평가영역	평가분야	세부분야	평가항목	관련근거		관련 AWS 제품	관련 보안 지침 가이드	운영현황
				CSAP	ISMS-P			
1. 침해사고관리	1.1. 침해사고 대응 절차 및 체계	1.1.1. 침해사고 대응 체계 구축	침해사고 발생 시 침해사고 대응절차에 따라 법적 통지 및 신고 의무를 준수하여야 한다. 또한 클라우드컴퓨팅서비스 이용자에게 발생 내용, 원인, 조치 현황 등을 신속하게 알려야 한다. 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 외부 기관 및 전문가들과 협조체계를 구축하여야 한다.	5.1.2. 침해사고 대응 체계 구축	2.11.1 사고 예방 및 대응체계 구축	CloudWatch, GuardDuty	클라우드보안-CloudWatch, GuardDuty	Y
	1.2. 침해사고 대응	1.2.1. 침해사고 처리 및 복구	침해사고 및 개인정보 유출 징후나 발생을 인지한 때에는 법적 통지 및 신고 의무를 준수하여야 하며, 절차에 따라 신속하게 대응 및 복구하고 사고분석 후 재발방지 대책을 수립하여 대응체계에 반영하여야 한다.	5.2.2. 침해사고 처리 및 복구	2.11.5 사고 대응 및 복구	CloudWatch, GuardDuty	클라우드보안-CloudWatch, GuardDuty	Y
2. 서비스연속성관리	2.1. 장애대응	2.1.1. 장애 대응절차 수립	관련 법률에서 규정한 클라우드컴퓨팅서비스의 중단으로부터 업무 연속성을 보장하기 위해 백업, 복구 등을 포함하는 장애 대응 절차를 마련하여야 한다.	6.1.1. 장애 대응절차 수립	2.9.2 성능 및 장애 관리	CloudWatch, GuardDuty	클라우드보안-CloudWatch, GuardDuty	Y
		2.1.2. 장애 보고	클라우드컴퓨팅서비스 중단이나 피해가 발생 시 장애 대응절차에 따라 법적 통지 및 신고 의무를 준수하여야 한다. 또한 클라우드컴퓨팅서비스 이용자에게도 발생 내용, 원인, 조치 현황 등을 신속하게 알려야 한다.	6.1.2. 장애 보고		CloudWatch, GuardDuty	클라우드보안-CloudWatch, GuardDuty	Y
		2.1.3. 장애 처리 및 복구	클라우드컴퓨팅서비스 중단이나 피해가 발생할 경우, 서비스 수준 협약(SLA)에 명시된 시간 내에 장애 대응절차에 따라 해당 서비스의 장애를 처리하고 복구시켜야 한다.	6.1.3. 장애 처리 및 복구		CloudWatch	클라우드보안-CloudWatch	Y
		2.1.4. 재발방지	장애 관련 정보를 활용하여 유사한 서비스 중단이 반복되지 않도록 장애 재발방지 대책을 수립하고, 필요한 경우 장애 대응절차도 변경하여야 한다.	6.1.4. 재발방지		Config	클라우드보안-Config	Y
	2.2. 서비스 가용성	2.2.1. 성능 및 용량 관리	클라우드컴퓨팅서비스의 가용성을 보장하기 위해 성능 및 용량에 대한 요구사항을 정의하고, 지속적으로 관리할 수 있는 모니터링 방법 또는 절차를 수립하여야 한다.	6.2.1. 성능 및 용량 관리		CloudWatch	클라우드보안-CloudWatch	Y
		2.2.2. 이중화 및 백업	정보처리설비(예 : 클라우드컴퓨팅서비스를 제공하는 물리적인 서버, 스토리지, 네트워크 장비, 통신 케이블, 접속 회선 등)의 장애로 서비스가 중단되지 않도록 정보 처리설비를 이중화하고, 장애 발생 시 신속하게 복구를 수행하도록 백업 체계도 마련하여야 한다.	6.2.2. 이중화 및 백업	2.9.3 백업 및 복구 관리	RDS-MultiAZ, Auto Scailing, CloudWatch, Lambda, RDS-Snapshot	클라우드보안-CloudWatch,RDS-스냅샷,MultiAZ	Y
3. 준거성	3.1. 법 및 정책 준수	3.1.1. 법적요구사항 준수	정보보호 관련 법적 요구사항을 식별하고 준수하여야 한다.	7.1.1. 법적요구사항 준수		Config	클라우드보안-Config	Y
	3.2. 정보시스템 감사	3.2.1. 독립적 보안감사	법적 요구사항 및 정보보호 정책 준수 여부를 보증하기 위해 독립적 보안감사 계획을 수립하여 시행하고 개선 조치를 취하여야 한다.	7.2.1. 독립적 보안감사		Config, Inspector	클라우드보안-Config,Inspector	Y
		3.2.2. 감사기록 및 모니터링	보안감사 증적(로그)은 식별할 수 있는 형태로 기록 및 모니터링 되어야 되고 비인가된 접근 및 변조로부터 보호되어야 한다.	7.2.2. 감사기록 및 모니터링	2.9.3 백업 및 복구 관리 2.9.4 로그 및 접속 기록 관리	Config, Inspector, S3	클라우드보안-Config,Inspector	Y
4. 가상화 보안	4.1. 가상화 인프라	4.1.1. 가상자원 관리	가상자원(가상 머신, 가상 스토리지, 가상 소프트웨어 등)의 생성, 변경, 회수 등에 대한 관리 방안을 수립하여야 한다.	9.1.1. 가상자원 관리		CloudWatch	클라우드보안-CloudWatch	Y
		4.1.2. 공개서버 보안	가상자원 및 서비스를 제공하기 위한 웹사이트 또는 공개서버를 제공하는 경우 기술적 보호대책을 수립하여야 한다.	9.1.5. 공개서버 보안	2.10.3 공개서버 보안	SecurityGroup, ACL, NetworkFirewall, WAF, Inspector	네트워크보안-Security Group, ACL,Network Firewall,WAF, 클라우드보안-Inspector	Y
	4.2. 가상 환경	4.2.1. 악성코드 통제	바이러스, 웜, 트로이목마 등의 악성코드로부터 이용자의 가상 환경(가상PC, 가상 서버, 가상 소프트웨어 등)을 보호하기 위한 악성코드 탐지, 차단 등의 보안기술을 지원하여야 한다. 또한 이상 징후 발견 시 이용자 통지하고 사용 중지 및 격리 조치를 수행하여야 한다.	9.2.1. 악성코드 통제		NetworkFirewall, WAF, CloudWatch	네트워크보안-Network Firewall,WAF, 클라우드보안-CloudWatch	Y
		4.2.2. 인터페이스 및 API 보안	가상 환경(가상PC, 가상 서버, 가상 소프트웨어 등) 접근을 위한 인터페이스 및 API에 대한 보안 취약점을 주기적으로 분석하고, 이에 대한 보호방안을 마련하여야 한다.	9.2.2. 인터페이스 및 API 보안		CloudTrail	클라우드보안-CloudTrail	Y
		4.2.3. 데이터 이전	이용자가 기존 정보시스템 환경에서 클라우드컴퓨팅서비스의 가상 환경으로 전환 시 안전하게 데이터를 이전하도록 암호화	9.2.3. 데이터 이전		VPN, SSL/TLS	네트워크보안-VPN	Y
		4.2.4. 가상 소프트웨어 보안	클라우드컴퓨팅서비스 제공자는 출처, 유통경로 및 제작자가 명확한 소프트웨어로 구성된 가상환경을 제공하여야 한다.	9.2.4. 가상 소프트웨어 보안		IAM	계정보안-IAM	Y
5. 접근통제	5.1. 접근통제 정책	5.1.1. 접근통제 정책 수립	비인가자의 접근을 통제할 수 있도록 접근통제 영역 및 범위, 접근통제 규칙, 방법 등을 포함하여 접근통제 정책을 수립하여야 한다.	10.1.1. 접근통제 정책 수립		SecurityGroup, IAM, ACL	네트워크보안-Security Group, ACL, 계정보안-IAM	Y
		5.1.2. 접근기록 관리	접근기록 대상을 정의하고 서비스 통제, 관리, 사고 발생 책임 추적성 등을 보장할 수 있는 형태로 기록되고 유지하여야 한다. 서버, 응용프로그램, 보안시스템, 네트워크시스템 등 정보시스템에 대한 사용자 접속기록, 시스템로그, 관한부여 내역 등의 로그유형, 보존기간, 보존방법 등을 정하고 위·변조, 도난, 분실 되지 않도록 안전하게 보존·관리하여야 한다.	10.1.2. 접근기록 관리	2.9.4 로그 및 접속 기록 관리	CloudTrail	클라우드보안-CloudTrail	Y
	5.2. 접근 권한 관리	5.2.1. 사용자 등록 및 권한부여	클라우드 시스템 및 중요정보에 대한 접근을 통제하기 위하여 공식적인 사용자 등록 및 해지 절차를 수립하고 업무 필요성에 따라 사용자 접근권한을 최소한으로 부여하여야 한다.	10.2.1. 사용자 등록 및 권한부여	2.5.1 사용자계정관리	CloudTrail, IAM	클라우드보안-CloudTrail,계정보안-IAM	Y
		5.2.2. 관리자 및 특수 권한관리	클라우드 시스템 및 중요정보 관리 및 특수 목적을 위해 부여한 계정 및 권한을 식별하고 별도 통제하여야 한다.	10.2.2. 관리자 및 특수 권한관리		IAM	계정보안-IAM	Y
		5.2.3. 접근권한 검토	클라우드 시스템 및 중요정보에 대한 접근을 관리하기 위하여 접근권한 부여, 이용(장기간 미사용), 변경(퇴직 및 휴직, 직무변경, 부서변경)의 적정성 여부를 정기적으로 점검하여야 한다.	10.2.3. 접근권한 검토		CloudTrail, IAM	클라우드보안-CloudTrail,계정보안-IAM	Y
	5.3. 사용자 식별 및 인증	5.3.1. 사용자 식별	클라우드 시스템에서 사용자를 유일하게 구분할 수 있는 식별자를 할당하고 추측 가능한 식별자 사용을 제한하여야 한다. 동일한 식별자를 공유하여 사용하는 경우 그 사유와 타당성을 검토하고 책임자의 승인을 받아야 한다.	10.3.1. 사용자 식별	2.5.2. 사용자식별	IAM	계정보안-IAM	Y
		5.3.2. 사용자 인증	클라우드 시스템에 대한 접근은 사용자 인증, 로그인 횟수 제한, 불법 로그인 시도 경고 등 안전한 사용자 인증 절차에 의해 통제하여야 한다.	10.3.2. 사용자 인증	2.5.3. 사용자관리 2.10.2 클라우드 보안	Config, CloudWatch, IAM, MFA	클라우드보안-Config, CloudWatch, 계정보안-IAM, MFA	Y
		5.3.3. 강화된 인증 수단 제공	이용자가 클라우드컴퓨팅서비스에 대해 다중 요소 인증 등 강화된 인증 수단을 요청하는 경우 이를 제공하기 위한 방안을 마련하여야 한다.	10.3.3. 강화된 인증 수단 제공		MFA, IAM	계정보안-IAM, MFA	Y
		5.3.4. 사용자 패스워드 관리	법적 요구사항, 외부 위협요인 등을 고려하여 패스워드 복잡도 기준, 초기 패스워드 변경, 변경주기 등 사용자 패스워드 관리절차를 수립·이행하고 패스워드 관리 책임이 사용자에게 있음을 주의시켜야 한다. 특히 관리자 패스워드는 별도 보호대책을 수립하여 관리하여야 한다.	10.3.4. 사용자 패스워드 관리	2.5.4. 비밀번호관리	Config	클라우드보안-Config	Y
6. 네트워크 보안	6.1. 네트워크 보안	6.1.1. 네트워크 보안 정책 수립	클라우드컴퓨팅서비스와 관련된 내·외부 네트워크에 대해 보안 정책과 절차를 수립하여야 한다. 보안시스템 유형별로 관리자 지정, 최신 정책 업데이트, 룰셋 변경, 이벤트 모니터링 등의 운영절차를 수립·이행하고 보안시스템별 정책적용 현황을 관리하여야 한다.	11.1.1. 네트워크 보안 정책 수립	2.10.1 보안시스템 운영	VPN, Security Group	네트워크보안-Security Group, VPN	Y
		6.1.2. 네트워크 모니터링 및 통제	DDoS, 비인가 접속 등으로 인한 서비스 중단 및 중요 정보 유출 등을 막기 위해 네트워크를 모니터링하고 통제하여야 한다. 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.	11.1.2. 네트워크 모니터링 및 통제	2.6.1 네트워크 접근 2.10.1 보안시스템 운영 2.11.3 이상행위 분석 및 모니터링	Security Group, ACL, GuardDuty, CloudWatch, Shield, Inspector, systems manager, Config, WAF	네트워크보안-Security Group, ACL, 클라우드보안-GuardDuty, CloudWatch, Shield, Inspector, systems manager, Config, WAF	Y
		6.1.3. 네트워크 정보보호시스템 운영	클라우드컴퓨팅서비스와 관련된 내·외부 네트워크를 보호하기 위하여 정보보호시스템(방화벽, IPS, IDS, VPN 등)을 운영하여야 한다.	11.1.3. 네트워크 정보보호시스템 운영	2.6.2 정보시스템 접근	Security Group, ACL, Network Firewall, WAF, VPN, NAT	네트워크보안-Security Group, ACL, Network Firewall, WAF, VPN, NAT	Y
		6.1.4. 네트워크 암호화	클라우드 시스템에서 중요 정보가 이동하는 구간에 대해서는 암호화된 통신채널을 사용하여야 한다	11.1.4. 네트워크 암호화	2.6.6 원격접근 통제 2.10.5 정보전송 보안	SSL/TLS, Bastion Host, VPN, Parameter Store	네트워크보안-VPN, RDS-Parameter Store	Y
		6.1.5. 네트워크 분리	클라우드컴퓨팅서비스 제공자의 관리 영역과 이용자의 서비스 영역, 이용자 간 서비스 영역의 네트워크 접근은 물리적 또는 논리적으로 분리하여야 하고, 취약점 점검, 접근통제, 인증, 정보 수집·저장·공개 절차 등 강화된 보호대책을 수립·이행하여야 한다.	11.1.5. 네트워크 분리	2.6.1 네트워크 접근 2.10.3 공개서버 보안	VPC, Subnet, Security Group, IAM, Inspector	네트워크보안-Security Group, 계정보안-IAM, 클라우드보안-Inspector	Y
7. 데이터 보호 및 암호화	7.1. 데이터 보호	7.1.1. 데이터 분류	데이터 유형, 법적 요구사항, 민감도 및 중요도에 따라 데이터를 분류하고 관리하여야 한다.	12.1.1. 데이터 분류		RDS-Private Access, RDS, Bastion Host	RDS-Private Access	Y
		7.1.3. 데이터 무결성	입·출력, 전송 또는 데이터 교환 및 저장소의 데이터에 대해 항상 데이터 무결성을 확인하여야 한다.	12.1.3. 데이터 무결성		RDS, VPN	RDS, 네트워크 보안-VPN	Y
		7.1.4. 데이터 보호	데이터에 대한 접근제어, 위·변조 방지 등 데이터 처리에 대한 보호 기능을 이용자에게 제공하여야 한다.	12.1.4. 데이터 보호		RDS, RDS-Private Access, IAM, Security Group	RDS-Private Access,계정보안-IAM,네트워크보안-Security Group	Y
		7.1.5. 데이터 추적성	이용자에게 데이터를 추적하기 위한 방안을 제공하고, 이용자가 요구하는 경우 구체적인 제공정보(이용자의 정보가 저장되는 국가의 명칭 등)를 공개하여야 한다.	12.1.5. 데이터 추적성		Systems manager, S3, CloudTrail	클라우드보안-systems manager, CloudTrail	Y
		7.1.6. 데이터 폐기	클라우드컴퓨팅서비스 종료, 이전 등에 따른 데이터 폐기 조치 시 이용자와 관련된 모든 데이터를 폐기하여야 하며, 폐기된 데이터를 복구할 수 없도록 삭제 방안을 마련하여야 한다. 개인정보의 보유기간 및 파기 관련 내부 정책을 수립하고 개인정보의 보유기간 경과, 처리목적 달성 등 파기 시점이 도달한 때에는 파기의 안전성 및 완전성이 보장될 수 있는 방법으로 지체 없이 파기하여야 한다.	12.1.6. 데이터 폐기	3.4.1 개인정보의 파기	RDS, Lambda	클라우드보안-CloudWatch, GuardDuty, CloudTrail, Config	Y
	7.2. 암호화	7.2.1. 암호 정책 수립	클라우드컴퓨팅서비스에 저장 또는 전송 중인 데이터를 보호하기 위해 암호화 대상, 암호 강도(복잡도), 키관리, 암호 사용에 대한 정책을 마련하여야 한다. 또한 정책에는 개인정보 저장 및 전송 시 암호화 적용 등 암호화 관련 법적 요구사항을 반드시 반영하여야 한다.	12.2.1. 암호 정책 수립	2.7.1 암호정책 적용	RDS-Parameter Store, 가명처리, SSL/TLS, Config	RDS-Parameter Store, 가명처리, 클라우드보안-Config	Y
		7.2.2. 암호키 관리	암호키 생성, 이용, 보관, 배포, 파기에 관한 안전한 절차를 수립하고, 암호키는 별도의 안전한 장소에 보관하여야 한다.	12.2.2. 암호키 관리	2.7.2 암호키 관리	Parameter Store, KMS	RDS-Parameter Store, S3보안-	Y
8. 시스템 개발 및 도입 보안	8.1. 시스템 분석 및 설계	8.1.1. 보안요구사항 정의	신규 시스템 개발 및 기존 시스템 변경 시 정보보호 관련 법적 요구사항, 최신 보안취약점, 정보보호 기본요소(기밀성, 무결성, 가용성) 등을 고려하여 보안요구사항을 명확히 정의하고 이를 적용하여야 한다.	13.1.1. 보안요구사항 정의	2.8.1 보안 요구사항 정의	Config, Systems manager	클라우드보안-Config, systems manager	Y
		8.1.2. 인증 및 암호화 기능	클라우드 시스템 설계 시 사용자 인증에 관한 보안요구사항을 반드시 고려하여야 하며 중요정보의 입·출력 및 송수신 과정에서 무결성, 기밀성이 요구될 경우 법적 요구사항을 고려하여야 한다.	13.1.2. 인증 및 암호화 기능		IAM, KMS, RDS-Parameter Store, SSL/TLS, VPN	계정보안-IAM, RDS-Parameter Store, 네트워크보안-VPN, S3보안 - KMS	Y
		8.1.3. 보안로그 기능	클라우드 시스템 설계 시 사용자의 인증, 권한 변경, 중요정보 이용 및 유출 등에 대한 감사증적을 확보할 수 있도록 하여야 한다. 서버, 응용프로그램, 보안시스템, 네트워크시스템 등 정보시스템에 대한 사용자 접속기록, 시스템로그, 권한부여 내역 등의 로그유형, 보존기간, 보존방법 등을 정하고 위·변조, 도난, 분실 되지 않도록 안전하게 보존·관리하여야 한다.	13.1.3. 보안로그 기능	2.9.4 로그 및 접속 기록 관리 2.9.5 로그 및 접속 기록 점검	CloudWatch, GuardDuty, CloudTrail, Config, S3	클라우드보안-CloudWatch, GuardDuty, CloudTrail, Config	Y
		8.1.4. 접근권한 기능	클라우드 시스템 설계 시 업무의 목적 및 중요도에 따라 접근권한을 부여할 수 있도록 하여야 한다.	13.1.4. 접근권한 기능	2.6.2 정보시스템 접근	IAM	계정보안-IAM	Y
	8.2. 구현 및 시험	8.2.1. 구현 및 시험	안전한 코딩방법에 따라 클라우드컴퓨팅서비스를 구현하고, 분석 및 설계 과정에서 도출한 보안요구사항이 정보시스템에 적용되었는지 확인하기 위하여 시험을 수행하여야 한다	13.2.1. 구현 및 시험	2.8.2 보안 요구사항 검토 및 시험	Config, Inspector	클라우드보안-Config,Inspector	Y
		8.2.2. 개발과 운영환경 분리	개발 및 시험 시스템은 운영시스템에 대한 비인가 접근 및 변경의 위험을 감소하기 위해 원칙적으로 분리하여야 한다. 단 분리하여 운영하기 어려운 경우 그 사유와 타당성을 검토하고 안전성 확보 방안을 마련하여야 한다.	13.2.2. 개발과 운영환경 분리	2.8.3 시험과 운영 환경 분리	SandBox, VPC, Subnet, Security Group, VPN, ACL	네트워크보안-Security Group, VPN, ACL	Y
		8.2.3. 시험 데이터 보안	시스템 시험 과정에서 운영데이터 유출을 예방하기 위해 시험데이터 생성, 이용 및 관리, 파기, 기술적 보호조치에 관한 절차를 수립하여 이행하여야 한다.	13.2.3. 시험 데이터 보안	2.8.4 시험 데이터 보안	IAM, RDS-가명처리	계정보안-IAM,RDS-가명처리	Y
		8.2.4. 소스 프로그램 보안	소스 프로그램에 대한 변경관리를 수행하고 인가된 사용자만이 소스 프로그램에 접근할 수 있도록 통제절차를 수립하여 이행하여야 한다. 또한 소스 프로그램은 운영환경에 보관하지 않는 것을 원칙으로 한다.	13.2.4. 소스 프로그램 보안	2.8.5 소스 프로그램 관리	IAM, Security Group, VPN	계정보안-IAM,네트워크보안-Security Group,VPN	Y
9. 공공기관 보안요구사항	9.1. 물리적 보호조치	9.1.1. 중요장비 이중화 및 백업체계 구축	클라우드컴퓨팅서비스를 제공하는 사업자는 네트워크 스위치, 스토리지 등 중요장비를 이중화하고 서비스의 가용성을 보장하기 위해 백업체계를 구축하여야 한다.	14.2.2. 중요장비 이중화 및 백업 체계 구축	2.9.3 백업 및 복구 관리	RDS-Snapshot,MultiAZ, S3, CloudWatch	클라우드보안-CloudWatch,RDS-스냅샷,MultiAZ	Y
10. 관리체계 수립 및 운영	10.1. 관리체계 점검 및 개선	10.1.1 법적 요구사항 준수 검토	조직이 준수하여야 할 정보보호 및 개인정보보호 관련 법적 요구사항을 주기적으로 파악하여 규정에 반영하고, 준수 여부를 지속적으로 검토하여야 한다.		1.4.1 법적 요구사항 준수 검토	Config, systems manager	클라우드보안-Config, systems manager	Y
11. 보호대책 요구사항	11.1. 인적보안	11.1.1. 직무분리	권한 오남용 등으로 인한 잠재적인 피해 예방을 위하여 직무 분리 기준을 수립하고 적용하여야 한다. 권한 오남용 등으로 인한 잠재적인 피해 예방을 위하여 직무 분리 기준을 수립하고 적용하여야 한다. 다만 불가피하게 직무 분리가 어려운 경우 별도의 보완대책을 마련하여 이행하여야 한다.	2.1.3. 직무 분리	2.2.2. 직무분리	IAM	계정보안-IAM	Y
	11.2. 정보시스템 도입 및 개발 보안	11.2.1. 운영환경 이관	신규 도입·개발 또는 변경된 시스템을 운영환경으로 이관할 때는 통제된 절차를 따라야 하고, 실행코드는 시험 및 사용자 인수 절차에 따라 실행되어야 한다.		2.8.6 운영환경 이관	EKS		Y
	11.3. 시스템 및 서비스 운영관리	11.3.1. 시간 동기화	로그 및 접속기록의 정확성을 보장하고 신뢰성 있는 로그분석을 위하여 관련 정보시스템의 시각을 표준시각으로 동기화하고 주기적으로 관리하여야 한다.		2.9.6 시간 동기화	S3, CloudTrail, CloudWatch	클라우드보안-CloudTrail, CloudWatch	Y
	11.4. 사고 예방 및 대응	11.4.1. 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.		2.11.2 취약점 점검 및 조치	Config, systems manager, Inspector	클라우드보안-Config, systems manager, Inspector	Y
12. 개인정보 처리 단계별 요구사항	12.1. 개인정보 보유 및 이용 시 보호조치	12.1.1. 개인정보 표시제한 및 이용 시 보호조치	개인정보의 조회 및 출력(인쇄, 화면표시, 파일생성 등) 시 용도를 특정하고 용도에 따라 출력 항목 최소화, 개인정보 표시제한, 출력물 보호조치 등을 수행하여야 한다. 또한 빅데이터 분석, 테스트 등 데이터 처리 과정에서 개인정보가 과도하게 이용되지 않도록 업무상 반드시 필요하지 않은 개인정보는 삭제하거나 또는 식별할 수 없도록 조치하여야 한다.		3.2.3 개인정보 표시제한 및 이용 시 보호조치	RDS-가명처리	RDS-가명처리	Y
		12.1.2. 개인정보 목적 외 이용 및 제공	개인정보는 수집 시의 정보주체(이용자)에게 고지·동의를 받은 목적 또는 법령에 근거한 범위 내에서만 이용 또는 제공하여야 하며, 이를 초과하여 이용·제공하려는 때에는 정보주체(이용자)의 추가 동의를 받거나 관계 법령에 따른 적법한 경우인지 확인하고 적절한 보호대책을 수립·이행하여야 한다		3.2.5 개인정보 목적 외 이용 및 제공	RDS-가명처리	RDS-가명처리	Y
	12.2. 개인정보 파기 시 보호조치	12.2.1. 처리목적 달성 후 보유 시 조치	개인정보의 보유기간 경과 또는 처리목적 달성 후에도 관련 법령 등에 따라 파기하지 아니하고 보존하는 경우에는 해당 목적에 필요한 최소한의 항목으로 제한하고 다른 개인정보와 분리하여 저장·관리하여야 한다.		3.4.2 처리목적 달성 후 보유 시 조치	RDS-가명처리	RDS-가명처리	Y