VENDOR RISK ASSESSMENT

Acme Cloud Services

Acme Identity Platform (SaaS)

Assessment date: 25 June 2026
Contact: Jane Doe <jane.doe@example.com>
Reference: 00000000-0000-0000-0000-00000000sample

Executive summary

Acme Cloud Services provides strong evidence for the majority of reviewed security and privacy requirements. Independently verified SOC 2 Type II and ISO 27001 certifications support core control areas. Two requirements lack supporting evidence and one conflict between documents requires vendor clarification before final approval.

REQUIREMENTS REVIEWED	EVIDENCE FOUND	MANUAL REVIEW
8	5	1
WITHOUT EVIDENCE	**CONFLICTS**	**FOLLOW-UP QUESTIONS**
1	1	5

Overall evidence strength: Moderate.

Recommended next actions

OVERALL ASSESSMENT

Evidence partially supports the reviewed requirements

Approve subject to receiving written EU data-residency confirmation and a reconciled breach-notification SLA. All other reviewed requirements are supported by independent

01 Request written confirmation of EU data residency from vendor before contract sign-off. — High priority

02	Ask vendor to reconcile breach-notification SLA between DPA and Security Policy.	Medium priority
03	Obtain the latest penetration test executive summary and remediation status.	Medium priority
04	Schedule annual reassessment aligned with SOC 2 report refresh cycle.	Low priority

Requirements mapping

Customer-supplied requirements mapped against vendor evidence. The centrepiece of this assessment.

REQ-01 • Evidence found — Evidence Strong — Follow-up —

Vendor must hold a current independent security certification (SOC 2 / ISO 27001).

SOC 2 Type II (BDO, 2025) and ISO 27001:2022 certificate provided.

Source: SOC 2 Report — page 4; ISO certificate

REQ-02 • Evidence found — Evidence Strong — Follow-up —

All customer data must be encrypted at rest and in transit.

AES-256 at rest, TLS 1.2+ in transit, documented in Security Whitepaper §3.2.

Source: Security Whitepaper — section 3.2

REQ-03 • Evidence found — Evidence Strong — Follow-up —

Multi-factor authentication enforced for all administrative access.

Confirmed in SOC 2 control CC6.1 and Access Control Policy §4.

Source: SOC 2 Report — page 22

REQ-04 ● No evidence Evidence None Follow-up Required

Customer data processed within EU/EEA boundaries.

No documentation found specifying processing regions or data residency commitments.

REQ-05 ● Partial evidence Evidence Partial Follow-up Required

Security incidents notified to customers within agreed SLA.

DPA states 24 hours; Security Policy states 72 hours. Conflict pending clarification.

Source: DPA §7.3; Security Policy §9

REQ-06 ● Manual review Evidence Manual Follow-up Required

Annual penetration testing performed by an independent third party.

Reference to annual pentests in Security Whitepaper, but no recent report provided.

Source: Security Whitepaper — section 5

REQ-07 ● Evidence found Evidence Strong Follow-up —

Documented Business Continuity and Disaster Recovery plan with annual testing.

BCP / DRP document provided with 2024 test results.

Source: BCP Document — page 12

REQ-08 ● Evidence found Evidence Strong Follow-up —

Sub-processor list maintained and customers notified of changes.

Sub-processor list provided; change notification process in DPA §6.

Source: DPA §6; Sub-processor list

Detailed findings

1 high 1 medium 1 low

● **SOC 2 Type II report covers all in-scope trust criteria** Low

Independent auditor opinion (BDO, 2025) confirms operating effectiveness of controls for Security, Availability and Confidentiality over a 12-month review period with no exceptions.

Data residency commitments not documented

High

Provided contracts and policies do not specify guaranteed processing regions for EU customer data. Required for GDPR data transfer assessment.

Incident notification SLA inconsistency

Medium

The DPA commits to 24-hour breach notification while the Security Policy references 72 hours. Vendor clarification required.

Requirements without supporting evidence

- Data residency / processing region commitments for EU customers
- Penetration test executive summary from the last 12 months

Conflicting information

Breach notification SLA

The Data Processing Addendum commits to 24-hour breach notification, while the Security Policy references 72 hours. The shorter commitment in the DPA should be confirmed as authoritative.

Sources: DPA §7.3; Security Policy §9

Supporting evidence

Topics supported by independent documents. Multiple sources strengthen the assessment.

Encryption controls

Encryption at rest (AES-256) and in transit (TLS 1.2+) is confirmed independently in the SOC 2 Type II report and the Security Whitepaper.

Sources: SOC 2 Report — page 18; Security Whitepaper — section 3.2

Access control governance

Role-based access control with MFA for administrators is consistent across the Access Control Policy and SOC 2 control CC6.1.

Sources: Access Control Policy §4; SOC 2 Report — page 22

Business continuity testing

Annual BCP/DRP testing is documented both in the BCP document and the SOC 2 report (control A1.2).

Sources: BCP Document — page 12; SOC 2 Report — page 28

Missing evidence

Documents that would strengthen this assessment if provided.

- Data Processing Addendum with explicit processing regions
- Most recent penetration test executive summary
- Business continuity plan test results from the last 12 months

Follow-up questions for the vendor

- 1. [HIGH] Can you confirm in writing that EU customer data is processed exclusively within the EU/EEA, and provide the relevant DPA addendum?
  Required for our GDPR transfer assessment.
- 2. [HIGH] Which SLA is authoritative for breach notification — 24 hours (DPA) or 72 hours (Security Policy)?
- 3. [MEDIUM] Please share the executive summary of your most recent independent penetration test and the remediation status of any findings.
- 4. [LOW] Do you maintain a customer-facing trust portal where sub-processor changes are communicated proactively?
- 5. [MEDIUM] Please confirm the retention period for customer data after contract termination.

Methodology

Governly maps customer-supplied requirements to vendor evidence across Information Security, Data Protection & Privacy, Access Control & Identity, Business Continuity & Resilience, Vendor Governance, and Documentation Completeness. Each requirement is independently evaluated; the report highlights what is supported, what is missing, and what requires manual verification.

SUPPLEMENTARY SCORING

Composite score	**78 / 100**
Information Security	86 / 100
Data Protection & Privacy	68 / 100
Access Control & Identity	84 / 100
Business Continuity & Resilience	74 / 100
Vendor Governance	80 / 100
Documentation Completeness	76 / 100

Numerical scores are supplementary. The primary assessment is the requirement-by-requirement evidence review above.