SAMPLE PACK · FICTIONAL COMPANY · EVERY NAME, ACCOUNT AND RESULT IN IT IS INVENTED

ASSAY · AUDIT EVIDENCE PACK · EXCERPT

ISO/IEC 27001:2022 audit pack for Acme Cloud Pvt Ltd

This is what Assay hands an auditor: where the company stands against each requirement, gaps first, with every claim backed by an evidence record collected read-only from the live systems or by a signed document. Assay's own code built it from invented data, so the layout and the records are exactly what a real pack contains.

In this excerpt

1. Summary: readiness, gaps first, the start of the requirement table
2. Statement of Applicability (first pages)
3. Policies and procedures in force
4. Six evidence records: a pass, a failure and a warning among them
5. A signed quarterly review: database network restrictions
6. One controlled policy document, approved by an independent approver

The full pack

Pages in the combined PDF	222
Requirements assessed	123
Evidence records	69, each with its raw capture and hash
Policies and procedures	26 in force, 1 draft
Quarterly reviews	1 signed
Also in the folder	raw captures, and a manifest hashing every file

Acme Cloud, its people, AWS account 123456789012 (AWS's documentation example), example.com and the addresses in 203.0.113.0/24 and 198.51.100.0/24 are placeholders. No real company's systems were read to make this sample.

SAMPLE PACK · FICTIONAL COMPANY · EVERY NAME, ACCOUNT AND RESULT IN IT IS INVENTED

AUDIT EVIDENCE PACK

ISO/IEC 27001:2022

Where Acme Cloud Pvt Ltd stands against each requirement: the documents in force and the evidence collected from the live systems. Gaps are listed first.

ORGANISATION	**Acme Cloud Pvt Ltd**
READINESS	**46% of controls ready**
REQUIREMENTS	**123**
EVIDENCE	**69 records**
DATE	**2026-10-18**

46% controls ready

4 requirements · Failing

3 requirements · No evidence

1 requirements · Attention

84 requirements · Policy only

31 requirements · Ready

69 evidence records

Every evidence record in this pack was produced by an automated, read-only collector (AWS API, Bitbucket API, TLS/HTTP probes, the report library) or is a record uploaded as a document. Each record carries the call that produced it, when it was collected, and the SHA-256 of its raw capture, which is included under `evidence/`. `raw/manifest.json` hashes every file in the pack. A requirement is **Ready** only when a document in force covers every mapped control and all evidence for it is passing and within its freshness window. Gaps are listed first and are not omitted.

1. Gaps (8)

REF	REQUIREMENT	STATUS	WHY
7.2	Competence	No evidence	HRS-05 Personnel Screening: No evidence not yet collected: Background verification (record)

A.5.16	Identity management	Failing	IAC-08.4 Disable Inactive Accounts: Failing E:3 1 active access key is older than 90 days (ci-deploy)
A.5.17	Authentication information	Failing	IAC-14 Authenticator Management: Failing E:3 1 active access key is older than 90 days (ci-deploy)
A.5.18	Access rights	Failing	IAC-10.1 Privileged Account Inventories: Failing E:3 1 active access key is older than 90 days (ci-deploy) IAC-14 Authenticator Management: Failing E:3 1 active access key is older than 90 days (ci-deploy)
A.5.33	Protection of records	No evidence	RSK-19 Data Protection Impact Assessment (DPIA): No evidence not yet collected: Data protection impact assessment (record)
A.6.1	Screening	No evidence	HRS-05 Personnel Screening: No evidence not yet collected: Background verification (record)
A.8.2	Privileged access rights	Failing	IAC-10.1 Privileged Account Inventories: Failing E:3 1 active access key is older than 90 days (ci-deploy)
A.8.8	Management of technical vulnerabilities	Attention	VPM-08 Software & Firmware Patching: Attention E:18 worker-1 has 2 security updates waiting for its maintenance window VPM-12 Vulnerability Scanning: Attention E:18 worker-1 has 2 security updates waiting for its maintenance window

2. Requirements

REF	REQUIREMENT	STATUS	POLICIES	EVIDENCE
CLAUSE 4 — CONTEXT OF THE ORGANISATION				
4.1	Understanding the organisation and its context 0/2 controls ready · CPL-02, GOV-03.3	Policy only	POL-LEGAL in force PRC-AUDIT in force	

			POL-ISMS in force	
4.2	Needs and expectations of interested parties 0/2 controls ready · AST-07, GOV-03.3	Policy only	POL-LEGAL in force POL-ASSET in force POL-ISMS in force	
4.3	Scope of the ISMS 0/1 controls ready · CPL-03	Policy only	POL-ISMS in force POL-LEGAL in force PRC-AUDIT in force	
4.4	Information security management system 1/2 controls ready · GOV-02, GOV-09	Policy only	POL-ISMS in force	E:63
CLAUSE 5 — LEADERSHIP				
5.1	Leadership and commitment 1/5 controls ready · GOV-02, GOV-04, GOV-05, GOV-09, PRM-05	Policy only	POL-ISMS in force PRC-DOC in force	E:63
5.2	Information security policy 0/2 controls ready · GOV-03.3, GOV-04	Policy only	POL-ISMS in force PRC-DOC in force	
5.3	Roles, responsibilities and authorities 1/3 controls ready · GOV-05, GOV-09, HRS-04	Policy only	POL-ISMS in force POL-HR in force	E:63
CLAUSE 6 — PLANNING				

3. Statement of Applicability (Annex A)

CONTROL	TITLE	APPLICABLE	JUSTIFICATION	IMPLEMENTATION
A.5.1	Policies for information security	Yes	Required to treat identified information security risks.	Policy only
A.5.2	Information security roles and responsibilities	Yes	Required to treat identified information security risks.	Policy only
A.5.3	Segregation of duties	Yes	Required to treat identified information security risks.	Policy only
A.5.4	Management responsibilities	Yes	Required to treat identified information security risks.	Policy only
A.5.5	Contact with authorities	Yes	Required to treat identified information security risks.	Policy only
A.5.6	Contact with special interest groups	Yes	Required to treat identified information security risks.	Policy only
A.5.7	Threat intelligence	Yes	Required to treat identified information security risks.	Ready
A.5.8	Information security in project management	Yes	Required to treat identified information security risks.	Policy only
A.5.9	Inventory of information and associated assets	Yes	Required to treat identified information security risks.	Policy only
A.5.10	Acceptable use of information and assets	Yes	Required to treat identified information security risks.	Policy only
A.5.11	Return of assets	Yes	Required to treat identified information security risks.	Policy only
A.5.12	Classification of information	Yes	Required to treat identified information security risks.	Policy only
A.5.13	Labelling of information	Yes	Required to treat identified information security risks.	Policy only
A.5.14	Information transfer	Yes	Required to treat identified information security risks.	Policy only
A.5.15	Access control	Yes	Required to treat identified information security risks.	Policy only
A.5.16	Identity management	Yes	Required to treat identified information security risks.	Failing
A.5.17	Authentication information	Yes	Required to treat identified information security risks.	Failing
A.5.18	Access rights	Yes	Required to treat identified information security risks.	Failing
A.5.19	Information security in supplier relationships	Yes	Required to treat identified information security risks.	Policy only

A.5.20	Information security in supplier agreements	Yes	Required to treat identified information security risks.	Policy only
A.5.21	ICT supply chain security	Yes	Required to treat identified information security risks.	Policy only
A.5.22	Monitoring and change of supplier services	Yes	Required to treat identified information security risks.	Policy only
A.5.23	Information security for cloud services	Yes	Required to treat identified information security risks.	Policy only
A.5.24	Incident management planning and preparation	Yes	Required to treat identified information security risks.	Ready
A.5.25	Assessment of information security events	Yes	Required to treat identified information security risks.	Policy only
A.5.26	Response to information security incidents	Yes	Required to treat identified information security risks.	Policy only
A.5.27	Learning from incidents	Yes	Required to treat identified information security risks.	Ready
A.5.28	Collection of evidence	Yes	Required to treat identified information security risks.	Policy only
A.5.29	Information security during disruption	Yes	Required to treat identified information security risks.	Ready
A.5.30	ICT readiness for business continuity	Yes	Required to treat identified information security risks.	Policy only
A.5.31	Legal, regulatory and contractual requirements	Yes	Required to treat identified information security risks.	Policy only
A.5.32	Intellectual property rights	Yes	Required to treat identified information security risks.	Policy only
A.5.33	Protection of records	Yes	Required to treat identified information security risks.	No evidence
A.5.34	Privacy and protection of PII	Yes	Required to treat identified information security risks.	Policy only
A.5.35	Independent review of information security	Yes	Required to treat identified information security risks.	Ready
A.5.36	Compliance with security policies and standards	Yes	Required to treat identified information security risks.	Ready
A.5.37	Documented operating procedures	Yes	Required to treat identified information security risks.	Policy only
A.6.1	Screening	Yes	Required to treat identified information security risks.	No evidence
A.6.2	Terms and conditions of employment	Yes	Required to treat identified information security risks.	Policy only
A.6.3	Security awareness, education and training	Yes	Required to treat identified information security risks.	Ready

A.8.24	Use of cryptography	Yes	Required to treat identified information security risks.	Ready
A.8.25	Secure development life cycle	Yes	Required to treat identified information security risks.	Policy only
A.8.26	Application security requirements	Yes	Required to treat identified information security risks.	Policy only
A.8.27	Secure system architecture and engineering	Yes	Required to treat identified information security risks.	Policy only
A.8.28	Secure coding	Yes	Required to treat identified information security risks.	Ready
A.8.29	Security testing in development and acceptance	Yes	Required to treat identified information security risks.	Ready
A.8.30	Outsourced development	Yes	Required to treat identified information security risks.	Policy only
A.8.31	Separation of development, test and production	Yes	Required to treat identified information security risks.	Policy only
A.8.32	Change management	Yes	Required to treat identified information security risks.	Ready
A.8.33	Test information	Yes	Required to treat identified information security risks.	Ready
A.8.34	Protection of systems during audit testing	Yes	Required to treat identified information security risks.	Policy only

4. Policies and procedures

REF	TITLE	STATE	VERSION	APPROVAL
POL-ACCESS	Access Control Policy	in force	1.0.0	Rohan Desai, 2026-10-18
POL-ASSET	Asset Management and Media Handling Policy	in force	1.0.0	Rohan Desai, 2026-10-18
POL-AUP	Acceptable Use Policy	in force	1.0.0	Ananya Iyer, 2026-10-18
POL-BCDR	Business Continuity, Disaster Recovery and Backup Policy	in force	1.0.0	Rohan Desai, 2026-10-18
POL-CHANGE	Change Management Policy	in force	1.0.0	Ananya Iyer, 2026-10-18
POL-CLASS	Information Classification and Handling Policy	in force	1.0.0	Rohan Desai, 2026-10-18
POL-CLOUD	Cloud Security Policy	in force	1.0.0	Rohan Desai, 2026-10-18

SAMPLE PACK · FICTIONAL COMPANY · EVERY NAME, ACCOUNT AND RESULT IN IT IS INVENTED

EVIDENCE RECORD · AMAZON WEB SERVICES

Access keys rotated and in use

No active IAM access key is older than 90 days or unused for 90 days.

ORGANISATION	Acme Cloud Pvt Ltd
APPLIES TO	AWS account 123456789012
RESULT	Fail 1 active access key is older than 90 days (ci-deploy)
COLLECTED	18 Oct 2026 21:15 IST
SOURCE	Amazon Web Services
RECORD	E:3 · SHA-256 861ad164f5dd77cc…

What it shows

- 2 active access keys
- ✗ ci-deploy's key is 142 days old (limit 90)
- ✓ Every key was used in the last 90 days

Captures

aws AWS account 123456789012 (Acme Cloud production) · Region ap-south-1 · Principal assay API CAPTURE · NOT A SCREENSHOT Captured 18 Oct 2026 21:15 IST

IAM › Users › Security credentials

Active access keys

Keys older than 90 days, or unused for 90 days, are highlighted

User	Key	Age	Last used
ci-deploy	AKIAIOSFODNN7EXAMPLE	142 days	0 days ago
kabir.shah	AKIAI44QH8DHBEXAMPLE	37 days	3 days ago

Produced read-only from Amazon Web Services as arn:aws:sts::123456789012:assumed-role/assay-evidence-readonly/assay (read-only calls), on 18 Oct 2026 21:15 IST. Command(s): `aws iam list-access-keys --user-name <user>` · `aws iam get-access-key-last-used --access-key-id <key>`. Values are the unmodified output; this is not a browser screenshot.

SAMPLE PACK · FICTIONAL COMPANY · EVERY NAME, ACCOUNT AND RESULT IN IT IS INVENTED

EVIDENCE RECORD · AMAZON WEB SERVICES

Database network restrictions

Every database accepts connections only from its application tier and the administrative address, sits on subnets without an internet route, and every security-group change since the last review is listed.

ORGANISATION	**Acme Cloud Pvt Ltd**
APPLIES TO	**AWS account 123456789012**
RESULT	**Pass** **1 database reachable only from its application tier — 1 database security-group change since 2026-08-19**
COLLECTED	**18 Oct 2026 20:39 IST**
SOURCE	**Amazon Web Services**
RECORD	**E:15 · SHA-256 0eb17dd549d15aa9…**

What it shows

- 1 database instance; 1 database security group; 2 inbound rules
- ✓ Only the application tier and the admin VPN address reach the database
- ✓ Database subnets have no route to the internet
- 1 change touched a database security group; it is listed for the quarterly review

Captures

aws AWS account 123456789012 (Acme Cloud production) · Region ap-south-1 · Principal assay API CAPTURE · NOT A SCREENSHOT Captured 18 Oct 2026 20:39 IST

RDS › Databases

Databases

Every RDS instance in the account

Database	Engine	Class	VPC	Port	Public	Encrypted	Multi-AZ	Deletion protection	Backups (days)	Security groups
acme-prod-db	postgres 16.4	db.r6g.large	vpc-0a1b2c3d4e5f60789	5432	No	Yes	Yes	Yes	14	sg-0db1a2b3c4d5e6f70

Produced read-only from Amazon Web Services as arn:aws:sts::123456789012:assumed-role/assay-evidence-readonly/assay (read-only calls), on 18 Oct 2026 20:39 IST. Command(s): `aws rds describe-db-instances` · `aws ec2 describe-security-groups --group-ids sg-0db1a2b3c4d5e6f70` · `aws ec2 describe-route-tables --filters Name=association.subnet-id,Values=<db subnets>` · `aws cloudtrail lookup-events --lookup-attributes AttributeKey=EventSource,AttributeValue=ec2.amazonaws.com`. Values are the unmodified output; this is not a browser screenshot.

aws AWS account 123456789012 (Acme Cloud production) · Region ap-south-1 · Principal assay **API CAPTURE · NOT A SCREENSHOT** Captured 18 Oct 2026 20:39 IST

VPC › Security groups

Database security-group rules

Every inbound and outbound rule on a database's security groups

Security group	Direction	Port	Source / destination	Kind	Rule description
acme-prod-db (sg-0db1a2b3c4d5e6f70)	Inbound	5432	sg-0ab1c2d3e4f506172 (acme-prod-app)	application tier	Application tier to Postgres
acme-prod-db (sg-0db1a2b3c4d5e6f70)	Inbound	5432	203.0.113.10/32 (admin VPN)	admin address	Admin VPN, for maintenance
acme-prod-db (sg-0db1a2b3c4d5e6f70)	Outbound	all	none	none	No outbound rules

Produced read-only from Amazon Web Services as arn:aws:sts::123456789012:assumed-role/assay-evidence-readonly/assay (read-only calls), on 18 Oct 2026 20:39 IST. Command(s): `aws rds describe-db-instances` · `aws ec2 describe-security-groups --group-ids sg-0db1a2b3c4d5e6f70` · `aws ec2 describe-route-tables --filters Name=association.subnet-id,Values=<db subnets>` · `aws cloudtrail lookup-events --lookup-attributes AttributeKey=EventSource,AttributeValue=ec2.amazonaws.com`. Values are the unmodified output; this is not a browser screenshot.

aws AWS account 123456789012 (Acme Cloud production) · Region ap-south-1 · Principal assay **API CAPTURE · NOT A SCREENSHOT** Captured 18 Oct 2026 20:39 IST

VPC › Route tables

Database subnet routing

No database subnet should route 0.0.0.0/0 to an internet gateway

Database	Subnet	CIDR	Route table	Routes	Internet route	Dead routes
acme-prod-db	acme-prod-db-a (subnet-0a1b2c3d4e5f60791)	10.20.21.0/24	rtb-0a1b2c3d4e5f60790	10.20.0.0/16 → local	No	—
acme-prod-db	acme-prod-db-b (subnet-0a1b2c3d4e5f60792)	10.20.22.0/24	rtb-0a1b2c3d4e5f60790	10.20.0.0/16 → local	No	—

Produced read-only from Amazon Web Services as arn:aws:sts::123456789012:assumed-role/assay-evidence-readonly/assay (read-only calls), on 18 Oct 2026 20:39 IST. Command(s): `aws rds describe-db-instances` · `aws ec2 describe-security-groups --group-ids sg-0db1a2b3c4d5e6f70` · `aws ec2 describe-route-tables --filters Name=association.subnet-id,Values=<db subnets>` · `aws cloudtrail lookup-events --lookup-attributes AttributeKey=EventSource,AttributeValue=ec2.amazonaws.com`. Values are the unmodified output; this is not a browser screenshot.

aws AWS account 123456789012 (Acme Cloud production) · Region ap-south-1 · Principal assay **API CAPTURE · NOT A SCREENSHOT** Captured 18 Oct 2026 20:39 IST

CloudTrail › Event history

Security-group changes since 2026-08-19

2 event(s); those on a database's group need a change record

Time (UTC)	Event	Security group	Database group	Principal	Source IP	Agent	Error
2026-09-15 17:54	AuthorizeSecurityGroupIngress	sg-0ab1c2d3e4f506172	No	ci-deploy	198.51.100.40	terraform/1.9.8	
2026-09-27 17:54	RevokeSecurityGroupIngress	sg-0db1a2b3c4d5e6f70	**Yes**	kabir.shah	203.0.113.10	terraform/1.9.8	

Produced read-only from Amazon Web Services as arn:aws:sts::123456789012:assumed-role/assay-evidence-readonly/assay (read-only calls), on 18 Oct 2026 20:39 IST. Command(s): `aws rds describe-db-instances` · `aws ec2 describe-security-groups --group-ids sg-0db1a2b3c4d5e6f70` · `aws ec2 describe-route-tables --filters Name=association.subnet-id,Values=<db subnets>` · `aws cloudtrail lookup-events --lookup-attributes AttributeKey=EventSource,AttributeValue=ec2.amazonaws.com`. Values are the unmodified output; this is not a browser screenshot.

SAMPLE PACK · FICTIONAL COMPANY · EVERY NAME, ACCOUNT AND RESULT IN IT IS INVENTED

EVIDENCE RECORD · AMAZON WEB SERVICES

Servers receive security patches

Every server installs security updates automatically, verified from live package inventory read through SSM, with SSM's own patch compliance beside it.

ORGANISATION	**Acme Cloud Pvt Ltd**
APPLIES TO	**AWS account 123456789012**
RESULT	Warning **worker-1 has 2 security updates waiting for its maintenance window**
COLLECTED	**18 Oct 2026 20:30 IST**
SOURCE	**Amazon Web Services**
RECORD	**E:18 · SHA-256 5613bef011535b05…**

What it shows

- ✓ unattended-upgrades installed on every server
- ✓ web-1 and web-2 fully patched
- ✗ worker-1: 2 missing security patches

Captures

aws AWS account 123456789012 (Acme Cloud production) · Region ap-south-1 · Principal assay API CAPTURE · NOT A SCREENSHOT Captured 18 Oct 2026 20:30 IST

SSM › Managed instances

Every server and what SSM says about it

Package inventory read live through SSM

Server	Kind	Platform	SSM	Unattended-upgrades	Inventory
web-1	application server	Ubuntu 24.04 LTS	Online	2.9.1ubuntu4	0.2 d ago
web-2	application server	Ubuntu 24.04 LTS	Online	2.9.1ubuntu4	0.2 d ago

Server	Kind	Platform	SSM	Unattended-upgrades	Inventory
worker-1	application server	Ubuntu 24.04 LTS	Online	2.9.1ubuntu4	0.2 d ago

Produced read-only from Amazon Web Services as arn:aws:sts::123456789012:assumed-role/assay-evidence-readonly/assay (read-only calls), on 18 Oct 2026 20:30 IST. Command(s): `aws ssm describe-instance-patch-states --instance-ids <ids>`. Values are the unmodified output; this is not a browser screenshot.

aws AWS account 123456789012 (Acme Cloud production) · Region ap-south-1 · Principal assay API CAPTURE · NOT A SCREENSHOT Captured 18 Oct 2026 20:30 IST

SSM › Patch manager

SSM patch compliance

What AWS's own patch compliance says about the fleet

Instance	Region	Operation	Missing	Failed	Installed	Snapshot time
i-0a1b2c3d4e5f60781	ap-south-1	Scan	0	0	612	2026-10-18T12:54:41+00:00
i-0a1b2c3d4e5f60783	ap-south-1	Scan	0	0	612	2026-10-18T12:54:41+00:00
i-0a1b2c3d4e5f60784	ap-south-1	Scan	2	0	612	2026-10-18T12:54:41+00:00

Produced read-only from Amazon Web Services as arn:aws:sts::123456789012:assumed-role/assay-evidence-readonly/assay (read-only calls), on 18 Oct 2026 20:30 IST. Command(s): `aws ssm describe-instance-patch-states --instance-ids <ids>`. Values are the unmodified output; this is not a browser screenshot.

SAMPLE PACK · FICTIONAL COMPANY · EVERY NAME, ACCOUNT AND RESULT IN IT IS INVENTED

EVIDENCE RECORD · THE APPLICATION URL, OVER THE PUBLIC INTERNET

HTTPS and edge protection

The environment's URL serves TLS 1.2+ with a valid certificate and HSTS, and whether an edge proxy fronts it.

ORGANISATION	**Acme Cloud Pvt Ltd**
APPLIES TO	**Production**
RESULT	**Pass** **TLS 1.3, HSTS one year, HTTP redirects to HTTPS**
COLLECTED	**18 Oct 2026 20:03 IST**
SOURCE	**The application URL, over the public internet**
RECORD	**E:27 · SHA-256 45710ba131f256ac…**

What it shows

- ✓ Negotiates TLS 1.3 and rejects TLS 1.1
- ✓ HSTS max-age one year with includeSubDomains
- ✓ Plain HTTP redirects to HTTPS

Captures

https app.example.com · anonymous visitor LIVE PROBE · NOT A SCREENSHOT — Captured 18 Oct 2026 20:03 IST

https://app.example.com/

HTTPS as a visitor sees it

One TLS handshake and one HEAD request, no login

TLS version negotiated	**TLSv1.3**
Rejects TLS 1.1	**Yes**
Certificate issuer	Amazon RSA 2048 M03

Certificate expires	2027-01-12
HSTS header	**max-age=31536000; includeSubDomains**
Plain HTTP redirects to HTTPS	**Yes**
Edge proxy	Amazon CloudFront
Server header	CloudFront
HTTP status	200

Produced read-only from The application URL, over the public internet as anonymous visitor, on 18 Oct 2026 20:03 IST. Command(s): `openssl s_client -connect app.example.com:443 -servername app.example.com` · `curl -sI https://app.example.com/` · `curl -sI http://app.example.com/`. Values are the unmodified output; this is not a browser screenshot.

SAMPLE PACK · FICTIONAL COMPANY · EVERY NAME, ACCOUNT AND RESULT IN IT IS INVENTED

EVIDENCE RECORD · AWS IAM + BITBUCKET MEMBERS, COMPARED WITH ASSAY'S STAFF LIST

Access review against the staff list

Every AWS and Bitbucket account belongs to a current person on the staff list; leavers and unknown accounts are listed.

ORGANISATION	**Acme Cloud Pvt Ltd**
APPLIES TO	**Organisation-wide**
RESULT	**Pass** Every AWS user and Bitbucket member has an owner on the staff list
COLLECTED	**18 Oct 2026 18:57 IST**
SOURCE	**AWS IAM + Bitbucket members, compared with Assay's staff list**
RECORD	**E:49 · SHA-256 147844caf9e8a1d4…**

What it shows

- ✓ 4 AWS IAM users, each owned by a current employee
- ✓ 5 Bitbucket members, all current employees
- ✓ No leaver still has access

Captures

aws + Bitbucket AWS account 123456789012 and workspace acme-cloud API CAPTURE · NOT A SCREENSHOT Captured 18 Oct 2026 18:57 IST

IAM › Credential report

AWS IAM users and who owns them

User	Account	Console	MFA	Active keys	Owner on staff list
meera.kulkarni	123456789012	Yes	Yes	No	Meera Kulkarni
rohan.desai	123456789012	Yes	Yes	No	Rohan Desai

User	Account	Console	MFA	Active keys	Owner on staff list
kabir.shah	123456789012	Yes	Yes	Yes	Kabir Shah
ci-deploy	123456789012	No	—	Yes	Kabir Shah

Produced read-only from AWS IAM + Bitbucket members, compared with Assay's staff list as read-only access, on 18 Oct 2026 18:57 IST. Command(s): `aws iam get-credential-report` · `GET /2.0/workspaces/acme-cloud/members`. Values are the unmodified output; this is not a browser screenshot.

aws + Bitbucket AWS account 123456789012 and workspace acme-cloud API CAPTURE · NOT A SCREENSHOT Captured 18 Oct 2026 18:57 IST

Workspace › Members

Bitbucket members and who they are

Member	Owner on staff list
Meera Kulkarni	Meera Kulkarni
Rohan Desai	Rohan Desai
Kabir Shah	Kabir Shah
Neha Joshi	Neha Joshi
Ananya Iyer	Ananya Iyer

Produced read-only from AWS IAM + Bitbucket members, compared with Assay's staff list as read-only access, on 18 Oct 2026 18:57 IST. Command(s): `aws iam get-credential-report` · `GET /2.0/workspaces/acme-cloud/members`. Values are the unmodified output; this is not a browser screenshot.

SAMPLE PACK · FICTIONAL COMPANY · EVERY NAME, ACCOUNT AND RESULT IN IT IS INVENTED

EVIDENCE RECORD · BITBUCKET CLOUD

Changes arrive through reviewed pull requests

Pull requests merged in the last 90 days were approved by someone other than their author.

ORGANISATION	**Acme Cloud Pvt Ltd**
APPLIES TO	**Organisation-wide**
RESULT	**Pass** **Every merge into main in the last 90 days had an independent approval**
COLLECTED	**18 Oct 2026 18:48 IST**
SOURCE	**Bitbucket Cloud (source control)**
RECORD	**E:52 · SHA-256 543cd23337a89348…**

What it shows

- 10 pull requests merged into main

✓ Every one approved by someone other than its author

Captures

Bitbucket workspace acme-cloud · read as assay-readonly **API CAPTURE · NOT A SCREENSHOT** Captured 18 Oct 2026 18:48 IST

Pull requests › Merged (last 90 days)

Merges into the main and release branches

Repository	Merged with independent approval	Merged without
acme-infra	2	0
acme-mobile	2	0
acme-platform	3	0
acme-web	3	0

Produced read-only from Bitbucket Cloud (source control) as assay-readonly (repository read), on 18 Oct 2026 18:48 IST. Command(s): `GET /2.0/repositories/acme-cloud/<repo>/pullrequests?state=MERGED&q=updated_on>-90d`. Values are the unmodified output; this is not a browser screenshot.

Bitbucket workspace acme-cloud · read as assay-readonly **API CAPTURE · NOT A SCREENSHOT** Captured 18 Oct 2026 18:48 IST

Pull requests › Merged without independent approval

Merges approved by nobody but their author

Repository	PR	Into	Title	Author	Merged by	Date
None						

0 merges without independent approval

Produced read-only from Bitbucket Cloud (source control) as assay-readonly (repository read), on 18 Oct 2026 18:48 IST. Command(s): `GET /2.0/repositories/acme-cloud/<repo>/pullrequests?state=MERGED&q=updated_on>-90d`. Values are the unmodified output; this is not a browser screenshot.

SAMPLE PACK · FICTIONAL COMPANY · EVERY NAME, ACCOUNT AND RESULT IN IT IS INVENTED

QUARTERLY REVIEW · OCTOBER-DECEMBER 2026

Database network review

Every item in the evidence below has a recorded decision. The window starts where the previous review ended, so nothing falls between two reviews.

ORGANISATION	**Acme Cloud Pvt Ltd**
PERIOD	**October-December 2026**
WINDOW	**2026-07-01 to 2026-10-18**
SCRUT TASK	**Network traffic restrictions for database (security group)**
EVIDENCE	**E:15 (AWS account 123456789012)**
STATUS	**Signed by Rohan Desai on 18 Oct 2026 23:24 IST**

Decisions

4 of 4 items that need a decision are decided; 3 keep, 1 matched to a change record.

Item	Detail	State	Decision	Note	Decided by
acme-prod-db (sg-0db1a2b3c4d5e6f70)					
Inbound 5432 AWS account 123456789012	sg-0ab1c2d3e4f506172 (acme-prod-app) — Application tier to Postgres	security-group	**Keep**		Meera Kulkarni
Inbound 5432 AWS account 123456789012	203.0.113.10/32 (admin VPN) — Admin VPN, for maintenance	admin	**Keep**	Needed for database maintenance; VPN address only.	Meera Kulkarni
Outbound all AWS account 123456789012	none — No outbound rules	none	**Keep**		Meera Kulkarni
Database security-group changes since the last review					
RevokeSecurityGroupIngress on sg-0db1a2b3c4d5e6f70 AWS account 123456789012 · 2026-09-27 17:54	by kabir.shah from 203.0.113.10 (terraform/1.9.8)	change	**Matched to a change record**	Matched to PLAT-398: removed an old rule for the retired reporting server.	Meera Kulkarni

Reviewer notes

No rule reaches the database from outside the application tier and the admin VPN.

Sign-off

Role	Name	When	Signature
Prepared by	Meera Kulkarni	18 Oct 2026 23:24 IST	—
Reviewed and signed by	Rohan Desai	18 Oct 2026 23:24 IST	typed name; recorded by Rohan Desai

Evidence E:15 — Database network restrictions, AWS account 123456789012

1 database reachable only from its application tier — 1 database security-group change since 2026-08-19 (collected 18 Oct 2026 20:39 IST)

aws AWS account 123456789012 (Acme Cloud production) · Region ap-south-1 · Principal assay API CAPTURE · NOT A SCREENSHOT Captured 18 Oct 2026 20:39 IST

RDS › Databases

Databases

Every RDS instance in the account

Database	Engine	Class	VPC	Port	Public	Encrypted	Multi-AZ	Deletion protection	Backups (days)	Security groups
acme-prod-db	postgres 16.4	db.r6g.large	vpc-0a1b2c3d4e5f60789	5432	No	Yes	Yes	Yes	14	sg-0db1a2b3c4d5e6f70

Produced read-only from Amazon Web Services as arn:aws:sts::123456789012:assumed-role/assay-evidence-readonly/assay (read-only calls), on 18 Oct 2026 20:39 IST. Command(s): `aws rds describe-db-instances` · `aws ec2 describe-security-groups --group-ids sg-0db1a2b3c4d5e6f70` · `aws ec2 describe-route-tables --filters Name=association.subnet-id,Values=<db subnets>` · `aws cloudtrail lookup-events --lookup-attributes AttributeKey=EventSource,AttributeValue=ec2.amazonaws.com`. Values are the unmodified output; this is not a browser screenshot.

SAMPLE PACK · FICTIONAL COMPANY · EVERY NAME, ACCOUNT AND RESULT IN IT IS INVENTED

POLICY · POL-NETWORK

Network Security Policy

Acme Cloud's rules for network security.

Document control

Reference	POL-NETWORK
Version	1.0.0
Status	Approved — in force
Document type	Policy
Owner	Meera Kulkarni
Approved by	Rohan Desai on 2026-10-18
Effective from	2026-10-18
Next review	2027-10-18
Classification	Internal
Framework references	iso27001:A.8.20, iso27001:A.8.21, iso27001:A.8.22, iso27001:A.8.23, soc2:CC6.6

Revision history

VERSION	APPROVED	CHANGE	WRITTEN BY	APPROVED BY
1.0.0	2026-10-18	First issue.	Meera Kulkarni	Rohan Desai

1. Purpose

This policy sets out the rules of Acme Cloud Pvt Ltd ("Acme") for network security, for its software service and the customer data it holds.

2. Scope

It applies to every employee and contractor of Acme, to the production environment in AWS ap-south-1, and to the tools used to build and run the service.

3. Policy

- Acme keeps this area under the control of a named owner, the Head of Security, who reports on it at each management review.
- Controls are set to the risks in Acme's risk register and are checked by evidence collected from the live systems, read-only. Database security groups admit only the application tier and the admin VPN `E:15`.
- Exceptions are recorded with a reason, an owner and an end date, and approved by the CTO.

4. Roles

ROLE	RESPONSIBILITY
Head of Security	owns this policy and keeps it current

ROLE	RESPONSIBILITY
CTO	approves it and any exception
Every employee	follows it and reports anything that looks wrong

5. Review

This policy is reviewed every 12 months, and sooner after a significant change or incident.

Approved by **Rohan Desai** on 2026-10-18. The approval signed this exact content:

`SHA-256 e7e68962f5cd70445af62e41699f9075939187a25f75c226daa974ea4c2a93b2`

Generated by Assay on 2026-10-18. Printed or downloaded copies are uncontrolled.