쉽게 이해하는
컴플라이언스
그리고 표준화

Cloud Compliance

0
들어가기 전에.

NIST 정의에 따른 클라우드 이해

주문형 셀프 서비스
On-demand self-service

광범위 네트워크 접근
Broad network Access

빠른 탄력성
Rapid Elasticity

리소스 풀링
Resource pooling

서비스 측정
Measured Service

NIST 정의에 따른 클라우드 이해

주문형 셀프 서비스
On-demand self-service

광범위 네트워크 접근
Broad network Access

빠른 탄력성
Rapid Elasticity

리소스 풀링
Resource pooling

서비스 측정
Measured Service

클라우드에 대한 본질적 이해 : 변하는 것과 변하지 않는 것

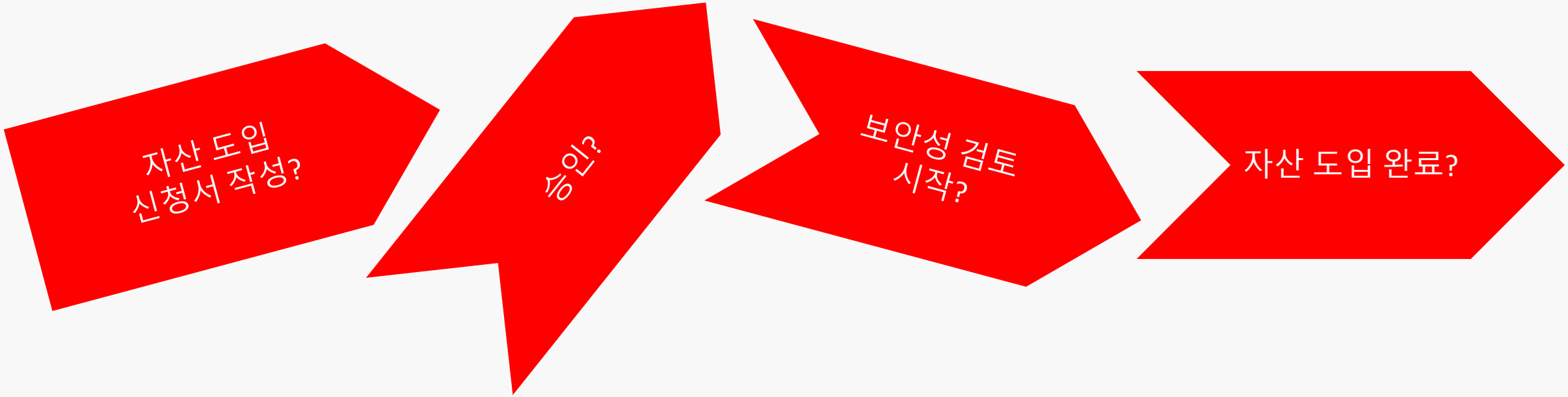
자산 도입
신청서 작성

승인

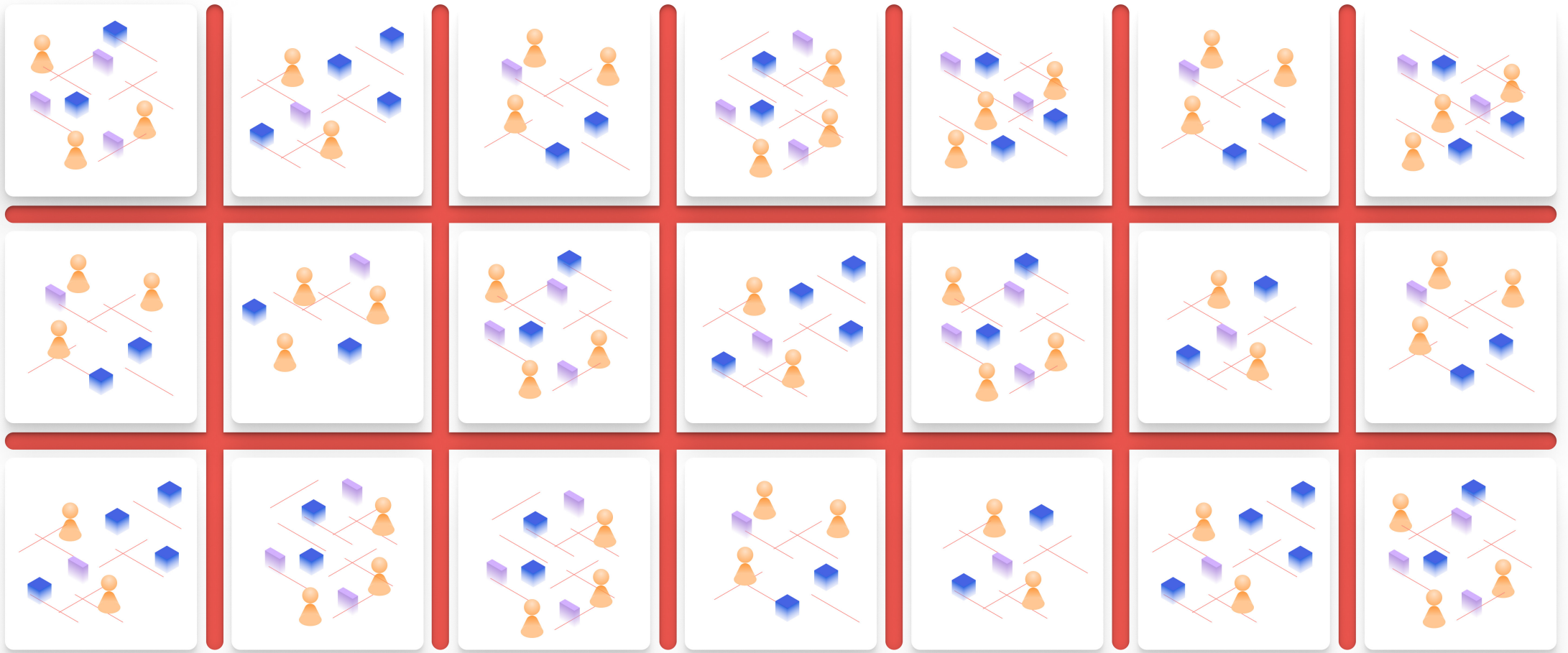
보안성 검토
시작

자산 도입 완료

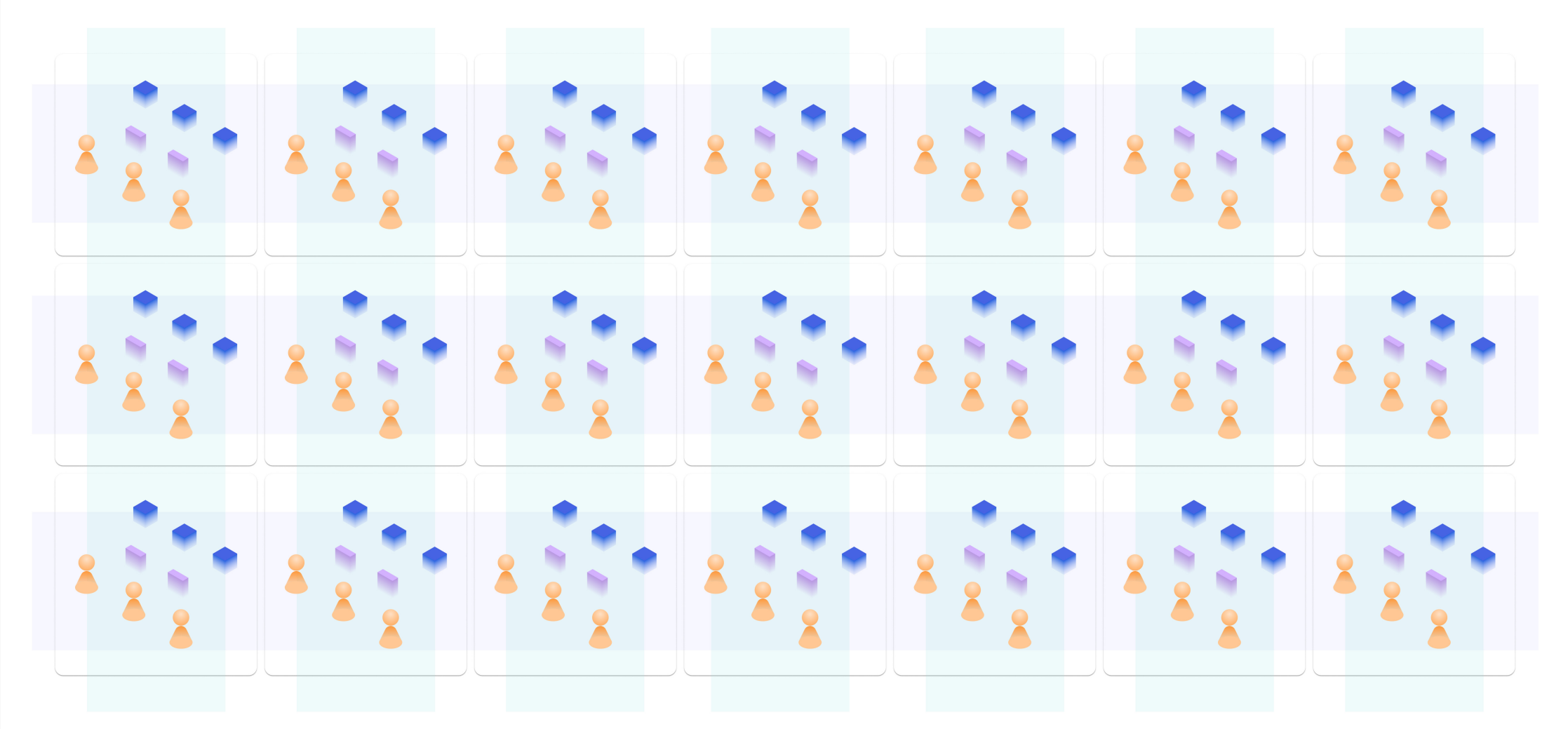
클라우드에 대한 본질적 이해 : 변하는 것과 변하지 않는 것



부서별 사일로 현상 심화로 인한 클라우드 보안 운영의 효율성 저하



클라우드에 최적화 된 절차 및 전략 재수립(BPR)을 통해 클라우드 보안 운영의 효율성 극대화 필요



1
컴플라이언스

- 정의 및 이해
- 접근 방향
- 표준화

컴플라이언스 이해 - 정의

컴플라이언스 란

법규준수 / 준법감시 / 내부통제 등 자발적으로 관련 법규 준수하기 위한 시스템

- 컴플라이언스는 사전 예방 성격(Proactive)
- 업무 내 녹여내어 스스로가 인지하지 못하더라도 준수할 수 있게 유도하는 것을 추구

➢ **임직원의 보안 내재화를 위해 끊임없이 시도 및 개선**

컴플라이언스 이해 - 시작점

자산 정의

모든 운영 및 보안에 대한 설계 및 이해의 시작점은 자산에 대한 정의로 시작

- 자산에 대한 큰 구분 점은 인프라와 데이터
  - **데이터** : 고객 이름, 주소, 신용카드 등 중요 정보 및 민감 정보
  - **인프라** : 데이터를 저장하고 처리하는 서버, 컨테이너와 같은 컴퓨팅 서비스, 스토리지 등

컴플라이언스 이해 - 표준화 첫걸음

프레임워크 선택

내부 운영 환경과 절차 그리고 확장성을 고려하여 프레임워크 선택

- NIST CSF : 사이버 보안 위험을 관리하기 위한 표준, 지침 및 모범 사례로 구성된 프레임워크
- CCM : 클라우드 보안 위험을 평가하는 데 도움이 되는 16개 도메인으로 기본 보안 원칙을 다루는 프레임워크

CCM™
Cloud Controls Matrix

컴플라이언스 이해 - 표준화 첫걸음

Table 1: Function and Category Unique Identifiers

Function Unique Identifier	Function	Category Unique Identifier	Category
ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
		ID.SC	Supply Chain Risk Management
PR	Protect	PR.AC	Identity Management and Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes and Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology
DE	Detect	DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
RS	Respond	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

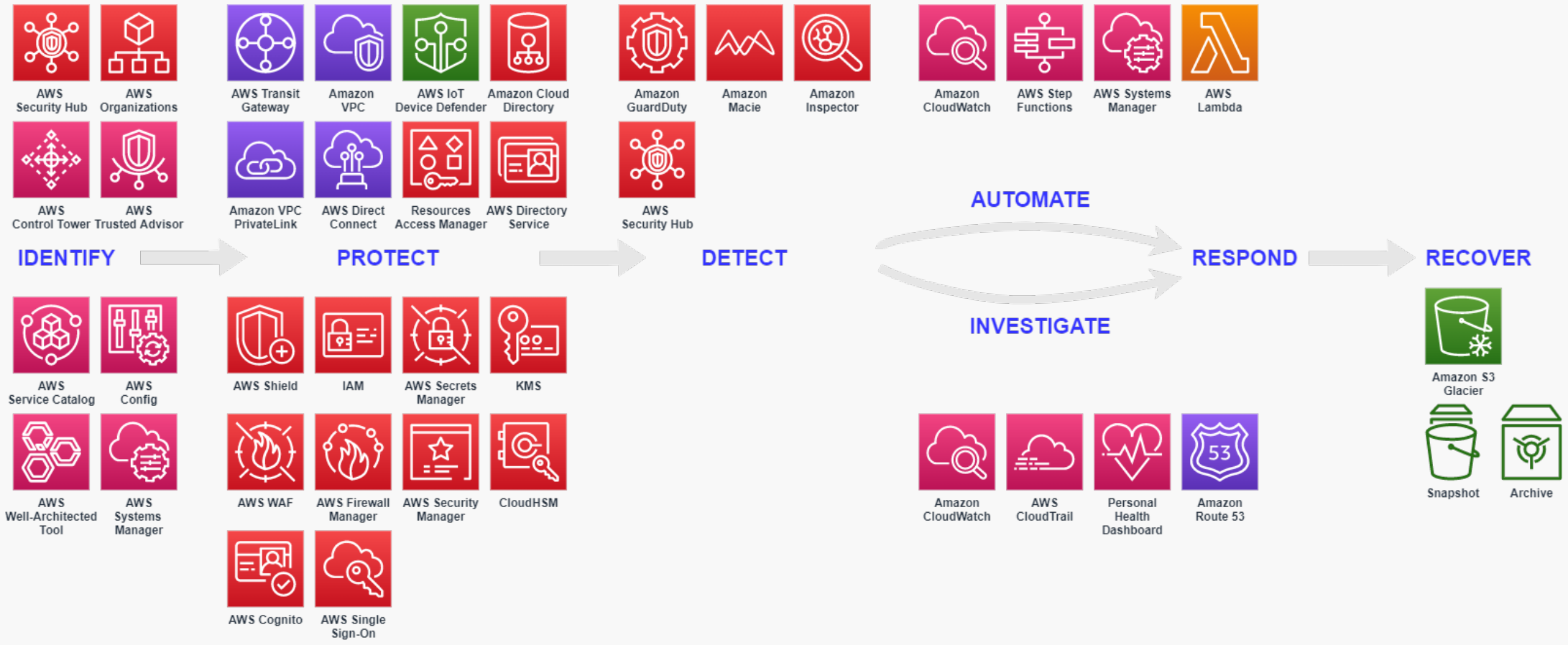
Table 2: Framework Core

Function	Category	Subcategory	Informative References
IDENTIFY (ID)	**Asset Management (ID.AM):** The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy.	**ID.AM-1:** Physical devices and systems within the organization are inventoried	**CIS CSC** 1 **COBIT 5** BAI09.01, BAI09.02 **ISA 62443-2-1:2009** 4.2.3.4 **ISA 62443-3-3:2013** SR 7.8 **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2 **NIST SP 800-53 Rev. 4** CM-8, PM-5
		ID.AM-2: Software platforms and applications within the organization are inventoried	**CIS CSC** 2 **COBIT 5** BAI09.01, BAI09.02, BAI09.05 **ISA 62443-2-1:2009** 4.2.3.4 **ISA 62443-3-3:2013** SR 7.8 **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2, A.12.5.1 **NIST SP 800-53 Rev. 4** CM-8, PM-5
		ID.AM-3: Organizational communication and data flows are mapped	**CIS CSC** 12 **COBIT 5** DSS05.02 **ISA 62443-2-1:2009** 4.2.3.4 **ISO/IEC 27001:2013** A.13.2.1, A.13.2.2 **NIST SP 800-53 Rev. 4** AC-4, CA-3, CA-9, PL-8
		ID.AM-4: External information systems are catalogued	**CIS CSC** 12 **COBIT 5** APO02.02, APO10.04, DSS01.02 **ISO/IEC 27001:2013** A.11.2.6 **NIST SP 800-53 Rev. 4** AC-20, SA-9
		ID.AM-5: Resources (e.g., hardware, devices, data, time, personnel, and software) are prioritized based on their classification, criticality, and business value	**CIS CSC** 13, 14 **COBIT 5** APO03.03, APO03.04, APO12.01, BAI04.02, BAI09.02 **ISA 62443-2-1:2009** 4.2.3.6 **ISO/IEC 27001:2013** A.8.2.1 **NIST SP 800-53 Rev. 4** CP-2, RA-2, SA-14, SC-6
		ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and	**CIS CSC** 17, 19 **COBIT 5** APO01.02, APO07.06, APO13.01, DSS06.03

2
클라우드 보안

- **NIST CSF - AWS**
- **CISA**

NIST CSF – AWS service mapping



출처: AWS Security services ecosystem diagram

클라우드 이전 및 운영 시 필수 요소

NIST Cyber Security Framework

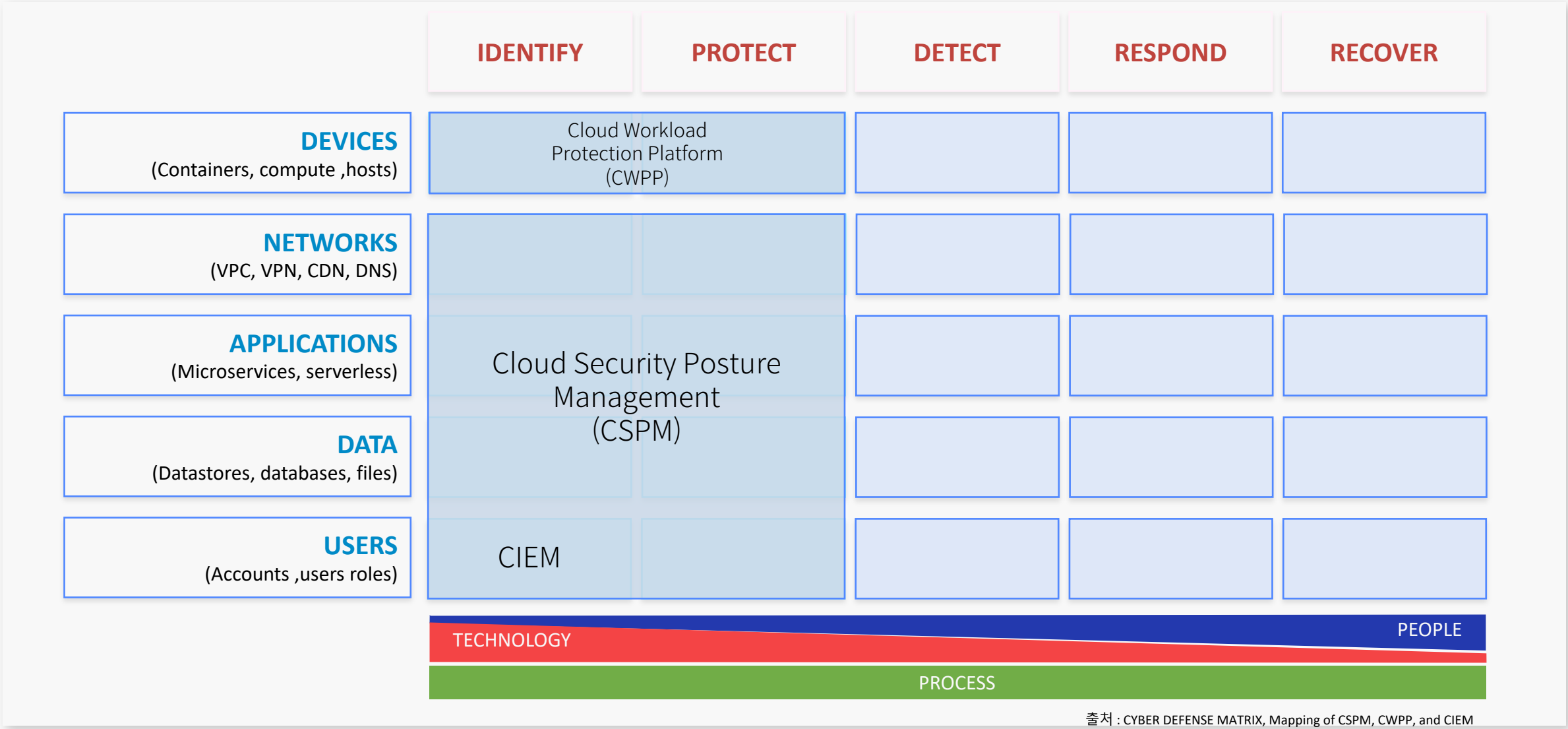
식별 Identify	보호 Protect	감지 Detect	대응 Respond	회복 Recover
거버넌스 Governance	Anti DDoS	SIEM	침해사고 대응	재해복구
자산 관리 Asset Management	IPS	IDS/IPS	장애 대응	침해사고 대응 계획
설정 관리 Configuration Management	방화벽 Firewall	취약점 스캐너 Vulnerability scanner	포렌식	장애 대응 계획
위험 평가 Risk Assessments	WAF	DLP		
컴플라이언스 Compliance	Application Segmentation	파일무결성 모니터링 File Integrity Monitoring, FIM		

NIST CSF(Cybersecurity Framework) 기반 보안 운영 기획

NIST Cyber Security Framework

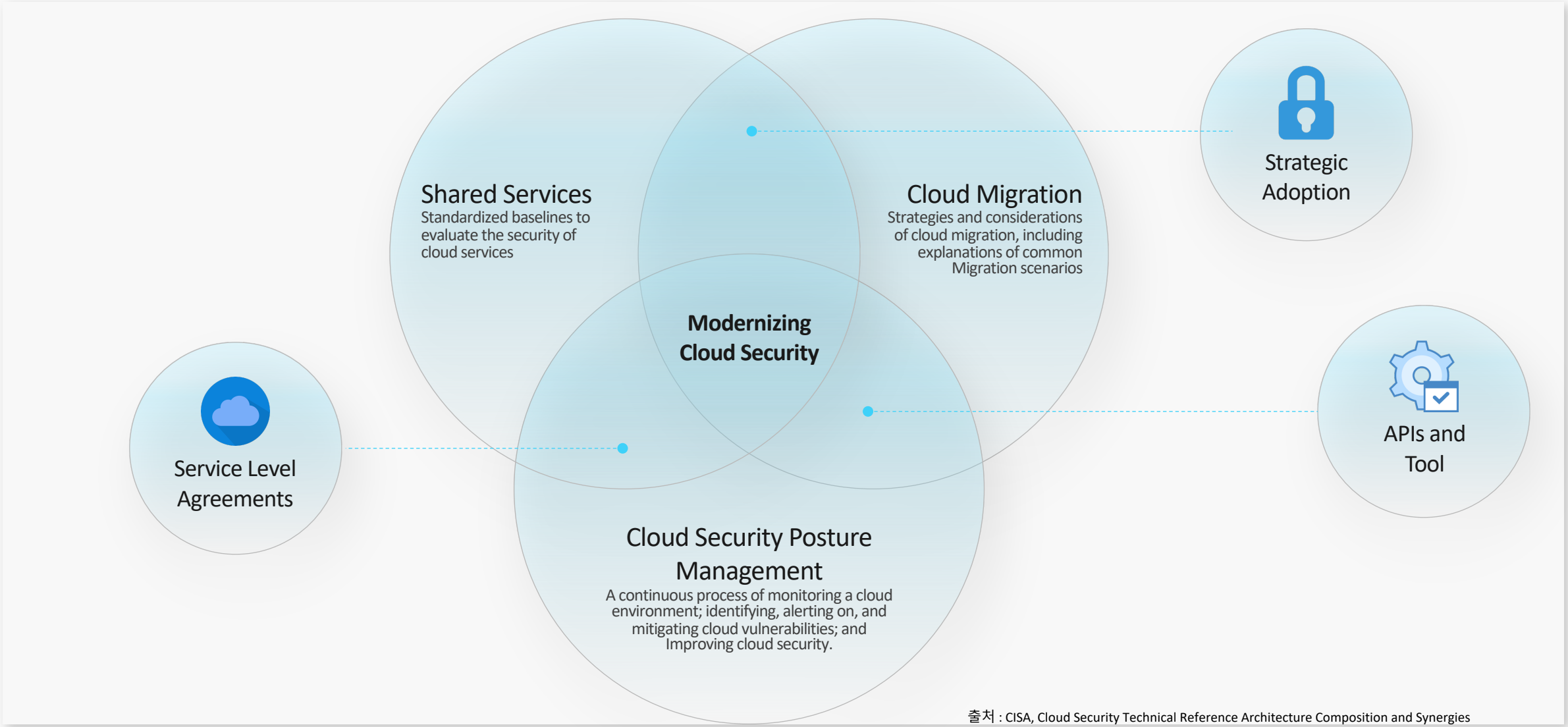
식별 Identify	보호 Protect	감지 Detect	대응 Respond	회복 Recover
거버넌스 Governance	Anti DDoS	SIEM	침해사고 대응	재해복구
자산 관리 Asset Management	IPS	IDS/IPS	장애 대응	침해사고 대응 계획
설정 관리 Configuration Management	방화벽 Firewall	취약점 스캐너 Vulnerability scanner	포렌식	장애 대응 계획
위험 평가 Risk Assessments	WAF	DLP		
컴플라이언스 Compliance	Application Segmentation	파일무결성 모니터링 File Integrity Monitoring, FIM		

NIST CSF 기반 자산 운영 표준화



출처 : CYBER DEFENSE MATRIX, Mapping of CSPM, CWPP, and CIEM

클라우드 보안 현대화 설계



출처 : CISA, Cloud Security Technical Reference Architecture Composition and Synergies

E.O.D