항목
Cloud Impact Assessment CheckList(Iaa
Cloud Impact Assessment CheckList(Iaa
Cloud Impact Assessment CheckList(Iaa

내용	배포일
- Eliminate Duplicate Checklists/Traces	6/4/2021
- Change checklist division - Added checklist item (related to ACS, Well-known port) - Removal of duplicate checklists/evidences - Added examples related to infrastructure/network traces	9/3/2021
- added approval person for data change, in-house I/F management and operation - Addition of access/change history management items for each service - Deleted items related to DB/server access control solution (duplicate items in personal information impact assessment) - Update ACL items - Added web page security enhancement item - Added internal traffic log item - Delete duplicate check item	7/29/2022

변경자
송기봉
송기봉
송기봉

[Implementation inspector Info.]

Implementation inspector(name/ title)
Department name
Checklist creation date
Implementation inspection approval manager (name/ title)

[System/Service Info.]

System/Service Name
System/Service Summary
Type of cloud service
CSP Info.

[System/Service Importance Rating self-evaluation]

Importance score (Confidentiality score + Integrity score + Availability score)

Confidentiality	Very Important(3)	when the total score of data in Informatior
	Important(2)	when the total score of data in Informatior
	Normal(1)	when the total score of data in Informatior
Integrity	Very Important(3)	when data in the system is tampered with, and affects other systems by interworking Ex) A system with a function to pass data
	Important(2)	when data in the system is tampered with, and is affected by other systems by interw Ex) A system that receives data from anoth
	Normal(1)	when data in the system is tampered with,
Availability	Very Important(3)	when system is failure or intrusion, if there
	Important(2)	when system is failure or intrusion, there is Ex) Admin system (there is no problem in
	Normal(1)	when system is failure or intrusion, some w Ex) In the event of a customer call center s

[Whether to fill out a checklist item]

1. Information self-evaluation
2. System Security Checklist
3. Cloud Design Security Checklist
4. Infra Architecture
5. Data(Service) Flowchart
6. IAM List
7. IP List(CIDR)
8. Security Group
9. Network ACL

ex) OOO / IT Manager
ex) Please enter the department name on the EP.
ex) YYYY.MM.DD
ex) OOO / Team leader

ex) cyber security server
ex) IaaS, SaaS, PaaS etc.
ex) GCP, AWS, Azure etc.

Score 8

ı Self-evaluation (cloud impact evaluation items) is 11 or more
ı Self-evaluation (cloud impact evaluation items) is 7 or more
ı Self-evaluation (cloud impact evaluation items) is less than 7 points
it is a system that causes problems in work or services with other systems to another system
it is a system that causes a failure in work or service orking with other systems ıer system
causes disruption to work or service
is no alternative system, the service is stopped
no alternative system, but some services continue the actual service, or there may be some influence)
ork or service is continued due to an alternative system system failure, some customer services can be performed through website chat consultation

Ex) O / X (In case of non-written, write reason)
Ex) O / X (In case of non-written, write reason)
Ex) O / X (In case of non-written, write reason)
Ex) O / X (In case of non-written, write reason)
Ex) O / X (In case of non-written, write reason)
Ex) O / X (In case of non-written, write reason)
Ex) O / X (In case of non-written, write reason)
Ex) O / X (In case of non-written, write reason)
Ex) O / X (In case of non-written, write reason)

[1. Information Self-evaluation]

Writing Guide

1. After identifying the data to be used by sending it to the external cloud, evaluate the importance ratir

***Same data table to personal information impact assessment. (Added only ratings evaluation)**

Secret Classification Criteria

Personal Infor

Category	Contents
Exclusive (1~5)	As a result (information) completed by LGE's efforts, information that has secured the know-ho exclusive right of the company
Risk (1~5)	Sensitive information that can lead to business setbacks, legal litigation, and damage to corpor image if leaked internally or externally
Economical (1~5)	Information that can cause direct or indirect economic loss or provide economic benefits to oth companies if leaked internally or externally
Criteria	Confidential Level (Total more than 11 points)
	Internal Use Only Level (Total more than 7 points)
	Normal Level (Total less than 7 points)

Confiden

Internal U Only

Description	Storage Purpose	Exclusive (1~5)	Risk (1~5)	Economical (1~5)
예) global repair data	for deep learning	2	4	2

ıg and write the rationale

mation Classification Criteria

Category		Define
tial	Grade 1	Sensitive personal information, financial information, or identification information given to distinguish a unique characteristic of an individual
Use	Grade 2	Important information that can identify an individual with two or more combinations of personal information other than the company
	Grade 3	Information that is difficult to identify or specify even with a combination of three or more information and information with low risk

Total	Field Review Opinion	Stored Data	Stored data Type	Value (example)
8	write reason	Region Name	string	KR, US, COM, EU
		Parts Desc5	string	

Stored data Description
country code

Collection Scenario (Time of Transmission) (UX)	Collection path (From → To)	M/O
	GSFS → GERP → EDW (LGE System) -> Intellytics	M
	GSFS → GERP → EDW (LGE System) -> Intellytics	M

Storage Location	How to save	Data Encryption
AWS S3	DB	N
AWS S3	DB	N

[2. System Security Checklist]

Writing Guide

1. After confirming whether the evaluat

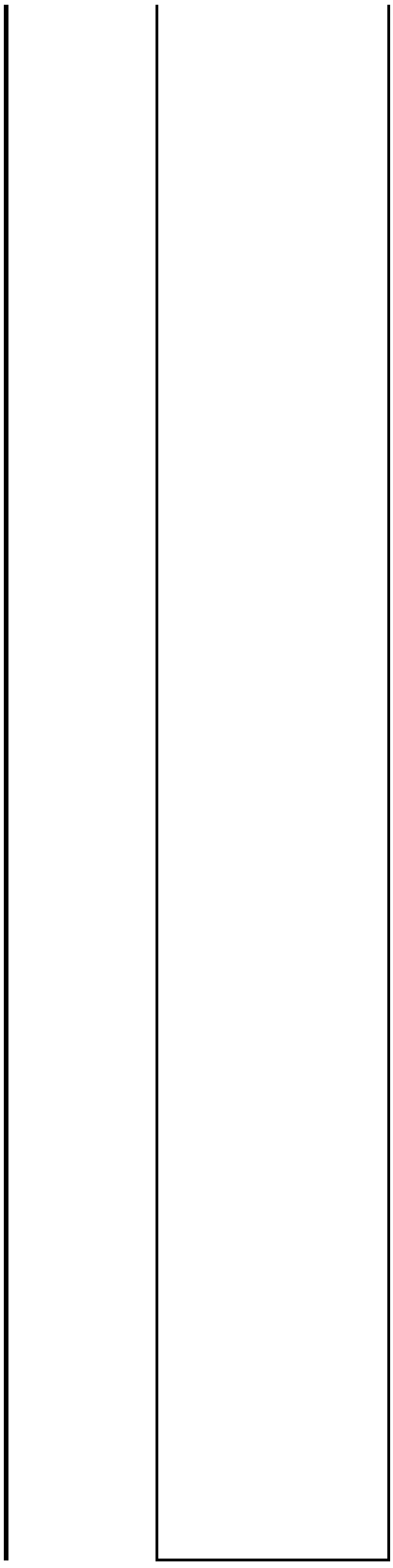
2. If answer (G) is YES, after you are che

3. If the answer (G) is No, N/A, write th

※ In the stage of pre-impact assessmer

Category	Evaluation Item
	MFA (Multi-Factor Authentication) applied

Access Control and Account Management	**Account Management**	




Key 관리
Key Management
데이터 정보 유출 방지
Data Breach Prevention
데이터 흐름 관리
Data flow Management
Database

	데이터 보안 **Sata Security**
	데이터 파기 **Data Destruction**
	사내, 클라우드간 인터페이스 **Between on-premises and Cloud Interface**

On-premises /Cloud Protection	
	네트워크 관리 **Network Management**

tion content/question is applied or not, select the answer (G) (Yes, No, N/A)
ck evidence contents(J), capture it in the remark(H).
e reason in the remark (H)
nt, write "I will apply" to the remark (H).

Evaluation Content	Importance
클라우드 생성 계정, 인프라 관리자 계정은 반드시 MFA를 적용한다. MFA must be applied to cloud-created accounts and infrastructure administrator accounts.	High
역할 별 사용자 계정 분리 검토를 해야 한다. Evaluate if user accounts are separated by role	High

클라우드 콘솔 이용 시 개인 업무메일을 이용하며, 1인 1계정을 생성한다. When using cloud console, personal company mail is used and one account is created per person..	High
사용자 및 관리자 계정 관리 방안을 수립해야 한다. User and Admin Account Management Policy	High
루트(root) 계정 사용자 엑세스 키는 삭제한다. Delete the root account user access key.	High

클라우드 계정 생성 적합성을 확인해야 한다 Cloud-generated account suitability	Medium
루트(root) 계정 사용자 엑세스 키는 삭제한다. Delete the root account user access key.	High
권한 할당 정책을 수립해야 한다. Accountability Policy	High
공용계정 (서비스/인프라 운영 계정 등)으로 SSH 접속 시 반드시 ACS를 통하여 접속한다. When connecting to SSH with a public account (service/infrastructure operation account, etc.), be sure to connect through ACS.	High

Key 관리 정책 및 기준 수립해야 한다 Review key management policies and standards	High
자원 접근 Key 변경에 대한 서비스 영향도 검토를 해야 한다. Assess the impact of changing access keys to assets in the service	High
데이터(WAS, DB)에 대한 부적절한 행위에 대해 통제 및 감사를 할 수 있어야 한다. It should be possible to control and audit inappropriate actions on data (WAS, DB).	High
시스템 및 인프라 간 데이터의 이동, 복제 단위로 관리 되어야 하며 직·간접적인 모든 데이터 흐름을 포함하며 등록 및 변경 시 업무혁신담당의 승인을 득해야 한다. The movement of data between systems and infrastructure must be managed on a per-replication basis, and must be approved by the Business Process Innovation Division for registration and change. (Department in charge : IT Infra Team)	High

자사 경영정보 및 1등급 정보의 저장영역은 자사 독립적(물리적 및 논리적)으로 제공해야 하며 타 부서간의 승인 없이 저장영역을 사용 및 재사용을 허용할 수 없다. ※ 경영정보 및 1등급 정보의 저장시에는 무조건 자사의 물리적으로 독립된 형태로 제공해야 합니다. 이 부분이 제공되지 않는 형태의 클라우드는 모든 항목에 평가를 PASS 하더라도 허용할 수 없습니다. The storage area of the company's management information and first-class information must be provided independently (physically and logically), and use and reuse of the storage area cannot be allowed without approval between other departments.	High
클라우드에 저장되는 데이터는 완전한 삭제를 위해 암호화하여 삭제하며, 이미 암호화되어 있는 경우에도 동일하게 진행한다. Data stored in the cloud is encrypted and deleted for complete deletion, and the same procedure is performed even if it is already encrypted.	High
사내 시스템과 외부 클라우드는 반드시 암호화 통신을 한다. The internal system and the external cloud must communicate encrypted.	High
사내 I/F관리 및 운영은 클라우드 시스템 운영부서에서 하며 I/F의 신규, 변경, 삭제, 통제는 업무혁신담당과 정보보호담당의 승인을 득해야 한다. In-company I/F management and operation are managed by the cloud system operation department, and new, changed, deleted, and controlled I/Fs must be approved by the IT department and Security department. (Department in charge : IT Infra Team, Cyber Securit Team)	High

사내 I/F를 받은 외부 클라우드의 스토리지 및 DB는 중요도에 따라 암호화 되어야 한다. Storage and DB of external cloud received in-company I/F should be encrypted according to importance.	High
사내망과 연동된 외부 클라우드의 IP 발급 및 네트워크 신규, 변경, 삭제는 업무력신담당의 승인을 득해야 한다. IP issuance of external cloud linked with the internal network, and network is new, change, or delete, approval must be obtained from Business Process Innovation Division (Department in charge : IT Infra Team)	High
전용선 및 IPsec-VPN 등 강화된 보안이 적용된 연결만 허용한다. Only connections with enhanced security such as leased lines and IPsec-VPN are allowed.	High

Question	Answer
클라우드 계정에 MFA 정책을 강제화 하고 있는가? Are you enforcing MFA policies on cloud accounts?	
클라우드 생성 계정에 대한 권한 분리를 하고 있는가?	

클라우드 콘솔 접근 시 사내 업무메일 계정을 이용하여 계정을 생성하고 있으며, 적절하게 사용하고 있는가? When accessing the cloud console, is the account created using work email ? and is it being used appropriately?	
클라우드 생성 계정에 대한 관리 대책이 존재하는가? Are there any policies regarding accounts created in the Cloud?	
루트(root) 계정 사용자 엑세스 키는 삭제하고, 관리자 계정을 생성하여 클라우드 리소스를 추가/수정을 하고 있는가? Have you deleted the root account user access key? Are you adding/modifying cloud resources by an administrator account?	

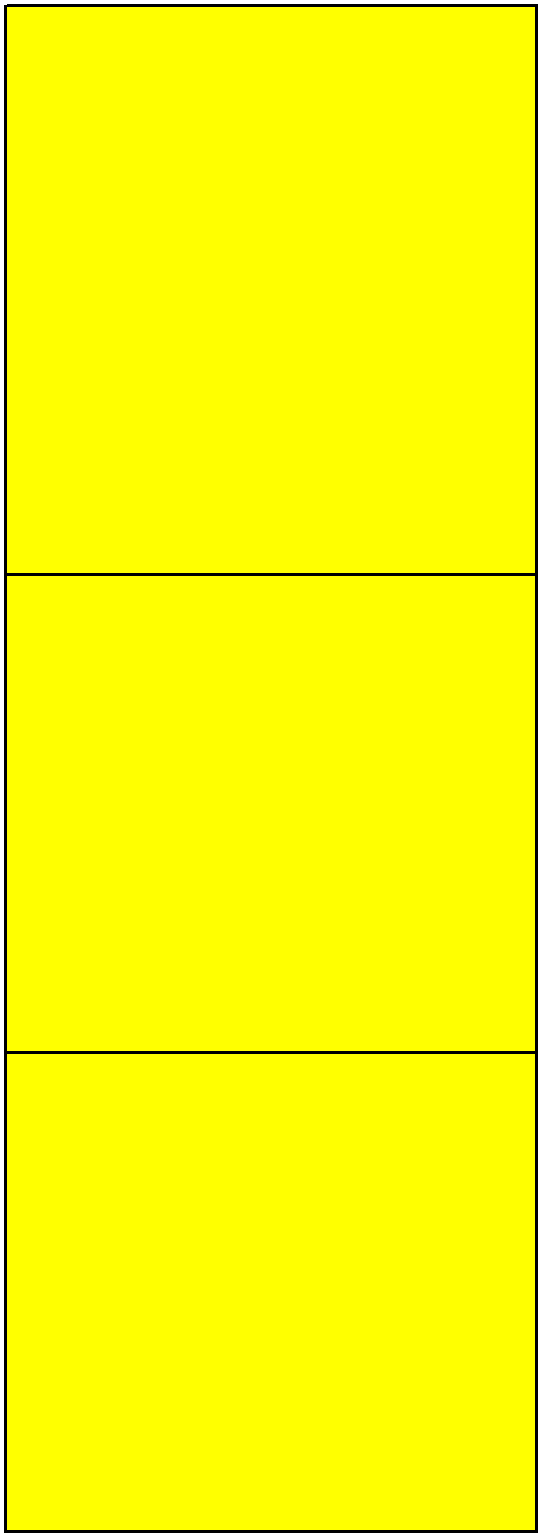
각 업무/부서 내 서비스 계정 생성시 Alias 메일을 이용하여 계정을 생성하였는가? 예) securityTeam@lge.com When creating work / department service accounts, was the account created via email Alias? ex) securityTeam@lge.com	
루트(root) 계정 사용자 엑세스 키는 삭제하고, 관리자 계정을 생성하여 클라우드 리소스를 추가/수정을 하고 있는가? Have you deleted the root account user access key? Are you adding/modifying cloud resources by an administrator account?	
클라우드 생성에 계정에 대한 그룹(Group) 별 권한 관리를 하는가? Is there a group control policy for accounts created in Cloud?	
공용계정으로 SSH 접속 시 ACS를 사용하는가? Do you use ACS for SSH access with a public account? ACS Guide : http://space.lge.com/collpack/collaboration/board/boardItem/readBoardItemLinkView.do?boardId=200147570164&itemId=200152880582&docPopup=true	

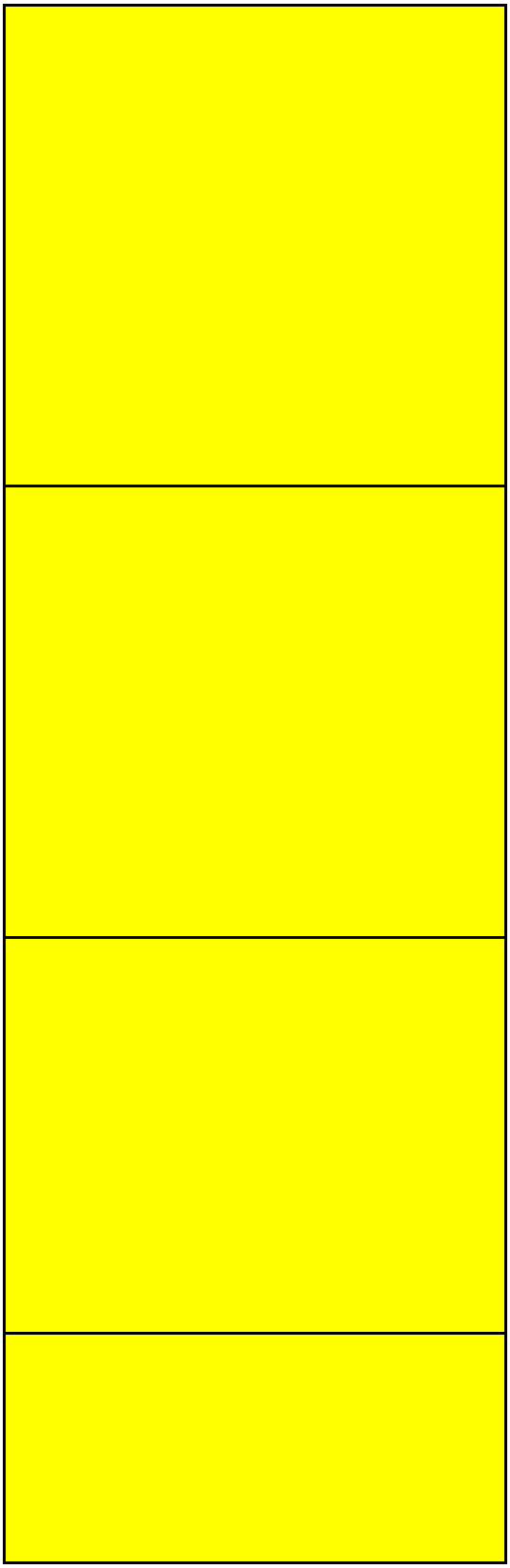
클라우드 구축 간 KEY에 대한 등록 및 관리를 수행하고 있으며, 관리는 정책에 따르고 있는가? Is there key registration and management of cloud deployments, so does this management follow the policy?	
클라우드에서 사용하는 키(Key)에 대한 사용 내역을 명확하게 파악하고 있는가? Is there clear control over key usages that are used in the Cloud?	
데이터(WAS, DB)에 대한 부적절한 행위에 대해서 통제할 수 있도록 감사로그를 기록하고 있는가? Do audit logs recorded to control inappropriate actions on data (WAS, DB)?	
데이터 이동, 복제 간에 작업이 필요할 경우 작업을 승인받고 있는가? If an operation is required between data movement and replication, does it request to approve?	

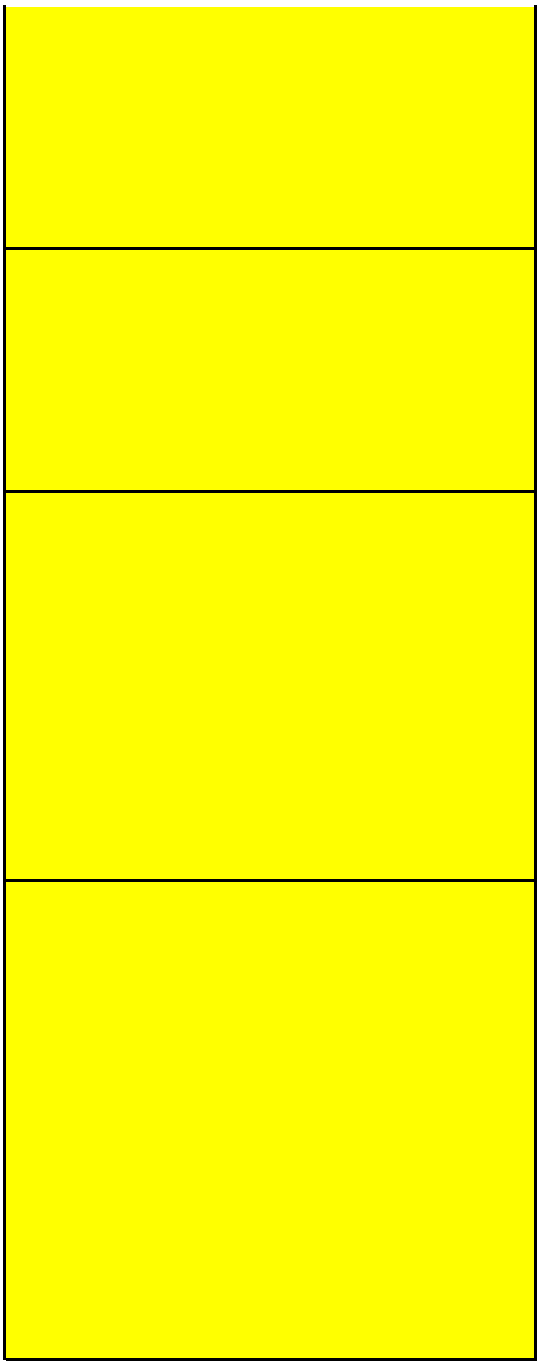
자사 경영정보 및 1등급 정보의 저장영역은 논리적으로 독립된 공간을 제공받아 구성하고 있는가? Are the storage areas of the company's management information and first-class information provided with a logically independent space?	
클라우드에 저장되는 데이터의 파기는 완전삭제 되고 있는가? When data stored in the cloud is destroyed, is it completely deleted?	
사내에서 연결되는 시스템과 대외로 서비스하는 클라우드는 암호화 통신을 하도록 하고 있는가? Are systems connected within company and cloud service using encrypted communication?	
클라우드 시스템의 신규, 변경, 삭제 작업 내역을 기록하고 있으며, 작업을 승인 받고 있는가? Is the history of new, changed, or deleted cloud systems being recorded, and does it request to approve?	

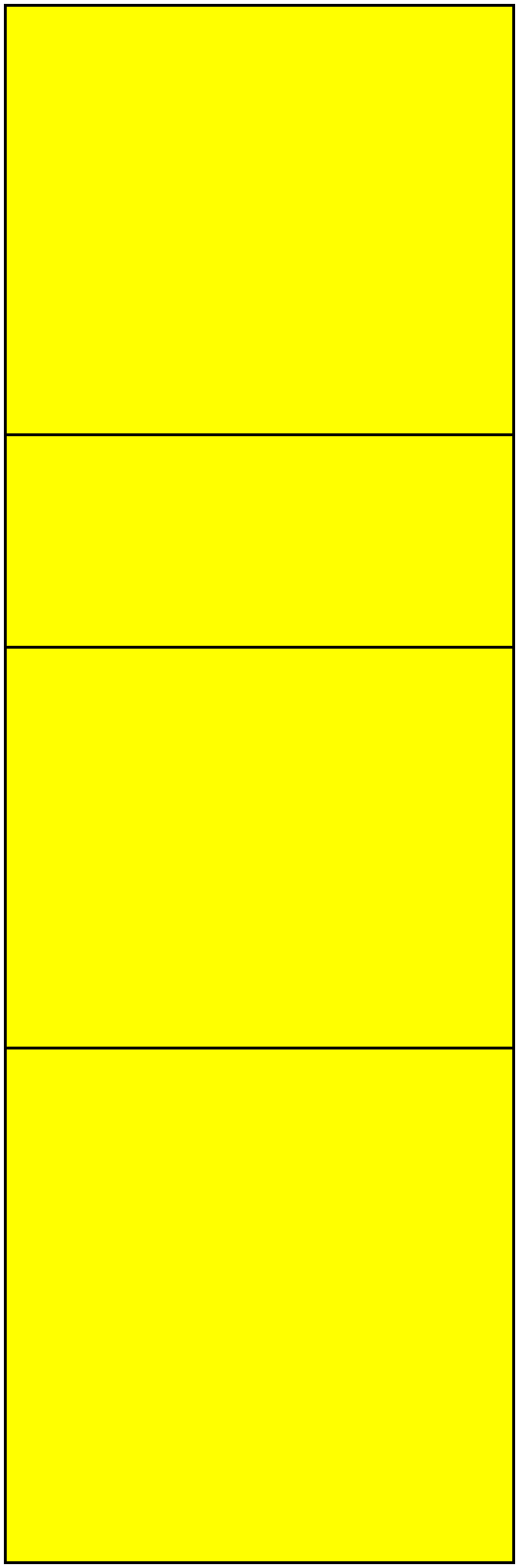
중요한 데이터를 보관하고 있는 클라우드 스토리지/DB는 암호화를 적용하고 있는가? Is encryption applied to cloud storage/DB storing sensitive data?	
사내망과 연동된 외부 클라우드의 네트워크 신규/변경/삭제 작업 시에 승인을 받고 있는가? when network of external cloud linked with the internal network is new, changed, or deleted, and does it request to approve?	
네트워크에 접근간IP-Sec-VPN 기술이 적용된 보안 연결을 사용하고 있는가? Are you using a secure connection with IP-Sec-VPN technology to access in-company network?	

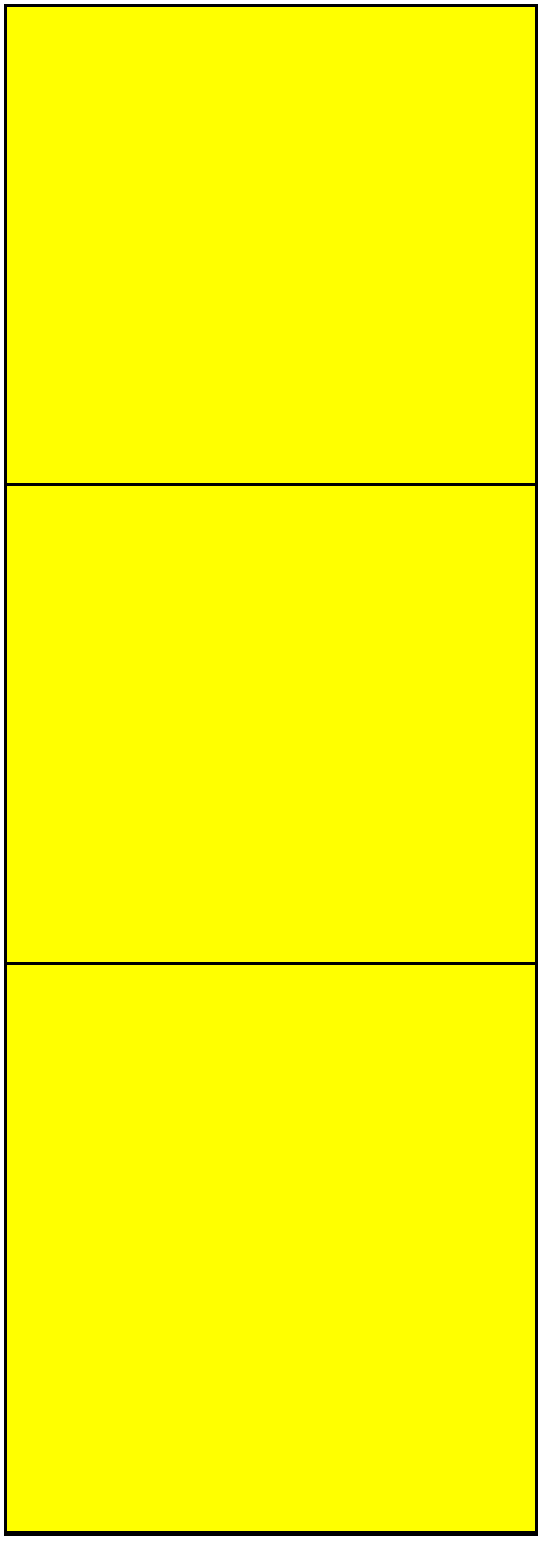
Fill out the checklist
Remark











Evaluation Criteria
(취약점 설명) 사용자 이름과 암호 외에 보안을 강화할 수 있는 방법으로 MFA를 활성화 하면 계정 로그인 간 사용자 이름/암호 뿐만 아니라 MFA 디바이스 인증을 통해 계정보안을 향상해야함 **(양호)** 계정 및 IAM을 통한 사용자 계정 로그인시 MFA가 활성화 되어 있을 경우 **(취약)** 계정 및 IAM 사용자 계정 로그인 시 MFA가 비활성화되어 있을 경우 (Vulnerability Description) Enabling MFA as a way to enhance security other than username and password should improve account security through MFA device authentication as well as username/password between account logins (Good) When MFA is enabled when logging in to an account and a user account through IAM (vulnerable) account and IAM user account login with MFA disabled * MFA(Multi-Factor Authentication) * IAM(Identify And Management)
(취약점 설명) 해당 항목은 생성된 계정에 대한 권한 분리를 하고 있어, Root 계정과 일반 계정의 권한 분리를 통해 비인가된 행위를 막고 인가 사용자에 대한 지속적인 관리를 통해 보안성을 향상해야 함 **(양호)** IAM을 통해 최소한의 인원에게만 권한을 주고, 권한자에게는 과도한 권한이 없는 경우 **(취약)** IAM을 통해 불필요한 인원이 포함되어 있으며, 권한 분류가 적절하게 됮 ㅣ않을 경우 (Vulnerability Description) This item separates the privileges of the created accounts, so it is necessary to prevent unauthorized actions through the separation of privileges between the root account and general accounts, and improve security through continuous management of authorized users. (Good) If permission is given to only the minimum Head Count through IAM, and the authority does not have excessive permission (Vulnerable) When unnecessary Head Count is included through IAM and permission classification is not properly done

(취약점 설명)
클라우드 콘솔 접근 시 루트 계정이나 공용 계정으로 접근하지 않고, 접근자별로 사내 메일 계정명으로 생성하고 접근하여야 계정별로 권한 분리가 설정이 용이하고, 침해사고 발생시 분석이 용이함

(양호) 클라우드 콘솔 접근 계정 목록내 "업무 계정"목록을 구성하고 있고,
계정명(OOO@lge.com)을 업무 메일로 사용하여 사용자를 식별할 수 있는 경우
(취약) 클라우드 콘솔 접근 계정 목록 내 공용 계정 및 루트 계정을 사용하고 있는 경우

(Vulnerability Description)
When accessing the cloud console, do not access the root account or public account, but create and access the in-house mail account name for each accessor, so it is easy to set the separation of privileges for each account and easy analysis in case of a breach

(Good) If the "work account" list in the cloud console access account list is configured and the user can be identified by using the account name (OOO@lge.com) as the work email
(Vulnerable) If you are using a public account and a root account in the list of cloud console access accounts

(취약점 설명)
해당 항목은 생성된 계정에 대한 권한 분리를 하고 있어, Root 계정과 일반 계정의 권한 분리를 통해 비인가된 행위를 막고 인가 사용자에 대한 지속적인 관리를 통해 보안성을 향상해야 함

(양호) 클라우드 생성 계정에 대해 적절하게 관리하고 있는 경우
(취약) 클라우드 생성 계정에 대한 관리 방안이 없는 경우

(Vulnerability Description)
This item separates the privileges of the created accounts, so it is necessary to prevent unauthorized actions through the separation of privileges between the root account and general accounts, and improve security through continuous management of authorized users.

(Good) Proper management of cloud-created accounts
(Vulnerable) If there is no management plan for cloud-created accounts

(취약점 설명)
root 계정 정보 유출 시 외부 클라우드의 시스템에 영향이 크기때문에 관리자 권한을 갖는 계정을 생성하고 해당 계정으로 클라우드 리소스를 운영해야함

(양호) Root 계정의 사용자 엑세스 키를 삭제하고, 다른 계정에 관리자 권한을 부여하여 클라우드 리소스 추가/수정을 진행하는 경우
(취약) Root 계정을 통해서 클라우드 리소스 추가/수정을 진행하는 경우

(Vulnerability Description)
When the root account information is leaked, the external cloud system is greatly affected, so you need to create an account with administrator privileges and operate cloud resources with that account.

(Good) When adding/modifying cloud resources by deleting the user access key of the root account and granting administrator rights to another account
(Vulnerable) When adding/modifying cloud resources through the root account

(취약점 설명)
해당 항목은 생성된 계정에 대한 소유권이 개인에게 종속되어 있을 경우, 담당자의 휴가 및 퇴사, 업무 변경 등과 같은 상황에도 계정 관리가 가능하지 않음으로, Alias 메일을 기준으로 계정을 생성해야함

(양호) 업무/부서별 계정을 가지고 있는 경우이거나 비슷한 형태로 계정을 생성하여 관리하고 있는 경우
(취약) 업무/부서별 관리 계정을 가지고 있지 않은 경우

(Vulnerability Description)
If the ownership of the created account is subordinated to the individual, account management is not possible even in situations such as vacation, resignation, or job change of the person in charge, so the account must be created based on the Alias mail.

(Good) If you have an account for each job/department or if you create and manage an account in a similar format

(취약점 설명)
root 계정 정보 유출 시 외부 클라우드의 시스템에 영향이 크기때문에 관리자 권한을 갖는 계정을 생성하고 해당 계정으로 클라우드 리소스를 운영해야함

(양호) Root 계정의 사용자 엑세스 키를 삭제하고, 다른 계정에 관리자 권한을 부여하여 클라우드 리소스 추가/수정을 진행하는 경우
(취약) Root 계정을 통해서 클라우드 리소스 추가/수정을 진행하는 경우

(Vulnerability Description)
When the root account information is leaked, the external cloud system is greatly affected, so you need to create an account with administrator privileges and operate cloud resources with that account.

(Good) When adding/modifying cloud resources by deleting the user access key of the root account and granting administrator rights to another account
(Vulnerable) When adding/modifying cloud resources through the root account

(취약점 설명)
해당 항목은 생성된 계정에 대한 권한 분리를 하고 있으며, Group 별 권한 분리를 통해 권한에 대한 접근 제어로 보안성을 향상해야 함

(양호) 클라우드 생성 계정에 대한 Group 별 권한 분리를 하고 잇는 경우
(취약) 클라우드 생성 계정에 대한 Group별 권한 분리를 하지 않는 경우

(Vulnerability Description)
For this item, the privileges of the created account are separated, and security should be improved by controlling access to privileges through the separation of privileges by group.

(Good) In case of separating permissions by group for cloud-created accounts
(Vulnerable) If you do not segregate permissions by group for cloud-created accounts

(취약점 설명)
공용계정을 통한 SSH 접속 시 누가의 접속 이력을 CSP Audtot Log에서 확인 하기 어려움.

(양호) ACS시스템을 통해 SSH를 접속하여 사용함.
(취약) ACS시스템을 통해 SSH를 접속하여 사용하지 않음.

(Vulnerability Description)
When accessing SSH through a public account, it is difficult to check Nougat's access history in

(취약점 설명)
클라우드의에서 사용하는 각종 Key에 대한 정의가 되어 있으며, Key에 대한 적절한 관리와 현황을 파악하고 있어, Key 노출 시 위험을 최소화 할 수 있어야 함

(양호) 클라우드에서 사용하는 Key관리를 정책이 있거나 Key관리를 적절하게 하고 있는 경우
(취약) 클라우드에서 사용하는 Key 관리를 하지 않는 경우

'(Vulnerability Description)

(취약점 설명)
클라우드의에서 사용하는 각종 Key에 대한 정의가 되어 있으며, Key에 대한 적절한 관리와 현황을 파악하고 있어, Key 노출 시 위험을 최소화 할 수 있어야 함

(양호) 클라우드에서 사용하는 Key가 현황을 적절하게 파악하고 있어, 임의의 키 번경에 따른 영향도에 대한 검토가 가능한 경우
(취약) 클라우드에서 사용하는 Key 현황을 적절하게 파악하지 않을 경우

(취약점 설명)
데이터에 대한 접근 통제와 접근자에 대한 감사로그를 기록하고 있으며, 데이터 유출과 같은 사고 발생간에 로그 분석이 용이하도록 구성할 수 있어야 함

(양호) 스토리지/DB에 대한 액세스 로그를 활성화하고 있는 경우
(취약) 스토리지/DB에 대한 로깅을 기록하지 않을 경우

(Vulnerability Description)
It records access control to data and audit logs for accessors, and it should be possible to configure log analysis easily between incidents such as data leakage.

(Good) If you are enabling log access to storage/DB
(Vulnerable) If you do not record logging for storage/DB

(취약점 설명)
데이터 이동, 복제 간에 작업이 필요할 경우 승인 절차를 기록하고 있어, 결제 절차를 통해 승인된 작업만 수행할 수 있어야 함

(양호) 데이터 이동 간에 승인 절차를 구성하고 있으며, 승인된 작업만 수행할 경우
(취약) 데이터 이동 간에 승인 절차가 구성되지 않을 경우

(Vulnerability Description)
If work is required between data movement and replication, the approval procedure is recorded, so only the work approved through the payment procedure should be able to be performed

(Good) When an approved procedure is configured between data movement and only approved tasks are performed
(Vulnerable) When an authorization procedure is not configured between data movements

(취약점 설명)
데이터에 대한 경영정보 및 1등급 정보의 저장영역에 대해서 독립된 형태의 데이터 공간 확보를 통해 데이터의 안전한 보관을 할 수 있어야 함

(양호) 데이터 저장공간 내 경영 정보 및 1등급 외 정보를 저장할 경우
(취약) 데이터 저장공간 내 경영 정보 및 1등급 저장 영역을 저장할 경우

(Vulnerability Description)
It should be possible to safely store data by securing an independent form of data space for the storage area of management information and first-class information for data.

(Good) When storing management information and information other than Level 1 in the data storage space
(Vulnerable) When storing management information and first-class storage area in data storage space

(취약점 설명)
클라우드에 저장되는 데이터의 삭제는 복구가 가능하지 않도록 완전한 삭제를 통해 삭제 되며, 이미 암호화 되어 있는 경우에도 동일하게 진행되어 안전한 데이터 파기가 가능해야 한다.

(양호) 데이터 삭제시 완전한 삭제(Wiping) 하는 경우
(취약) 데이터 삭제시 완전한 삭제(Wiping)를 지원하지 않는 경우

(취약점 설명)
사내시스템 <> 대외 클라우드 간 서비스하는 통신 구간에 대해서는 전송구간 암호화를 전용하여 네트워크 상에 평문으로 노출되지 않아야 함

(양호) 전송 구간 암호화(HTTPS Only)가 적용되어 있을 경우
(취약) 전송 구간에 대한 암호화가 적용되지 않을 경우

(Vulnerability Description)
For communication section between internal system <> external cloud service, transmission section encryption is dedicated and should not be exposed as plaintext on the network.

(Good) When transmission section encryption (HTTPS Only) is applied
(Vulnerable) When encryption for the transmission section is not applied

(취약점 설명)
운영기 I/F 관리는 적절한 의사결정하에 신규, 변경, 삭제가 진행되도록 해야 하며 I/F 작업에 대한 결제 절차를 통해 승인된 작업만 수행할 수 있어야 함

(양호) 운영기 인프라의 신규, 변경, 삭제 작업 간에 결제 절차를 구성하여 승인된 작업만 수행할 경우
(취약) 운영기 인프라에 대한 승인 절차가 구성되지 않을 경우
(N/A) 운영기 시스템이 아닌 경우

(Vulnerability Description)
Operational I/F management should allow new, changed, and deleted operations to proceed under appropriate decision-making, and only operations approved through the payment procedure for I/F operations should be able to be performed.

(Good) When only approved operations are performed by configuring a payment procedure between new, changed, and deleted operations of the operator infrastructure
(Vulnerable) If the approval procedure for the operator infrastructure is not configured

(취약점 설명)
사내 I/F를 받은 외부 클라우드의 스토리지 및 DB의 중요도를 확인하여 암호화를 실시하여야 한다. 암호화를 통해 데이터 보호 대책을 적용할 수 있어야 함

(양호) 클라우드 스토리지/DB의 암호화 설정을 적용한 경우
(취약) 클라우드 스토리지/DB에 암호화 설정을 적용하지 않은 경우
(N/A) 암호화 적용 대상 시스템이 아닌 경우

(Vulnerability Description)
Encryption should be performed by checking the importance of storage and DB in the external cloud that received in-house I/F. Encryption should be able to apply data protection measures

(Good) When encryption setting of cloud storage/DB is applied
(Vulnerable) When encryption settings are not applied to cloud storage/DB
(N/A) If it is not a system to which encryption is applied

(취약점 설명)
사내망과 연동된 외부 클라우드 IP 발급과 네트워크 신규/변경/삭제 작업이 필요할 경우 승인 절차를 기록하고 있어, 결제 절차를 통해 승인된 작업만 수행할 수 있어야 함

(양호) 네트워크 작업 간에 승인 절차를 구성하고 있으며, 승인된 작업만 수행할 경우
(취약) 네트워크 작업 간에 승인 절차가 구성되지 않을 경우

(Vulnerability Description)
When external cloud IP issuance and network new/change/delete operations linked to the internal network are required, the approval procedure is recorded, so only the operations approved through the payment procedure should be able to be performed

(Good) When an approval procedure is configured between network operations and only approved operations are performed
(vulnerable) when an authorization procedure is not configured between network operations

(취약점 설명)
네트워크 접근은 보안이 적용된 연결만 가능하도록 구성하고, 통신 구간에 대한 평문 노출이 가능하지 않도록 안전한 연결만을 제공해야 함

(양호) SSH, HTTPS, sFTP 등과 전송 구간 암호화 기술이 적용된 기술을 사용하거나, 별도의 전용 접근을 구성하여 인가된 사용자의 연결만 허용하는 경우
(취약) 보안 연결 기술을 적용하지 않았거나, 암호화 통신 이외의 평문 통신 기술 연결을 제공하는 경우

(Vulnerability Description)
Network access should be configured so that only a secure connection is possible, and only a secure connection should be provided so that plaintext exposure of the communication section is not possible.

(Good) When using SSH, HTTPS, sFTP, etc. with transmission section encryption technology, or configuring a separate dedicated access to allow only authorized users to connect
(vulnerable) If secure connection technology is not applied, or if plaintext communication technology connection other than encrypted communication is provided

Evidence Contents
#1. 클라우드 생성 계정, 인프라 관리자 계정 목록 #2. 각 사용자 계정에 대한 MFA 적용 내역 #1. List of Cloud Created Accounts and Infra Manager Accounts #2. List of MFA applied history for each user account

#1. 클라우드 콘솔 계정 목록 **(콘솔 계정 명 검토)** **#1. List of cloud console account** **(Review console account name)**	

#CSP내 Group 구성 내역 **Group configuration in CSP**	

#1. 데이터 파기 확인 확인서 혹은 그에 준하는 문서 (인증서, 감사리포트 등) ※ AWS, GCP, Azure 사용 시 별도 증적 필요 없음 #1. Confirmation of Data Destruction Confirmation Or equivalent documents (certificates, audit reports, etc.) ※ No need for separate evidence when using AWS, GCP, or Azure	
#1. I/F 신규/변경/삭제에 대한 승인을 득한 기안 (품의, CSR, 메일 증적 #1. A draft that has obtained approval for I/F new/modified/deleted (product, CSR, mail evidence)	

#1. 클라우드 인스턴스에서 스토리지/DB의 암호화 적용 화면 **- 필수 : 스토리지 암호화 적용 화면** **- 중요정보 : 오브젝트 암호화** **#1 Storage/DB encryption application screen in cloud instance** **- Required: Storage encryption application screen** **- Important information: object encryption**	
#1. 네트워크 작업에 대해 승인을 득한 기안 (품의, CSR, 메일 증적) **#1. A draft that has been approved for network work (approval, CSR, e-mail evidence)**	

[3. Cloud Design Security Checklist]

Writing Guide
1. Select the answer (H) after confirming the application/non-application according to the evaluation content/question (Yes, No, N/A)
2. If the answer (H) is Yes, check the evidence (K) and attach it to the remark (I)
3. If the answer (H) is No, N/A, write the reason in the remark (I)
※ In case of GCP, Security Group and Network ACL items are replaced with firewall
※ In the stage of the pre-confirmation of the impact assessment implementation, write "I will apply" to the remark (I).

Category	Evaluation Item	Evaluation Content	Importance
	IP configuration policy	생성되는 가상 네트워크에 임의 IP 할당을 방지 해야 한다. Prevent random IP configuration from the created virtual network	Medium
	Network Separation	사용 용도에 따른 가상 네트워크 망 분리를 해야 한다. Separation of virtual network according to type of use	High
		내,외부 하위 네트워크 (subnet) 분리를 해야 한다. Check need to separate internal and external subnets	High

Network		inblound 및 outbound 트래픽 제어를 해야 한다 inbound and outbound traffic control evaluation criteria	High
		IP 및 Port 기반 통제 구현을 해야 한다. Check for IP and Port based control	High
		네트워크 간 불필요한 연동을 최소화 해야 한다. Minimize unnecessary synchronization between networks	High
			High

	Traffic control		High
		외부 공격에 대한 대응 방안을 적용해야 한다. Evaluate defense methods against external attacks	High
			High
			High
		공인 IP 사용 및 외부 연동이 필요한 서버에 대한 보안 강화를 해야 한다. Security enhancement of servers using public IP and requiring external interoperability	High

	Traffic monitoring and Tracking Control	가상 네트워크에서 발생하는 네트워크 트래픽 모니터링 해야 한다. Network traffic monitoring that occurs on the virtual network	Medium
		클라우드 사업자 제공 서비스 사용 시 불필요한 외부 호출 최소화 해야 한다. Minimize Unnecessary Outside Calls When Using Cloud Provider Provided Services	Medium
		윈도우 접근 보안 강화 방안을 마련 해야한다. Strengthen Windows Access Security	High

VM Server	**Windows OS 보안**	윈도우 서버의 보안 강화 방안을 마련해야 한다. Should come up with a plan to strengthen the security of Windows Server.	High
	사용 이력 관리	운영자 및 사용자의 명령어 오남용에 대한 추적 관리를 해야 한다. Managing misuse of commands by operators and users	Medium
	접근제어	서버(VM)에 대한 접근 제어를 검토 해야 한다. Should review access control to the Server(VM).	High
	암호화 **Encryption**	데이터 중요도에 따른 암호화 적합성을 확인해야 한다. Adequacy of encryption according to data importance	High

Database	**접근제어** **Access Control**	DB에 대한 접근 제어를 검토 해야 한다. Should review access control to the DB.	High
	데이터 관리 **Data Management**	저장중인 데이터에 대한 접근 이력을 확인 해야 한다. Should check the access history to the data being saved	High
	암호화 **Encrpytion**	암호화 구현 방식 및 적합성 검토를 해야 한다. Review the encryption method and its compliance	High

스토리지 **Storage**	**스토리지 접근 제어** **Storage Access Control**	Object 스토리지의 외부 노출여부 검토를 해야 한다. Review if Object Storage is likely to leak to external media	High
		Object Storage 권한 부여 현황 확인 해야한다. Status of responsibilities given for Object Storage access	High
	스토리지 데이터 관리 **Storage Data Management**	저장중인 데이터에 대한 변경 이력 추적을 해야 한다. Track change history of stored data	Medium
		백업 주기 및 정책 수립해야 한다. Backup Interval and its policies	Medium

	로그 및 자원 관리 **Log and Resource Management**	로그 중앙 집중 관리 및 비인가된 데이터 접근 추적이 되어야 한다. Centralized log management and tracking of disallowed data access	Medium
		명시적 인프라 자원 관리가 되어야 한다. Transparent Infrastructure Resource Management	Medium
Infra	**인벤토리 관리** **Inventory Management**	변경되는 자원에 대한 실시간 추적 관리 방안을 검토해야 한다. Real-time tracking policy for resources that change	High
		비 인가된 보안 설정 변경 모니터링 및 추적 관리를 해야한다. Monitor and track changes to unauthorized security settings	High

	로그 및 자원 관리 **Log and Resource Management**	인프라 자원 사용량 모니터링을 할 수 있어야 한다. Infra resource usage monitoring	Medium
		명시적 인프라 자원 관리를 해야 한다. Transparent Infrastructure Resource Management	Medium

Question	Answer
임의 IP 할당을 하지 않도록 IP할당 정책을 통해 IP를 할당하고 있는가? Is IP being configured according to the configuration policy to avoid random assignment?	
운영, QA, PRD 등 환경에 따라 VPC를 분리 분리하고 있는가? Is VPC being separated according to operating environment, QA, PRD, etc.?	
Public 영역과 Private 영역의 IP 할당이 되도록 Network를 구성하고 있는가? Is the network being configured so that IP can be allocated to public and private domains?	

In/Out bound 트래픽을 통제하고 있고, 트래픽 통제 이력에 대해 관리하고 있는가 - Security Group, NACL, VPC방화벽, VPC Service Controls 설정 여부 Are you controlling in/out bound traffic and managing traffic control history? - Whether Security Group, NACL, VPC Firewall, or VPC Service Controls are set	
내/외부 트래픽에 대한 IP와 Port 기반의 통제가 구축되어 있는가? Is there a control for internal / external traffic based on IP and Port?	
네트워크 내 불필요한 연동이 최소화 되어 있는가? Are unnecessary synchronizations between networks minimized?	
Web Server 구성 시 SSRF(Server-side request forgery) 취약점 대응 하였는가? - WEB Backend Sever 인경우 WAF 적용 - WAF설정에 PUT Deny 설정 필수 - AWS EC2를 사용하는경우 IMDSv2 사용 - GCP 사용 시 "N/A" Did you respond to the SSRF (Server-side request forgery) vulnerability when configuring the Web Server? - In case of WEB Backend Server, WAF is applied - PUT Deny setting required for WAF setting - If using AWS EC2, use IMDSv2 - "N/A" when using GCP	

시스템 내 웹페이지를 제공하는 경우 HTTPS를 적용 하였는가? - 시스템 내 웹페이지를 제공하지 않는 경우 "N/A" Using HTTPS when providing a web page within the system? - "N/A" if the system does not provide a web page	
Well-Known Port 사용 시 Port를 변경/제한하여 사용하는가? When using a Well-Known Port, do you change/restrict the port?	
외부 및 타 시스템 연동 시 적절한 암호화 통신을 적용하여 통신을 하고 있는가? - 외부 및 타 시스템과 연동 사항이 없는 경우 N/A When interworking with external and other systems, are you communicating by applying appropriate encryption communication? - N/A when there is no connection with external or other systems	
클라우드를 구성한 네트워크 내 WAF와 IPS 또는 웹 방화벽이 적용되어 있는가? Are WAF and IPS or web firewall applied in the network that constitutes the cloud?	
외부 연동이 필요한 서버의 공인 IP 사용에 대한 명확한 Src/Dest 에대한 정의가 되어 있는가? Is there a clear definition of Src / Dest for public IP use by servers that need external interoperability?	

네트워크에서 발생하는 트래픽에 대한 Log 설정 및 모니터링을 하고 있는가? Is monitoring and configuration of the log related to traffic occurring on the network being performed?	
클라우드 제공 서비스 이용 시 불필요한 외부 연계에 대한 검토를 수행하였는가? Has it been analyzed if there are unnecessary connections to the external environment when using Cloud services?	
윈도우 서버의 원격 접근을 위한 RDP 사용 및 보안 강화 방안이 있는가? Is there an RDP usage and security enforcement policy for remote access to Windows Server? - "N/A" when Windows OS is not used	

윈도우 서버에 대해 백신을 설치 하였는가? - 윈도우OS 미사용 시 "N/A Have you installed antivirus for Windows Server? - "N/A" when Windows OS is not used	
클라우드 서버 운영상 요청하는 명령어에 대한 기록을 기록하고 있는가? Is there a record for the requested commands on the server(VM)?	
서버(VM)에 대한 접근 제어(IP기반 접근제어, 권한기반 접근제어) 를 하고 있는가? Are you controlling access(IP based access control, authorized based access control) to the Server(VM)?	
DBMS에서 데이터 중요도에 데이터를 검토하였으며, 이에 따라 데이터 암호화를 하고 있는가? The levels of importance of data in DBMS were evaluated, so that encryption occurs based on it?	

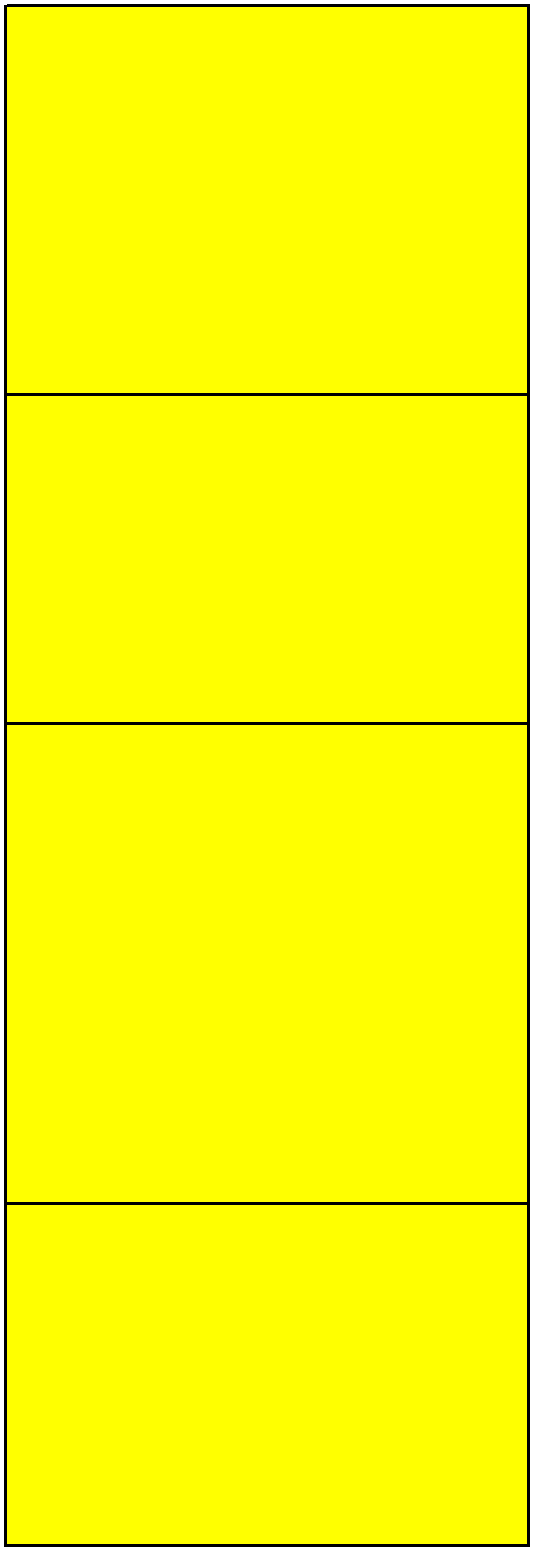
DB 서버에 대한 접근 제어(IP기반 접근제어, 권한기반 접근제어) 를 하고 있는가? Are you controlling access(IP based access control, authorized based access control) to the DB service?	
데이터 베이스에 대한 적절한 인가자의 접근 및 Query 요청 이력을 관리하고 있는가? Is there a control of the history of queries requested as well as user access that can access the database?	
안전한 데이터 보관을 위해 스토리지에 대한 암호화를 적용하고 있는가? Is encryption being used in storage to enable secure data storage?	

Object Storage에 Public Access가 미설정 되어 있는가? Are there any access controls applied to Object Storage?	
Object Storage에 대한 접근 제어와 각종 Method(View/Edit)에 대한 요청 권한 분류가 되어 있는가? Are there different classifications for assigning access responsibilities for Object Storage and for different Method (View/Edit)?	
스토리지에 대한 데이터의 변경 이력을 남기고 있으며, 이력관리에 대한 방안이 존재하는가? Is there a history of DB / Storage data changes and is there a plan for managing this history?	
스토리지에 대한 백업/복구에 대한 절차가 존재하는가? Are there Storage backup / recovery procedures?	

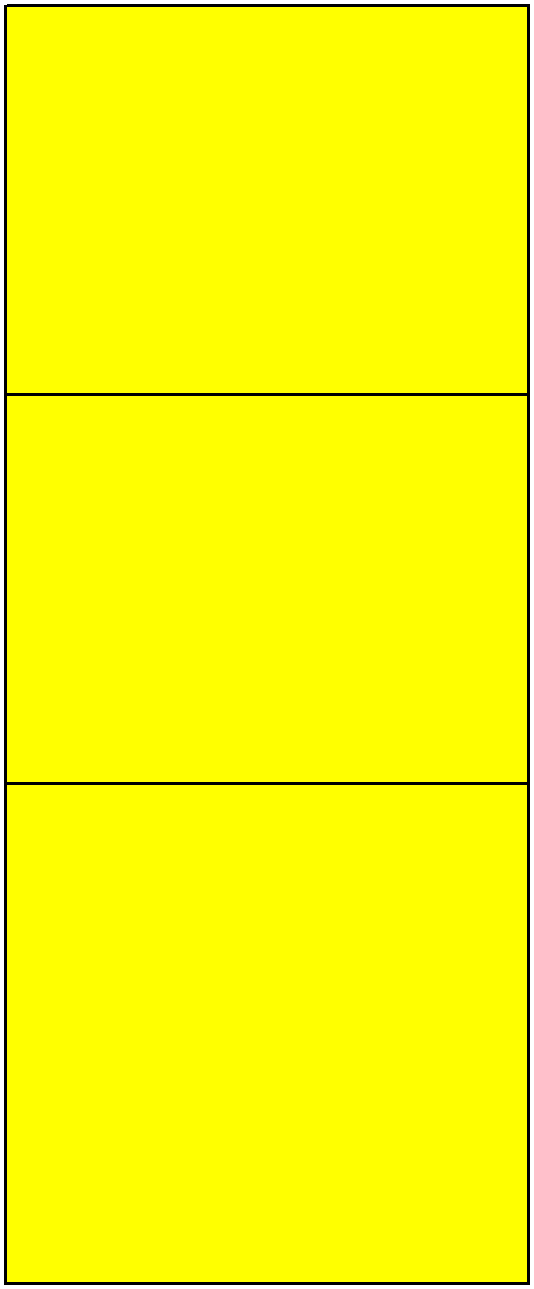
스토리지 사용 Log 기록하고 있으며, 로그 기록을 하고 있고 보관기간이 적절하게 수립되어 있는가? Is there storage in the Object Storage usage log, so was the storage period well established as well?	
스토리지 관리를 위한 네이밍에 대한 기준이 있으며, 이에 따라 Tagging을 하고 있는가? Is there a naming criterion for Storage management and is Tagging being performed correctly?	
인프라 자원에 대한 생성/변경/삭제에 대해 추적이 가능하도록 구성되어 있는가? Is it possible to trace the creation / modification / deletion of Infra resources?	
클라우드에 구축된 보안 설정에 대한 설정 변경 모니터링 및 증적을 기록하고 있는가? Is there monitoring and recording of evidence of changes to security settings deployed in the cloud?	

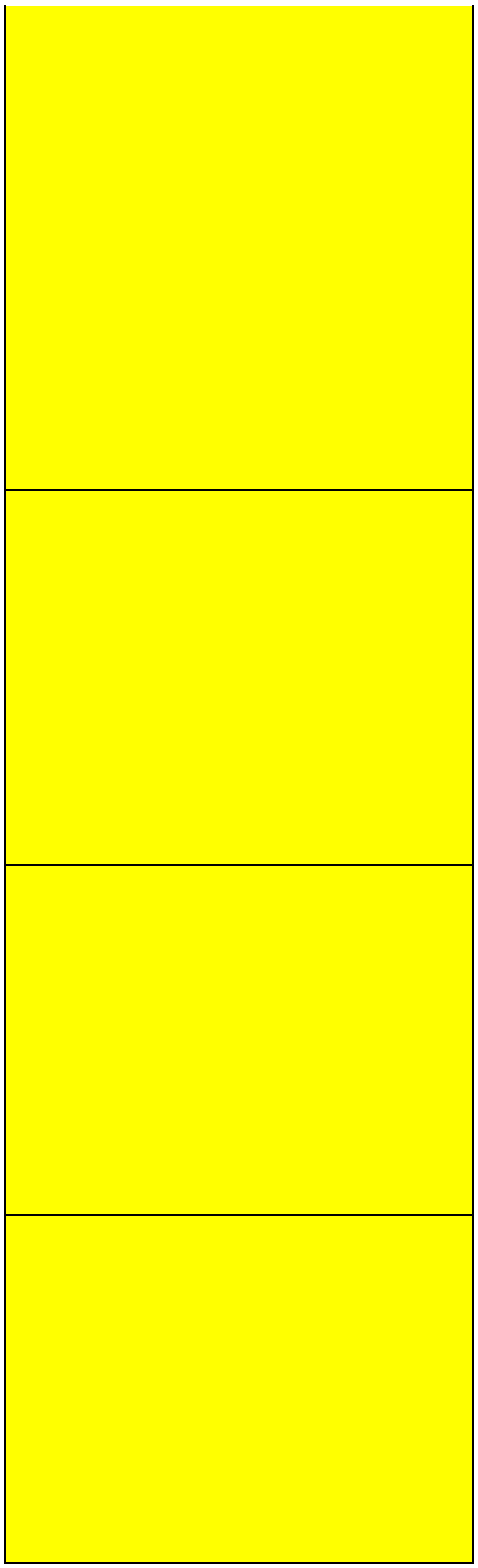
인프라 자원에 대한 사용량 모니터링을 수행하고 있는가? Is monitoring of the use of Infra resources being carried out?	
인프라 관리를 위한 각 서버(인스턴스)에 대한 네이밍에 대한 기준이 있으며, 이에 따라 Tagging을 하고 있는가? Is there a server naming criterion (Instance) that allows Infra management, and proper tagging is being performed?	

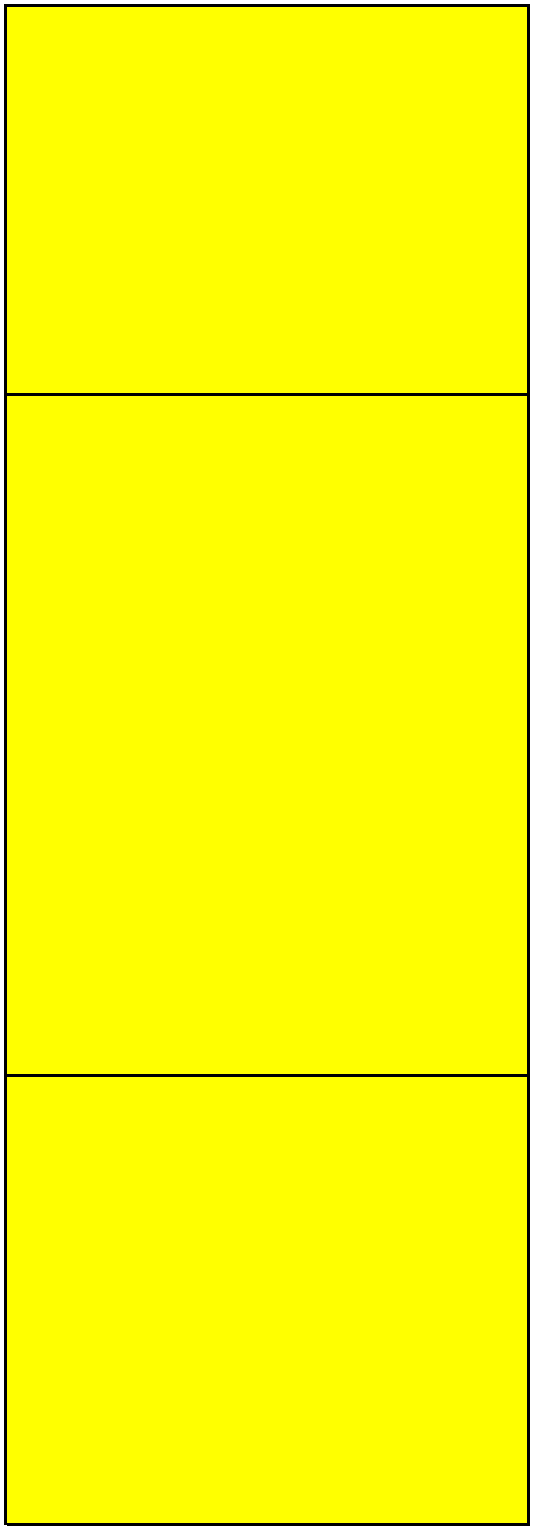
Fill out the checklist
Remark

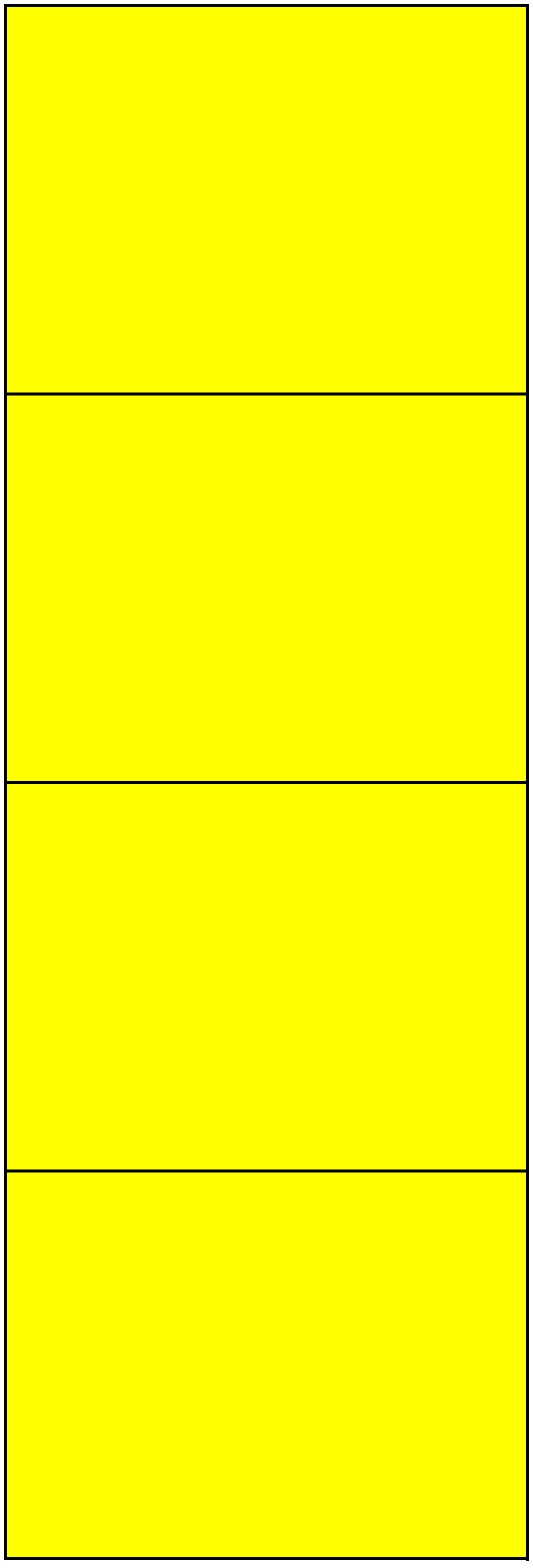


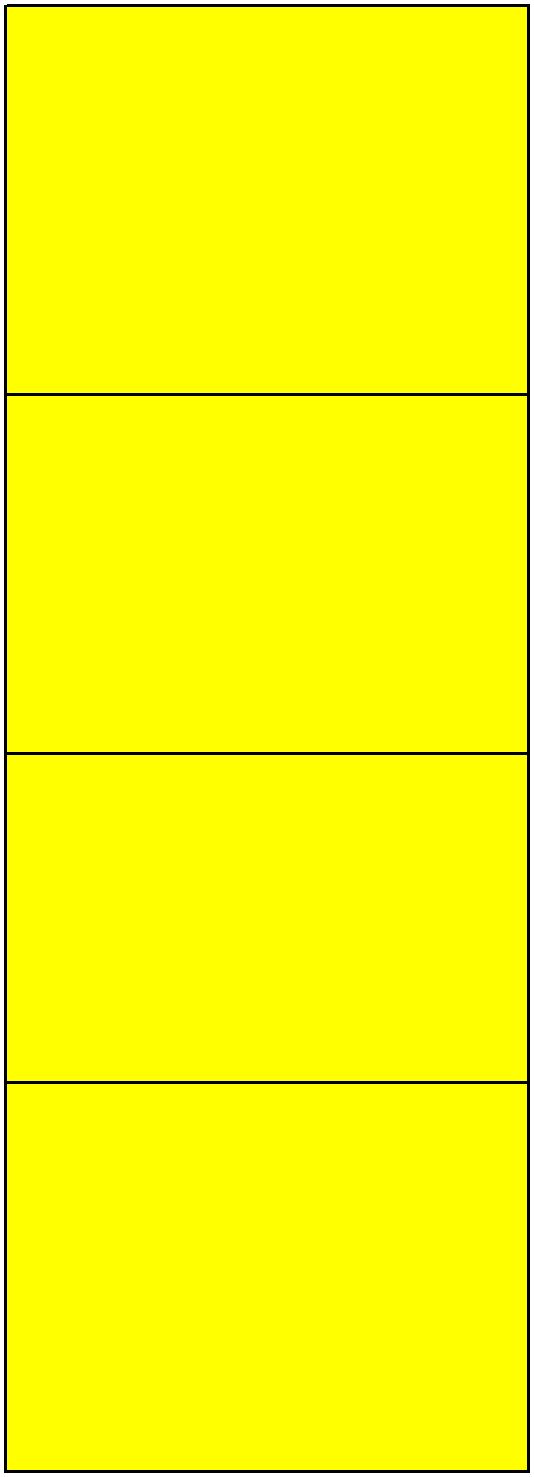
증적 내용 필수

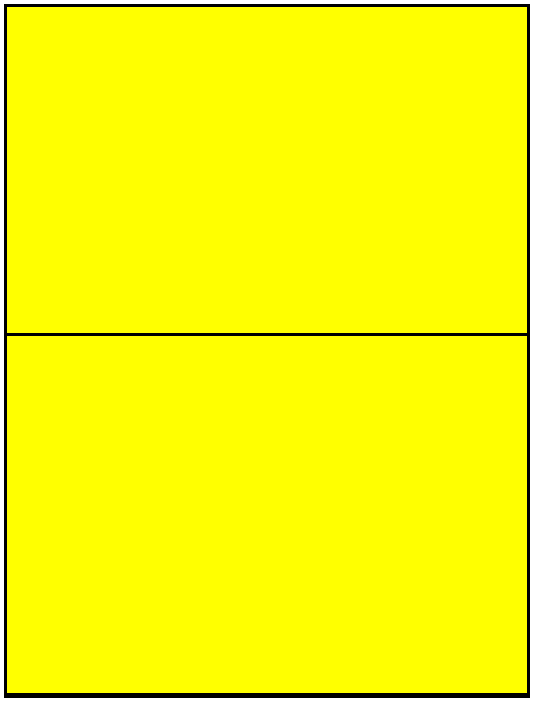












Evaluation Criteria
(취약점 설명) 클라우드 내 구축되는 시스템은 임의로 IP를 할당하지 않고, IP 할당 정책을 통해 IP를 할당하고 있어, IP 관리를 통해 네트워크 보안을 향상해야함 **(양호)** IP 할당 기준 및 할당을 하고 있음 **(취약)** IP 할당 기준이 없음 '(Vulnerability Description) The system built in the cloud does not allocate IP arbitrarily, but allocates IP through IP allocation policy, so network security needs to be improved through IP management. (Good) IP allocation criteria and allocation
(취약점 설명) 클라우드에서 사용하는 네트워크 구성을 각 환경(운영, QA, Prod) 별로 분리하여 운영하고 있어, 네트워크에 환경에 대한 혼용이 없어야 함 (GCP의 경우 별도의 VPC운영) **(양호)** ACL를 통해 네트워크에 대한 환경 분리를 하고 있으며, 해당 리소스 들이 배치되어 있음 **(취약)** ACL를 통해 각 영역이 환경별로 구성되어 있지 않음 '(Vulnerability Description) The network configuration used in the cloud is operated separately for each environment (operation, QA, prod), so there should be no mixed environment in the network (In case of GCP, separate VPC operation)
(취약점 설명) 클라우드에서 사용하는 리소스는 ACL을 통해 접근 제어를 해야하며, 접근 제어는 Public 영역과, Private에 대한 영역 분리 및 리소스 배치를 하여 각각의 리소스를 보호할 수 있어야 함 (GCP의 경우 VPC내 방화벽 설정) **(양호)** ACL를 통해 Public/Private 환경 분리를 하고 있으며, 해당 리소스 들이 배치되어 있음 **(취약)** Security Group을 통해 Public/Private 환경 분리를 하고 있지 않으며, 모든 리소스가 Public을 통해 노출이 되어 있는 경우 '(Vulnerability Description) Resources used in the cloud must be accessed through ACL, and access control must be able to protect each resource by separating the public and private areas and arranging resources. (For Google Cloud, set up a firewall within the VPC) (Good) Public/Private environment is separated through ACL, and the corresponding resources are placed

(취약점 설명)
클라우드에서 사용하는 리소스는 In/Out bound에 대한 기준이 있어야 하며, 기준 별로 접근 제어를 수행해야 네트워크에 대한 안정성을 확보할 수 있음

(양호) ACL 서비스를 적용하고 있고, 트래픽 통제 이력을 관리하고 있는 경우
(취약) ACL 서비스를 적용하지 않거나, 적용하였지만 트래픽 통제 이력에 대해서 관리하고 있지 않은 경우

(Vulnerability Description)
Resources used in the cloud must have standards for in/out bounds, and access control must be performed for each criterion to ensure network stability.

(Good) When ACL service is applied and traffic control history is managed
(취약점 설명)

클라우드 네트워크에서 ACL과 같은 접근 제어를 통해 IP/Port에 대한 접근제어를 구축하고 있어야 함

(양호) ACL 기반의 통제가 구축되어 있는 경우
(취약) ACL 기반의 통제가 구축되지 않은 경우

(Vulnerability Description)
Access control for IP/Port must be established through access control such as ACL in cloud network

(Good) When ACL-based controls are in place
(vulnerable) when ACL-based controls are not in place

(취약점 설명)
클라우드에서 사용하는 리소스에 대한 NACL을 통해 네트워크 접근제어를 해야 하며 네트워크에 대한 불필요한 연동이 없도록 검토하고 설계해야 함
(GCP의 경우 VPC내 방화벽 설정)

(양호) NACL 적용 내역과 설계도를 통해 NACL 적용에 대한 검토서가 존재하는 경우
(취약) NACL 구성에 대한 검토가 이루어지지 않은 경우

(Vulnerability Description)
Network access control for resources used in the cloud should be controlled through NACL, and it should be reviewed and designed so that there is no unnecessary interworking with the network.
(For Google Cloud, set up a firewall within the VPC)

(Good) If there is a review of NACL application through NACL application details and Engineering Drawings
(vulnerable) NACL configuration not reviewed

(취약점 설명)
SSRF취약점에 대응할 수 있는 방안이 작용되어 있음.

(양호) EC2를 통해 Web Backend Server 구현 시 WAF적용이 되어 있는 경우
(취약) EC2를 통해 Web Backend Server 구현 시 WAF적용이 되어 있지 않는 경우.

'(Vulnerability Description)
Measures to respond to SSRF vulnerabilities are in operation.

(Good) When WAF is applied when implementing Web Backend Server through EC2
(Vulnerable) When implementing Web Backend Server through EC2, WAF is not applied

(취약점 설명)
시스템 내 웹페이지를 제공하는 경우 HTTPS가 적용 되어 있음.

(양호) HTTPS가 적용 되어 있는 경우
(취약) HTTPS가 적용 되어 있지 않은 경우

'(Vulnerability Description)
HTTPS is applied when providing web pages within the system

(Good) HTTPS is applied
(Vulnerable) HTTPS is not applied

(취약점 설명)
외부에서 예상 가능한 Well-Known Port port 사용 시 변경하여 사용 필요(ex, ssh)
Well-known Port 를 특정 IP만 허용 필요 (외부오픈 지양) (ex. Icmp)

(양호) Well-Known Port port를 변경하여 사용
(취약) Well-Known Port port를 그대로 사용

'(Vulnerability Description)
When using an externally predictable Well-Known Port port, you need to change it and use it (ex, ssh)
Required to allow only specific IPs for well-known ports (avoid external open) (ex. Icmp)

(취약점 설명)
다른 시스템 <> 클라우드 간 서비스하는 통신 구간에 대해서는 전송구간 암호화를 전용하여 네트워크 상에 평문으로 노출되지 않아야 함

(양호) 전송 구간 암호화(TLS1.2이상, HTTPS, sFTP)가 적용되어 있거나 IP 접근 제어가 적용되어 있을 경우
(취약) 전송 구간에 대한 암호화가 적용되지 않거나 IP 접근제어가 없는 경우

'(Vulnerability Description)
For the communication section serviced between other systems <> cloud, the transmission section encryption should be dedicated and not exposed as plaintext on the network.

(취약점 설명)
클라우드에서 구성한 네트워크 구성도 내 WAF와 IPS와 같은 방화벽이 배치 되어 있어 이를 통해 네트워크에 대한 보호조치를 적용해야 함

(양호) 네트워크 설계도 내 "ACL" 적용과 같은 규칙이 존재하거나, 클라우드에서 제공되는 보안 기능(WAF, CloudTrail)을 적용한 내역이 있을 경우
(취약) 리소스에 대한 보안 적용을 하지 않은 경우

'(Vulnerability Description) Firewalls such as WAF and IPS are placed in the network configuration in the cloud, so protection

(취약점 설명)
클라우드에서 사용하는 리소스가 공인IP를 사용하는 경우, 명확한 Src/Dest에 대한 정의가 되어 있으며, 이를 통해 대외에 존재하는 리소스에 대한 보호 조치가 적용되어야 함

(양호) 공인 IP를 가지는 리소스에 대한 Src/Dest에 대해 정의가 되거나 공인IP로 구성이 되지 않은 경우
(취약) 공인 IP를 가지면서 Src/Dest에 대한 정의 명확하지 않은 경우

(Vulnerability Description)
If the resource used in the cloud uses a public IP, there is a clear definition of Src/Dest, and through this, protection measures for external resources must be applied.

(Good) If Src/Dest for a resource with a public IP is defined or is not configured with a public IP
(Weak) If the definition of Src/Dest is not clear while having a public IP

(취약점 설명)
클라우드에서 발생하는 트래픽에 대한 모니터링을 위해 트래픽에 대한 로그를 남기고 검토하여 리소스를 관리하여야 서비스에 대한 무중단 서비스가 가능할 수 있어야 함

(양호) 네트워크 트래픽에 대한 모니터링을 하는 경우
(취약) 네트워크 트래픽에 대한 모니터링을 하지 않는 경우

(Vulnerability Description)
In order to monitor traffic generated in the cloud, it is necessary to manage resources by leaving and reviewing traffic logs so that uninterrupted service can be possible.

(Good) When monitoring network traffic
(Vulnerable) If network traffic is not monitored

(취약점 설명)
클라우드의 제공 서비스를 이용하여 서비스를 제공할 경우, 불필요한 외부 시스템 연동과 같은 작업이 이루어지지 않아야 하며, 이를 사전에 검토하여야 함

(양호) 클라우드 제공 서비스 사용 시 불필요한 외부 연계에 대해서 검토를 진행한 경우
(취약) 클라우드 제공 서비스 사용 시 불필요한 외부 연계가 존재하거나 외부 연계에 대한 검토를 진행하지 않은 경우

(Vulnerability Description)
In the case of providing a service using the cloud provided service, unnecessary work such as interworking with external systems should not be performed, and this should be reviewed in advance.

(Good) In case of reviewing unnecessary external linkage when using cloud-provided services
(Vulnerable) When using cloud-provided services, unnecessary external linkage exists or external linkage has not been reviewed

(취약점 설명)
클라우드에서 윈도우 OS로 구축 간에 RDP 서비스를 활용하여 원격 서버 접근을 할 경우 무분별한 접근을 방지 하기 위해 인가된 사용자에게만 접근할 수 있도록 구성해야 함

(양호) RDP 서비스 접근 간 IP 접근과 같은 접근 제어가 존재하는 경우
(취약) RDP 통해 인가되지 않은 사용자가 접근을 시도할 수 있는 경우
{N/A) OS에서 RDP를 통해 원격 접근 제어를 사용하지 않는 경우

(Vulnerability Description)
In case of remote server access using RDP service between cloud and Windows OS deployments, it should be configured to allow access only to authorized users to prevent reckless access.

(Good) When access control such as IP access exists between RDP service access
(Vulnerable) When an unauthorized user can try to access through RDP
{N/A) When OS does not use remote access control via RDP

(취약점 설명)
클라우드에서 윈도우 OS로 구축 간에 보안 강화를 위해 백신을 설치해야 함

(양호) 원도우 OS 서버에 백신을 설치 한 경우
(취약) 윈도우 OS 서버에 백신을 설치 하지 않은 경우
(**N/A)** 윈도우 OS 서버를 사용하지 않는 경우

해외 : SEP 백신 홈페이지(https://v3.lge.com)를 통해 다운로드
국내 : SEP 설치 파일의 경우 IT인프라팀(ssora.lee@lge.com) 문의

(Vulnerability Description)
Antivirus must be installed to enhance security between deployments from cloud to Windows OS

(Good) When antivirus is installed on Windows OS server
(Vulnerable) When antivirus is not installed on Windows OS server

Overseas: Download through the SEP vaccine website (https://v3.lge.com)

(취약점 설명)
클라우드 서버에서 운영상 요청하는 명령어에 대한 기록을 통해 오남용 명령어에 대한 로깅을 하고 있어, 침해 사고 발생 간 악성 행위 분석이 용이함

(양호) 클라우드 서버에서 요청하는 명령어를 로깅하고 있는 경우
(취약) 클라우드 서버에서 요청하는 명령어를 로깅하지 않는 경우

(Vulnerability Description)
It is easy to analyze malicious behaviors between incidents by logging abused commands by recording commands requested for operation from the cloud server.

(Good) If you are logging commands requested by the cloud server

(취약점 설명)
클라우드에서 사용하는 서버(VM)에 대한 접근 제어를 위해 인가된 사용자만 접근을 하도록 구현해야 함

(양호) 서버(VM)를 사용하며 인가된 사용자만 접근이 가능하도록 구성한 경우
(취약) 서버(VM)를 사용하며 별도의 접근제어가 없는 경우
{N/A) 서버(VM)를 사용하지 않을 경우

(Vulnerability Description)
To control access to the server(VM) used in the cloud, it should be implemented so that only authorized users have access.

(Good) When using a server(VM) and configured so that only authorized users can access
(vulnerable) When using a server(VM) and there is no separate access control
(N/A) When not using server(VM)

(취약점 설명)
스토리지 및 DB의 중요도를 확인하여 암호화를 실시하여야 한다. 암호화를 통해 데이터 보호 대책을 적용할 수 있어야 함

(양호) 클라우드 DB의 암호화 설정을 적용한 경우
(취약) 클라우드 DB에 암호화 설정을 적용하지 않은 경우
(N/A) 암호화 적용 대상 시스템이 아닌 경우

(Vulnerability Description)
Encryption should be performed by checking the importance of storage and DB. Encryption should be able to apply data protection measures

(Good) When encryption settings of cloud DB are applied

(취약점 설명)
클라우드에서 사용하는 DB에 대한 접근 제어를 위해 인가된 사용자만 접근을 하도록 구현해야 함

(양호) DB 서비스를 사용하며 인가된 사용자만 접근이 가능하도록 구성한 경우
(취약) DB 서비스를 사용하며 별도의 접근제어가 없는 경우
{N/A) DB 서비스를 사용하지 않을 경우

(Vulnerability Description)
To control access to the DB service used in the cloud, it should be implemented so that only authorized users have access.

(Good) When using a DB service and configured so that only authorized users can access
(vulnerable) When using a DB service and there is no separate access control
(N/A) When not using DB service

(취약점 설명)
클라우드에서 데이터 베이스에 대한 적절한 권한 분리를 하고 있어, Root 계정과 운영 계정을 분리를 통해 과도한 권한 부여를 제한해야 하며, DB Query 요청에 대한 이력 관리를 통해 데이터 베이스에 보안에 대한 보안성을 향상할 수 있어야 함

(양호) 데이터 베이스에 대한 변경 이력을 로깅 하고 있는 경우
(취약) 데이터 베이스에 대한 변경 이력을 로깅 하지 않을 경우
(N/A) 데이터 베이스를 사용하지 않는 경우
(Vulnerability Description)
In the cloud, appropriate authorization for the database is segregated, so excessive authorization must be restricted by separating the root account and the operating account. should be able

(Good) When logging change history to the database
(Vulnerable) If the change history to the database is not logged
(N/A) When the database is not used

AWS RDS Audit Log setting : https://aws.amazon.com/ko/blogs/database/configuring-an-audit-log-to-capture-database-activities-for-amazon-rds-for-mysql-and-amazon-aurora-with-mysql-compatibility/
DynamoDB API CloudTrail setting : https://docs.aws.amazon.com/ko_kr/amazondynamodb/latest/developerguide/logging-using-cloudtrail.html
Cloud SQL Audit Log setting : https://cloud.google.com/sql/docs/audit-logging

(취약점 설명)
스토리지에 저장되는 데이터의 안전한 보관을 위해 스토리지에 대한 암호화 적용이 되어 있어, 스토리지 내 데이터가 유출 시에 암호화 된 데이터가 노출될 수 있어 스토리지 암호화를 적용하여 보안성을 향상할 수 있어야 함

(양호) 스토리지 암호화 설정을 적용한 경우
(취약) 스토리지 암호화 설정을 적용하지 않은 경우
(N/A) 암호화 적용 대상 시스템이 아닌 경우

(Vulnerability Description)
Because encryption is applied to the storage for safe storage of data stored in the storage, encrypted data may be exposed when the data in the storage is leaked, so it is necessary to apply storage encryption to improve security

(Good) When the storage encryption setting is applied
(Vulnerable) When storage encryption settings are not applied

(취약점 설명)
클라우드에서 Object Storage를 사용하고 있을 경우, 접근 제한에 대한 적용이 되어 있어야 스토리지에 대한 보안성을 향상할 수 있음

(양호) Object Storage에 대한 접근 권한 적용되어 있는 경우
(취약) Object Storage에 대한 접근 권한 적용되어 있지 않은 경우
(N/A) Object Storage를사용하지 않는 경우

(Vulnerability Description)
When using Object Storage in the cloud, the security of storage can be improved only when access restrictions are applied.

(Good) When access right to Object Storage is applied
(Vulnerable) When access right to Object Storage is not applied

(취약점 설명)
클라우드에서 Object Storage를 사용하고 있을 경우, 접근 제한에 대한 적용이 되어 있어야 스토리지에 대한 보안성을 향상할 수 있음

(양호) Object Storage에 대한 접근 권한 적용되어 있는 경우
(취약) Object Storage에 대한 접근 권한 적용되어 있지 않은 경우
(N/A) Object Storage를사용하지 않는 경우

(Vulnerability Description)
When using Object Storage in the cloud, the security of storage can be improved only when access restrictions are applied.

(Good) When access right to Object Storage is applied
(Vulnerable) When access right to Object Storage is not applied

(취약점 설명)
클라우드에서 Object Storage에 대한 변경 이력 관리를 통해 데이터 베이스에 보안에 대한 보안성을 향상할 수 있어야 함

(양호) Object Storage에 대한 데이터 변경에 대한 이력 관리를 하는 경우
(취약) Object Storage에 대한 데이터 변경에 대한 이력 관리를 하고 있지 않는 경우
(N/A) Object Storage를 사용하지 않는 경우

(Vulnerability Description)
It should be possible to improve the security of the database through change history management for Object Storage in the cloud.

(Good) When managing the history of data changes for object storage
(Vulnerable) In case of not managing the history of data changes for object storage

(취약점 설명)
클라우드에서 발생하는 트래픽에 대한 모니터링을 위해 트래픽에 대한 로그를 남기고 검토하여 리소스를 관리하여야 서비스에 대한 무중단 서비스가 가능할 수 있어야 함

(양호) 클라우드에 적절한 주기에 따라 백업을 하고 있으며, 복구 방안이 있는 경우
(취약) 클라우드에 백업/복구 방안 수립되지 않는 경우

(Vulnerability Description)
In order to monitor traffic generated in the cloud, it is necessary to manage resources by leaving and reviewing traffic logs so that uninterrupted service can be possible.

(Good) If the cloud is backed up at an appropriate interval and there is a recovery plan
(Vulnerable) If a backup/restore plan is not established in the cloud

(취약점 설명)
클라우드에서 Object Storage에 대한 변경 이력 관리를 통해 데이터 베이스에 보안에 대한 보안성을 향상할 수 있어야 함

(양호) Object Storage에 로깅을 하고 있으며, 로그 보관을 하고 있는 경우
(취약) Object Storage에 로깅을 하지 않는 경우
(N/A) Object Storage를 사용하지 않는 경우

(Vulnerability Description)
It should be possible to improve the security of the database through change history management for Object Storage in the cloud.

(Good) When logging to Object Storage and keeping logs
(Vulnerable) When not logging to Object Storage

(취약점 설명)
클라우드에서 인프라에 대한 네이밍 기준이 있어, 이에 따라 네밍을 통해 적절한 인스턴스 관리와 그룹 설정이 할 수 있어야 함

(양호) 클라우드 인스턴스에 대한 네이밍 규칙 및 규칙에 따라 네이밍을 하는 경우
(취약) 클라우드 인스턴스에 대한 네이밍 규칙이 없고, 무분별하게 생성한 경우

(Vulnerability Description)
In the cloud, there is a naming standard for infrastructure, so appropriate instance management and group setting should be possible through naming

(Good) Naming according to the naming rules and rules for cloud instances

(취약점 설명)
클라우드 인프라는 설정 변경에 따른 영향도가 클 수 있으므로 인프라 변경 행위에 대한 변경이록을 기록해야 함

(양호) 클라우드에서 변경하는 변경이력 로깅을 하고 있을 경우
(취약) 클라우드에서 변경하는 변경이력 로깅을 하고 있지 않은 경우

(Vulnerability Description)
Cloud infrastructure can have a large impact on configuration changes, so it is necessary to record changes to infrastructure changes.

(Good) When logging change history in the cloud

(취약점 설명)
클라우드에서 사용하는 각종 인프라 설정은 편리한 UI로 제공 됨에 따라 변경에 따른 영향력이 예측할 수 없는 경우가 있음에 따라, 설정 변경이력에 대해서 기록할 수 있어야 함

(양호) 클라우드의 보안 설정 변경에 대해 모니터링이 가능하도록 변경이력을 기록하는 경우
(취약) 클라우드에서 보안 설정 변경에 대해서 기록하지 않는 경우

(Vulnerability Description)
As various infrastructure settings used in the cloud are provided with a convenient UI, the impact of changes may not be predictable, so it is necessary to record the history of setting changes.

(Good) When recording change history to enable monitoring of changes to security settings in the cloud
(Vulnerable) If the cloud does not log changes to security settings

(취약점 설명)
클라우드에서 자원에 대한 모니터링을 하고 있어 무중단 서비스가 가능할 수 있어야 함

(양호) 클라우드 리소스 모니터링을 하는 경웅
(취약) 클라우드 리소스 모니터링을 하지 않는 경우

(Vulnerability Description)
Monitoring of resources in the cloud should enable uninterrupted service

(Good) Kyung-woong monitoring cloud resources
(Vulnerable) If you do not monitor cloud resources

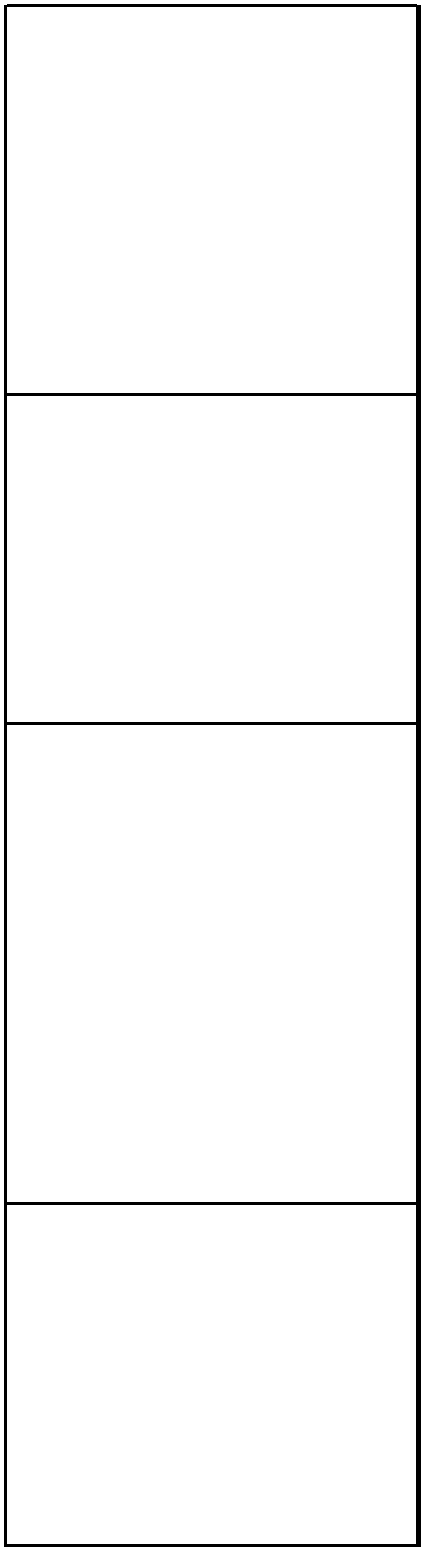
(취약점 설명)
클라우드에서 인프라에 대한 네이밍 기준이 있어, 이에 따라 네밍을 통해 적절한 인스턴스 관리와 그룹 설정이 할 수 있어야 함

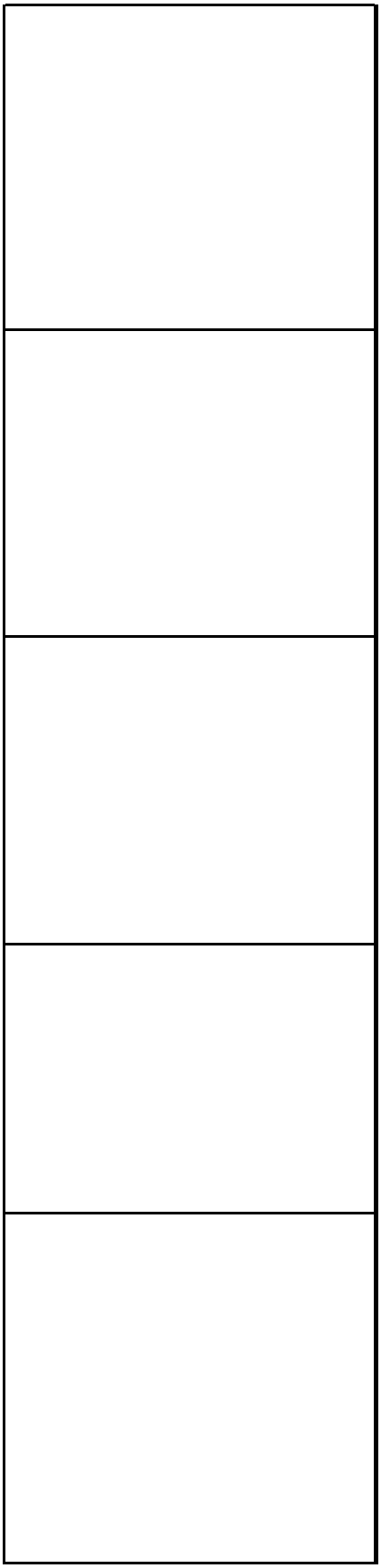
(양호) 클라우드 인스턴스에 대한 네이밍 규칙 및 규칙에 따라 네이밍을 하는 경우
(취약) 클라우드 인스턴스에 대한 네이밍 규칙이 없고, 무분별하게 생성한 경우

(Vulnerability Description)
In the cloud, there is a naming standard for infrastructure, so appropriate instance management and group setting should be possible through naming

(Good) Naming according to the naming rules and rules for cloud instances

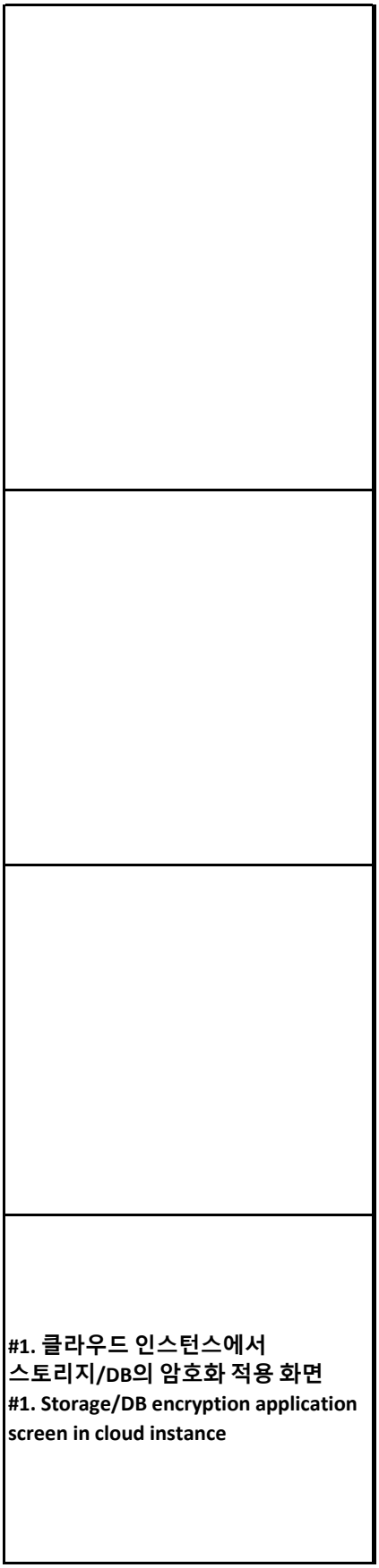
Evidence Contents





#1. 클라우드 네트워크 트래픽 기록 화면 캡쳐

#.1 Cloud network traffic recording screen capture



#1. 클라우드 인스턴스에서 스토리지/DB의 암호화 적용 화면

#1. Storage/DB encryption application screen in cloud instance

#1. CSP별 DB서비스 Audit Log 설정 화면 **AWS** **- DynamoDB : Cloud Trail Log** **- RDS/Aurora : Audit Log 설정 증적** **GCP** **- Cloud SQL : Audit Log 설정 증적** **#1. DB service audit log setting screen by CSP** **AWS** **- DynamoDB : Cloud Trail Log setting screen capture** **- RDS/Aurora : Audit Log setting screen capture** **GCP** **- Cloud SQL : Audit Log setting screen capture**
#1. 클라우드 인스턴스에서 스토리지 암호화(Encrytion) 적용 화면 **#1. Storage encryption application screen in cloud instance**

#1. Object Storage 외부 접근 설정 내역 #1. Object storage external access setting details
#1. Object Storage 에 변경 이력 로깅 화면 - AWS : CloudTrail 설정 내역 증적 - GCP : Audit Log 설정 증적 #One. Change history logging screen in Object Storage - AWS: CloudTrail setting history trace - GCP: Audit Log setting trace
#1. 클라우드 백업 정책 #2. 클라우드 백업 설정 화면 #1. Cloud Backup Policy #2. Cloud Backup Settings Screen

#1. Object Storage의 로깅 화면 - AWS : CloudTrail 설정 내역 증적 - GCP : Audit Log 설정 증적 #1. Logging screen of Object Storage - AWS: CloudTrail setting history trace - GCP: Audit Log setting trace
#1. 클라우드 변경이력 기록 화면 - AWS : CloudTrail 설정 내역 증적 - GCP : Audit Log 설정 증적 #1. Cloud change history record screen - AWS: CloudTrail setting history screen capture - GCP: Audit Log setting screen capture

#1. 클라우드 리소스 모니터링화면 증적 **#1. Cloud resource monitoring screen capture**
#1. 클라우드 인스턴스 네이밍(Tagging) 룰 **#1.** **Cloud instance naming (Tagging) rules**

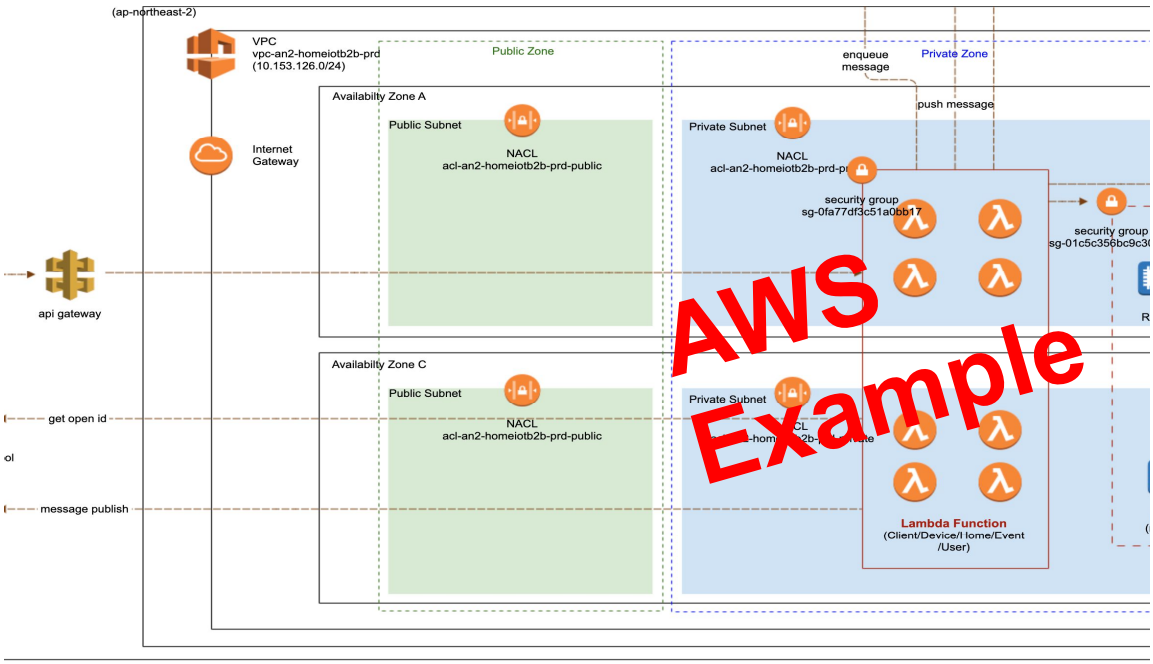
[4. Infra Architecture]

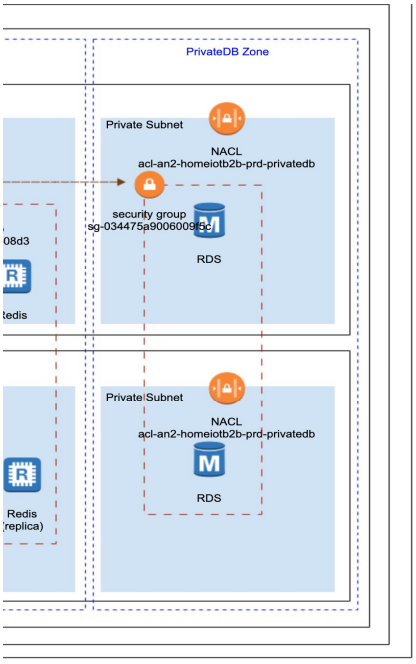
Writing Guide

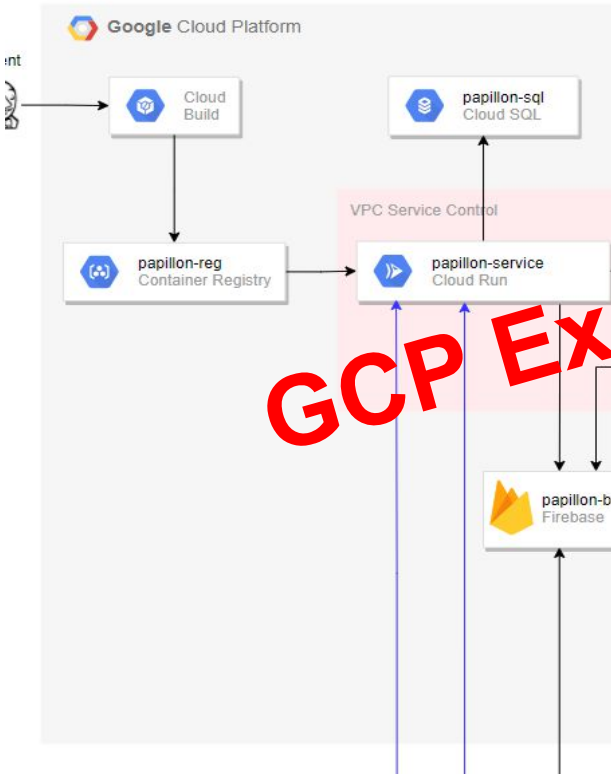
1. Write when the type of external cloud service is IaaS or PaaS

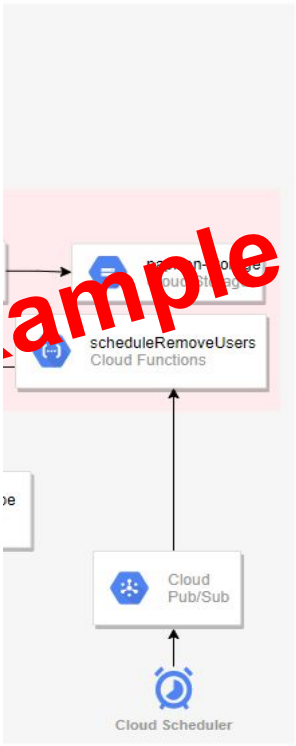
2. Please draw security groups, network ACLs.

※ In the case of GCP, draw as a firewall.




PrivateDB Zone
Private Subnet
NACL
acl-an2-homeiotb2b-prd-privatedb
security group
RDS
Private Subnet
NACL
acl-an2-homeiotb2b-prd-privatedb
RDS
Redis


Google Cloud Platform
Cloud Build
papillon-sql
Cloud SQL
VPC Service Control
papillon-reg
Container Registry
papillon-service
Cloud Run
GCP Ex
Firebase

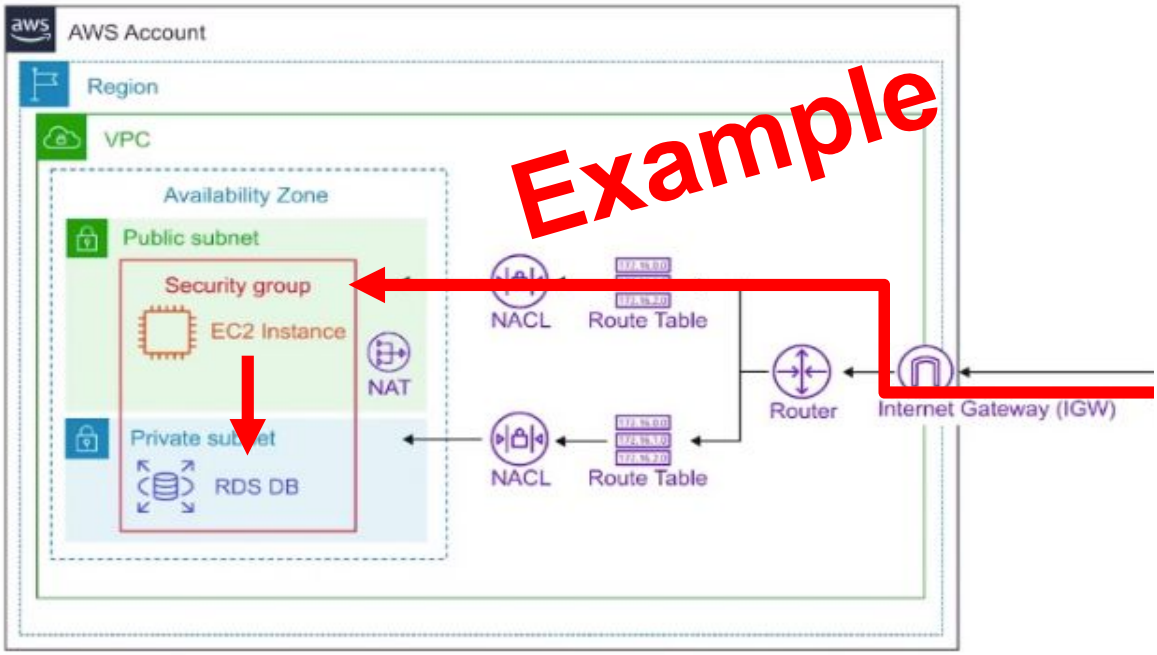

ample
scheduleRemoveUsers
Cloud Functions
Cloud
Pub/Sub
Cloud Scheduler

[5. Data(Service) Flowchat]

Writing Guide

1. Write when the type of external cloud service is IaaS or PaaS

2. display movement path of data within the infra architecture to arrows indicate




The Internet

[6. IAM List]

Writing Guide

1. Capture IAM list provided by CSP Console

example

비밀번호 수명	마지막 활동	MFA
27 일	4 일	가상
26 일	오늘	가상
27 일	4 일	가상
26 일	오늘	가상

[7. IP List(CIDR)]

[8. Security Group]

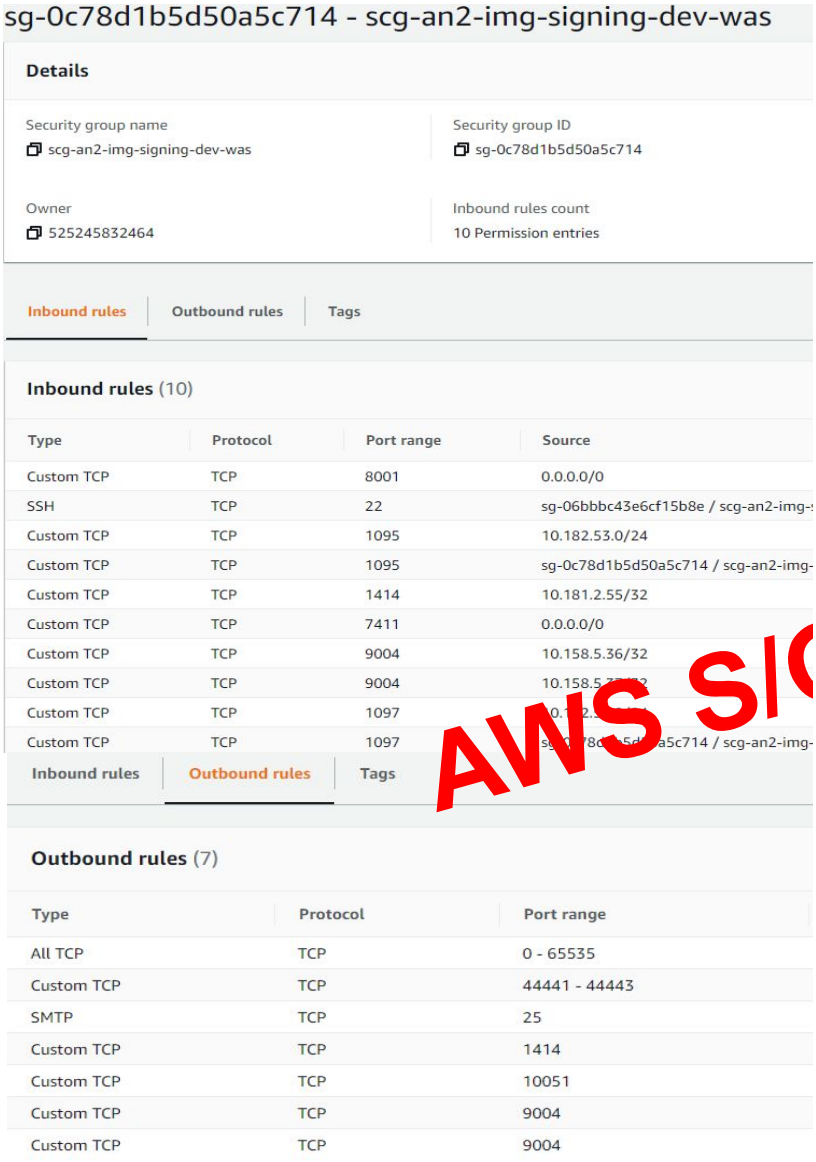
Writing Guide

1. Write when the type of external cloud service is IaaS or PaaS

2. Capture Security Group list provided by CSP

- AWS : Capture Security Group details

- GCP: not written



sg-0c78d1b5d50a5c714 - scg-an2-img-signing-dev-was

Details

Security group name scg-an2-img-signing-dev-was	Security group ID sg-0c78d1b5d50a5c714
Owner 525245832464	Inbound rules count 10 Permission entries

Inbound rules | Outbound rules | Tags

Inbound rules (10)

Type	Protocol	Port range	Source
Custom TCP	TCP	8001	0.0.0.0/0
SSH	TCP	22	sg-06bbbc43e6cf15b8e / scg-an2-img-
Custom TCP	TCP	1095	10.182.53.0/24
Custom TCP	TCP	1095	sg-0c78d1b5d50a5c714 / scg-an2-img-
Custom TCP	TCP	1414	10.181.2.55/32
Custom TCP	TCP	7411	0.0.0.0/0
Custom TCP	TCP	9004	10.158.5.36/32
Custom TCP	TCP	9004	10.158.5.[illegible]
Custom TCP	TCP	1097	10.[illegible]
Custom TCP	TCP	1097	sg-[illegible]a5c714 / scg-an2-img-

AWS SI

Inbound rules | Outbound rules | Tags

Outbound rules (7)

Type	Protocol	Port range
All TCP	TCP	0 - 65535
Custom TCP	TCP	44441 - 44443
SMTP	TCP	25
Custom TCP	TCP	1414
Custom TCP	TCP	10051
Custom TCP	TCP	9004
Custom TCP	TCP	9004

Description
ssh

VPC ID
vpc-07f86ddbfc6d0ad7f

Outbound rules count
7 Permission entries

	Description - optional
	Custom SSHD Port, from LGE Internal Network
-signing-dev-bastion	ssh was connection
	Java RMI [illegible] Port, from DEV VPC
-signing-dev-was	Java RMI Object Port, from DEV WAS
	DB Interface Port, from DEV MQ
	Apache HTTP Port, from LGE Internal Network
	HSM Connection Port, from HSM VS #1
	HSM Connection Port, from HSM VS #2
	Java RMI Registry Port, from DEV VPC
-signing-dev-was	Java RMI Registry Port, from DEV WAS

Destination	Description - optional
10.182.53.0/24	–
10.185.246.59/32	SSO Server (DEV)
156.147.51.104/32	SMTP Server (OPER), lgekrhqsy01.lge.com
10.181.2.55/32	DB Interface Port, from DEV MQ
10.185.248.250/32	CMS Monitoring
10.158.5.37/32	HSM Connection port
10.158.5.36/32	HSM Connection port

[9. Network ACL]

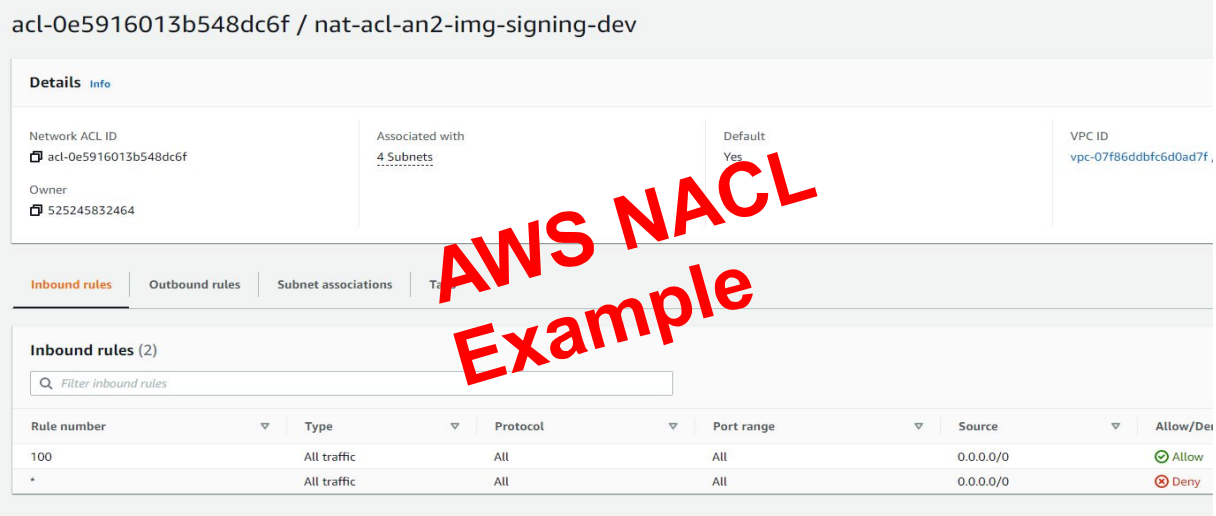
Writing Guide

1. Write when the type of external cloud service is IaaS or PaaS

2. Capture Network ACL list provided by CSP

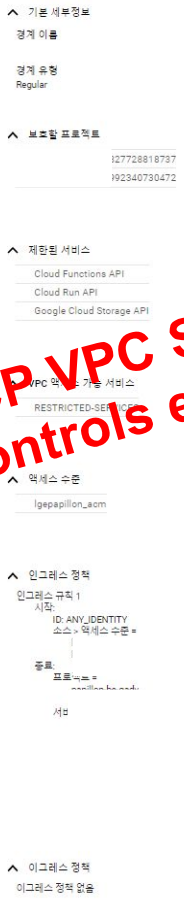
- AWS: Capture Network ACL details

- GCP: Firewall, GCP VPC Service Controls detailed item capture



이름	유형	대상	필터	프로토콜/포트	작업
default-allow-internal	수신	전체 적용	IP 범위: 10.128.0.0/9	tcp:0-65535 udp:0-65535	허용

GCP firewall example



GCP VPC Service Controls example

우선순위	네트워크 ↑	로그
65534	default	사용 안함