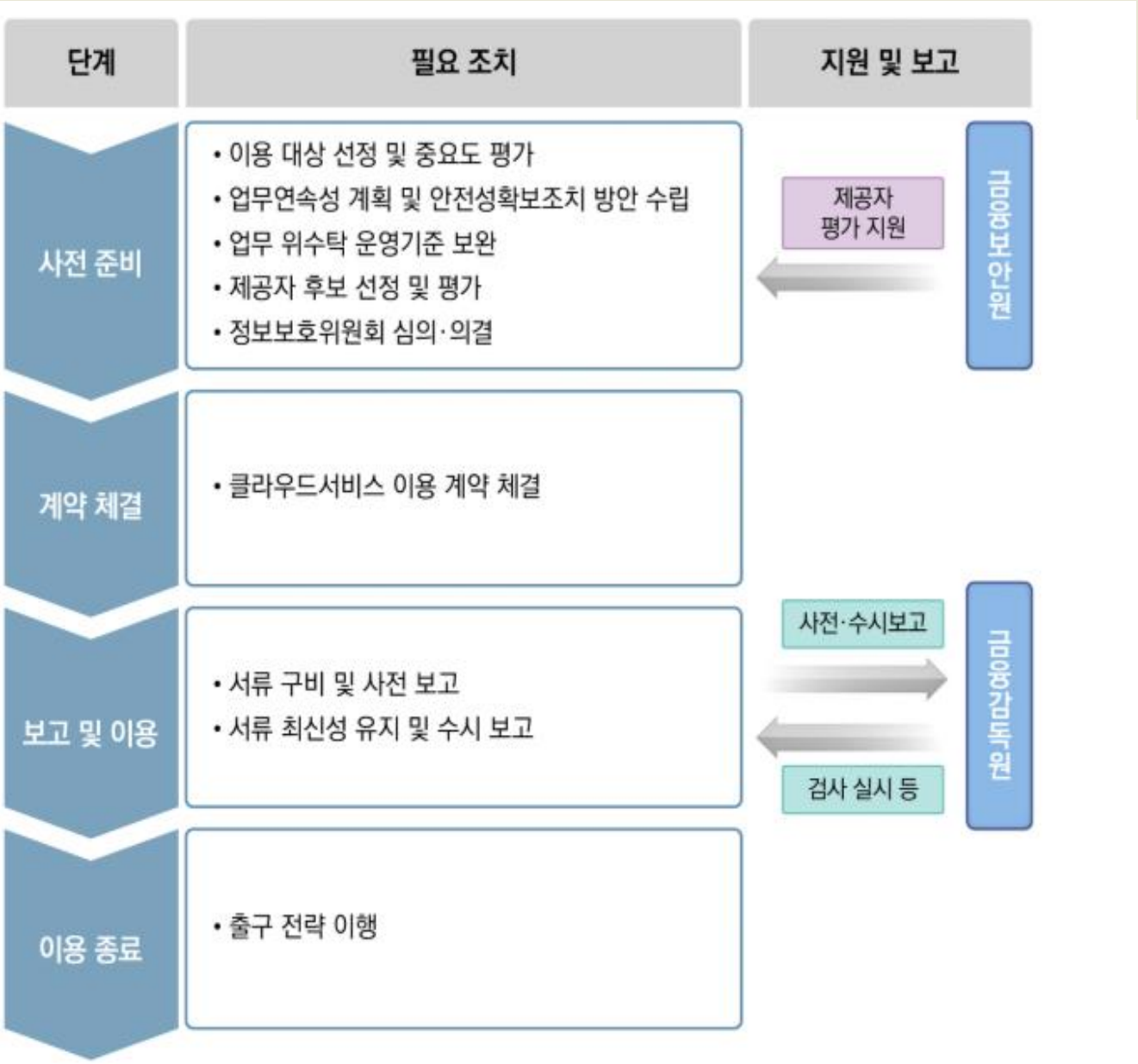
□ 클라우드서비스 제공자는 감독규정 제3조제3호 또는 제4호에 따라 전자금융보조업자에 해당

◆ 클라우드는 아웃소싱의 하나로 「정보처리 업무위탁」에 해당

◆ 클라우드서비스 제공자는 「전자금융보조업자」로서 제한적으로 감독을 받음

- **보조업자의 책임** : 클라우드 서비스 제공자의 고의·과실은 **금융회사의 고의 · 과실로 간주**
- **금융회사 준수사항** : **보안 · 비상 · 백업대책** 등을 수립·운영하고 **보안점검을 실시해야 함**
- **감독 · 검사** : 금융회사의 정보처리업무 **위탁계약 시정 · 보완 요구권**(법 제40조제2항), 보조업자에 대한 **수탁계약서 · 부속자료 등의 제출요구권 보유**(법 제40조제3항,4항,5항)

클라우드 서비스 이용 절차도



클라우드컴퓨팅서비스 제공자의 건전성 및 안전성 평가

제14조의2(클라우드컴퓨팅서비스 이용절차 등)

① 금융회사 또는 전자금융업자는 「클라우드컴퓨팅 발전 및 이용자 보호에 관한 법률」 제2조제3호에 따른 클라우드컴퓨팅서비스를 이용하고자 하는 경우 다음 각 호의 절차를 수행하여야 한다.

1. 자체적으로 수립한 기준에 따른 이용대상 정보처리시스템의 중요도 평가
2. 〈별표 2의2〉의 항목을 포함한 클라우드컴퓨팅서비스 제공자의 건전성 및 안전성 등 평가
3. 〈별표 2의3〉에서 정하는 사항을 반영한 자체 업무 위수탁 운영기준의 마련 및 준수

- **클라우드서비스 제공자 평가**는 기본적으로 **금융회사가 수행 주체**이며, 금융회사 요청 시 침해사고대응기관이 안전성 평가 지원*(건전성 평가는 금융회사에서 직접 수행)

* 침해사고대응기관: 금융보안원

평가항목 기준

기본
보호조치

클라우드서비스 제공자가 준수해야 할 일반적 보안 기준

금융부문
추가 보호 조치

금융분야 특화 기준

평가 항목 일부 적용 예외

➜ 국내·외 클라우드 보안인증제에 대해 상기 기준 부합여부를 검토 결과 아래 4개 보안인증 취득 시 '기본 보호조치' 평가 생략 가능

구분	인증제도명	평가생략 근거
국내	클라우드 서비스 보안인증제(CSAP)	• 과기정통부 주관, KISA가 평가·인증 • 국내 주요 클라우드 사업자가 인증 취득 • 평가항목수가 최대 120여개
해외	FedRAMP(High) (미국)	• 정부(FedRAMP 관리국) 주관 • 평가항목 수가 최대 400여개
	CSA STAR Certification(Gold) (Global)	• 400여개의 클라우드 사업자가 회원인 글로벌 클라우드 보안협회(CSA*) 주관 * CSA : Cloud Security Alliance • 평가항목 수가 최대 300여개
	MTCS(Level 3) (싱가포르)	• 정보통신미디어개발청(IMDA) 주관

※ 위 리스트는 상기 기준에 부합하여 평가 생략이 가능한 인증 제도를 열거한 것이며, 동 기준에 부합하는 국내·외 클라우드 보안인증제가 추가로 확인되는 경우, 지속 업데이트할 계획

첨부1 기본 보호조치 세부 평가항목(IaaS, SaaS)

1. 관리적 보호조치

구 분			세부 조치사항	IaaS	SaaS
1. 정보보호 정책 및 조직	1.1. 정보보호 정책	1.1.1 정보보호 정책 수립	정보보호 정책을 문서화하고, 정보보호 최고책임자의 승인 후 정책에 영향을 받는 모든 임직원 및 외부 업무 관련자에게 제공하여야 한다.	O	O
		1.1.2 정보보호 정책 검토 및 변경	정보보호 정책의 타당성 및 효과를 연 1회 이상 검토하고, 관련 법규 변경 및 내·외부 보안사고 발생 등 중대한 사유가 발생할 경우에는 추가로 검토하고 변경하여야 한다.	O	O
		1.1.3 정보보호 정책문서 관리	정보보호 정책 및 정책 시행문서의 이력관리 절차를 수립하고 시행하며, 최신본으로 유지하여야 한다.	O	O
	1.2 정보보호 조직	1.2.1. 조직 구성	정보보호 활동을 계획, 실행, 검토하는 정보보호 전담조직을 구성하고 정보보호최고책임자를 임명하여야 한다.	O	O
		1.2.2. 역할 및 책임 부여	정보자산과 보안에 관련된 모든 임직원 및 외부업무 관련자의 정보보호 역할과 책임을 명확하게 정의하여야 한다. 또한 서비스 이용자의 정보보호 역할과 책임도 서비스 수준 협약 등을 통해 명확히 정의하여야 한다.	O	O
2. 인적보안	2.1 내부인력 보안	2.1.1 고용계약	고용 계약서에 정보보호 정책 및 관련 법률을 준수하도록 하는 조항 또는 조건을 포함시키고, 새로 채용하거나 합류한 근무 인력이 클라우드컴퓨팅서비스의 설비, 자원, 자산에 접근이 허용되기 이전에 서명을 받아야 한다.	O	O
		2.1.2 주요 직무자 지정 및 감독	클라우드컴퓨팅서비스의 시스템 운영 및 개발, 정보보호 등에 관련된 임직원의 경우 주요 직무자로 지정하여 관리하고, 직무 지정 범위는 최소화하여야 한다.	O	O
		2.1.3 직무 분리	권한 오남용 등 내부 임직원의 고의적인 행위로 발생할 수 있는 잠재적인 위협을 줄이기 위하여 직무분리 기준을 수립하고 적용하여야 한다.	O	O
		2.1.4 비밀유지 서약서	정보보호와 개인정보보호 등을 위해 필요한 사항을 비밀유지 서약서에 정의하고 주기적으로 갱신하여야 한다.	O	O
		2.1.5 상벌규정	정보보호 정책을 위반한 임직원에 대한 징계 규정을 수립하고, 위반 사항이 발생 시 규정에 명시된 대로 징계 조치를 취하여야 한다. 또한 정보보호 정책을 충실히 이행한 임직원에 대한 보상 방안도 마련하여야 한다.	O	X
		2.1.6 퇴직 및 직무변경	임직원의 퇴직 또는 직무변경에 관한 책임을 명시적으로 정의하고 수행하여야 한다. 또한 이에 대한 접근권한도 제거하여야 한다.	O	X
	2.2 외부인력 보안	2.2.1 외부인력 계약	외부인력(외부유지보수직원, 외부 용역자 포함)에 의한 정보자산 접근등과 관련된 보안요구사항을 계약에 반영하여야 한다.	O	X
		2.2.2 외부인력 보안이행 관리	계약서에 명시한 보안요구사항 준수여부를 주기적으로 점검하고 위반사항이나 침해사고 발생 시 적절한 조치를 수행하여야 한다.	O	X
		2.2.3 계약 만료시 보안	외부 인력과의 계약 만료 시 자산 반납, 접근권한의 회수, 중요정보 파기, 업무 수행 시 알게 된 정보에 대한 비밀유지서약 등을 확인하여야 한다.	O	X
2. 인적보안	2.3 정보보호 교육	2.3.1 교육 프로그램 수립	모든 임직원 및 외부 업무 관련자를 포함하여 연간 정보보호 교육 프로그램을 수립하여야 한다.	O	X
		2.3.2 교육 시행	모든 임직원 및 외부 업무 관련자를 대상으로 연 1회 이상 정보보호 교육을 시행하고 정보보호 정책 및 절차의 중대한 변경, 내·외부 보안사고 발생, 관련 법규 변경 등의 사유가 발생하면 추가 교육을 실시하여야 한다.	O	O
		2.3.3 평가 및 개선	정보보호 교육 시행에 대한 기록을 남기고 결과를 평가하여 개선하여야 한다.	O	X
3. 자산관리	3.1 자산 식별 및 분류	3.1.1 자산 식별	클라우드컴퓨팅서비스에 사용된 정보자산(정보시스템, 정보보호시스템, 정보 등)에 대한 자산분류기준을 수립하고 식별된 자산의 목록을 작성하여 관리하여야 한다.	O	O
		3.1.2 자산별 책임할당	식별된 자산마다 책임자 및 관리자를 지정하여 책임소재를 명확히 하여야 한다.	O	X
		3.1.3 보안등급 및 취급	기밀성, 무결성, 가용성, 법적요구사항 등을 고려하여 자산의 보안등급을 부여하고, 보안 등급별 취급절차에 따라 관리하여야 한다.	O	X
	3.2 자산 변경관리	3.2.1 변경관리	클라우드컴퓨팅서비스에 사용된 자산(시설, 장비, 소프트웨어 등)의 변경이 필요한 경우 보안 영향 평가를 통해 변경 사항을 관리하여야 한다. 또한 이용자에게 큰 영향을 주는 변경에 대해서는 사전에 공지를 하여야 한다.	O	O
		3.2.2 변경 탐지 및 모니터링	클라우드컴퓨팅서비스에 사용된 자산(시설, 장비, 소프트웨어 등)의 변경을 지속적으로 모니터링하여 허가 받지 않은 변경을 탐지하고 최신의 변경 이력을 유지하여야 한다.	O	X
		3.2.3 변경 후 작업검증	클라우드컴퓨팅서비스에 사용된 자산(시설, 장비, 소프트웨어 등)의 변경 후에는 보안성 및 호환성 등에 대한 작업검증을 수행하여야 한다.	O	X
	3.3 위험관리	3.3.1 위험관리 계획수립	관리적, 기술적, 물리적, 법적 분야 등 정보보호 전 영역에 대한 위험식별 및 평가가 가능하도록 위험관리 방법과 계획을 사전에 수립하여야 한다.	O	X
		3.3.2 취약점 점검	취약점 점검 정책에 따라 주기적으로 기술적 취약점(예: 유·무선 네트워크, 운영체제 및 인프라, 응용 프로그램 취약점 등)을 점검하고 보완하여야 한다.	O	O
		3.3.3. 위험분석 및 평가	위험관리 방법 및 계획에 따라 정보보호 전 영역에 대한 위험 식별 및 평가를 연 1회 이상 수행하고 그 결과에 따라 수용 가능한 위험 수준을 설정하여 관리하여야 한다.	O	X
		3.3.4 위험처리	법규 및 계약관련 요구사항과 위험수용 수준을 고려하여 위험평가 결과에 따라 통제할 수 있는 방법을 선택하여 처리하여야 한다.	O	X
4. 서비스 공급망 관리	4.1 공급망 관리정책	4.1.1 공급망 관리 정책 수립	클라우드컴퓨팅서비스에 대한 접근과 서비스 연속성을 저해하는 위험을 식별하고 최소화하기 위해 공급망과 관련한 보안 요구사항을 정의하는 관리 정책을 수립하여야 한다.	O	O
		4.1.2 공급망 계약	클라우드컴퓨팅서비스 범위 및 보안 요구사항을 포함하는 공급망 계약을 체결하고 다자간 협약 시 책임을 개별 계약서에 각각 명시해야하며, 해당 서비스에 관련된 모든 이해관계자에게 적용하여야 한다.	O	O

첨부2 **금융부문 추가 보호조치**

국내·외 클라우드 보안인증제를 취득하여 평가 생략이 가능한 **기본 보호조치 항목과 별도**로, 금융회사가 전자금융감독규정 등 **법규 준수를 위해 꼭 필요한 사항**을 **지원 및 협조** 받을 수 있는지를 평가한다.

1. 클라우드서비스 제공자의 건전성에 관한 사항

□ 전자금융보조업자 재무건전성 평가(감독규정 제60조제1항제10호)에 준하여 실시

> 제60조(외부주문등에 대한 기준) ① 10. 전자금융보조업자에 대한 재무건전성을 연1회 이상 평가하여 재무상태 악화에 따른 도산에 대비하고 전자금융보조업자의 주요 경영활동에 대해 상시 모니터링을 실시

2. 금융회사의 의무 준수를 위해 클라우드서비스 제공자의 지원 및 협조가 필수적인 사항

금융부문 추가 보호조치 항목	세부 조치사항	감독규정 관련 조문
2.1 사고 보고 및 분석 수행 절차 확보	사고보고 및 분석을 위해 사고조사 지원, 훈련 지원 등 금융위원회, 금융감독원, 침해사고대응기관의 협조 요청에 대응할 수 있도록 체계가 마련되어 있는가?	제37조의4(침해사고대응기관 지정 및 업무범위 등), 제73조(정보기술부문 및 전자금융사고보고)
	전산장애, 전자적 침해행위 등 발생 시 금융회사 및 침해사고대응기관에 즉시 알리고 적절히 대처할 수 있는 방안이 마련되어 있는가?	
2.2 금융권 통합보안관제 수행 체계 지원	금융권 통합 보안관제수행을 위한 관리적·물리적·기술적 지원 체계가 마련되어 있는가?	
2.3 취약점 분석평가 수행 체계 지원	관계 법규에 따라 금융회사가 취약점 분석.평가를 수행할 수 있도록 지원 체계가 마련되어 있는가?	제37조의2(전자금융기반시설의 취약점 분석·평가 주기, 내용 등)
	전자금융기반시설의 취약점 분석.평가 전문기관의 취약점 분석.평가 업무 수행을 위해 전산실 및 정보처리시스템에 대한 접근을 허용(필요시 물리적 접근 포함)하도록 절차가 마련되어 있는가?	
	금융회사의 취약점분석평가 결과에 따라 취약점의 제거 또는 이에 상응하는 조치를 수행하는 절차가 마련되어 있는가?	
2.4 합동비상대응 훈련 지원	금융회사가 수립한 비상대책에 따른 비상대응훈련 및 재해복구전환훈련 실시에 대해 협조 및 지원하도록 체계가 마련되어 있는가?	제24조(비상대응훈련 실시)
	필요한 경우 금융위원회가 실시하는 금융분야 합동비상대응훈련에 참여하고 지원하도록 체계가 마련되어 있는가?	
2.5 건물·전원·전산실 금융회사 수준 구축 (* 금융회사 시스템을 운영하는 클라우드서비스 제공자의 데이터센터는 금융회사 전산실로 볼 수 있어 관련 규정 준수 필요)	화재, 침수, 진동 등 외부요인으로부터 적절한 보호대책이 마련되어 있는가?	제9조(건물에 관한 사항), 제10조(전원, 공조 등 설비에 관한 사항), 제11조(전산실 등에 관한 사항)
	전산실내 주요시설에 출입통제, 감시제어를 위한 설비가 마련되어 있는가?	
	전력공급중단에 대비하여 적절한 대책이 마련되어 있는가? (자가발전설비, 전력선 이중화, UPS 등)	
	전산실내 적정한 온도 및 습도 유지를 위한 설비가 마련되어 있는가?	
	(고유식별정보 및 개인신용정보 처리시) · 관련된 모든 정보처리시스템을 국내에 설치할 수 있는가? · 무선통신망이 미설치되어 있는가?	
2.6 전산자료 보호	사용자계정과 비밀번호를 개인별로 부여하고, 관리하기 위한 기능을 제공하는가?	제13조(전산자료 보호대책)
	전산자료를 정기적으로 백업하고 검증할 수 있도록 지원 체계가 마련되어 있는가?	
	정보처리시스템 관리자의 주요 업무 관련 행위를 책임자 또는 금융회사가 이중확인 및 모니터링 할 수 있는 기능을 제공하는가?	
	정보처리시스템의 가동기록을 1년 이상 보존하고 있는가?	
	정보처리시스템 접속 기록(일시, 접속자, 접근확인), 전산자료 접근기록(일시, 사용자, 자료내용), 전산자료 처리 내용 기록(사용자 로그인, 액세스 로그 등)이 접속 성공 여부와 상관없이 자동으로 기록·유지에 협조 및 지원하도록 체계가 마련되어 있는가?	
	금융회사의 정보처리시스템과 관련된 단말기 및 전산자료에 접근권한이 부여되는 정보처리시스템 관리자에 대하여 적절한 통제장치를 마련·운용하는가?	
2.7 이중화 및 백업체계 구축	(주요 전산장비의 경우) 금융회사가 이중화 또는 예비장치를 확보할 수 있도록 협조 및 지원 체계가 마련되어 있는가?	제23조(비상대책 등의 수립·운용)
	금융회사가 각 업무별로 지정한 복구목표시간을 준수할 수 있도록 협조 및 지원 체계가 마련되어 있는가?	
	장애·재해·파업·테러 등 긴급한 상황이 발생하더라도 업무가 중단되지 않도록 상황별 대응절차, 재해복구계획, 비상대응조직의 구성 및 운용, 모의훈련, 비상연락체계, 파업 시 비상지원인력, 업무매뉴얼 등을 포함한 업무지속성 확보방안을 수립·준수하고 주기적으로 점검하는가?	
2.8 해킹 등 방지대책	시스템프로그램 등의 긴급하고 중요한 보정(patch)사항에 대하여 즉시 보정작업을 실시하고 있는가?	제15조(해킹 등 방지대책)
	내부 업무용시스템 설치 시 인터넷 등 외부통신망과 분리·차단 및 접속을 금지(물리적 또는 논리적) 할 수 있도록 기능을 제공하고 지원하도록 체계가 마련되어 있는가?	
	패치 수행 등을 위해 중앙에서 파일을 배포할 경우 무결성 검증을 수행하는가?	
	클라우드서비스 제공자 내에서 클라우드 시스템 관리를 목적으로 클라우드 시스템에 직접 접속하는 단말기에 대해서는 인터넷 등 외부통신망으로부터 분리(물리적 또는 논리적) 하는가?	
	금융회사가 클라우드서비스 이용 정보처리시스템 및 정보통신망에 대해 정보보호시스템을 설치·운영할 수 있도록 지원 체계가 마련되어 있는가?	
	해킹 등 전자적 침해행위로 인한 사고를 방지하기 위해 적절한 정보보호 시스템을 설치하여 안전하게(이력보관, 접근통제 등) 운영하고 있는가?	
2.9 기타	금융회사가 재무건전성 평가 등 주요 경영활동에 대해 상시 모니터링을 실시할 수 있도록 지원 체계가 마련되어 있는가?	제60조(외부주문 등에 대한 기준)
	금융회사가 서비스 품질수준을 평가할 수 있도록 지원 체계가 마련되어 있는가?	
	금융회사의 정보처리업무 위탁과 관련한 계약서, 계약서 부속자료 및 그 밖의 전자금융업무와 관련한 자료 등을 금융감독원의 요구를 수용하도록 체계가 마련되어 있는가?	제61조(전자금융보조업자 자료제출 기준)
	금융회사가 개인(신용)정보 관련 규제 등 기타 금융관련 법령을 준수하는데 필요한 사항에 지원 및 협조하도록 체계가 마련되어 있는가?	-

Microsoft, ISMS 인증 획득

인증번호/유효기간 : ISMS-18-073 / 18-11-19~21-11-18

한국인터넷진흥원(https://isms.kisa.or.kr/) 인증서 발급현황 조회

Microsoft, ISMS 인증 범위

마이크로소프트 클라우드 서비스(Azure) 한국 리전의 인프라 운영

Microsoft 한국 리전에 해당하는 데이터센터(한국 중부/남부)의 인프라와 한국 리전에서 서비스되는 Microsoft Azure 서비스의 운영 부문

Public Cloud를 신청, 이용하는 고객 웹사이트 및 스마트폰앱

- Microsoft Azure를 소개하고 서비스 신청을 접수하는 웹사이트
- 서비스 가입 이후 Azure를 운영, 관리하기 위한 Microsoft Azure Portal(클라우드 콘솔)
- Microsoft Azure 스마트폰 앱(Android, Apple)

Microsoft 한국 리전에서 제공하는 모든 Azure 서비스

- Compute, 네트워킹, Storage, 웹+모바일, 컨테이너, 데이터베이스, 분석, IoT, 통합, 보안+ID, 개발자 도구, 관리 도구 등의 카테고리에서 제공되는 서비스
- 기타, 한국 중부/남부에서 제공되는 모든 Azure 서비스

https://azure.microsoft.com/ko-kr/global-infrastructure/services/

Microsoft Azure를 개발, 운영, 보안하는 조직(미국 본사, 한국 법인 및 데이터센터), 정책/절차 및 관련 업무시스템

Microsoft Azure로 가능한 ISMS 보안통제

1. 관리체계 수립 및 운영 (16)
   - 1.1 관리체계 기반 마련 (6)
   - 1.2 위험관리 (4)
   - 1.3 관리체계 운영 (3)
   - 1.4 관리체계 점검 및 개선 (3)

2. 보호대책 요구사항 (64)
   - 1. 정책, 조직, 자산 관리 (3)
   - 2. 인적 보안 (6)
   - 3. 외부자 보안 (4)
   - 4. 물리 보안 (7)
   - 5. 인증 및 권한관리 (6)
   - 6. 접근통제 (7)
   - 7. 암호화 적용 (2)
   - 8. 정보시스템 도입 및 개발보안 (6)
   - 9. 시스템 및 서비스 운영관리 (7)
   - 10. 시스템 및 서비스 보안관리 (9)
   - 11. 사고 예방 및 대응 (5)
   - 12.재해복구 (2)

3. 개인정보 처리 단계별 요구사항 (22)
   - 3.1 개인정보 수집 시 보호조치 (7)
   - 3.2 개인정보 보유 및 이용 시 보호조치 (5)
   - 3.3 개인정보 제공 시 보호조치 (4)
   - 3.4 개인정보 파기 시 보호조치 (3)
   - 3.5 정보주체 권리보호 (3)

정보보호 관리체계 인증기준 (80)

- 1. 관리체계 수립 및 운영 (16)
- 2. 보호대책 요구사항 (64)

ISMS

Microsoft Azure로 가능한 보안통제

정보보호 및 개인정보보호 관리체계 인증기준 (102)

- 1. 관리체계 수립 및 운영 (16)
- 2. 보호대책 요구사항 (64)
- 3. 개인정보 처리단계별 요구사항 (22)

ISMS-P

ISMS인증기준(보호대책 요구사항)을 만족하는 Cloud 운영환경 예시

On Premise 환경과 다른 특징으로, Cloud 이용자는 물리적 보안관리 의무 최소화

- 1. 정책, 조직, 자산 관리
- 2. 인적 보안
- 3. 외부자 보안
- **4. 물리 보안**
- 5. 인증 및 권한관리
- 6. 접근통제
- 7. 암호화 적용
- 8. 정보시스템 도입 및 개발보안
- **9. 시스템 및 서비스 운영관리**
- 10. 시스템 및 서비스 보안관리
- 11. 사고 예방 및 대응
- 12.재해복구

		On Premise 환경	Cloud Region 환경
2.4.1 보호구역 지정 2.4.2 출입통제 2.4.4 보호설비 운영 2.4.6 반출입 기기 통제	정보통신망 이용촉진 및 정보보호 등에 관한 법률 제46조(집적정보통신시설의 보호)에 따른 IDC는 과학기술정보통신부의 집적정보 통신시설 보호지침(고시)에 맞추어 물리적 보안 기준(**접근제어 및 감시, 가용성, 방호성, 방재성, 보호관리체계화**)을 만족		
	이용고객 • 방문자 출입 관리 고객 시스템 반입, 반출 관리		이용고객 • 방문자 출입 불가 고객 시스템 반입, 반출 불가
	해당 출입과 시스템 반출입 내역은 이용고객이 직접 관리		*Not Applicable*
2.4.3 정보시스템 보호 2.4.5 보호구역 내 작업	출입 인가 인원에 대한 작업은 이용고객이 직접 관리 반입 시스템에 대한 배치, 관리는 이용고객이 직접 관리		*Not Applicable*
			※ 물리적 자산은 Cloud 서비스 제공자의 책임 영역이나,고객 소유 가상자원에 대한 접근, 작업은 고객 책임이며 책임추적을 위해 모든 행위는 로깅이 이루어짐
2.9.7 정보자산의 재사용 및 폐기	정보시스템 저장매체의 데이터 파기는 복원이 불가능한 방법을 적용하여 이용고객이 직접 관리		*Not Applicable*

이용자 정보자산에 대한 물리보안

ISMS-P 2.4. 물리 보안은 Microsoft의 책임영역으로 이용자는 보안통제 입증 불필요

물리 데이타센터

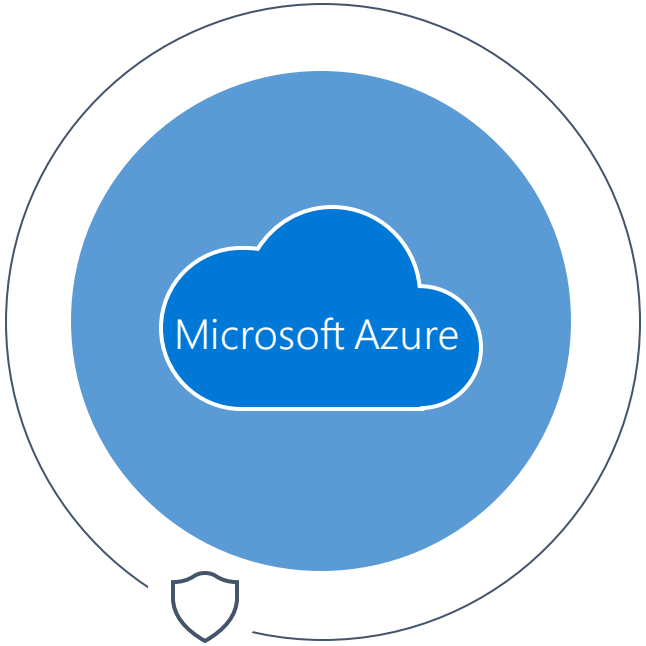
전세계 100+ 데이타 센터
다중 레이어 보호 및 물리적 접근 통제
전세계 주요 컴플라이언스 준수

Azure 인프라

HW기반 보안모듈이 탑재된 맞춤형 HW
네트워크 인프라 보호 (e.g. DDoS)
상시 보안 Patch 적용 및 보안 테스트 수행

보안 절차에 따른 운영

Microsoft의 운용인력도 고객의 데이타 접근을 제한
24x7 모니터링
전세계 3500+ 명의 보안 전문가

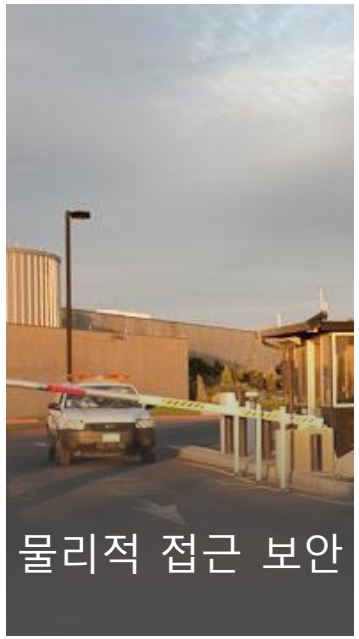


데이타센터 관리를
Microsoft 가 수행

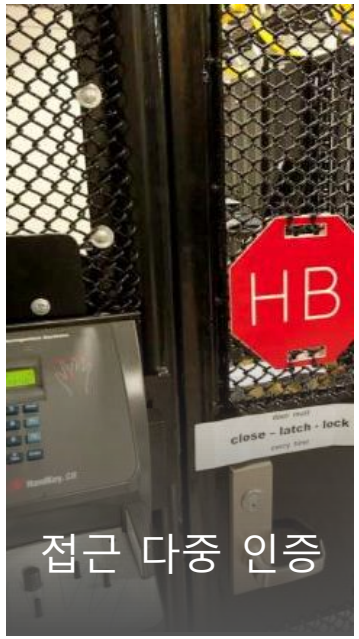
Microsoft의 데이터센터 보안통제
ISMS-P 2.4. 물리 보안통제를 만족하는 데이터센터 운영

보호구역 지정, 출입통제, 시스템 배치 및 관리, 케이블 보안, 보호설비, 보호구역 내 작업, 모바일 기기 반출입 등의 물리적 보안 요구사항을 포함하는 통제 적용

[데이터 센터 시설/장비 보안 상세]


물리적 접근 보안


화재 방지



접근 다중 인증


광범위 모니터링

지진 내구성 제공

24x7 상주 보안 요원

백업을 위한 몇 일 간의 별도 전력 제공

Azure 데이터센터의 물리보안

ISMS-P 2.4. 물리 보안통제 대부분은 Microsoft가 ISMS 인증을 유지하며 입증

No	인증기준	상세 내용	통제 구현	
			MS Azure	신청기관
2.4.1	보호구역 지정	물리적·환경적 위협으로부터 개인정보 및 중요정보, 문서, 저장매체, 주요 설비 및 시스템 등을 보호하기 위하여 통제구역·제한구역·접견구역 등 물리적 보호구역을 지정하고 각 구역별 보호대책을 수립·이행하여야 한다.	데이터 센터	데이터 센터 外 보호구역
2.4.2	출입통제	보호구역은 인가된 사람만이 출입하도록 통제하고 책임추적성을 확보할 수 있도록 출입 및 접근 이력을 주기적으로 검토하여야 한다.	데이터 센터	
2.4.3	정보시스템 보호	정보시스템은 환경적 위협과 유해요소, 비인가 접근 가능성을 감소시킬 수 있도록 중요도와 특성을 고려하여 배치하고, 통신 및 전력 케이블이 손상을 입지 않도록 보호하여야 한다.	데이터 센터	

Azure 데이터센터의 물리보안

ISMS-P 2.4. 물리 보안통제 대부분은 Microsoft가 ISMS 인증을 유지하며 입증

No	인증기준	상세 내용	통제 구현	
			MS Azure	신청기관
2.4.4	보호설비 운영	보호구역에 위치한 정보시스템의 중요도 및 특성에 따라 온도·습도 조절, 화재감지, 소화설비, 누수감지, UPS, 비상발전기, 이중전원선 등의 보호설비를 갖추고 운영절차를 수립·운영하여야 한다.	데이터 센터	데이터 센터 外 보호구역
2.4.5	보호구역 내 작업	보호구역 내에서의 비인가행위 및 권한 오·남용 등을 방지하기 위한 작업 절차를 수립·이행하고, 작업 기록을 주기적으로 검토하여야 한다.	데이터 센터	
2.4.6	반출입 기기 통제	보호구역 내 정보시스템, 모바일 기기, 저장매체 등에 대한 반출입 통제절차를 수립·이행하고 주기적으로 검토하여야 한다.	데이터 센터	
2.4.7	업무환경 보안	공용으로 사용하는 사무용 기기(문서고, 공용 PC, 복합기, 파일서버 등) 및 개인 업무환경(업무용 PC, 책상 등)을 통해 개인정보 및 중요정보가 비인가자에게 노출 또는 유출되지 않도록 클린데스크, 정기점검 등 업무환경 보호대책을 수립·이행하여야 한다.	데이터 센터 內 업무환경	개인 또는 공용 사무공간, 기기

ISMS인증기준(보호대책 요구사항)을 만족하는 Cloud 운영환경 예시

Cloud 운영환경 內 시스템(Virtual Machine) 관리 및 개발/암호통제 환경을 활용한 ISMS구축

1. 정책, 조직, 자산 관리
2. 인적 보안
3. 외부자 보안
4. 물리 보안
5. 인증 및 권한관리
6. 접근통제
7. 암호화 적용
8. 정보시스템 도입 및 개발보안
9. 시스템 및 서비스 운영관리
10. 시스템 및 서비스 보안관리
11. 사고 예방 및 대응
12.재해복구

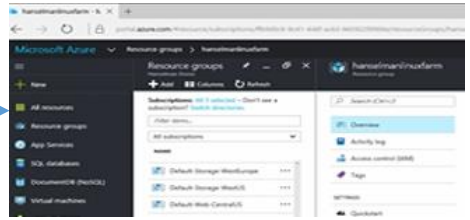
2.1.3 정보자산 관리

2.8.2 보안요구사항 검토 및 시험
2.8.3 시험과 운영환경 분리
2.8.4 시험 데이터 보안
2.8.5 소스프로그램 보안
2.8.6 운영환경 이관

2.7.1 암호정책 적용
2.7.3 암호키 관리

Microsoft Azure Portal

통합된 단일 콘솔에서 모든 Azure 제품을 구축, 관리, 모니터링

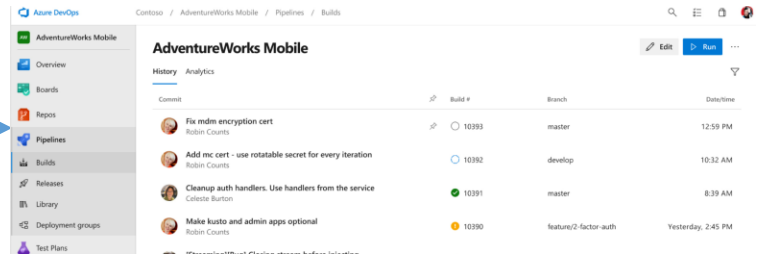


Virtual Machines

빠른 속도로 Windows 및 Linux 가상 머신 프로비전

Azure DevOps

팀 간의 코드 공유, 작업 추적 및 소프트웨어 전송을 위한 서비스



Key Vault

키 및 기타 암호의 보호 및 유지 관리 제어

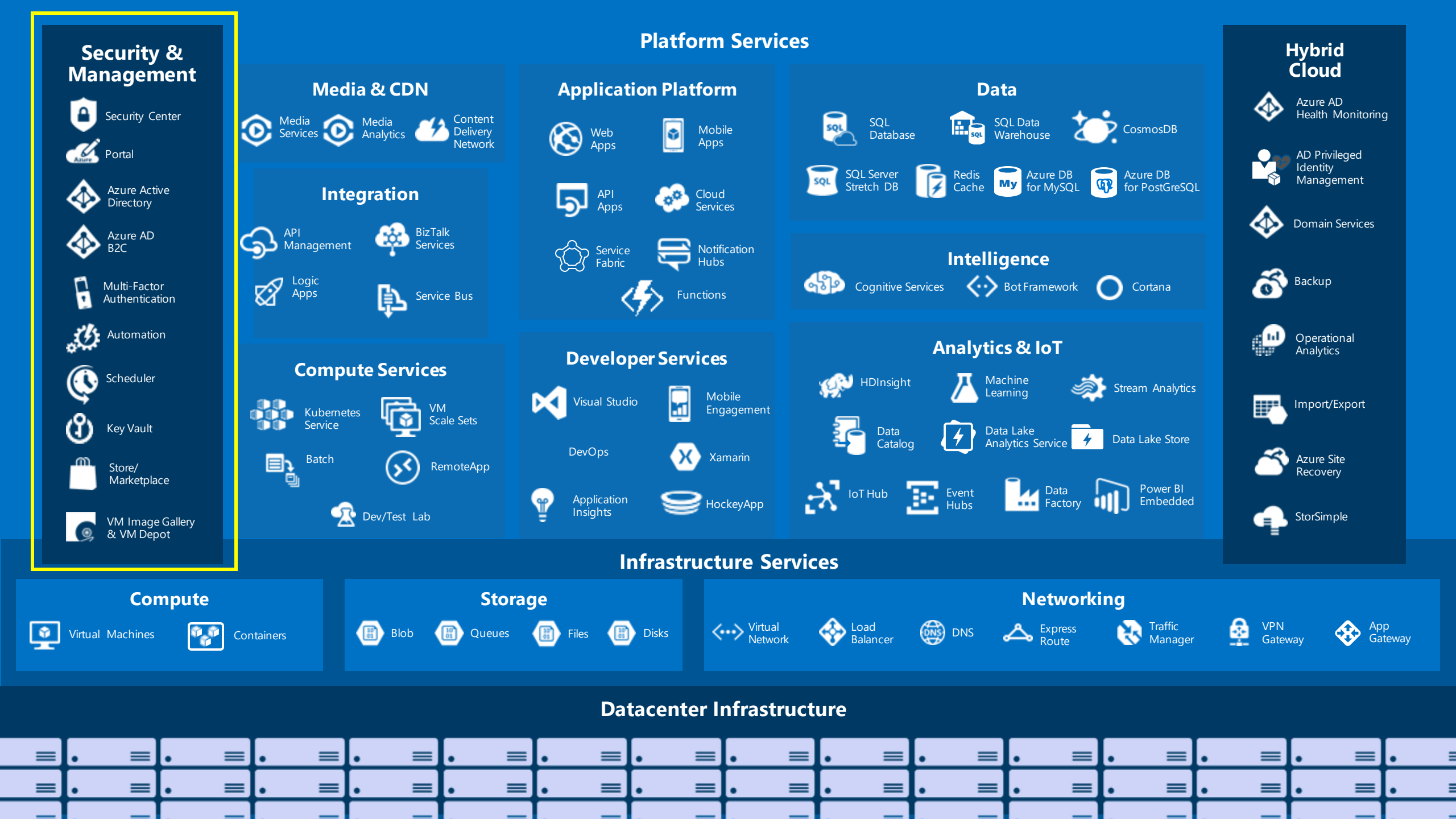
FIPS 140-2 레벨 2 유효성이 검증된 HSM을 사용

SSL/TLS 인증서에 대해 작업을 간소화하고 자동화

Azure Portal을 이용한 정보자산 식별

ISMS-P 1.2.1 정보자산 식별, 2.1.3 정보자산 관리 보안통제를 구현 가능

No	인증기준	상세 내용	통제 구현	
			MS Azure	신청기관
1.2.1	정보자산 식별	조직의 업무특성에 따라 정보자산 분류기준을 수립하여 관리체계 범위 내 모든 정보자산을 식별·분류하고, 중요도를 산정한 후 그 목록을 최신으로 관리하여야 한다.	Portal (Console)	운영부서
2.1.3	정보자산 관리	정보자산의 용도와 중요도에 따른 취급 절차 및 보호대책을 수립·이행하고, 자산별 책임소재를 명확히 정의하여 관리하여야 한다.	Portal (Console)	보안부서 운영부서


Security & Management
Security Center
Portal
Azure Active Directory
Azure AD B2C
Multi-Factor Authentication
Automation
Scheduler
Key Vault
Store/ Marketplace
VM Image Gallery & VM Depot
Platform Services
Media & CDN
Media Services
Media Analytics
Content Delivery Network
Integration
API Management
BizTalk Services
Logic Apps
Service Bus
Compute Services
Kubernetes Service
VM Scale Sets
Batch
RemoteApp
Dev/Test Lab
Application Platform
Web Apps
Mobile Apps
API Apps
Cloud Services
Service Fabric
Notification Hubs
Functions
Developer Services
Visual Studio
Mobile Engagement
DevOps
Xamarin
Application Insights
HockeyApp
Data
SQL Database
SQL Data Warehouse
CosmosDB
SQL Server Stretch DB
Redis Cache
Azure DB for MySQL
Azure DB for PostGreSQL
Intelligence
Cognitive Services
Bot Framework
Cortana
Analytics & IoT
HDInsight
Machine Learning
Stream Analytics
Data Catalog
Data Lake Analytics Service
Data Lake Store
IoT Hub
Event Hubs
Data Factory
Power BI Embedded
Hybrid Cloud
Azure AD Health Monitoring
AD Privileged Identity Management
Domain Services
Backup
Operational Analytics
Import/Export
Azure Site Recovery
StorSimple
Infrastructure Services
Compute
Virtual Machines
Containers
Storage
Blob
Queues
Files
Disks
Networking
Virtual Network
Load Balancer
DNS
Express Route
Traffic Manager
VPN Gateway
App Gateway
Datacenter Infrastructure

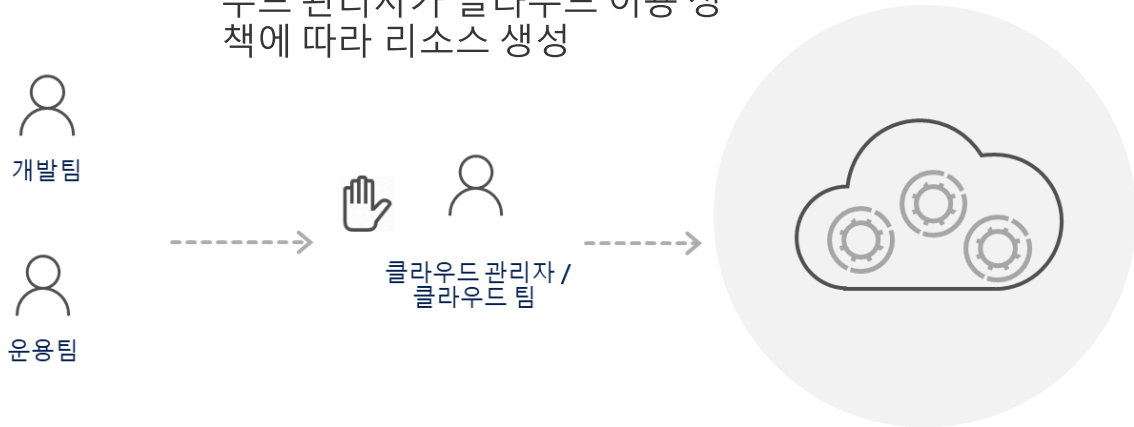
클라우드 보안 및 위험관리 필요성

ISMS-P 보안통제를 구현하기 위한 클라우드 서비스 보안 요구사항 확인

보안팀의 고민 – 실무 팀들에게 어떻게 클라우드 서비스를 안전하게 제공할 것인가?

- 클라우드 포탈 접근 권한은?
- 클라우드 리소스의 비용 제어는?
- VM에 방화벽 룰을 어떻게 강제할 것인지?
- 데이타 encryption과 같은 Compliance 준수여부 어떻게 감시할 것인지?
- VM을 방화벽이 설정된 특정 서브넷에만 생성하도록 하려면?
- 네트워크 설정이나 리소스 설정을 변경에 대한 추적은?
- 보안팀에서 설정한 네트워크 설정과 리소스 설정에 대한 변경을 못하게 하려면?
- 보안 SW 탑제된 custom VM 이미지만을 사용하도록 강제할 것인가?
- 리소스를 생성하는 사용자 ID 및 부서를 관리하려면? Tagging을 강제
- GDPR을 준수하기 위해 특정 국가의 스토리지 서비스만 허용하려면?
- VM에서의 인터넷 접근은 어떻게 통제할 것인지?
- VM에서 실행되는 어플리케이션들을 어떻게 제한할 것인지?
- 각 팀에서 사용하는 리소스들의 보안 환경을 어떻게 통합 모니터링 할 것인지?

예전에는 실무 부서 요청 시 클라우드 관리자가 클라우드 이용 정책에 따라 리소스 생성



Azure Policy를 이용한 보안, 위험관리

위험관리를 포함한 각종 보안 규칙을 설정하고 상시 점검

Azure Policy를 이용하여 Azure 리소스를 생성하고 구성할때 따라야 하는 규칙을 정의

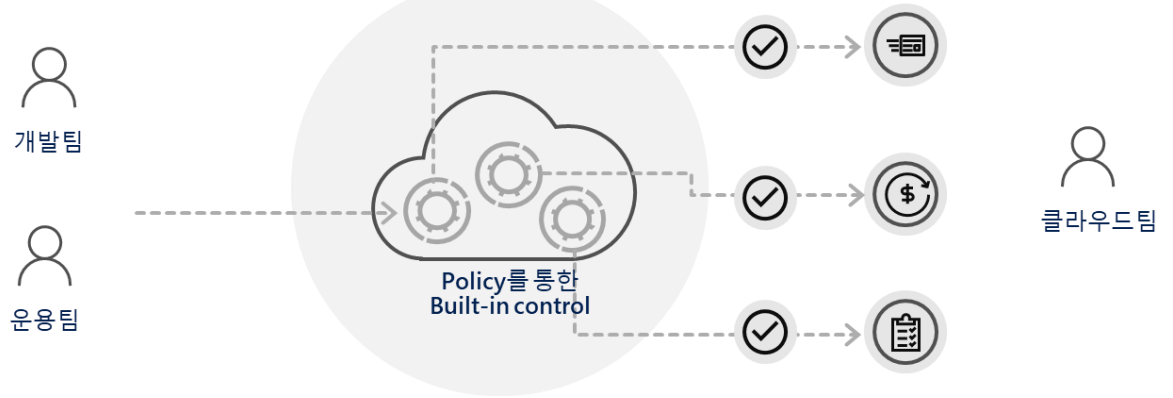
- 각 팀에서 사용하는 각 구독에 또는 리소스 그룹단위로 설정

Azure 상에 리소스 생성 시 구독에 정의된 Policy에 위배되지 않는지 검사. 위반 감지시 강제로 Policy에 정의된 규칙을 적용

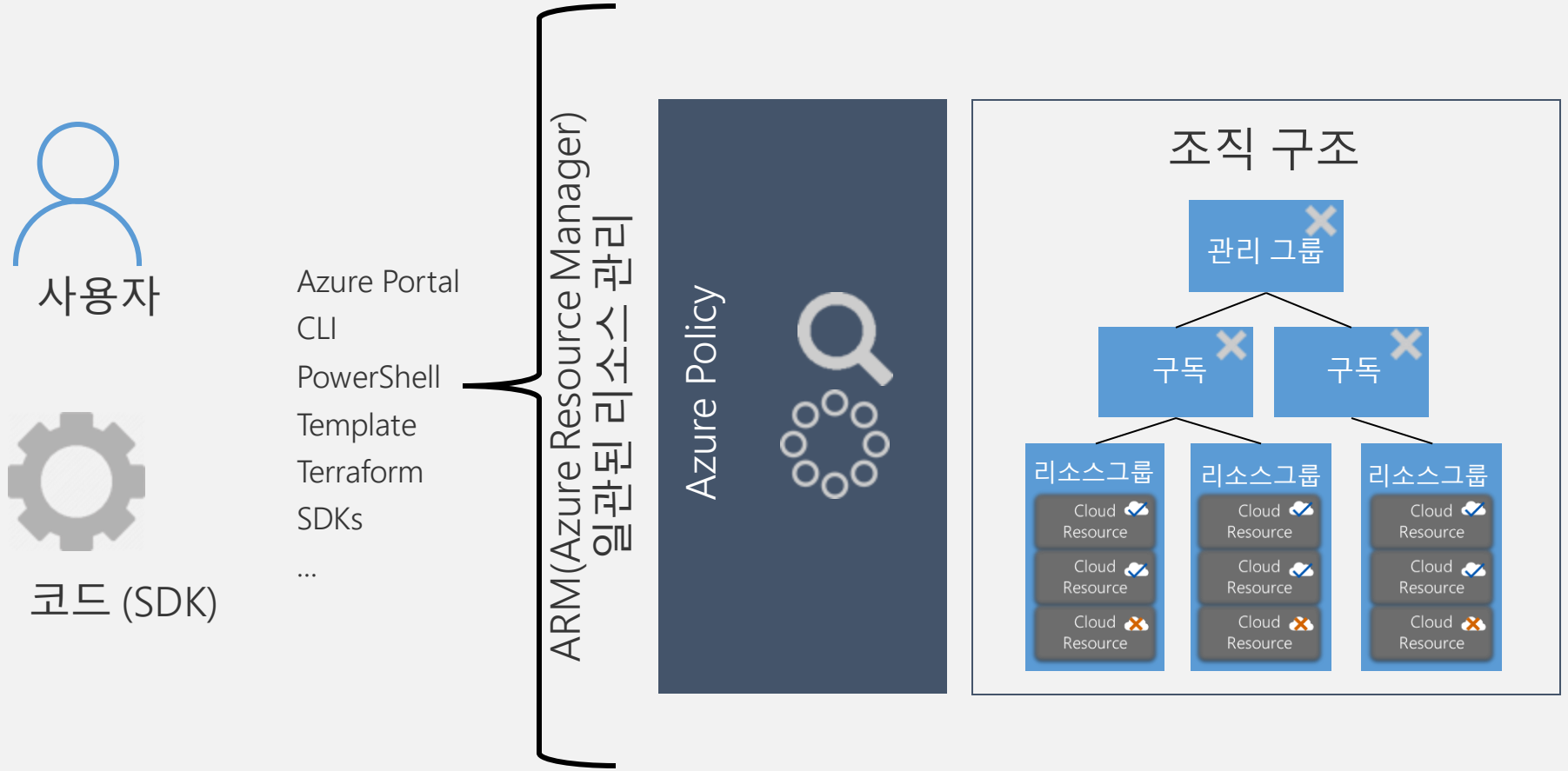
- 특정 resource type 또는 VM type들로 리소스 생성을 제한
- VM 또는 스토리지를 생성할 수 있는 Azure region을 제한
- VM 생성 시 특정 Custom Image만을 사용하도록 제한
- Resource 생성 시 필수로 특정 tag를 지정하도록 요구

보안 및 컴플라이언스 요구사항을 준수, 비용통제 및 인프라 설계의 일관성있는 방법을 제공

다양한 Built-in Policy 제공 및 custom Policy 정의 지원



Azure Policy 동작원리



Azure IAM을 활용한 인증 및 권한관리

ISMS-P 2.5 인증 및 권한관리 보안통제를 구현

No	인증기준	상세 내용	통제 구현	
			MS Azure	신청기관
2.5.1	사용자 계정 관리	정보시스템과 개인정보 및 중요정보에 대한 비인가 접근을 통제하고 업무 목적에 따른 접근권한을 최소한으로 부여할 수 있도록 사용자 등록·해지 및 접근권한 부여·변경·말소 절차를 수립·이행하고, 사용자 등록 및 권한부여 시 사용자에게 보안책임이 있음을 규정화하고 인식시켜야 한다.	IAM	운영부서
2.5.2	사용자 식별	사용자 계정은 사용자별로 유일하게 구분할 수 있도록 식별자를 할당하고 추측 가능한 식별자 사용을 제한하여야 하며, 동일한 식별자를 공유하여 사용하는 경우 그 사유와 타당성을 검토하여 책임자의 승인 및 책임추적성 확보 등 보완대책을 수립·이행하여야 한다.	IAM	운영부서
2.5.3	사용자 인증	정보시스템과 개인정보 및 중요정보에 대한 사용자의 접근은 안전한 인증절차와 필요에 따라 강화된 인증방식을 적용하여야 한다. 또한 로그인 횟수 제한, 불법 로그인 시도 경고 등 비인가자 접근 통제방안을 수립·이행하여야 한다.	IAM	운영부서

Azure IAM을 활용한 인증 및 권한관리

ISMS-P 2.5 인증 및 권한관리 보안통제를 구현

No	인증기준	상세 내용	통제 구현	
			MS Azure	신청기관
2.5.4	비밀번호 관리	법적 요구사항, 외부 위협요인 등을 고려하여 정보시스템 사용자 및 고객, 회원 등 정보서비스 이용자가 사용하는 비밀번호 관리절차를 수립·이행하여야 한다.	IAM	운영부서
2.5.5	특수 계정 및 권한 관리	정보시스템 관리, 개인정보 및 중요정보 관리 등 특수 목적을 위하여 사용하는 계정 및 권한은 최소한으로 부여하고 별도로 식별하여 통제하여야 한다.	IAM, JIT	운영부서
2.5.6	접근권한 검토	정보시스템과 개인정보 및 중요정보에 접근하는 사용자 계정의 등록·이용·삭제 및 접근권한의 부여·변경·삭제 이력을 남기고 주기적으로 검토하여 적정성 여부를 점검하여야 한다.	IAM	운영부서

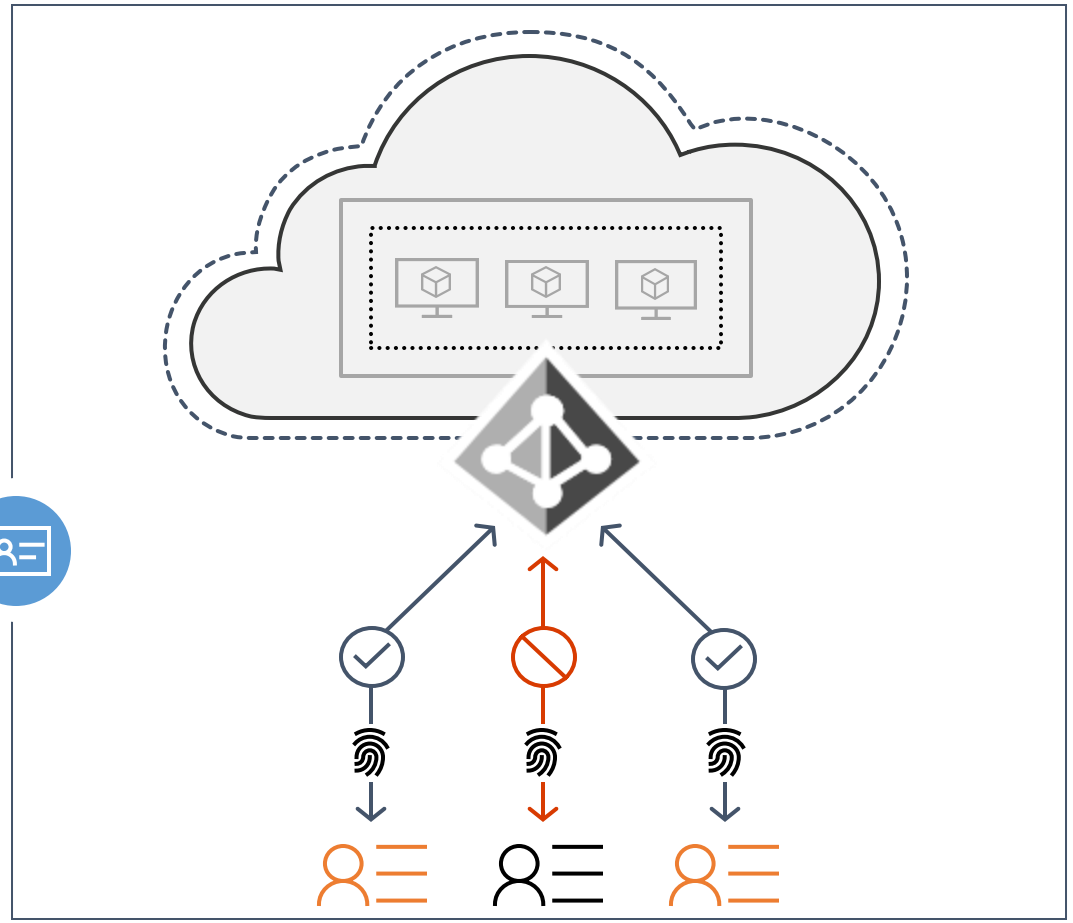
Identity & access management (IAM)

ISMS-P 2.5 인증 및 권한관리 보안통제를 구현

1. 고객 on-premises의 AD를 클라우드로 확장. 동일한 sign-on 및 single sign-on(SSO) 경험을 제공
   - Azure AD
   - Azure Active Directory Connect

2. 최소 권한 원칙 (Principle of least privilege)
   - Azure Role Based Access Control(RBAC)
   - Conditional Access based policy: 사용자, 그룹, sign-in risk 점수, 디바이스, 회사 네트워크 내부, 국가, 지역

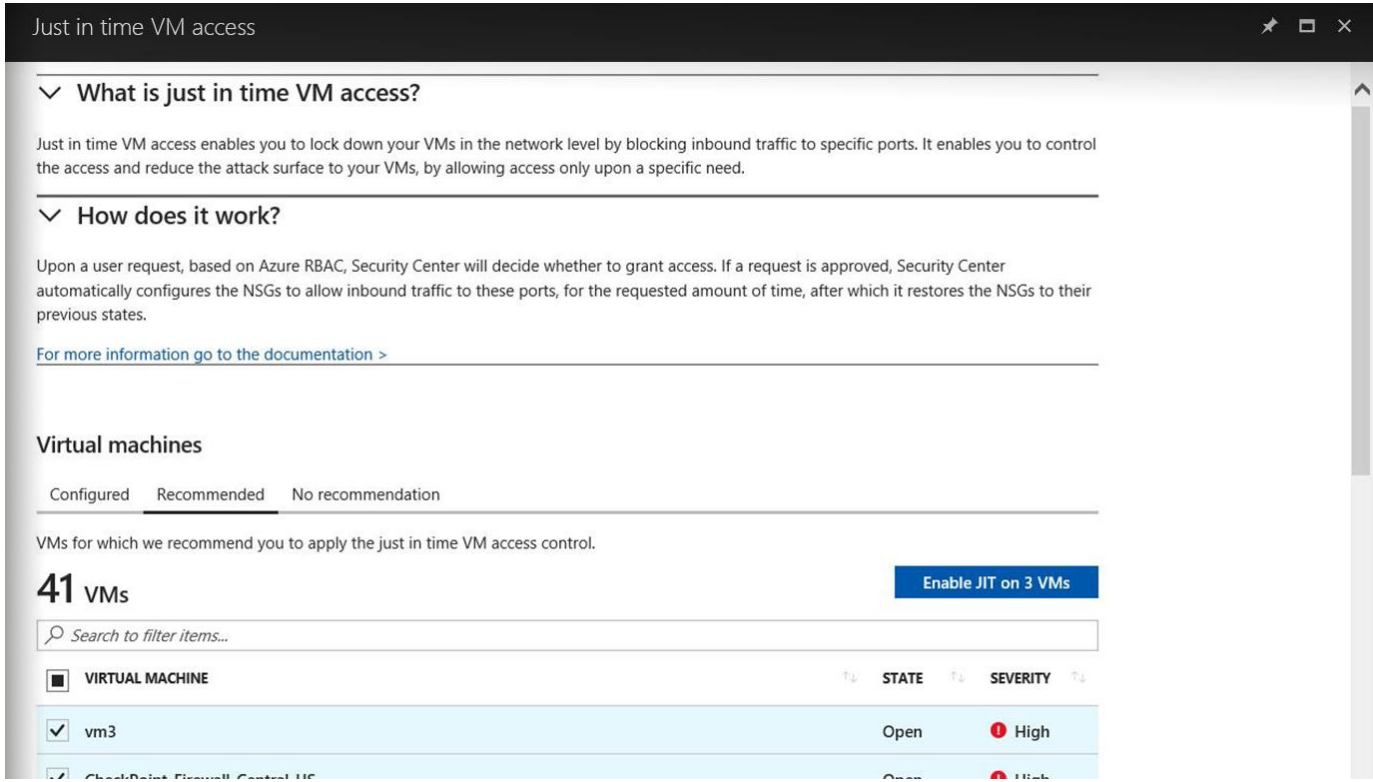
3. 보다 강력한 Identity 보호
   - Multi-factor 인증 (MFA)
   - Azure AD Privileged Identity Management를 이용한 privileged accounts 관리
   - Azure AD Identity Protection Management



Just-in-Time Access를 이용한 호스트 보안

ISMS-P 2.6.2 정보시스템 접근 보안통제를 구현

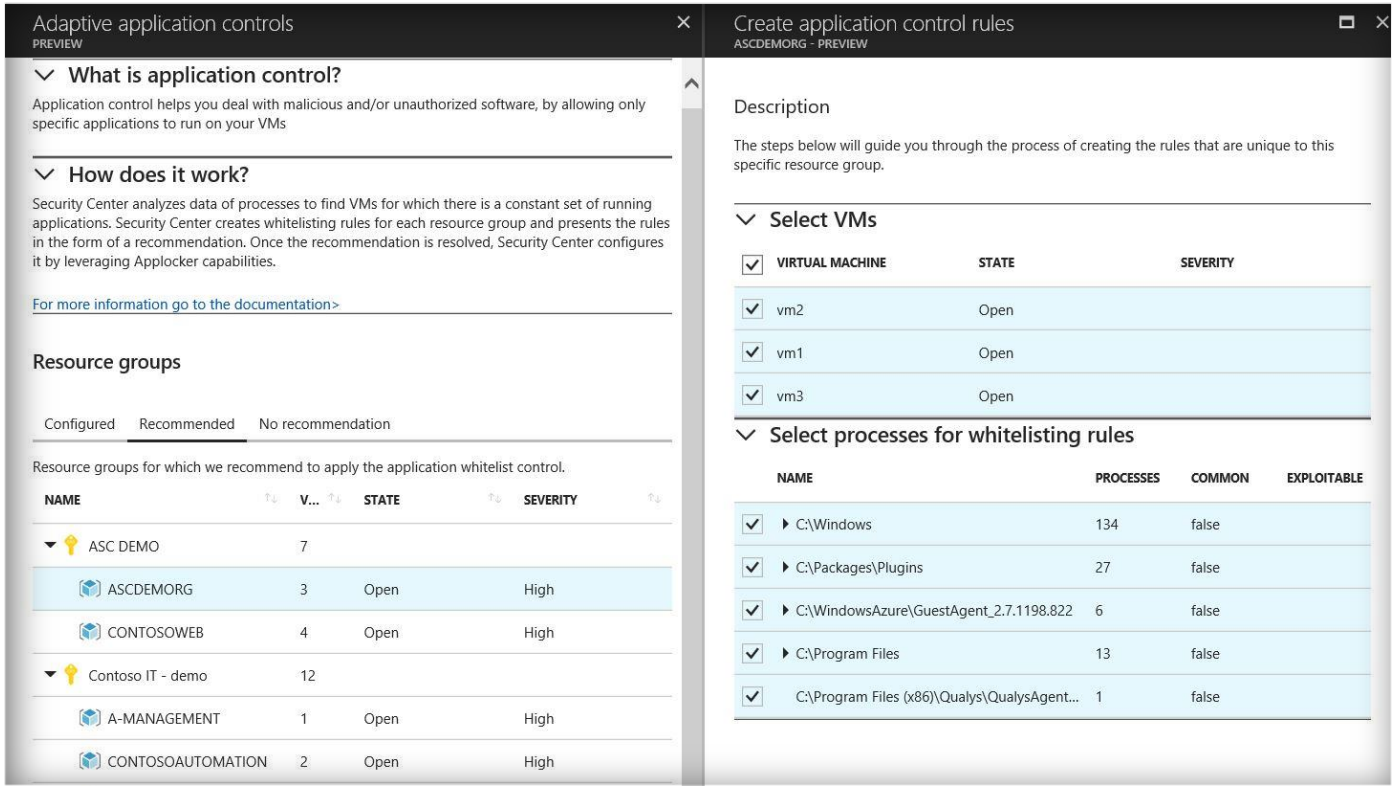
- 인터넷 노출된 관리 포트로의 Brute Force Attack을 방어
- 인터넷에 노출된 VM은 RDP, SSH 관리 포트를 대상으로 1달 평균 수만번의 brute force 공격을 받음
- 제한된 시간동안 특정 관리자 IP에 대해서만 접근을 허용하여 공격에 노출을 최소화



Application Whitelisting

ISMS-P 2.6.7 인터넷 접속 통제를 구현

- 말웨어 및 의도하지 않은 어플리케이션의 실행을 방지하고 안전한 어플리케이션만 허용
- Adaptive Whitelisting 기능으로 자동으로 VM의 어플리케이션 실행 패턴을 파악하여 Whitelist 대상 어플리케이션 목록을 제안



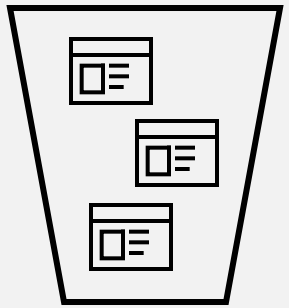
Application Whitelisting

ISMS-P 2.6.7 인터넷 접속 통제를 구현

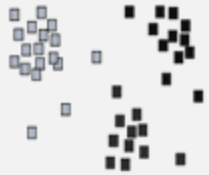
Machine Learning 적용으로 Application Whitelisting 관리를 간단히 수행

로그 수집

안정화 여부 확인



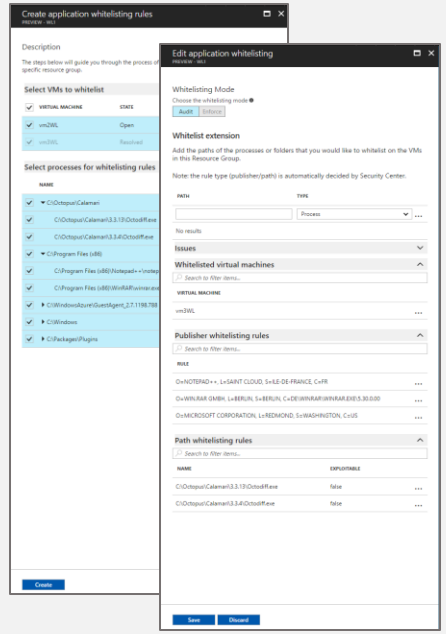
Application Baseline 작성



Grouping

MACHINE LEARNING

Recommendation



MANAGEMENT & AUDITING

Azure 데이터 보안 기능을 활용한 보안통제

ISMS-P 2.7 암호화 적용 통제를 구현

No	인증기준	상세 내용	통제 구현	
			MS Azure	신청기관
2.7.1	암호정책 적용	개인정보 및 주요정보 보호를 위하여 법적 요구사항을 반영한 암호화 대상, 암호 강도, 암호 사용 정책을 수립하고 개인정보 및 주요정보의 저장·전송·전달 시 암호화를 적용하여야 한다.	해당 서비스	개발부서
2.7.2	암호키 관리	암호키의 안전한 생성·이용·보관·배포·파기를 위한 관리 절차를 수립·이행하고, 필요 시 복구방안을 마련하여야 한다.	Azure Key Vault	보안부서 해당부서

Data 보호 기능 및 Azure Key Vault

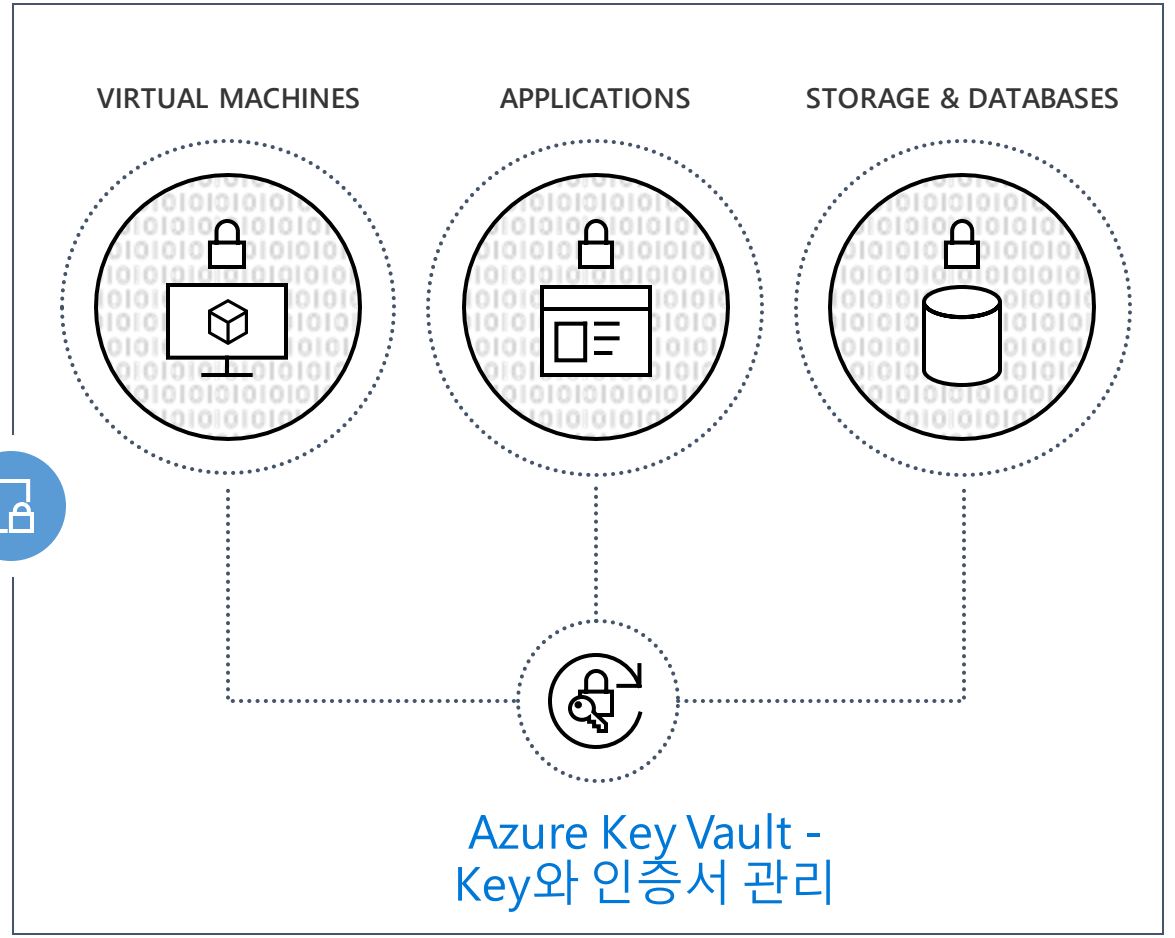
ISMS-P 2.7 암호화 적용 보안통제를 구현

1 built-in encryption across resources
- Azure Storage 암호화
- Azure Disk 암호와
- SQL TDE/Always Encrypted

2 방화벽
- Azure SQL database firewall
- Azure Storage Firewall
- 호스트 기반 파트너 방화벽 솔루션
- 가상 appliance 기반 파트너 방화벽 솔루션

3 스토리지 접근 위임 (Shared Access Signature)
- 접근 권한 부여시 접근 허용 기간, write/delete/list 허용여부, 허용 IP (대역), HTTP/HTTPS 여부를 명시

4 Azure Key Vault를 이용한 안전한 Key 관리
- 고객 Application에서 사용하는 암호, 토큰, 인증서, API Key를 안전하게 저장. (don't put the key in the app)
- HW Security Module(HSM) 지원 (FIPS 140-2)
- 인증서를 생성, 관리



Azure Security Center를 활용한 보안통제

ISMS-P 2.9, 2.10 시스템 및 서비스 운영 및 보안관리 등의 통제를 구현

No	인증기준	상세 내용	통제 구현	
			MS Azure	신청기관
2.10.2	클라우드 보안	클라우드 서비스 이용 시 서비스 유형(SaaS, PaaS, IaaS 등)에 따른 비인가 접근, 설정 오류 등에 따라 중요정보 및 개인정보가 유·노출되지 않도록 관리자 접근 및 보안 설정 등에 대한 보호대책을 수립·이행하여야 한다.	Azure Security Center	보안부서
2.11.2	취약점 점검 및 조치	정보시스템의 취약점이 노출되어 있는지를 확인하기 위하여 정기적으로 취약점 점검을 수행하고 발견된 취약점에 대해서는 신속하게 조치하여야 한다. 또한 최신 보안취약점의 발생 여부를 지속적으로 파악하고 정보시스템에 미치는 영향을 분석하여 조치하여야 한다.	Azure Security Center	보안부서 운영부서

Azure Security Center

ISMS-P 2.10.2 클라우드 보안, 2.11.2 취약점 점검 및 조치 보안통제를 구현

클라우드와 온프라미스 보안에 대한 통합 관리 기능을 제공

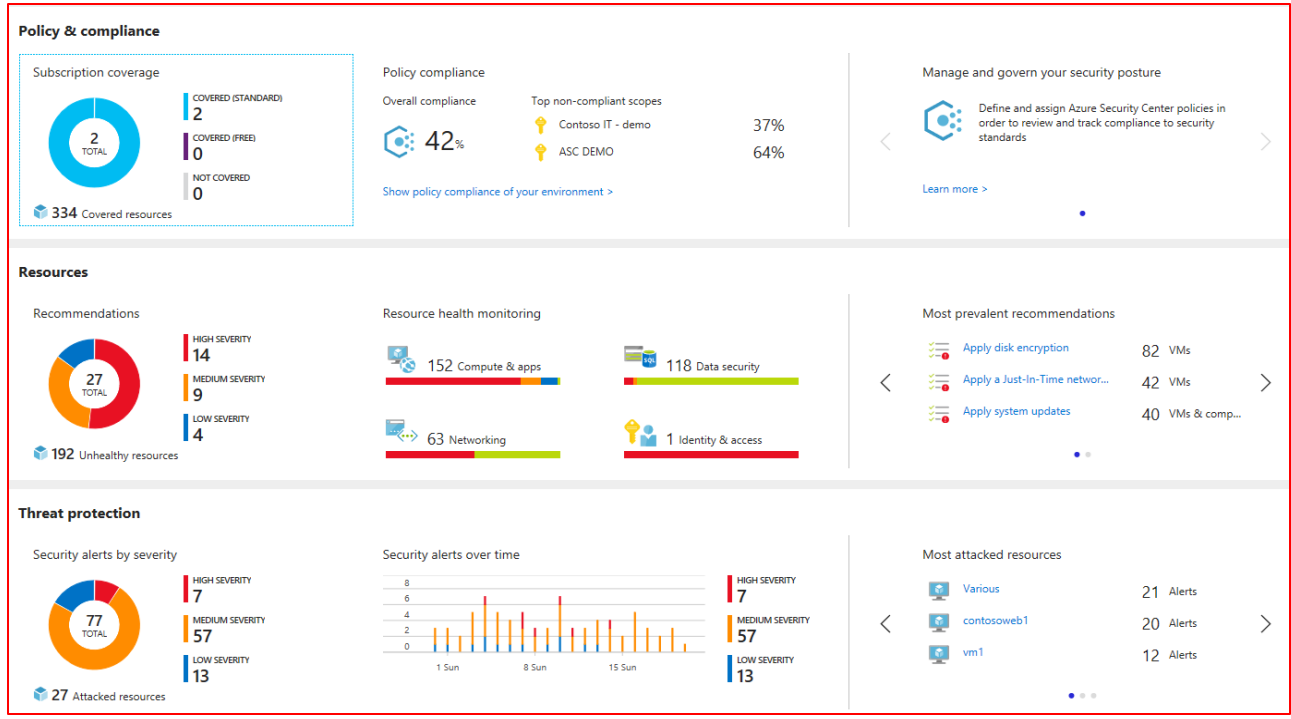
Azure 각 구독에 설정된 Azure Policy에 대한 Compliance 여부를 통합 관리

상시적으로 보안 취약점 여부를 점검. 발견된 취약점에 대해 개선 방법들을 권고

기본 탑재된 수백개의 보안 검사 항목을 대상으로 보안 취약점 검사 수행.

Custom 검사 항목 추가 가능

Azure 리소스들에 대한 공격 내역 및 Alert을 한눈에 제공



Microsoft 보안 인텔리전스를 활용한 보안통제

ISMS-P 2.11 사고 예방 및 대응 통제를 구현

No	인증기준	상세 내용	통제 구현	
			MS Azure	신청기관
2.11.1	사고 예방 및 대응체계 구축	침해사고 및 개인정보 유출 등을 예방하고 사고 발생 시 신속하고 효과적으로 대응할 수 있도록 내·외부 침해시도의 탐지·대응·분석 및 공유를 위한 체계와 절차를 수립하고, 관련 외부기관 및 전문가들과 협조체계를 구축하여야 한다.	Azure Security Center	보안부서
2.11.3	이상행위 분석 및 모니터링	내·외부에 의한 침해시도, 개인정보유출 시도, 부정행위 등을 신속하게 탐지·대응할 수 있도록 네트워크 및 데이터 흐름 등을 수집하여 분석하며, 모니터링 및 점검 결과에 따른 사후조치는 적시에 이루어져야 한다.	Azure Security Center	보안부서 운영부서
2.11.4	사고 대응 훈련 및 개선	침해사고 및 개인정보 유출사고 대응 절차를 임직원과 이해관계자가 숙지하도록 시나리오에 따른 모의훈련을 연 1회 이상 실시하고 훈련결과를 반영하여 대응체계를 개선하여야 한다.	-	보안부서
2.11.5	사고 대응 및 복구	침해사고 및 개인정보 유출 징후나 발생을 인지한 때에는 법적 통지 및 신고 의무를 준수하기 위한 절차를 마련하여야 하며, 절차에 따라 신속하게 대응 및 복구하고 재발방지 대책을 수립하여 적용하여야 한다.	-	해당부서

보안 인텔리전스 – sources of Threat Intelligence

2억5천만 사용자

수백만 사용자

매년 **수십억** 개의 malware 삭제

Malicious Software Removal Tool

7억 PCs / month

400 억번 실행 ('05-'14)

350억 messages / month

180+ 억 page scans / month

수백만대 PC

4.2억 active users

Microsoft
Digital Crimes Unit(DCU)

Microsoft
Security Response Center(MSRC)

수많은 보안 센서로 부터 보안 위협에 대한 정보를 수집하여 사이버 보안을 강화

보안 인텔리전스

Threat intelligence

Microsoft의 글로벌 Threat intelligence를 활용하여 알려진 위협 인자를 발견

이상징후(Anomaly) 감지

통계적 프로파일링을 통해 과거 패턴에 대한 베이스라인을 구축

베이스라인에서 이탈하고 false Positive 여부를 확인 후 알람을 생성

행위 분석

알려진 공격 패턴으로 위협 행위 감지

파트너 솔루션

파트너 솔루션의 알람과 로그 정보를 Security Center와 연동하여 분석

Fusion

위협 이벤트 및 알람들의 연관관계를 분석하여 Incident를 생성

Powered by Microsoft Intelligent Security Graph

Azure를 활용한 재해복구 체계 구축

ISMS-P 2.12 재해복구 보안통제를 구현

No	인증기준	상세 내용	통제 구현	
			MS Azure	신청기관
2.12.1	사고 예방 및 대응체계 구축	자연재해, 통신·전력 장애, 해킹 등 조직의 핵심 서비스 및 시스템의 운영 연속성을 위협할 수 있는 재해 유형을 식별하고 유형별 예상 피해규모 및 영향을 분석하여야 한다. 또한 복구 목표시간, 복구 목표시점을 정의하고 복구 전략 및 대책, 비상시 복구 조직, 비상연락체계, 복구 절차 등 재해 복구체계를 구축하여야 한다.	Site Recovery	운영부서
2.12.2	이상행위 분석 및 모니터링	재해 복구 전략 및 대책의 적정성을 정기적으로 시험하여 시험결과, 정보시스템 환경변화, 법규 등에 따른 변화를 반영하여 복구전략 및 대책을 보완하여야 한다.	Site Recovery	운영부서

※ Microsoft는 Azure 이용자 책임영역에 대한 재해복구 책임은 없으나, 이용자 책임영역에 대한 재해복구 구현을 돕기 위해 재해복구(DR)와 관련된 서비스를 제공하고 있음

Azure의 기본 제공 DRaaS

ISMS-P 2.12. 재해복구 보안통제를 구현

Azure의 기본 제공 DRaaS(Disaster Recovery as a Service)

Azure Site Recovery를 통해 복제, 장애 조치(failover) 및 복구 프로세스를 배포하면 계획된 중단 및 계획되지 않은 중단 기간에 고객의 서비스 연속성을 보장

- 간단하게 Azure Portal에서 직접 Azure VM을 다른 Azure 지역에 복사하여 Azure Site Recovery를 설정
- 완전히 통합된 제품인 Site Recovery는 새로운 Azure 기능이 릴리스되면 자동으로 업데이트됨
- 여러 가상 머신에서 실행되는 다중 계층 응용 프로그램의 순서를 지정하여 복구 문제를 최소화 가능
- 프로덕션 워크로드 또는 최종 사용자에게 영향을 주지 않고 재해 복구 계획을 테스트하여 규정 준수를 보장
- 온-프레미스에서 Azure로 또는 Azure에서 다른 Azure 지역으로 자동 복구를 통해 중단 중에 응용 프로그램의 가용성을 유지