SOC 2® TYPE II

READINESS & CONTROL ASSESSMENT

2026 Sample Report · Illustrative Sample Deliverable

ApexCloud Technologies, Inc.

Fictional U.S.-Based SaaS & Cloud Technology Company

Trust Services Criteria — Security, Availability & Confidentiality

CONFIDENTIAL — SAMPLE / DEMONSTRATION

FICTIONAL SAMPLE REPORT — NOT AN ACTUAL SOC 2 ATTESTATION

This document is a simulated SOC 2 Type II Readiness & Control Assessment created by TMG Security to demonstrate report structure, Type II testing methodology, evidence handling, findings, and professional reporting standards. ApexCloud Technologies, Inc. is fictional. No actual SOC 2 examination, independent service auditor's report, attestation opinion, or certification was performed or issued.

Assessment Period	01 Jan 2026 – 31 Aug 2026	**Report Date**	03 September 2026
Report Version	1.0	**Classification**	**Confidential**
Assessment Performed By	TMG Security	**Assessment Type**	Type II Readiness & Control Assessment

CONFIDENTIALITY NOTICE

This document, including all findings and illustrative data herein, is provided by TMG Security strictly as a demonstration sample. Distribution outside its intended demonstration purpose without written consent is discouraged. This report does not constitute, and must not be represented as, an actual SOC 2 report, SOC 2 certification, attestation, audit opinion, or independent service auditor's report. An actual SOC 2 Type II examination and attestation report must be performed and issued by an appropriately qualified independent service auditor in accordance with applicable AICPA professional standards.

DOCUMENT CONTROL

Document Owner	TMG Security — Governance, Risk & Compliance (GRC) Practice
Prepared By	TMG Security Assessment Team
Reviewed By	TMG Security Quality Assurance Lead
Version	1.0
Issue Date	03 September 2026
Classification	CONFIDENTIAL — SAMPLE / DEMONSTRATION
Assessment Type	Fictional SOC 2 Type II Readiness & Control Assessment
Assessment Period	01 January 2026 – 31 August 2026
Assessment Subject	ApexCloud Technologies, Inc. (Fictional Entity)
Performed By	TMG Security

Document Change History

Version	Date	Description	Author
1.0	03 Sep 2026	Initial issue of sample report	TMG Security Assessment Team

Distribution List

Name / Role	Organization	Purpose
Chief Executive Officer (Fictional)	ApexCloud Technologies, Inc.	Primary recipient
Chief Information Security Officer (Fictional)	ApexCloud Technologies, Inc.	Primary recipient
VP Engineering (Fictional)	ApexCloud Technologies, Inc.	Platform & change management oversight
Engagement Lead	TMG Security	Quality assurance / archival

IMPORTANT NOTICE

FICTIONAL SAMPLE REPORT — NOT AN ACTUAL SOC 2 ATTESTATION

This report has been produced solely for demonstration and portfolio purposes on behalf of TMG Security. It is intended to illustrate the structure, depth, Type II testing methodology, and professional standard of a SOC 2 Type II readiness and control assessment deliverable. To ensure there is no ambiguity regarding the nature of this document, TMG Security sets out the following clarifications:

- ApexCloud Technologies, Inc. is a fictional entity. It does not correspond to any real company, and any resemblance to an actual organization is purely coincidental.
- No actual SOC 2 examination, readiness review, or control assessment was performed against any real environment, system, or organization.
- No production environment, system, or network of any kind was accessed, scanned, or tested in the creation of this report; no real customer data or confidential business information was accessed at any point.
- No SOC 2 certification, attestation opinion, or independent service auditor's report has been issued to any party as a result of this document. TMG Security has not issued an AICPA SOC 2 attestation opinion through this sample, and no fictional CPA firm, auditor license, or AICPA authorization is represented anywhere in this document.
- All Type II testing results, sample selections, populations, evidence references, exceptions, findings, risk ratings, illustrative dates, control statuses, and management responses contained in this report are illustrative and fictional. They were constructed to demonstrate realistic reporting and testing conventions and do not describe any actual security or compliance condition.
- The fictional tabletop exercise scenario referenced in Section 26 (Incident Response & Security Operations) is provided solely to demonstrate TMG Security's incident response assessment methodology. No actual incident, breach, or security event occurred.
- TMG Security is not representing, and this document must not be interpreted as representing, that TMG Security is an independent service auditor, CPA firm, or that it performed an actual AICPA SOC 2 examination.

Intended Use

This sample report may be shared with prospective clients, partners, and other interested parties to illustrate TMG Security's SOC 2 readiness assessment methodology, documentation standards, and reporting quality. It should not be relied upon for any compliance, legal, contractual, procurement, or risk decision. An actual SOC 2 Type II examination and attestation report must be performed and issued by an appropriately qualified independent service auditor in accordance with applicable AICPA professional standards, and organizations should consult qualified legal and compliance counsel regarding their own SOC 2 readiness.

Type II Concept — Important Note

A SOC 2 Type II report differs fundamentally from a point-in-time (Type I) assessment: it evaluates not only the design of controls but their operating effectiveness across an assessment period, based on sampled evidence, identified exceptions, and management's remediation. This sample report is styled as a Type II-style readiness and operating-effectiveness assessment — using illustrative sampling, testing procedures, and exception reporting consistent with Type II methodology — to demonstrate how TMG Security approaches this deeper level of control testing. It remains, in all respects, an illustrative readiness assessment prepared by TMG Security and not an independent SOC 2 attestation.

TABLE OF CONTENTS

Document Control 2
Important Notice 3
01 Executive Summary 5
02 Assessment Overview 6
03 Organization Profile 6
04 Assessment Objectives 7
05 Scope & Boundaries 8
06 Trust Services Criteria Framework 8
07 SOC 2 Applicability & Assessment Approach 9
08 Assessment Methodology 10
09 System Description & System Boundaries 12
10 Infrastructure & Technology Architecture 14
11 Data Flow & Information Classification 15
12 Governance & Security Organization 16
13 Control Environment 16
14 Risk Assessment 17
15 Communication & Information 20
16 Monitoring Activities 20
17 Logical & Physical Access Controls 21
18 System Operations 21
19 Change Management 22
20 Risk Mitigation 23
21 Availability Controls 23
22 Confidentiality Controls 24
23 Vendor & Third-Party Risk Management 25
24 Security Awareness & Workforce Management 25
25 Vulnerability & Patch Management 26
26 Incident Response & Security Operations 27
27 Business Continuity & Disaster Recovery 28
28 Backup & Recovery 28
29 Encryption & Data Protection 29
30 Findings Summary 30
31 Detailed Control Exceptions & Findings 31
32 Risk Heatmap 39
33 Type II Operating Effectiveness Summary 40
34 90-Day Remediation Roadmap 41
35 Management Action Plan 42
36 Final Assessment & Conclusion 43
37 Evidence Register 45
38 Control Testing Register 45
39 Finding Register 48
40 SOC 2 Control Matrix 49
41 Management Assertion & Responsibility 51
42 Regulatory / Framework Watch — 2026 52
43 Assessment Limitations 52
44 Glossary 53
45 Contact & Disclaimer 53

01 EXECUTIVE SUMMARY

TMG Security has prepared this fictional, illustrative SOC 2 Type II Readiness & Control Assessment sample to represent ApexCloud Technologies, Inc., a hypothetical U.S.-based enterprise SaaS and cloud technology company. This section presents a fictional executive-level summary of the simulated Type II-style operating-effectiveness assessment, prepared in the style and format TMG Security would use for an actual readiness engagement.

ALL METRICS, FINDINGS, AND SCORES ON THIS PAGE ARE FICTIONAL SAMPLE DATA

Overall Illustrative Assessment Status

PARTIALLY EFFECTIVE

ApexCloud's simulated environment demonstrates a mature foundational Security, Availability, and Confidentiality control program, with a defined set of fictional Type II-style exceptions requiring remediation before an independent SOC 2 Type II examination. This illustrative status reflects a sample readiness assessment and does not represent an official SOC 2 opinion, attestation, or certification.

Fictional Sample Control & Findings Dashboard

72	56	11	5	14
Controls Assessed	Effective	Partially Effective	Not Effective	Findings / Observations

0	3	6	3	2
Critical	High	Medium	Low	Observations

Executive Risk Narrative

The fictional Type II-style assessment tested 72 illustrative controls across the Security (common criteria), Availability, and Confidentiality Trust Services Criteria, sampling evidence across the 01 January 2026 – 31 August 2026 assessment period rather than evaluating design alone. No sample finding was rated Critical. Three high-severity findings concern privileged access review evidence retention across cloud, container, and database administrative tiers; emergency-change retroactive approval and post-implementation review documentation; and governance of vulnerability remediation exceptions. Six medium-severity findings span security event alert-triage evidence, disaster recovery testing coverage for two business-critical services, delayed annual vendor risk reassessment, security awareness training completion tracking, incident response tabletop exercise scenario coverage, and backup restoration evidence for a secondary database. Three low-severity findings reflect narrower confidentiality-labeling, control-monitoring documentation, and business continuity contact-validation gaps, and two observations note forward-looking hardening and documentation-currency opportunities that did not rise to the level of a control exception.

Across these fictional results, ApexCloud's simulated program shows particular strength in its identity architecture and MFA enforcement, centralized SIEM monitoring, vulnerability identification coverage, documented incident response planning, cloud security baseline, backup architecture, and vendor governance framework, alongside developing maturity in privileged access recertification evidence, emergency-change documentation discipline, vulnerability exception governance, disaster recovery test coverage, vendor reassessment timeliness, and Type II evidence-retention consistency more broadly. TMG Security's simulated recommendation is that ApexCloud prioritize closure of the three high-severity findings within the first 30 days of the fictional remediation roadmap (see Section 34), with remaining items addressed across a 90-day window, ahead of engaging an independent service auditor for an actual SOC 2 Type II examination.

This summary, and every figure, finding, and status on this page and throughout this report, is entirely fictional and constructed for demonstration purposes only. It does not describe the security, availability, or confidentiality posture of any real organization, and does not constitute a SOC 2 report, SOC 2 certification, attestation opinion, or independent service auditor's report.

02 ASSESSMENT OVERVIEW

This fictional sample report presents the results of a simulated SOC 2 Type II Readiness & Control Assessment performed by TMG Security on behalf of ApexCloud Technologies, Inc. The assessment is designed to illustrate how TMG Security evaluates an organization's control environment against the AICPA Trust Services Criteria using Type II-style operating-effectiveness testing, and how TMG Security documents and reports the results of that evaluation ahead of an actual independent SOC 2 examination.

Engagement Summary

Assessment Type	SOC 2 Type II Readiness & Control Assessment (Illustrative)
Assessment Period	01 January 2026 – 31 August 2026 (Fictional)
Assessment Subject	ApexCloud Technologies, Inc. (Fictional Entity)
Performed By	TMG Security
Trust Services Criteria	Security (common criteria — mandatory), Availability, Confidentiality
Overall Illustrative Status	Partially Effective

Purpose of This Report

This report is intended to give ApexCloud's leadership a structured, evidence-referenced view of the organization's fictional control design and operating effectiveness at a point in time, including illustrative Type II-style testing exceptions, associated risk, and a prioritized remediation path. Consistent with TMG Security's actual engagement deliverables, the report combines a system description, a Trust Services Criteria control review, illustrative operating-effectiveness testing, and a formal risk assessment into a single consulting-format deliverable — the kind of readiness work an organization typically completes before engaging an independent CPA firm for an actual SOC 2 Type II examination.

How to Read This Report

- Sections 1–11 establish context: organization profile, objectives, scope, the Trust Services Criteria framework applied, methodology, the system description, infrastructure architecture, and data flow/classification.
- Sections 12–29 present the detailed control-area review, organized around governance and the nine Security common criteria (CC1–CC9), followed by Availability, Confidentiality, and supporting operational domains including vendor risk, workforce awareness, vulnerability management, incident response, business continuity, backup, and encryption.
- Sections 30–36 consolidate findings into a Findings Summary, Detailed Control Exceptions & Findings, Risk Heatmap, Type II Operating Effectiveness Summary, 90-Day Remediation Roadmap, Management Action Plan, and Final Assessment & Conclusion.
- Sections 37–45 provide the supporting appendix: Evidence Register, Control Testing Register, Finding Register, SOC 2 Control Matrix, Management Assertion, the 2026 Regulatory/Framework Watch, Assessment Limitations, Glossary, and Contact & Disclaimer.

03 ORGANIZATION PROFILE

Organization	ApexCloud Technologies, Inc. (Fictional)
Industry	Cloud Software / SaaS / Enterprise Technology
Headquarters	Austin, Texas, USA

Employees	Approximately 850
Customers	Approximately 2,400 enterprise and mid-market customers
Assurance Status	Treated as pursuing SOC 2 Type II readiness for purposes of this fictional demonstration

Business Description (Fictional)

ApexCloud Technologies, Inc. is presented as a U.S.-based provider of an enterprise SaaS platform, cloud-hosted business applications, API services, analytics and reporting, and identity and access management integrations, supporting approximately 2,400 enterprise and mid-market customers. This narrative is illustrative and constructed solely to give context to the sample findings that follow.

Technology Environment (Fictional)

In this fictional scenario, ApexCloud's platform runs on AWS cloud infrastructure using Kubernetes/containerized workloads, PostgreSQL databases, object storage, and API gateways, deployed through CI/CD pipelines from Git-based source control. The environment includes an enterprise SSO/identity provider with MFA, centralized SIEM, EDR, vulnerability management, endpoint management, backup and disaster recovery infrastructure, an ITSM/ticketing platform, and a customer support platform, alongside a defined population of third-party SaaS subservice organizations. The organization's simulated environment processes customer business data, user account and authentication information, business contact information, application telemetry, customer-generated content, and confidential business information.

Major Strengths (Fictional)

- Centralized SSO with MFA enforced on the primary platform, administrative consoles, and remote-access paths.
- Mature vulnerability identification program with continuous automated scanning across cloud, container, and endpoint layers.
- Documented, exercised Incident Response Plan with defined severity classification and escalation roles.
- Immutable, encrypted backup architecture with a defined restoration testing program.
- Structured vendor risk management framework with contractual security and incident-notification requirements.

Major Gaps (Fictional)

- Privileged access recertification evidence not consistently retained across cloud, container, and database administrative tiers (see SOC2-ACC-001).
- Emergency-change retroactive approval and post-implementation review documentation incomplete for select changes (see SOC2-CHG-002).
- Vulnerability remediation exceptions not consistently routed through the formal risk-acceptance process (see SOC2-VUL-003).

Immediate Priorities (Fictional)

- Migrate privileged access recertification into a centralized, system-evidenced IAM governance workflow.
- Close the three high-severity findings related to access governance, emergency-change documentation, and vulnerability exception governance.
- Complete outstanding disaster recovery testing and vendor reassessment cycles ahead of engaging an independent service auditor.

04 ASSESSMENT OBJECTIVES

This fictional assessment was designed to evaluate ApexCloud's SOC 2 readiness against five core objectives, consistent with the structure TMG Security applies to an actual Type II-style readiness engagement.

- Evaluate the design and Type II-style operating effectiveness of ApexCloud's control environment against the Security common criteria (CC1–CC9).

- Assess ApexCloud's Availability commitments, including backup, disaster recovery, and infrastructure resilience controls.
- Assess ApexCloud's Confidentiality controls, including data classification, access restriction, and encryption of confidential information.
- Review ApexCloud's oversight of subservice organizations and third-party vendors supporting the in-scope system.
- Identify control exceptions and readiness gaps that should be remediated prior to engaging an independent service auditor for an actual SOC 2 Type II examination.

Scope & Boundaries

The table below presents the fictional scope boundary defined for this sample assessment. Scope determinations shown are illustrative and follow the general structure TMG Security uses to document engagement boundaries during an actual SOC 2 readiness engagement.

Component	Description	Scope Determination
Enterprise SaaS Platform & API Services	Core customer-facing application, API gateway, and customer administrative interface.	IN SCOPE
AWS Cloud Infrastructure	Compute, storage, networking, and managed database services underlying the platform.	IN SCOPE
CI/CD & Source Control	Git-based source control and the CI/CD pipeline supporting production deployment.	IN SCOPE
Identity, MFA & Privileged Access	SSO/IdP, MFA enforcement, and privileged access paths to in-scope systems.	IN SCOPE
Subservice Organizations (10 categories sampled)	Cloud hosting, identity, monitoring, backup, CI/CD, email, CRM, payment, HR, and ITSM providers.	IN SCOPE — THIRD PARTY
Security Monitoring & Incident Response	SIEM, EDR, and the incident response program supporting in-scope systems.	IN SCOPE
Backup, DR & Business Continuity	Backup infrastructure, disaster recovery, and business continuity planning for in-scope services.	IN SCOPE
Corporate HR / Payroll Administration Systems	Internal HR and payroll administration with no customer data processing.	OUT OF SCOPE
Marketing Website & CMS	Public marketing website with no authenticated customer data processing.	OUT OF SCOPE
Processing Integrity & Privacy (Trust Services Categories)	Not selected as primary criteria for this illustrative engagement.	OUT OF SCOPE

06 TRUST SERVICES CRITERIA FRAMEWORK

This assessment is structured around the AICPA 2017 Trust Services Criteria, with the 2022 revised Points of Focus, as currently applied in SOC 2 examinations. The table below summarizes the framework components applied throughout this report.

Selected Trust Services Categories

Security is the mandatory common criterion underlying every SOC 2 examination; ApexCloud has additionally selected Availability and Confidentiality as applicable criteria for this fictional engagement, consistent with the nature of its SaaS platform and its commitments to enterprise customers regarding uptime and confidential data handling. Processing Integrity and Privacy were not selected as primary criteria for this illustrative engagement and are treated as out of scope.

Trust Services Category	Role in This Engagement	Coverage in This Report
Security (Common Criteria)	Mandatory / Core	Sections 12–20 — CC1 Control Environment through CC9 Risk Mitigation.
Availability	Additional Criterion — Selected	Section 21 — Availability commitments, SLA monitoring, backup, DR, and resilience.
Confidentiality	Additional Criterion —	Section 22 — Data classification, access restriction, and encryption of confidential

Trust Services Category	Role in This Engagement	Coverage in This Report
	Selected	information.
Processing Integrity	Not Selected — Out of Scope	Not assessed in this illustrative engagement.
Privacy	Not Selected — Out of Scope	Not assessed in this illustrative engagement.

Security Common Criteria Categories (CC1–CC9)

CC1	Control Environment
CC2	Communication and Information
CC3	Risk Assessment
CC4	Monitoring Activities
CC5	Control Activities
CC6	Logical and Physical Access Controls
CC7	System Operations
CC8	Change Management
CC9	Risk Mitigation

This report references specific Trust Services Criteria (e.g., CC6.2, A1.3, C1.1) and their general subject matter where relevant to a control or finding. No proprietary AICPA implementation guidance text is reproduced; criteria references are used solely to indicate the general control category being assessed.

07 SOC 2 APPLICABILITY & ASSESSMENT APPROACH

This section presents TMG Security's fictional applicability determination for ApexCloud, and explains the Type II-style assessment approach applied throughout this sample report.

Applicability Determination (Fictional)

ApexCloud Technologies, Inc. is treated in this fictional scenario as a service organization providing SaaS, API, and data processing services to enterprise and mid-market customers who rely on ApexCloud's controls as part of their own vendor risk management and, in many cases, their own compliance obligations. A SOC 2 report — Type I (design, point-in-time) or Type II (design and operating effectiveness, over a period) — is the standard mechanism by which such a service organization provides independent assurance to its customers. This report is styled as a Type II-style readiness and operating-effectiveness assessment to prepare ApexCloud for an actual independent examination.

Type I vs. Type II — Why This Report Is Styled as Type II

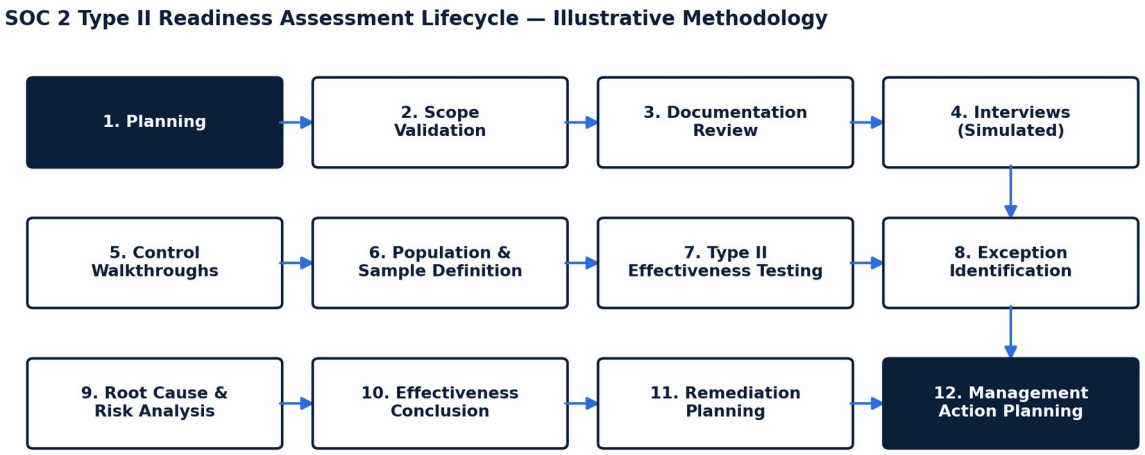
A Type I report addresses whether controls are suitably designed and implemented as of a specific date. A Type II report addresses that same design question and, in addition, whether the controls operated effectively throughout a defined period — typically 6 to 12 months — based on the service auditor's testing of a sample of evidence generated during that period. This sample report adopts Type II-style methodology (population definition, sample selection, evidence testing, exception identification, and conclusion) across the 01 January 2026 – 31 August 2026 assessment period to demonstrate the deeper level of assurance a Type II engagement provides, while remaining, in every respect, an illustrative TMG Security readiness assessment rather than an actual independent examination.

Assessment Approach Summary

Control Design Assessment	Confirmed each in-scope control is appropriately designed to meet its stated control objective.
Control Implementation Walkthrough	Walked through each control with the fictional control owner to confirm the control is implemented as designed.
Type II Operating Effectiveness Testing	Selected samples of evidence generated during the assessment period and tested for consistent operation (see Section 38, Control Testing Register).
Exception Identification & Root Cause Analysis	Documented any sampled instance where a control did not operate as designed, and the underlying root cause.
Evidence Sufficiency Evaluation	Assessed whether the evidence obtained was sufficient and appropriate to support a testing conclusion.
Management Remediation & Retest Planning	Captured management's response to each exception and defined retest requirements for the next assessment cycle.

08 ASSESSMENT METHODOLOGY

TMG Security applies a structured, repeatable twelve-stage methodology across every SOC 2 readiness engagement, illustrated here in a fictional context. Because this is a demonstration report, every interview, evidence review, and technical validation step referenced throughout this document is simulated: no actual ApexCloud personnel were interviewed, no actual ApexCloud systems were accessed, and no actual evidence was collected or reviewed.



SOC 2 Type II Readiness Assessment Lifecycle — Illustrative Methodology

Methodology Stages

1. Planning	Define engagement objectives, Trust Services Criteria scope, and assessment timeline with ApexCloud stakeholders.
2. Scope Validation	Confirm the boundary of in-scope systems, subservice organizations, and the system description.
3. Documentation Review	Review policies, standards, prior risk assessments, and control narratives.
4. Interviews / Simulated Interviews	Interview (in this fictional scenario, simulate interviews with) control owners across engineering, security, and operations.
5. Control Walkthroughs	Observe and walk through key control-environment, access, and operational controls to confirm design and implementation.
6. Population & Sample Definition	Define the full population of instances for each control and select a representative sample for testing.
7. Type II Operating Effectiveness Testing	Test the selected sample of evidence generated throughout the assessment period, not merely a point-in-time snapshot.
8. Exception Identification	Document any sampled instance where a control did not operate exactly as designed.
9. Root Cause & Risk Analysis	Determine the underlying cause of each exception and assess likelihood, impact, and residual risk.
10. Control Effectiveness Conclusion	Reach an Effective / Partially Effective / Not Effective conclusion for each tested control.
11. Remediation Planning	Develop actionable, prioritized remediation guidance for each finding, including a required retest scope.
12. Management Action Planning	Present findings to management and align on ownership, priority, and target remediation dates.

Illustrative Type II Sampling Approach

Consistent with Type II methodology, TMG Security selected samples spanning the full 01 January 2026 – 31 August 2026 assessment period rather than a single point in time. Representative fictional sample sizes applied in this assessment include:

- 8 quarterly/monthly privileged access review cycles

- 25 terminated-user access-revocation records
- 12 change-management tickets (standard, normal, and emergency)
- 6 monthly vulnerability remediation cycles
- 10 backup restoration evidence records
- 20 security awareness training completion records
- 15 vendor risk assessments

Every population, sample size, testing procedure, and result referenced in this report is fictional and provided solely to demonstrate TMG Security's Type II-style testing methodology (see Section 38, Control Testing Register, for the full illustrative testing model).

09 SYSTEM DESCRIPTION & SYSTEM BOUNDARIES

This section presents a fictional SOC 2-style system description for ApexCloud's in-scope platform, covering the services provided, principal service commitments, system components, and boundaries — structured the way TMG Security would document a system description in an actual readiness engagement.

Services Provided

- Enterprise SaaS platform for business workflow, reporting, and collaboration.
- Cloud-hosted business applications and customer-configurable modules.
- API services enabling customer and partner system integrations.
- Customer data processing, analytics, and reporting.
- Identity and access management integrations (SSO/SAML) for customer end-users.
- Enterprise customer support via a dedicated support platform.

Principal Service Commitments (Illustrative)

ApexCloud's fictional service commitments to customers include: maintaining the confidentiality of customer data submitted to the platform; maintaining logical access controls restricting system access to authorized users; monitoring the production environment for security events; maintaining defined availability and backup/recovery commitments; and notifying customers of security incidents affecting their data in accordance with contractual and applicable legal obligations. These commitments are illustrative and do not represent actual contractual terms.

System Components

Infrastructure	AWS multi-availability-zone cloud infrastructure; Kubernetes-orchestrated containerized workloads; managed PostgreSQL databases; object storage; API gateways.
Software	The ApexCloud SaaS application, internal administrative tooling, CI/CD pipeline, SIEM, EDR, vulnerability management, and endpoint management platforms.
People	Engineering, Security Operations, IT, Third-Party Risk, Compliance/GRC, and Customer Support functions, together with defined control owners for each in-scope control.
Procedures	Documented policies and control procedures covering access management, change management, incident response, backup/recovery, and vendor risk management.
Data	Customer business data, user account and authentication information, business contact information, application telemetry, customer-generated content, and confidential business information.

System Boundaries

The in-scope system boundary includes the ApexCloud SaaS platform, its supporting AWS cloud infrastructure, the CI/CD deployment pipeline, the corporate identity and endpoint management environment, and the ten subservice organization categories described below. It excludes internal HR/payroll administration systems and the public marketing website, neither of which process customer data within the platform boundary.

Subservice Organizations

ApexCloud relies on a defined set of subservice organizations to deliver its platform. The table below presents fictional/industry-standard subservice categories, the associated dependency, relevant risk, and the shared-responsibility model applied to each — consistent with how a SOC 2 system description discloses subservice organizations under the carve-out or inclusive method.

Category	Service / Dependency	Relevant Risk / Responsibility Model
Cloud Infrastructure Provider	Compute, storage, managed database, and networking infrastructure underlying the ApexCloud platform. *Dependency: Foundational — all production services depend on this provider's availability and physical/environmental security controls.*	Risk: Regional outage, infrastructure-layer misconfiguration, or a provider-side security incident. Provider: physical security, hypervisor/host security, infrastructure availability. ApexCloud: configuration, identity, application, and data-layer security (shared responsibility model).
Identity Provider (IdP)	Centralized SSO and MFA enforcement for workforce and administrative access. *Dependency: High — supports the primary logical access control (CC6.1) across nearly all in-scope*	Risk: IdP outage affecting workforce access, or compromise of the IdP tenant itself. Provider: authentication infrastructure availability and platform-level security. ApexCloud: conditional access policy configuration, MFA enrollment enforcement, and

Category	Service / Dependency	Relevant Risk / Responsibility Model
	systems.	access provisioning/deprovisioning.
Email & Collaboration Platform Provider	Corporate email, messaging, and document collaboration. *Dependency: Moderate — a channel for both internal communication and a potential confidentiality/phishing attack surface.*	Risk: Phishing/business email compromise, or misconfigured sharing permissions on collaboration content. Provider: platform availability and baseline security controls. ApexCloud: DLP configuration, sharing policy, and workforce awareness training.
CRM / Customer Support Platform	Customer relationship management and support-ticketing platform used by Customer Success and Support teams. *Dependency: Moderate — stores customer business contact information and support interaction records.*	Risk: Excessive internal access to customer records, or a platform-side security incident. Provider: platform security and availability. ApexCloud: role-based access provisioning and data minimization within the platform.
Payment Processing Platform	Subscription billing and payment processing for customer accounts. *Dependency: Moderate — ApexCloud does not directly store full payment card data; processing is tokenized through the provider.*	Risk: Provider-side payment data incident (outside ApexCloud's direct control boundary) or billing-integration misconfiguration. Provider: payment data security and applicable card-network compliance. ApexCloud: secure integration configuration and access restriction to billing administration functions.
Monitoring / SIEM Provider	Cloud-hosted SIEM and log-aggregation platform supporting security monitoring. *Dependency: High — supports CC7.2 security event monitoring across the environment.*	Risk: Monitoring platform outage or misconfiguration resulting in a detection gap. Provider: platform availability and log-ingestion reliability. ApexCloud: alert rule configuration, triage staffing, and disposition documentation.
Backup & Recovery Provider	Offsite and immutable backup storage for production databases and critical configuration. *Dependency: High — supports A1.2 availability/backup commitments.*	Risk: Backup data unavailability, corruption, or failure to meet recovery point objectives. Provider: storage durability and immutability enforcement. ApexCloud: backup scheduling, encryption key management, and restoration testing.
Source Code Repository / CI-CD Platform	Git-based source control and CI/CD pipeline orchestration. *Dependency: High — supports CC8.1 change management and software supply chain integrity.*	Risk: Compromise of build pipeline credentials or an unreviewed change reaching production. Provider: platform availability and access-control infrastructure. ApexCloud: branch protection rules, review requirements, and deployment approval gates.
HR / Workforce Platform	Human resources system of record, used to trigger onboarding, role-change, and termination workflows. *Dependency: Moderate — supports CC6.2/CC6.3 joiner-mover-leaver access lifecycle automation.*	Risk: Delayed or failed synchronization between HR status changes and access provisioning/deprovisioning systems. Provider: platform availability. ApexCloud: integration configuration and reconciliation between HR status and access state.
ITSM / Ticketing Platform	IT service management platform used for change management, incident tracking, and access request workflows. *Dependency: Moderate — supports CC8.1 change management and CC7.3 incident response documentation.*	Risk: Platform outage affecting the organization's ability to log or evidence changes and incidents during the outage window. Provider: platform availability. ApexCloud: workflow configuration, SLA enforcement, and evidence retention.

No certification, assurance status, or compliance claim is made or implied for any real vendor or provider category. Subservice organization names are generic and illustrative.

Shared Responsibility Matrix

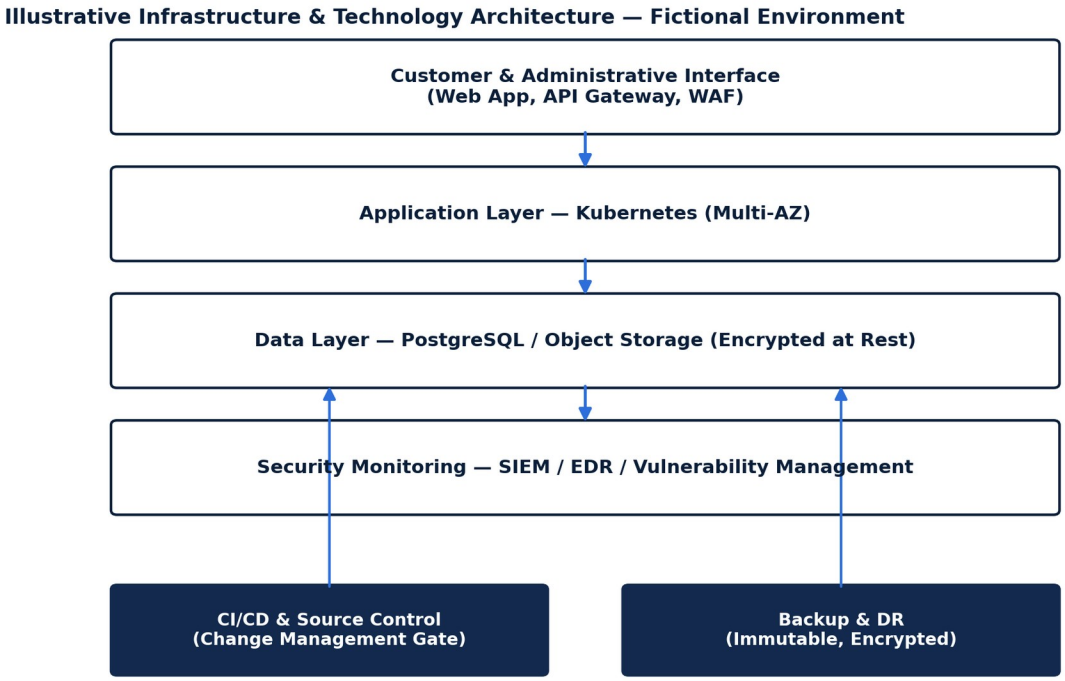
The matrix below summarizes, at a high level, how control responsibility is divided among ApexCloud, its customers, and its subservice organizations across key domains.

Area	ApexCloud	Customer	Subservice Org.
Physical & Environmental Security	Not applicable (cloud-hosted)	Not applicable	Full responsibility (cloud infrastructure provider)
Infrastructure Availability	Configuration, redundancy design, monitoring	Not applicable	Underlying compute/network/storage availability
Network & Platform Security Configuration	Full responsibility	Not applicable	Shared (provider-level network controls)
Application-Layer Security	Full responsibility	Not applicable	Not applicable
Identity & Access Management (Workforce)	Full responsibility (provisioning, MFA policy, review)	Not applicable	Authentication infrastructure availability (IdP)
Identity & Access Management (Customer End-Users)	Platform-level authentication controls and SSO/SAML support	Full responsibility (end-user account administration within their tenant)	Not applicable
Data Encryption (At Rest / In Transit)	Full responsibility	Not applicable	Underlying storage/KMS infrastructure
Data Classification & Handling	Full responsibility (policy, enforcement)	Responsible for data submitted to the platform	Not applicable
Change Management	Full responsibility	Not applicable	Underlying CI/CD platform availability
Vulnerability & Patch Management	Full responsibility (application, container, and configuration layers)	Not applicable	Underlying infrastructure/hypervisor patching (cloud provider)
Backup & Recovery	Full responsibility (scheduling, testing, restoration)	Not applicable	Storage durability and immutability
Incident Response	Full responsibility (detection, response, customer notification)	Reporting suspected incidents observed within their use of the platform	Notification of subservice-side incidents affecting ApexCloud
Security Awareness Training	Full responsibility (workforce)	Responsible for their own end-user security practices	Not applicable
Vendor / Subservice Risk Management	Full responsibility (assessment,	Not applicable	Cooperation with due-diligence requests

Area	ApexCloud	Customer	Subservice Org.
	monitoring)		and SOC report provision
Business Continuity Planning	Full responsibility	Maintaining their own continuity plans for platform dependency	Underlying infrastructure resilience

10 INFRASTRUCTURE & TECHNOLOGY ARCHITECTURE

The diagram below presents a fictional, representative architecture for ApexCloud's simulated environment, from customer access through the application, data, and monitoring layers. It is provided to illustrate how TMG Security documents infrastructure architecture in an actual assessment deliverable.



Illustrative Infrastructure & Technology Architecture — Fictional Environment. Not representative of any real system.

Architecture Layers

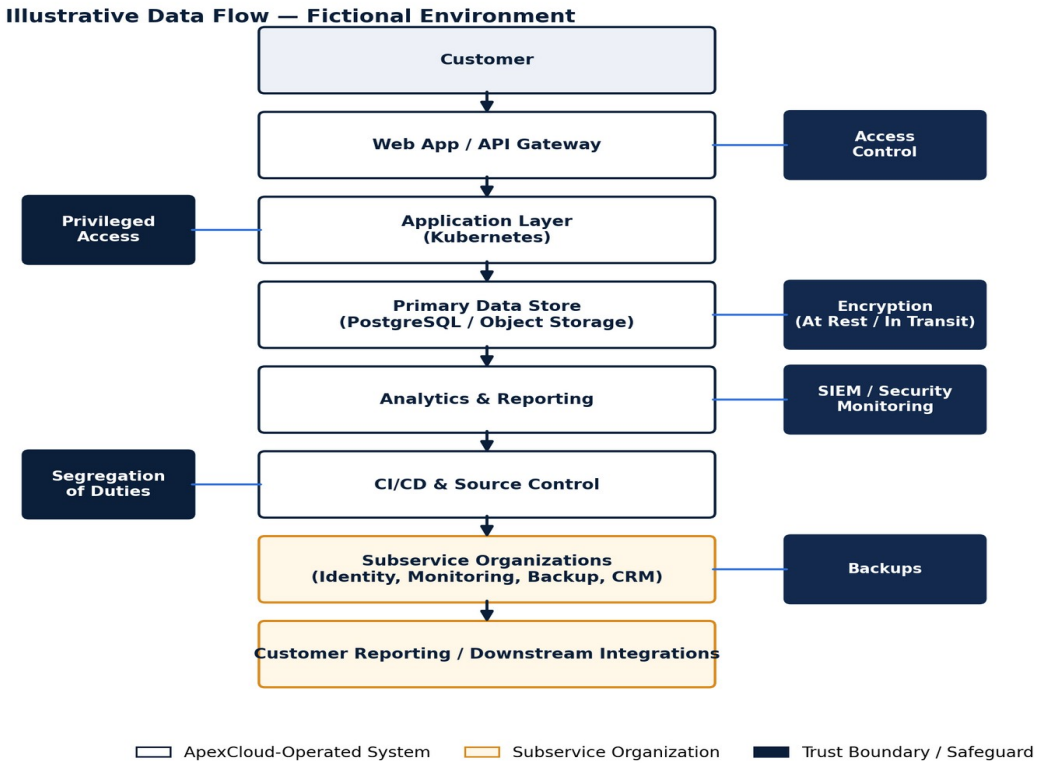
- Customer & Administrative Interface: web and API access points for customer end-users and ApexCloud administrators, fronted by a WAF and API gateway.
- Application Layer: containerized application services orchestrated by Kubernetes across multiple availability zones.
- Data Layer: managed PostgreSQL databases and object storage, encrypted at rest, with automated backup scheduling.
- CI/CD & Source Control: Git-based source control and pipeline orchestration supporting the change management program (see Section 19).
- Security Monitoring: centralized SIEM aggregating logs across infrastructure, application, and endpoint layers, supporting the controls in Section 18 and Section 26.

Architecture Observations (Fictional)

- Multi-availability-zone deployment and automated failover support the Availability commitments assessed in Section 21.
- Infrastructure-as-code with mandatory peer review governs cloud configuration changes; drift-detection coverage for manually applied emergency configuration changes is not yet complete across all accounts (see RA-003).
- Network segmentation between administrative endpoint tiers and production management interfaces is partially implemented and identified as a risk-treatment priority (see RA-002).

11 DATA FLOW & INFORMATION CLASSIFICATION

The diagram below presents a fictional, representative data flow for ApexCloud's simulated environment, from customer data ingestion through processing, storage, and downstream subservice organization integrations.



Illustrative Data Flow — Fictional Environment. Not representative of any real system.

Data Repositories & Trust Boundaries

- Customer Ingestion: primary intake point for customer-submitted business data via the web application and API.
- Application & Processing Layer: application services that process, transform, and enrich customer data.
- Primary Data Store: the production PostgreSQL database and object storage tier holding customer business data and account information.
- Analytics & Reporting: a downstream analytics environment supporting customer reporting and dashboards.
- Subservice Organizations: identity, monitoring, backup, and CRM/support platform integrations exchanging data outside ApexCloud's direct infrastructure boundary.

Information Classification

ApexCloud's fictional Data Classification Policy defines four illustrative tiers, summarized below.

Classification Tier	Description	Example Data
Restricted	Highest-sensitivity data; access limited to a narrowly defined group with a documented business need.	Production database credentials, encryption keys, customer contract terms.
Confidential	Business or customer data intended for internal or need-to-know use only.	Customer business data, contract summaries, security assessment reports.
Internal	Data intended for use within the workforce but not customer- or public-facing.	Internal process documentation, non-sensitive operational metrics.
Public	Data approved for external release.	Marketing content, published documentation, the public Trust Center.

Diagram Notes

- Privileged Access: administrative access paths into the database and cloud environment are highlighted as an elevated-risk trust boundary (see Section 17, RA-004 / RA-008).
- Endpoints: workforce endpoints represent an additional trust boundary subject to EDR and encryption controls (see Section 29).
- Backups: backup copies of customer data are shown as a distinct boundary subject to the availability and recovery controls in Section 28.

12 GOVERNANCE & SECURITY ORGANIZATION

This section presents ApexCloud's fictional security governance structure — the roles, committees, and reporting lines through which the organization's Security, Availability, and Confidentiality program is directed and overseen.

Governance Structure (Fictional)

Chief Information Security Officer (CISO)	Accountable for the overall Security, Availability, and Confidentiality control program and for this SOC 2 readiness effort.
Security Leadership Team	Cross-functional body (security, engineering, IT, GRC) meeting monthly to review control monitoring results, exceptions, and risk-acceptance decisions.
GRC Program Manager	Owns the control monitoring program, the risk register, and coordination of readiness and future independent SOC 2 activities.
Engineering Director, Platform	Accountable for change management, CI/CD pipeline controls, and platform reliability.
IAM Program Manager	Accountable for identity, access provisioning, and privileged access governance.
Third-Party Risk Manager	Oversees vendor and subservice organization due diligence, contracting, and reassessment.
Executive Leadership / Board Reporting	Receives quarterly reporting on program status, material findings, and remediation progress.

Governance Observations (Fictional)

- Executive leadership reviews the security and compliance program quarterly, with documented minutes and action tracking (CC1.2).
- Control ownership is assigned and tracked in the GRC platform for each in-scope control, supporting accountability under CC1.5.
- Reporting from operational functions (access governance, change management, vulnerability management, vendor oversight) into the governance structure is in place but would benefit from further centralization and automation, consistent with several findings in this report.

13 CONTROL ENVIRONMENT

The Control Environment criteria (CC1) address the foundation for all other Trust Services Criteria: integrity and ethical values, board/governance oversight, organizational structure, commitment to competence, and accountability for internal control.

Illustrative Assessment Summary

Criterion	Area Assessed	Status
CC1.1	Code of Conduct documented, distributed, and acknowledged annually.	Effective
CC1.2	Executive leadership reviews the security and compliance program quarterly.	Effective
CC1.3	Security roles, responsibilities, and reporting lines documented in the org chart and security RACI.	Effective
CC1.4	Workforce completes annual security awareness and role-based training.	Partially Effective
CC1.5	Individual control ownership assigned and tracked for each in-scope control.	Effective

Observations (Fictional)

ApexCloud's control environment demonstrates consistent design and operation across four of five assessed CC1 criteria. The one partial exception — annual training completion tracking — is addressed in detail in Section 24 (Security Awareness & Workforce Management) and SOC2-TRN-007.

14 RISK ASSESSMENT

CC3 requires the organization to specify objectives with sufficient clarity to enable the identification and assessment of risks, to identify and analyze risk (including fraud risk) as a basis for determining how risk should be managed, and to consider the potential for significant change that could impact the system of controls. This section presents ApexCloud's fictional illustrative enterprise risk register, developed as part of this sample assessment's simulated risk assessment exercise.

ILLUSTRATIVE FICTIONAL RISK REGISTER — DEMONSTRATION METHODOLOGY ONLY

Risk Rating Methodology

Each fictional risk below is rated by combining a Likelihood assessment (Rare, Unlikely, Possible, Likely, Almost Certain) with an Impact assessment (Insignificant, Minor, Moderate, Major, Severe) to produce an inherent risk rating, consistent with the Risk Heatmap presented in Section 32. Existing controls are then factored in to produce a residual risk rating and a recommended treatment (Mitigate, Transfer, Accept, or Avoid).

RA-001 — Credential Compromise Leading to Unauthorized Platform Access	Inherent Risk: **High**			
Threat	External threat actor obtains valid workforce or customer-facing credentials through phishing, credential stuffing, or a third-party breach involving reused passwords.			
Vulnerability	A subset of legacy internal tooling does not yet enforce MFA, and password-reuse detection is not applied to all account populations.			
Existing Controls	SSO with MFA enforced for the primary platform and administrative consoles; centralized identity provider; conditional access policies; SIEM alerting on anomalous authentication patterns.			
Likelihood	**Impact**	**Residual**	**Treatment**	**Related Control**
Possible	Major	Medium	Mitigate	CC6.1 / CC6.6 SOC2-ACC-001

RA-002 — Ransomware Affecting Production or Backup Infrastructure	Inherent Risk: **High**			
Threat	Ransomware deployed via a compromised endpoint, exposed remote-access pathway, or compromised third-party software spreads to production or backup systems.			
Vulnerability	Incomplete network segmentation between administrative endpoint tiers and production management interfaces increases lateral-movement potential.			
Existing Controls	EDR on all managed endpoints; centralized SIEM monitoring; immutable/isolated backup architecture; documented incident response and disaster recovery procedures; quarterly restoration testing (partially evidenced — see SOC2-BKP-010).			
Likelihood	**Impact**	**Residual**	**Treatment**	**Related Control**
Unlikely	Severe	Medium	Mitigate	CC7.1 / A1.2 SOC2-BKP-010

RA-003 — Cloud Misconfiguration Exposing Customer Data			Inherent Risk: **High**	
Threat	A misconfigured cloud storage bucket, security group, or IAM policy inadvertently exposes customer data or internal systems to unintended access.			
Vulnerability	Infrastructure-as-code templates are peer reviewed, but drift-detection coverage for manually applied emergency configuration changes is not yet complete across all AWS accounts.			
Existing Controls	Infrastructure-as-code with mandatory peer review; automated cloud security posture management (CSPM) scanning; quarterly cloud configuration review; least-privilege IAM policy baseline.			
Likelihood	**Impact**	**Residual**	**Treatment**	**Related Control**
Possible	Major	Medium	Mitigate	CC6.1 / CC6.6 SOC2-ASSET-014

RA-004 — Insider Threat — Misuse of Privileged Access			Inherent Risk: **Medium**	
Threat	A workforce member with privileged access intentionally or inadvertently misuses that access to view, exfiltrate, or modify customer or business data.			
Vulnerability	Privileged access recertification evidence is not consistently retained, limiting the organization's ability to promptly detect access that should have been revoked.			
Existing Controls	Role-based access control; segregation of duties for high-impact actions; audit logging of privileged actions; background screening as part of onboarding; periodic (though inconsistently evidenced) privileged access review.			
Likelihood	**Impact**	**Residual**	**Treatment**	**Related Control**
Unlikely	Major	Medium	Mitigate	CC6.2 / CC6.3 SOC2-ACC-001

RA-005 — Supply Chain Compromise via Third-Party Software Dependency			Inherent Risk: **Medium**	
Threat	A compromised open-source package, CI/CD build dependency, or third-party library introduces malicious code into the ApexCloud software supply chain.			
Vulnerability	Dependency scanning is integrated into the CI/CD pipeline, but the process for evaluating and approving new third-party dependencies prior to first use is not uniformly enforced across all engineering teams.			
Existing Controls	Automated software composition analysis (SCA) scanning in CI/CD; signed build artifacts; restricted production deployment credentials; code review requirements.			
Likelihood	**Impact**	**Residual**	**Treatment**	**Related Control**
Unlikely	Major	Medium	Mitigate	CC7.1 / CC8.1 SOC2-VUL-003

RA-006 — Extended Availability Outage Affecting Customer-Facing Services			Inherent Risk: **Medium**	
Threat	A regional cloud provider outage, cascading infrastructure failure, or failed deployment causes an extended interruption to customer-facing services.			
Vulnerability	Multi-region failover is implemented for the primary application platform, but the disaster recovery testing cadence for two business-critical services has not been fully evidenced within the assessment period.			
Existing Controls	Multi-availability-zone architecture; automated health checks and failover for the primary platform; documented incident management process; status-page and customer communication procedures.			
Likelihood	**Impact**	**Residual**	**Treatment**	**Related Control**
Unlikely	Major	Medium	Mitigate	A1.1 / A1.3 SOC2-BCP-005

RA-007 — Unauthorized Disclosure of Confidential Customer or Business Data			Inherent Risk: **Medium**	
Threat	Confidential business or customer data is disclosed to an unauthorized internal or external party through misconfigured sharing permissions, human error, or a targeted attack.			
Vulnerability	Data classification labeling and access-restriction enforcement for internal collaboration-platform repositories is applied manually rather than through automated tooling.			
Existing Controls	Data Classification Policy; confidentiality provisions in workforce and vendor agreements; role-based repository access; DLP monitoring on email and endpoint egress channels.			
Likelihood	**Impact**	**Residual**	**Treatment**	**Related Control**

Unlikely	Moderate	Low	Mitigate	C1.1 SOC2-ENC-011

RA-008 — Weak Privileged Access Governance Across Cloud and Database Tiers				Inherent Risk: **High**
Threat	Inconsistent recertification of privileged accounts across AWS IAM, Kubernetes, and database administrative tiers allows excessive or stale privileged access to persist undetected.			
Vulnerability	Privileged access review is coordinated manually across multiple systems rather than through a single centralized governance workflow.			
Existing Controls	Centralized IAM governance platform for standard user access; documented Access Control Policy; audit logging across all privileged tiers.			
Likelihood	**Impact**	**Residual**	**Treatment**	**Related Control**
Possible	Major	Medium	Mitigate	CC6.2 / CC6.3 SOC2-ACC-001

RA-009 — Failed Backup Restoration During an Actual Recovery Event				Inherent Risk: **Medium**
Threat	A backup restoration attempted during an actual outage or data-loss event fails or does not meet the committed recovery point/time objectives.			
Vulnerability	Restoration testing evidence for one secondary database was not available for one quarter within the assessment period.			
Existing Controls	Automated backup scheduling with encryption at rest; immutable backup storage tier; documented Backup Policy; restoration testing program (partially evidenced — see SOC2-BKP-010).			
Likelihood	**Impact**	**Residual**	**Treatment**	**Related Control**
Unlikely	Major	Low	Mitigate	A1.2 SOC2-BKP-010

RA-010 — Third-Party / Subservice Organization Security Compromise				Inherent Risk: **Medium**
Threat	A security incident at a critical subservice organization (cloud hosting, identity, or monitoring provider) affects the confidentiality, integrity, or availability of ApexCloud systems or customer data.			
Vulnerability	Annual reassessment of High-risk vendors is not consistently completed within the 12-month policy target, delaying visibility into changes to vendor security posture.			
Existing Controls	Vendor risk classification and onboarding due diligence; contractual security and incident-notification requirements; annual reassessment program (partially evidenced — see SOC2-TPR-006); SOC report review for critical subservice organizations.			
Likelihood	**Impact**	**Residual**	**Treatment**	**Related Control**
Unlikely	Major	Low	Mitigate	CC9.2 SOC2-TPR-006

RA-011 — Change Failure Causing Service Disruption or Security Weakness				Inherent Risk: **Medium**
Threat	An inadequately reviewed or tested production change introduces an outage, data-integrity issue, or security weakness (e.g., an inadvertently exposed configuration).			
Vulnerability	Emergency-change retroactive approval and post-implementation review are not consistently completed within policy-defined timeframes.			
Existing Controls	Peer code review requirement; CI/CD pipeline testing gates; independent deployment approval for the primary deployment pathway; documented rollback procedures.			
Likelihood	**Impact**	**Residual**	**Treatment**	**Related Control**
Possible	Moderate	Medium	Mitigate	CC8.1 SOC2-CHG-002

RA-012 — Exploitation of an Unremediated Known Vulnerability				Inherent Risk: **High**
Threat	A threat actor exploits a publicly known vulnerability in internet-facing infrastructure, a container image, or a third-party dependency that has exceeded ApexCloud's internal remediation SLA without a documented exception.			
Vulnerability	SLA-exceeding vulnerability findings are not consistently routed through the formal exception/risk-acceptance process.			
Existing Controls	Continuous automated vulnerability scanning; internal remediation SLA targets; patch management program; web application firewall on internet-facing endpoints; exception/risk-acceptance register (partially evidenced — see SOC2-VUL-003).			
Likelihood	**Impact**	**Residual**	**Treatment**	**Related Control**
Possible	Major	Medium	Mitigate	CC7.1 SOC2-VUL-003

Risk Assessment Summary

Of the 12 fictional risks in this sample register, 3 (RA-001 Credential Compromise, RA-003 Cloud Misconfiguration, and RA-008 Weak Privileged Access Governance) carry a High inherent risk rating, driven primarily by the potential severity of impact combined with the access-governance gaps identified elsewhere in this report. RA-002 (Ransomware) and RA-012 (Vulnerability Exploitation) are also rated High inherent risk given their severe/major potential impact. The remaining risks are rated Medium inherent risk, reflecting either lower likelihood or more contained potential impact. After existing controls are factored in, all 12 fictional risks reduce to a Medium or Low residual rating, reflecting ApexCloud's simulated mitigating control environment. TMG Security's simulated recommendation is that ApexCloud prioritize risk treatment for RA-001, RA-004, and RA-008 — all tied to privileged and credential access governance — within the first 30 days of the remediation roadmap (Section 34).

15 COMMUNICATION & INFORMATION

CC2 addresses how the organization obtains or generates and uses relevant, quality information to support the functioning of internal control, and how it communicates information internally and externally regarding the objectives and responsibilities for internal control.

Criterion	Area Assessed	Status
CC2.1	Security policies and objectives communicated via the policy portal and onboarding process.	Effective
CC2.2	Individual security responsibilities communicated through role-based training and policy acknowledgement.	Effective
CC2.3	Security commitments and incident notification procedures communicated externally via the Trust Center and customer agreements.	Effective

A confidential reporting channel exists for workforce members to raise suspected security or ethics concerns, and ApexCloud's Trust Center publicly communicates the organization's security and availability commitments to prospective and current customers.

16 MONITORING ACTIVITIES

CC4 addresses the organization's selection, development, and performance of ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning, and the communication of identified deficiencies for corrective action on a timely basis.

Control Monitoring Program (Fictional)

- Monthly control monitoring reviews present key metrics (access reviews, changes, vulnerabilities, incidents, training) to the GRC Program Manager and Security Leadership Team.
- Identified control deficiencies are tracked to remediation with assigned owners and target dates in the GRC platform.
- An independent penetration test of the production environment is performed annually (see EV-025).

Observations (Fictional)

Of 8 sampled monthly control monitoring review cycles, 6 had retained minutes documenting the substance of the review; 2 had confirmed meeting occurrence but no retained minutes (see SOC2-MON-012). The underlying monitoring activity — metrics review, deficiency identification, and remediation tracking — was evidenced as occurring consistently across the sampled population; the exception relates specifically to documentation retention for 2 of 8 cycles.

17 LOGICAL & PHYSICAL ACCESS CONTROLS

CC6 addresses logical and physical access security — restricting access to system resources, software, and data to authorized users and processes, and administering that access consistently across the joiner-mover-leaver lifecycle. This section presents ApexCloud's fictional illustrative access control program, including the Type II-style testing sample results supporting SOC2-ACC-001.

Identity & Access Lifecycle (Fictional)

- Joiner: access requests require documented manager and system-owner approval prior to provisioning; new hires complete security awareness training before receiving system access.
- Mover: role changes trigger a re-evaluation of assigned access via the HR-system-triggered provisioning workflow implemented in Q1 2026.
- Leaver: access is revoked across all in-scope systems within one business day of a workforce termination (see Control Testing Register, Section 38 — 25 of 25 sampled terminations effective).

Authentication & Privileged Access

- Single sign-on (SSO) via a centralized identity provider is enforced for the primary platform, administrative consoles, and internal tooling.
- Multi-factor authentication (MFA) is enforced for administrative consoles, the primary platform, and remote access, with conditional access policies applied at the identity-provider layer.
- Role-based access control (RBAC) governs standard user permissions within the platform and internal systems.
- Privileged access (AWS IAM, Kubernetes cluster-admin, database superuser) is managed through a combination of a centralized IAM governance platform (standard access) and manual, system-specific processes (privileged tiers).
- Break-glass emergency access accounts are maintained for production incident response, with use logged and subject to post-use review.
- Password controls (complexity, rotation exemption under MFA, and secure storage) and session timeout/idle-lockout controls are enforced across in-scope systems.
- Service accounts used for system-to-system authentication are inventoried and subject to the same periodic review cadence as human privileged accounts.

Periodic & Privileged Access Review — Type II Testing Result

Control	Description	Status	Finding
Standard User Access Review	Quarterly review of standard user access by system owners.	Effective	—
Privileged Access Review	Recurring review of privileged/administrative access across cloud, container, and database tiers with retained evidence.	Not Effective	SOC2-ACC-001
MFA Enforcement	MFA enforced for administrative and primary platform access.	Effective	—
Timely Termination Access Revocation	Access revoked within one business day of termination.	Effective	—

Physical Access Controls (CC6.4 / CC6.5)

ApexCloud's Austin, TX corporate office uses badge-based access control with visitor logging; production infrastructure is hosted entirely within the cloud infrastructure provider's data centers, and ApexCloud personnel do not have physical data-center access (see Section 9, Shared Responsibility Matrix). Decommissioned physical media and hardware are securely disposed of or wiped in accordance with the Data Classification Policy.

18 SYSTEM OPERATIONS

CC7 addresses the organization's processes to detect and monitor for anomalies and security events, respond to identified security incidents, and manage the capacity and performance of the system supporting its service commitments.

Security Operations Program (Fictional)

- A centralized SIEM aggregates security-relevant logs across infrastructure, application, and endpoint layers, generating alerts for anomalous activity.
- Endpoint detection and response (EDR) is deployed on all managed workforce endpoints with centralized alerting to the SOC.
- Automated vulnerability scanning covers cloud infrastructure, container images, and internet-facing endpoints on a continuous basis (see Section 25).
- A threat intelligence feed informs SIEM detection rule tuning and SOC analyst triage prioritization.
- Security metrics (alert volume, mean time to triage, vulnerability aging, change SLA adherence) are compiled and reviewed monthly by the SOC Manager and reported to the Security Leadership Team.
- Escalation procedures route confirmed security events to the Incident Response Manager per the classification thresholds in the Incident Response Plan (see Section 26).

Alert Triage — Type II Testing Result

Control	Description	Status	Finding
Security Event Monitoring	SIEM aggregates security-relevant logs and generates alerts for anomalous activity.	Effective	—
High-Priority Alert Triage	High-priority alerts triaged and dispositioned within one business day.	Partially Effective	SOC2-LOG-004
Capacity & Performance Monitoring	Infrastructure capacity and application performance continuously monitored with threshold alerting.	Effective	—

Of 10 weekly SIEM alert-triage periods sampled across the assessment period, 7 evidenced full compliance with the one-business-day triage target; 3 weeks (concentrated around holiday and reduced-coverage periods) showed delayed dispositions for a combined 14 high-priority alerts, all ultimately closed as false positives or benign. See SOC2-LOG-004 for full testing detail.

19 CHANGE MANAGEMENT

CC8 addresses the organization's process for authorizing, designing, developing, configuring, documenting, testing, approving, and implementing changes to infrastructure, data, software, and procedures to meet its objectives.

Change Management Program (Fictional)

- Standard changes: routine, pre-approved change types (e.g., configuration adjustments within defined parameters) follow a lightweight ticketed process.
- Normal changes: require a documented peer code review and a separately recorded, independent deployment approval prior to production deployment.
- Emergency changes: may be deployed ahead of full approval when business-critical, but require documented business justification and retroactive approval within 2 business days, plus a post-implementation review.
- All production code changes are tested in a non-production environment prior to deployment, and infrastructure-as-code (IaC) changes require peer review prior to apply.
- Production deployment credentials are restricted from the general engineering population, providing segregation of duties between code authorship and deployment execution for the primary deployment pathway.
- Documented rollback procedures exist and are tested annually for critical services.

Change Testing — Type II Testing Result

Control	Description	Status	Finding
Peer Code Review	Production code changes require documented peer review prior to merge.	Effective	—

Control	Description	Status	Finding
Independent Deployment Approval	Production deployments require approval independent of the code author.	Effective	SOC2-CHG-009
Emergency Change Retroactive Approval	Emergency changes receive documented retroactive approval within 2 business days.	Not Effective	SOC2-CHG-002
Segregation of Duties in Deployment	Production deployment credentials restricted from general engineering population.	Effective	—

Of 12 change-management tickets sampled (8 standard/normal, 4 emergency), 2 of the 4 emergency changes had retroactive approval recorded outside the 2-business-day policy window and 1 lacked a documented post-implementation review (SOC2-CHG-002); within the standard/normal population, 1 of 8 tickets had a deployment approval recorded shortly after rather than strictly before the CI/CD deployment timestamp, assessed as an observation rather than a control exception (SOC2-CHG-009).

20 RISK MITIGATION

CC9 addresses the organization's processes for identifying, selecting, and developing risk mitigation activities for risks arising from potential business disruptions, and for managing risks associated with vendors and business partners.

Business Disruption Risk Mitigation

Identified availability and business-disruption risks (see Section 14, Risk Assessment) have documented mitigation or transfer strategies, reviewed annually by the CISO and Security Leadership Team as part of the enterprise risk assessment cycle.

Vendor & Business Partner Risk Mitigation

ApexCloud's vendor risk mitigation program spans onboarding due diligence, annual reassessment, contractual security requirements, and offboarding — detailed in full in Section 23 (Vendor & Third-Party Risk Management). This section confirms the risk-mitigation design element of CC9.2; operating-effectiveness testing results, including the reassessment-timeliness exception underlying SOC2-TPR-006, are presented in Section 23.

Control	Description	Status	Finding
Vendor Onboarding Due Diligence	New vendors undergo security due diligence prior to onboarding.	Effective	—
Vendor Annual Reassessment	High/Critical risk-tier vendors reassessed annually.	Partially Effective	SOC2-TPR-006
Vendor Offboarding & Access Termination	Vendor access and data-sharing arrangements terminated upon contract end.	Effective	—
Change-Driven Risk Reassessment	Significant business/IT changes trigger a documented risk reassessment.	Not Effective	—

21 AVAILABILITY CONTROLS

Availability is one of two additional Trust Services Criteria selected for this fictional engagement, addressing whether information and systems are available for operation and use to meet ApexCloud's illustrative service commitments and system requirements.

Illustrative Availability Commitments

ApexCloud's fictional service commitments include maintaining production platform availability consistent with its customer agreements, monitoring uptime against internal SLA targets, and maintaining documented backup, disaster recovery, and business continuity capabilities. No universal SOC 2 requirement mandates a specific uptime percentage, RTO, or RPO; the commitments below are ApexCloud's own organizational targets, presented here as fictional/illustrative figures.

Illustrative Uptime Target	99.9% monthly availability for the primary platform (organizational commitment, not a SOC 2 mandate).
Illustrative Recovery Time Objective (RTO)	4 hours for the primary application platform; varies by service criticality tier.
Illustrative Recovery Point Objective (RPO)	1 hour for the primary production database; varies by service criticality tier.
Capacity Planning	Infrastructure capacity planned and monitored against forecasted demand.
Infrastructure Redundancy	Multi-availability-zone deployment with automated failover for the primary platform.

Availability — Type II Testing Results

Control	Description	Status	Finding
Uptime / SLA Monitoring	Service availability continuously monitored against internal SLA commitments.	Effective	—
Infrastructure Redundancy	Multi-AZ deployment with automated failover.	Effective	—
Backup Scheduling & Encryption	Production data backed up on a defined schedule, encrypted at rest.	Effective	—
Backup Restoration Testing	Quarterly restoration testing for in-scope production databases.	Partially Effective	SOC2-BKP-010
Disaster Recovery Plan Maintenance	DR Plan reviewed and updated at least annually.	Effective	—
Disaster Recovery Testing	Business-critical services undergo DR testing on a defined cadence.	Not Effective	SOC2-BCP-005
Business Continuity Contact Validation	Emergency contact rosters validated semi-annually.	Partially Effective	SOC2-DR-013

Detailed coverage of business continuity planning, disaster recovery testing methodology, and the fictional tabletop exercise scenario appears in Section 27; backup architecture and restoration testing detail appears in Section 28.

22 CONFIDENTIALITY CONTROLS

Confidentiality is the second additional Trust Services Criterion selected for this fictional engagement, addressing whether information designated as confidential is protected consistent with ApexCloud's illustrative commitments and objectives.

Confidentiality Program (Fictional)

- Data classification: a four-tier classification model (Restricted, Confidential, Internal, Public) governs labeling and handling expectations (see Section 11).
- Access restriction: repositories containing Confidential-tier data are expected to be restricted to the minimum-necessary access group.
- Encryption: Confidential-tier data stores are encrypted at rest using a current, industry-standard algorithm; data in transit is encrypted using current TLS standards.
- Data retention & secure disposal: confidential data is deleted or the underlying storage sanitized at the end of its defined retention period.
- Customer data segregation: customer data is logically segregated by tenant within the multi-tenant platform architecture.
- Data loss prevention (DLP): DLP monitoring is applied to email and endpoint egress channels for Confidential-tier data patterns.
- Confidentiality agreements: workforce members and vendors with access to Confidential data execute confidentiality/NDA agreements.
- Third-party confidentiality: vendor contracts include confidentiality obligations consistent with the data shared (see Section 23).

Confidentiality — Type II Testing Results

Control	Description	Status	Finding
Confidential Data Identification & Labeling	Confidential-tier data identified and labeled per policy.	Partially Effective	SOC2-ENC-011
Access Restriction for Confidential Data	Repositories restricted to minimum-necessary access group.	Partially Effective	SOC2-ENC-011
Encryption of Confidential Data at Rest	Confidential-tier data stores encrypted at rest.	Effective	—
Secure Data Disposal	Confidential data securely deleted at end of retention period.	Effective	—
Confidentiality Agreements	Workforce and vendors execute confidentiality/NDA agreements.	Effective	—
Data Loss Prevention Monitoring	DLP applied to email and endpoint egress channels.	Effective	—

A sample review of 18 internal shared repositories judgmentally selected from the Sales, Legal, and Customer Success functions identified 2 repositories containing unlabeled Confidential-tier documents with broader-than-intended internal access; both were remediated upon identification. See SOC2-ENC-011 for full testing detail.

23 VENDOR & THIRD-PARTY RISK MANAGEMENT

This section assesses ApexCloud's fictional program for managing risk associated with vendors and subservice organizations (see Section 9 for the full subservice organization inventory), consistent with CC9.2.

Vendor Risk Program (Fictional)

- Onboarding: new vendors undergo security due diligence, including a security questionnaire and, where applicable, review of a SOC report or equivalent assurance artifact, prior to onboarding.
- Risk classification: vendors are classified by risk tier (Low, Moderate, High, Critical) at onboarding based on data access and service criticality.
- Contractual requirements: vendor contracts include security, confidentiality, and incident-notification requirements proportional to risk tier.
- Penetration test / assurance evidence: for Critical-risk subservice organizations, TMG Security's fictional methodology requests the vendor's most recent penetration test summary or SOC report as part of due diligence.
- Annual reassessment: High and Critical risk-tier vendors are reassessed annually, including an updated questionnaire and current assurance artifact review.
- Incident notification: vendor contracts require timely notification of security incidents affecting ApexCloud data.
- Termination / offboarding: vendor access and data-sharing arrangements are terminated upon contract end, with confirmation tracked in the vendor risk register.

Vendor Risk — Type II Testing Result

Control	Description	Status	Finding
Vendor Risk Classification	Vendors classified by risk tier at onboarding.	Effective	—
SOC Report / Assurance Review	SOC reports reviewed for Critical-risk subservice organizations.	Effective	—
Vendor Annual Reassessment	High/Critical risk-tier vendors reassessed annually within 12 months.	Not Effective	SOC2-TPR-006
Vendor Incident Notification Requirements	Contracts require timely incident notification.	Effective	—

Of 15 vendor risk assessments sampled (weighted toward High and Critical risk-tier vendors), 4 High-risk vendors were reassessed 14–19 months after the prior cycle, exceeding the 12-month policy target; no Critical-risk vendor exceeded the target. See SOC2-TPR-006 for full testing detail.

24 SECURITY AWARENESS & WORKFORCE MANAGEMENT

This section assesses ApexCloud's fictional workforce security awareness and competence program under CC1.4, supporting the broader control environment described in Section 13.

Security Awareness Program (Fictional)

- New-hire training: all new hires complete security awareness training as part of onboarding, prior to receiving system access.
- Annual refresher training: all workforce members complete annual security awareness refresher training covering phishing, data handling, and incident reporting.
- Role-based training: engineering and administrative personnel complete additional role-based training (e.g., secure coding, cloud security fundamentals).

- Phishing simulation: simulated phishing exercises are conducted quarterly, with individual results tracked and remedial training assigned for repeat click-throughs.
- Policy acknowledgement: the Information Security Policy is acknowledged annually alongside training completion.
- Completion tracking: training completion is tracked centrally in the learning management system (LMS), with non-completion escalation defined in policy.

Security Awareness — Type II Testing Result

Control	Description	Status	Finding
New-Hire Security Training	Completed as part of onboarding, prior to system access.	Effective	—
Annual Refresher Training	All workforce members complete annual refresher training.	Partially Effective	SOC2-TRN-007
Phishing Simulation Program	Quarterly simulated phishing exercises with tracked results.	Effective	—
Role-Based Security Training	Engineering/administrative personnel complete role-based training.	Effective	—

Of 20 workforce training completion records sampled, 17 evidenced on-time completion; 3 evidenced completion 30–45 days after the annual deadline with no escalation notice recorded in the intervening period, attributable to a 60-day (rather than earlier) manager-escalation threshold in the LMS. See SOC2-TRN-007 for full testing detail.

25 VULNERABILITY & PATCH MANAGEMENT

This section assesses ApexCloud's fictional vulnerability identification, prioritization, and remediation program under CC7.1. Internal remediation SLA targets referenced in this section are ApexCloud's own organizational policy commitments — SOC 2 does not itself mandate a specific vulnerability remediation deadline — and are labeled accordingly throughout.

Vulnerability Management Program (Fictional)

- Asset discovery: cloud infrastructure, container images, and internet-facing endpoints are continuously enumerated to support scanning coverage (see Section 10, Section 32/SOC2-ASSET-014).
- Scanning: automated vulnerability scanning runs continuously across infrastructure and on a monthly cycle basis for reporting purposes.
- Risk rating: findings are rated using a standard severity scale (Critical/High/Medium/Low) informed by exploitability and asset criticality.
- Remediation: findings are routed to the responsible engineering or infrastructure team against an internal organizational-policy SLA (Critical: 15 days; High: 30 days — organizational policy, not a SOC 2 or regulatory mandate).
- Exception process: SLA-exceeding findings require documented risk acceptance from the Security Leadership Team, including a compensating control or target closure date.
- Compensating controls: where remediation is delayed, compensating controls (e.g., WAF rules, network restriction) may be applied and documented in the exception record.
- Validation: remediated findings are rescanned to confirm closure before being marked resolved.
- Reporting & oversight: vulnerability metrics are reported monthly to the Security Leadership Team, including open Critical/High findings and SLA-exceeding exception counts.

Vulnerability Management — Type II Testing Result

Control	Description	Status	Finding
Vulnerability Detection & Scanning	Automated scanning across cloud, container, and internet-facing endpoints.	Effective	—
Vulnerability Exception Governance	SLA-exceeding findings routed through documented risk-acceptance process.	Not Effective	SOC2-VUL-003
Remediation Validation	Remediated findings rescanned to confirm closure.	Effective	—

Of 6 monthly vulnerability remediation cycles sampled, 9 individual Critical/High findings exceeded the internal SLA; formal risk-acceptance documentation was located for 4 of the 9, leaving 5 SLA-exceeding findings without a contemporaneous, approved exception record. All 5 were eventually remediated. See SOC2-VUL-003 for full testing detail.

26 INCIDENT RESPONSE & SECURITY OPERATIONS

This section assesses ApexCloud's fictional incident response program under CC7.3 / CC7.4, including a fictional tabletop exercise scenario used to demonstrate TMG Security's incident response assessment methodology. No actual incident, breach, or security event occurred.

Incident Response Program (Fictional)

- Classification: incidents are classified into defined severity classes (data breach, availability incident, insider/credential-compromise incident) with corresponding response procedures.
- Detection: SIEM, EDR, and vulnerability management alerting feed into the incident detection process (see Section 18).
- Triage: the SOC triages potential incidents against the classification framework to confirm severity and required response.
- Containment & eradication: documented containment procedures (account suspension, network isolation, credential rotation) and eradication steps are defined per incident class.
- Recovery: recovery procedures restore affected systems to normal operation, coordinated with the disaster recovery program where applicable (see Section 27).
- Notification: customer and, where applicable, regulatory notification procedures are defined and tested as part of the incident response program.
- Evidence preservation: forensic evidence is preserved per a documented chain-of-custody procedure for incidents warranting investigation.
- Lessons learned & management reporting: a post-incident review documents root cause, remediation, and lessons learned, reported to the Security Leadership Team.

Fictional Tabletop Exercise Scenario — Illustrative Only

FICTIONAL SCENARIO — NO ACTUAL INCIDENT OCCURRED

As part of this fictional sample, TMG Security's simulated tabletop exercise scenario for the credential-compromise incident class was: a workforce member's laptop is infected with credential-stealing malware following a phishing click; the threat actor uses the harvested credentials to authenticate to an internal administrative tool from an unrecognized location. Simulated participants included the Incident Response Manager, SOC Manager, IAM Program Manager, and a Legal/Communications representative. The exercise tested detection (anomalous login alerting), containment (credential rotation, session termination), and escalation procedures, and produced a documented after-action report with three follow-up action items, all closed prior to this report's issuance.

Incident Response — Type II Testing Result

Control	Description	Status	Finding
Incident Classification & Response	Incidents classified, triaged, and responded to per the IR Plan.	Effective	—
Incident Response Exercise Testing	IR Plan exercised annually across all defined severity classes.	Partially Effective	SOC2-IR-008
Incident Recovery & Lessons Learned	Post-incident review documents root cause, remediation, and lessons learned.	Effective	—

One tabletop exercise (the credential-compromise scenario above) was completed and documented within the assessment period; documented coverage of the data-breach and availability-incident scenario classes was not evidenced within the 01 Jan – 31 Aug 2026 window, though an availability-scenario exercise was scheduled for October 2026. See SOC2-IR-008 for full testing detail.

27 BUSINESS CONTINUITY & DISASTER RECOVERY

This section assesses ApexCloud's fictional business continuity and disaster recovery program supporting the Availability criteria (A1.2, A1.3).

Business Continuity & DR Program (Fictional)

- Business impact analysis (BIA): services are classified by criticality tier, informing recovery prioritization and testing scope.
- Critical services: 5 services are currently classified as business-critical, including the primary application platform, primary database tier, analytics/reporting service, and customer notification service.
- RTO / RPO: illustrative recovery time and recovery point objectives are defined per criticality tier (see Section 21).
- Backup strategy: automated, encrypted, immutable backups with offsite/multi-region storage (see Section 28 for full detail).
- Failover: multi-availability-zone architecture supports automated failover for the primary platform.
- Disaster recovery testing: an annual full failover exercise and quarterly tabletop exercises are the defined testing cadence.
- Lessons learned & management review: DR test results and identified gaps are reviewed by the Backup & Infrastructure Manager and reported to the Security Leadership Team.

Fictional DR Tabletop Scenario — Illustrative Only

FICTIONAL SCENARIO — NO ACTUAL DISASTER OR OUTAGE OCCURRED

TMG Security's simulated DR tabletop scenario modeled a regional AWS availability-zone failure affecting the primary application platform. Simulated participants exercised the failover runbook, confirmed automated traffic rerouting to the secondary availability zone, and validated the customer communication workflow. The exercise identified a fictional 12-minute gap between automated failover completion and customer-facing status-page update, resulting in a recommended runbook update to automate the status-page trigger.

BCP / DR — Type II Testing Result

Control	Description	Status	Finding
Disaster Recovery Plan Maintenance	DR Plan reviewed and updated at least annually.	Effective	—
Disaster Recovery Testing (Business-Critical Services)	All business-critical services tested within the defined cadence.	Not Effective	SOC2-BCP-005
Business Continuity Contact Validation	Emergency contact rosters validated semi-annually across all tiers.	Partially Effective	SOC2-DR-013

The annual full failover exercise was completed and evidenced for 3 of 5 business-critical services; the analytics/reporting service and the customer notification service — both added to the business-critical inventory during a Q2 2026 classification review — did not have documented recovery test evidence within the assessment period. See SOC2-BCP-005 for full testing detail.

28 BACKUP & RECOVERY

This section assesses ApexCloud's fictional backup architecture and restoration testing program supporting Availability criterion A1.2.

Backup Architecture (Fictional)

- Production databases and critical configuration are backed up on an automated daily schedule.
- Backups are encrypted at rest and stored in an immutable, access-restricted storage tier isolated from production administrative credentials, reducing ransomware-driven backup-tampering risk.

- Backups are replicated to a geographically separate region to support recovery from a regional infrastructure event.
- Restoration testing is performed quarterly for in-scope production databases, with results documented in the restoration test log.

Backup & Restoration — Type II Testing Result

Control	Description	Status	Finding
Backup Scheduling & Encryption	Production data backed up on a defined schedule with encryption at rest.	Effective	—
Backup Immutability & Isolation	Backup storage isolated from production administrative credentials.	Effective	—
Backup Restoration Testing	Quarterly restoration testing for all in-scope production databases.	Partially Effective	SOC2-BKP-010

Of 10 backup restoration evidence records sampled across 3 quarters, 8 evidenced a completed and successful restoration test; the secondary reporting database lacked restoration test evidence for one quarter, attributable to a resourcing gap during a Q2 2026 platform migration project. The gap has since been remediated with a completed Q3 2026 test. See SOC2-BKP-010 for full testing detail.

29 ENCRYPTION & DATA PROTECTION

This section assesses ApexCloud's fictional encryption and data protection controls supporting both the Security common criteria (CC6.6, CC6.7) and the Confidentiality criterion (C1.2). Language throughout this section is risk-based rather than absolutist: SOC 2 does not itself mandate a specific encryption algorithm, and ApexCloud's Encryption Standard is presented here as an organizational policy commitment.

Encryption Coverage (Fictional)

Data at Rest	Production databases and object storage encrypted at rest using the current, industry-standard algorithm defined in ApexCloud's Encryption Standard.
Data in Transit	All customer, API, and backend service transmission encrypted using current TLS standards.
Portable Devices	Workforce laptops issued with full-disk encryption enabled by default via endpoint management policy.
Backups	Backup data encrypted at rest, consistent with the production data-at-rest standard.
Cloud Storage	Object storage buckets configured for default encryption at rest; access governed by least-privilege IAM policy.
Databases	Managed database services configured for encryption at rest and in-transit connections.
APIs	API traffic encrypted in transit; API authentication tokens are not logged in plaintext.
Email Transmission	Email transmission uses opportunistic TLS where supported by the receiving mail system; sensitive attachments follow the Data Classification Policy's handling requirements.

Encryption & Data Protection — Type II Testing Result

Control	Description	Status	Finding
Encryption of Confidential Data at Rest	Confidential-tier data stores encrypted at rest.	Effective	—
Transmission Encryption	Data in transit encrypted using current TLS standards.	Effective	—
Endpoint / Portable Device Encryption	Full-disk encryption enabled by default on workforce laptops.	Effective	—

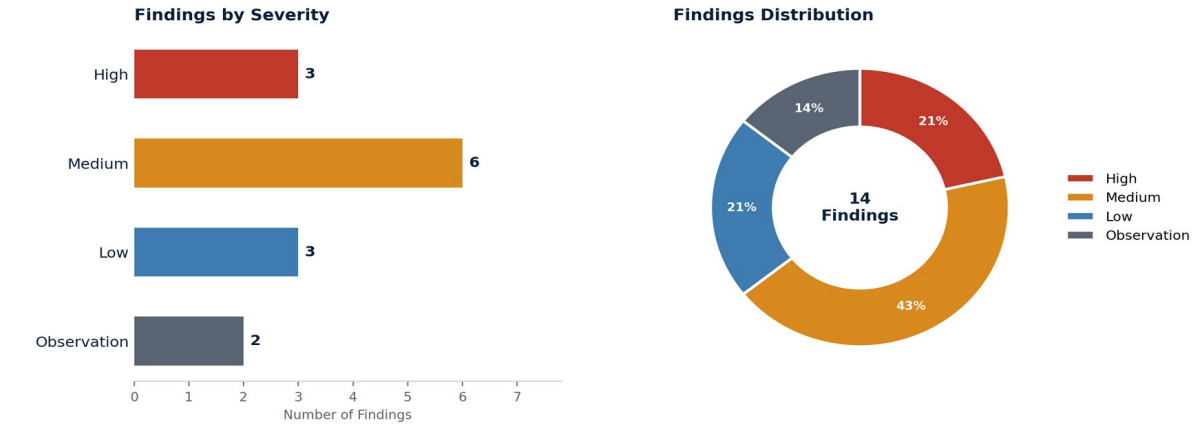
No sample exception was identified in the encryption-coverage testing population for this fictional assessment. Confidentiality-labeling and access-restriction gaps identified for a subset of internal repositories are addressed separately under SOC2-ENC-011 (Section 22) and relate to access governance rather than encryption coverage.

30 FINDINGS SUMMARY

This fictional sample assessment produced a total of 14 illustrative findings and observations across ApexCloud's Security, Availability, and Confidentiality control domains, identified through Type II-style operating-effectiveness testing. The dashboard below summarizes findings by severity for demonstration purposes; the illustrative Type II Operating Effectiveness Summary in Section 33 presents effectiveness status by domain, and the SOC 2 Control Matrix in Section 40 presents status by individual control.

0	3	6	3	2
Critical	High	Medium	Low	Observations

Fictional Sample Findings Dashboard — Illustrative Data Only



Fictional Sample Findings Dashboard — Illustrative Data Only

Findings by Domain

Domain	Findings
Logical & Physical Access Controls	1
Change Management	2
Vulnerability & Patch Management	1
Incident Response & Security Operations	2
Business Continuity & Disaster Recovery	2
Vendor & Third-Party Risk Management	1
Security Awareness & Workforce Management	1
Backup & Recovery	1
Confidentiality Controls	1
Monitoring Activities	1
Governance & Security Organization	1

Interpretation

No finding in this fictional sample was rated Critical. Three high-severity findings span privileged access review evidence across cloud, container, and database administrative tiers, emergency-change retroactive approval and post-implementation review documentation, and governance of vulnerability remediation exceptions. Six medium-severity findings are distributed across security event alert-triage evidence, disaster recovery testing coverage, delayed vendor risk reassessment, security awareness training completion tracking, incident response tabletop exercise coverage, and backup restoration evidence. Three low-severity findings reflect narrower confidentiality-labeling, control-monitoring documentation, and business continuity contact-validation gaps, and two observations note forward-looking hardening and documentation-currency opportunities that did not rise to the level of a control exception.

31 DETAILED CONTROL EXCEPTIONS & FINDINGS

Every fictional sample finding is presented below in full Type II consulting-format detail: control objective, criteria, condition, testing procedure, population/sample, evidence expected and reviewed, exception identified, root cause, risk/business impact, likelihood/impact/residual risk, recommendation, management response, owner, target date, status, and retest requirement. All findings, evidence, and management responses on this page are entirely fictional.

ILLUSTRATIVE EVIDENCE REFERENCE — NO ACTUAL CLIENT EVIDENCE

SOC2-ACC-001 — Privileged Access Review Evidence Not Consistently Retained	**HIGH**
Trust Services Criteria: CC6.2 / CC6.3 — Logical Access: Prior to Issuing, Modifying, or Removing Access	**Illustrative Assessment Status: Not Effective**
Control Objective	Privileged access to production systems, cloud infrastructure, and customer data stores is reviewed on a recurring basis by an accountable owner, with review outcomes (confirmations, exceptions, and revocations) formally evidenced.
Criteria	ApexCloud's Access Control Policy requires quarterly review of all privileged (administrative, database, and cloud root/IAM) accounts by the applicable system owner, with documented sign-off retained for the assessment period.
Condition	Of 8 quarterly/monthly privileged access review cycles sampled across the AWS IAM, Kubernetes cluster-admin, and PostgreSQL superuser account populations, 3 cycles lacked a retained, signed review artifact demonstrating that the assigned reviewer completed and approved the cycle.
Testing Procedure	Inspected the privileged access review tracker and requested the underlying review workpaper (exported account listing, reviewer attestation, and any identified exceptions with remediation evidence) for each sampled cycle; corroborated reviewer identity against the IAM group population.
Population / Sample Selected	8 of 24 monthly/quarterly privileged access review cycles occurring within the 01 Jan 2026 – 31 Aug 2026 assessment period, stratified across AWS IAM, Kubernetes, and database administrative account populations.
Evidence Expected	A completed review artifact for each cycle showing the account population reviewed, reviewer identity, review date, disposition of each account (retain/revoke), and evidence that identified exceptions were remediated.
Evidence Reviewed	Review trackers and exported account listings for 8 sampled cycles; reviewer attestations were present for 5 of 8 cycles.
Exception Identified	3 of 8 sampled cycles (2 Kubernetes cluster-admin cycles and 1 database superuser cycle) had no retained reviewer attestation; the underlying account listings were exported but review completion could not be independently corroborated.
Root Cause	Privileged access reviews are coordinated manually via a shared spreadsheet and email confirmation rather than a centralized workflow tool; reviewer confirmations sent by email were not consistently archived to the central evidence repository.
Risk / Business Impact	Without consistently retained review evidence, ApexCloud cannot demonstrate — to itself or to a future independent auditor — that privileged access to production and customer-data-bearing systems is being recertified on the defined cadence, increasing the risk that excessive or stale privileged access persists undetected.
Likelihood / Impact / Residual Risk	**Possible** (Likelihood) | **Major** (Impact) | Residual: **Medium**
Evidence Reference	*EV-004, EV-029 (Illustrative Evidence Reference — No Actual Client Evidence)*
Recommendation	Migrate privileged access recertification into the centralized IAM governance platform already used for standard user access reviews, with system-enforced reviewer attestation, automatic escalation for overdue cycles, and evidence retained natively rather than via email.
Management Response	*Agreed. ApexCloud will extend its existing IAM governance platform to cover all privileged account populations, including Kubernetes cluster-admin and database superuser roles, with attestation workflows enforced beginning Q4 2026.*
Owner / Target Date / Status	**IAM Program Manager** | 31 Oct 2026 | **Open**
Retest Requirement	*Retest required in a follow-up assessment: sample no fewer than 4 subsequent review cycles post-remediation to confirm consistent, system-evidenced completion.*

SOC2-CHG-002 — Emergency Change Documentation Incomplete	**HIGH**
Trust Services Criteria: CC8.1 — Change Management	**Illustrative Assessment Status: Not Effective**
Control Objective	Emergency changes deployed outside the standard change window are subject to expedited but documented approval, and retroactive review, sufficient to demonstrate that unauthorized or unreviewed changes are not introduced into production.

Criteria	ApexCloud's Change Management Policy requires that emergency changes be logged in the change ticketing system with a documented business justification, an accountable approver (obtained retroactively within 2 business days when pre-approval is impractical), and evidence of post-implementation review.
Condition	Of 12 change-management tickets sampled, 4 were emergency changes; of those 4, 2 lacked a documented retroactive approval within the policy-defined window, and 1 lacked evidence of post-implementation review.
Testing Procedure	Selected a sample of change tickets from the CI/CD and infrastructure change log stratified across standard, normal, and emergency change types; inspected each ticket for requestor, business justification, peer/technical review, approval, testing evidence, and (for emergency changes) retroactive approval and post-implementation review.
Population / Sample Selected	12 of 340 change-management tickets logged during the assessment period, including 4 emergency changes selected judgmentally to bias toward higher-risk production changes.
Evidence Expected	For each emergency change: incident/justification narrative, deploying engineer identity, retroactive approver identity and timestamp within 2 business days, and a documented post-implementation review confirming the change performed as intended without adverse impact.
Evidence Reviewed	Change tickets and associated Slack/ITSM approval threads for the 4 sampled emergency changes.
Exception Identified	2 of 4 emergency changes had retroactive approval recorded 4–6 business days after deployment (outside the 2-business-day policy window), and 1 of 4 had no documented post-implementation review entry in the ticket.
Root Cause	Emergency-change approvers are not systematically notified when a change is logged outside business hours, and the ticketing system does not enforce a policy-defined SLA reminder for retroactive approval or post-implementation review completion.
Risk / Business Impact	Incomplete or delayed documentation of emergency-change approval and review reduces ApexCloud's ability to demonstrate that expedited production changes received timely, accountable oversight, and increases the risk that an inadequately reviewed emergency change could introduce instability or a security weakness.
Likelihood / Impact / Residual Risk	**Possible** (Likelihood) | **Major** (Impact) | Residual: **Medium**
Evidence Reference	*EV-012, EV-013 (Illustrative Evidence Reference — No Actual Client Evidence)*
Recommendation	Configure the ITSM/change platform to automatically flag emergency changes lacking retroactive approval or post-implementation review after 2 business days, with escalation to the engineering director; incorporate emergency-change SLA adherence into monthly change-management metrics.
Management Response	*Agreed. ApexCloud will implement automated SLA tracking and escalation for emergency-change approval and post-implementation review within the ITSM platform.*
Owner / Target Date / Status	**Engineering Director, Platform** | 15 Nov 2026 | **Open**
Retest Requirement	*Retest required: sample a minimum of 6 subsequent emergency changes to confirm consistent, timely retroactive approval and post-implementation review evidence.*

SOC2-VUL-003 — Vulnerability Remediation Exceptions Not Consistently Governed	**HIGH**
Trust Services Criteria: CC7.1 — System Operations: Detection and Monitoring of Vulnerabilities	**Illustrative Assessment Status: Not Effective**
Control Objective	Vulnerabilities identified through automated scanning are remediated within organizationally defined SLA targets, and any exception to those targets is formally risk-accepted by an accountable owner with a documented compensating control or remediation plan.
Criteria	ApexCloud's internal Vulnerability Management SLA (an organizational policy, not a SOC 2 or regulatory mandate) targets remediation of Critical findings within 15 days and High findings within 30 days of confirmed detection; exceptions require documented risk acceptance from the Security Leadership Team.
Condition	Of 6 vulnerability remediation cycles sampled, 9 individual Critical/High findings exceeded the internal SLA; of those 9, formal risk-acceptance documentation was located for 4, leaving 5 SLA-exceeding findings without a retained exception record.
Testing Procedure	Selected 6 monthly vulnerability scan cycles across the assessment period; for each cycle, identified findings exceeding the internal SLA target and inspected the exception/risk-acceptance register for a corresponding documented approval, compensating control, and target closure date.
Population / Sample Selected	6 of 8 monthly vulnerability scanning cycles occurring during the assessment period, covering cloud infrastructure, container images, and internet-facing application endpoints.
Evidence Expected	A risk-acceptance record for each SLA-exceeding finding, including the accepting owner, business justification, compensating control (if any), and a target remediation or re-evaluation date.
Evidence Reviewed	Vulnerability scan reports, the remediation tracking spreadsheet, and the exception/risk-acceptance register for the 6 sampled cycles.
Exception Identified	5 of 9 SLA-exceeding Critical/High findings across the sampled cycles had no corresponding entry in the exception register; remediation was eventually completed for all 5, but outside the SLA and without a contemporaneous, approved exception.
Root Cause	The exception/risk-acceptance process is initiated manually by the remediation owner rather than triggered automatically when a finding crosses its SLA threshold, resulting in inconsistent submission of exception requests.

Risk / Business Impact	Without consistent exception governance, SLA-exceeding vulnerabilities may remain unremediated for extended periods without accountable, risk-informed sign-off, increasing the window of exposure for exploitable weaknesses in internet-facing and cloud infrastructure components.
Likelihood / Impact / Residual Risk	**Likely** (Likelihood) | **Major** (Impact) | Residual: **Medium**
Evidence Reference	*EV-010, EV-011 (Illustrative Evidence Reference — No Actual Client Evidence)*
Recommendation	Automate exception-register triggering directly from the vulnerability management platform when a finding crosses its SLA threshold, requiring Security Leadership Team sign-off before the finding can be marked deferred; report open exceptions in the monthly security metrics review.
Management Response	*Agreed. ApexCloud will integrate automated SLA-threshold alerting between the vulnerability management platform and the exception register, with mandatory Security Leadership Team approval prior to SLA deferral.*
Owner / Target Date / Status	**Vulnerability Management Lead** | 30 Nov 2026 | **Open**
Retest Requirement	*Retest required: sample a minimum of 3 subsequent scanning cycles to confirm all SLA-exceeding findings have a contemporaneous, approved exception record.*

SOC2-LOG-004 — Security Event Review Evidence Inconsistent	**MEDIUM**
Trust Services Criteria: CC7.2 — System Operations: Monitoring for Anomalies and Security Events	**Illustrative Assessment Status: Partially Effective**
Control Objective	Security events and alerts generated by the SIEM and endpoint detection platforms are triaged by the security operations team on a defined cadence, with disposition (escalated, false positive, or closed) formally documented.
Criteria	ApexCloud's Security Operations Runbook requires daily triage of SIEM-generated high-priority alerts, with a documented disposition recorded in the SOC ticketing queue for each alert within one business day.
Condition	Of 10 weeks of SIEM alert-triage evidence sampled across the assessment period, 3 weeks showed gaps where high-priority alerts lacked a documented disposition within the one-business-day target, though all were eventually reviewed.
Testing Procedure	Selected 10 weekly periods from the SIEM alert queue; for each period, inspected the SOC ticketing system to confirm each high-priority alert generated during the week had a documented triage disposition and timestamp.
Population / Sample Selected	10 of 35 weekly SIEM alert-triage periods within the assessment period.
Evidence Expected	A disposition entry (escalated / false positive / closed, with analyst identity and timestamp) for every high-priority alert generated during the sampled week, recorded within one business day of alert generation.
Evidence Reviewed	SIEM alert export logs cross-referenced against SOC ticketing queue disposition records for the 10 sampled weeks.
Exception Identified	In 3 of 10 sampled weeks, a combined total of 14 high-priority alerts were dispositioned 2–4 business days after generation rather than within the one-business-day target; all were ultimately closed as false positives or benign.
Root Cause	Analyst staffing coverage during two identified holiday and reduced-coverage weeks was not adjusted to reflect the fixed one-business-day triage SLA.
Risk / Business Impact	Delayed alert triage narrows the window in which a genuine security event would be identified and escalated, though the absence of any missed true-positive alert in the sampled population indicates the underlying detection capability remains sound.
Likelihood / Impact / Residual Risk	**Possible** (Likelihood) | **Moderate** (Impact) | Residual: **Low**
Evidence Reference	*EV-007, EV-026 (Illustrative Evidence Reference — No Actual Client Evidence)*
Recommendation	Establish a documented staffing contingency plan for the SOC covering holiday and reduced-coverage periods, and configure automated SLA-breach alerting within the SIEM/ticketing integration.
Management Response	*Agreed. ApexCloud will formalize SOC on-call and holiday staffing coverage and enable automated SLA-breach notifications.*
Owner / Target Date / Status	**SOC Manager** | 15 Nov 2026 | **Open**
Retest Requirement	*Retest recommended in the next assessment cycle: sample weekly triage evidence including at least one holiday/reduced-coverage period.*

SOC2-BCP-005 — Disaster Recovery Testing Coverage Gap	**MEDIUM**
Trust Services Criteria: A1.2 / A1.3 — Availability: Environmental Protections, Backup, and Recovery	**Illustrative Assessment Status: Partially Effective**
Control Objective	Disaster recovery procedures for services classified as business-critical are tested on a defined cadence, with test results, identified gaps, and remediation formally documented and reviewed by management.
Criteria	ApexCloud's Disaster Recovery Plan commits to an annual full failover exercise across all business-critical services and quarterly tabletop exercises for the remaining in-scope service tiers.

Condition	Of the services classified as business-critical, the annual full failover exercise was completed and evidenced for the primary application platform and primary database tier, but 2 of 5 business-critical services (the analytics/reporting service and the customer notification service) did not have a documented recovery test within the assessment period.
Testing Procedure	Obtained the current business-critical service inventory and the disaster recovery testing schedule; inspected test completion evidence (test plan, execution record, results summary, and remediation tracking) for each in-scope service.
Population / Sample Selected	All 5 services classified as business-critical within the assessment period's disaster recovery scope.
Evidence Expected	A completed test plan, execution evidence, and management-reviewed results summary for each business-critical service within its defined testing cadence.
Evidence Reviewed	Disaster recovery test plans and results summaries for 3 of 5 business-critical services.
Exception Identified	The analytics/reporting service and the customer notification service had no documented recovery test evidence within the assessment period.
Root Cause	The disaster recovery testing calendar was not updated to reflect two services added to the business-critical inventory during a Q2 2026 service-classification review.
Risk / Business Impact	Untested recovery procedures for the affected services create uncertainty as to whether documented recovery time and recovery point commitments for those services would be achievable in an actual disaster scenario.
Likelihood / Impact / Residual Risk	**Unlikely** (Likelihood) | **Moderate** (Impact) | Residual: **Low**
Evidence Reference	*EV-016, EV-017 (Illustrative Evidence Reference — No Actual Client Evidence)*
Recommendation	Update the disaster recovery testing calendar to reflect the current business-critical service inventory and schedule recovery tests for the two untested services within the current remediation cycle.
Management Response	*Agreed. Recovery tests for the analytics/reporting and customer notification services will be scheduled and completed, with the testing calendar reconciled against the service-classification register going forward.*
Owner / Target Date / Status	**Backup & Infrastructure Manager** | 15 Dec 2026 | **Open**
Retest Requirement	*Retest required: confirm completed, documented recovery test evidence for both previously untested services.*

SOC2-TPR-006 — Vendor Risk Reassessment Evidence Delayed	**MEDIUM**
Trust Services Criteria: CC9.2 — Risk Mitigation: Vendor and Business Partner Risk	**Illustrative Assessment Status: Partially Effective**
Control Objective	Vendors and subservice organizations classified as high or critical risk are reassessed on an annual basis, with the reassessment evidencing current SOC report review, security questionnaire completion, and risk-tier confirmation.
Criteria	ApexCloud's Third-Party Risk Management Policy requires annual reassessment of all vendors classified as High or Critical risk, completed within 12 months of the prior assessment.
Condition	Of 15 vendor risk assessments sampled, 4 vendors classified as High risk had reassessments completed 14–19 months after the prior assessment, exceeding the 12-month policy target.
Testing Procedure	Selected a sample of vendor risk records from the vendor risk register weighted toward High and Critical risk-tier vendors; compared the current assessment completion date against the prior assessment date for each sampled vendor.
Population / Sample Selected	15 of 42 active vendors in the vendor risk register, including all Critical-risk vendors and a judgmental sample of High-risk vendors.
Evidence Expected	A completed reassessment record (updated security questionnaire, current SOC report or equivalent assurance artifact, and risk-tier confirmation) dated within 12 months of the prior assessment for each sampled vendor.
Evidence Reviewed	Vendor risk register entries and reassessment records for the 15 sampled vendors.
Exception Identified	4 of 15 sampled vendors (all High risk-tier) had reassessment gaps of 14–19 months; no Critical-risk vendor exceeded the reassessment target.
Root Cause	Reassessment due dates are tracked in the vendor risk register but are not linked to an automated reminder workflow, resulting in manual tracking gaps for a subset of the High-risk vendor population.
Risk / Business Impact	Delayed reassessment of High-risk vendors reduces visibility into changes to those vendors' security posture during the gap period, though no adverse vendor security event was identified for any of the affected relationships during the assessment period.
Likelihood / Impact / Residual Risk	**Possible** (Likelihood) | **Moderate** (Impact) | Residual: **Low**
Evidence Reference	*EV-018, EV-019 (Illustrative Evidence Reference — No Actual Client Evidence)*
Recommendation	Implement automated reassessment-due reminders within the vendor risk management platform, escalating to the Third-Party Risk Manager 60 days prior to the 12-month deadline.
Management Response	*Agreed. ApexCloud will enable automated reassessment reminders and complete outstanding reassessments for the 4 identified vendors.*
Owner / Target Date / Status	**Third-Party Risk Manager** | 31 Dec 2026 | **Open**
Retest Requirement	*Retest required: confirm completed reassessments for the 4 identified vendors and evidence of automated reminder configuration.*

SOC2-TRN-007 — Security Awareness Completion Tracking Gap	MEDIUM
Trust Services Criteria: CC1.4 — Control Environment: Commitment to Competence	**Illustrative Assessment Status: Partially Effective**
Control Objective	All workforce members complete annual security awareness training and acknowledge the Information Security Policy, with completion centrally tracked and non-completion escalated for follow-up.
Criteria	ApexCloud's Security Awareness Program requires 100% completion of annual training and policy acknowledgement by all active employees and contractors with system access, tracked in the learning management system (LMS).
Condition	Of 20 workforce training completion records sampled, 17 evidenced on-time completion; 3 evidenced completion 30–45 days after the annual deadline with no documented escalation in the interim.
Testing Procedure	Selected a sample of workforce members from the active headcount roster with system access; inspected LMS completion records against the annual training deadline and reviewed the non-completion escalation log for the sampled population.
Population / Sample Selected	20 of 850 active workforce members with system access, stratified across engineering, support, and administrative functions.
Evidence Expected	An LMS completion timestamp on or before the annual deadline for each sampled workforce member, or, where late, evidence of an escalation notice issued to the individual and their manager.
Evidence Reviewed	LMS completion export and the non-completion escalation log for the sampled population.
Exception Identified	3 of 20 sampled workforce members completed training 30–45 days late with no escalation notice recorded in the log for the intervening period.
Root Cause	The LMS sends an automated reminder to the individual at the deadline but does not currently escalate to the individual's manager or the People/HR team until 60 days past due, allowing a gap window in which overdue completions are not visible to management.
Risk / Business Impact	Delayed training completion for a small subset of the workforce modestly extends the period in which those individuals may be less current on security policy and phishing-awareness expectations, though the underlying training content and program design were confirmed to be current and role-appropriate.
Likelihood / Impact / Residual Risk	**Possible** (Likelihood) | **Moderate** (Impact) | Residual: **Low**
Evidence Reference	*EV-020 (Illustrative Evidence Reference — No Actual Client Evidence)*
Recommendation	Reduce the manager-escalation threshold in the LMS from 60 days to 15 days past the annual deadline, and incorporate training completion rate into the monthly security metrics reported to the Security Leadership Team.
Management Response	*Agreed. ApexCloud will reduce the escalation threshold and add training completion metrics to the monthly security reporting package.*
Owner / Target Date / Status	**Training & Awareness Lead** | 30 Nov 2026 | **Open**
Retest Requirement	*Retest recommended: sample a subsequent training cycle to confirm the reduced escalation threshold is operating and completion rates have improved.*

SOC2-IR-008 — Incident Response Exercise Documentation Incomplete	MEDIUM
Trust Services Criteria: CC7.3 / CC7.4 — System Operations: Incident Response and Recovery	**Illustrative Assessment Status: Partially Effective**
Control Objective	The Incident Response Plan is exercised at least annually through a tabletop or simulation exercise, with participation, scenario coverage, identified gaps, and follow-up actions formally documented.
Criteria	ApexCloud's Incident Response Plan requires an annual tabletop exercise covering at least one scenario relevant to each of the plan's defined incident severity classes (data breach, availability incident, and insider/credential-compromise incident), with a documented after-action report.
Condition	One tabletop exercise (a simulated credential-compromise scenario) was completed and documented with an after-action report during the assessment period; documented coverage of the data-breach and availability-incident scenario classes was not evidenced.
Testing Procedure	Requested the annual tabletop exercise schedule and after-action reports for the assessment period; compared exercise scenario coverage against the three incident severity classes defined in the Incident Response Plan.
Population / Sample Selected	All tabletop/simulation exercises conducted during the 01 Jan 2026 – 31 Aug 2026 assessment period.
Evidence Expected	An after-action report for at least one exercise covering each of the three defined incident severity classes, including participants, scenario narrative, identified gaps, and follow-up action tracking.
Evidence Reviewed	One after-action report (credential-compromise scenario, conducted March 2026).
Exception Identified	No documented tabletop exercise covering a data-breach or availability-incident scenario was evidenced within the assessment period; the second exercise, addressing an availability scenario, was scheduled for October 2026 (after the assessment period end date).
Root Cause	The annual exercise calendar allots exercises across the calendar year rather than the SOC 2 assessment period, resulting in incomplete scenario-class coverage when measured against the January–August assessment window specifically.

Risk / Business Impact	Incomplete scenario coverage within the assessment period limits the evidenced assurance that the incident response team has recently exercised its response procedures for data-breach and availability-incident scenarios specifically, though the completed credential-compromise exercise did evidence a functioning exercise program overall.
Likelihood / Impact / Residual Risk	**Unlikely** (Likelihood) | **Moderate** (Impact) | Residual: **Low**
Evidence Reference	*EV-008, EV-009 (Illustrative Evidence Reference — No Actual Client Evidence)*
Recommendation	Realign the annual tabletop exercise calendar to ensure all three defined incident severity classes are exercised within each rolling 12-month assessment window, and retain after-action reports centrally in the compliance evidence repository.
Management Response	*Agreed. The October 2026 availability-scenario exercise remains scheduled, and a data-breach scenario exercise will be added to the Q1 2027 calendar; future exercise scheduling will be aligned to the assessment period.*
Owner / Target Date / Status	**Incident Response Manager** | 31 Mar 2027 | **Open**
Retest Requirement	*Retest required in the subsequent assessment period: confirm after-action reports exist for all three defined incident severity classes.*

SOC2-BKP-010 — Backup Restoration Evidence Not Available for All Critical Services	**MEDIUM**
Trust Services Criteria: A1.2 — Availability: Backup and Recovery	**Illustrative Assessment Status: Partially Effective**
Control Objective	Backups of production data supporting business-critical services are periodically restored and validated to confirm recoverability, with restoration test results documented.
Criteria	ApexCloud's Backup Policy requires quarterly restoration testing for production databases supporting business-critical services, with results documented in the restoration test log.
Condition	Of 10 backup restoration evidence records sampled, 8 evidenced a completed and successful restoration test; 2, both relating to a secondary reporting database, had no restoration test evidence for one of the four quarters in the assessment period.
Testing Procedure	Selected a sample of restoration test records across the in-scope production database population; inspected the restoration test log for test execution date, scope, outcome, and any identified issues with remediation evidence.
Population / Sample Selected	10 restoration test records spanning the 3 full quarters within the assessment period across the primary application database, primary customer data store, and secondary reporting database.
Evidence Expected	A documented restoration test for each in-scope database each quarter, including test scope, outcome, and time-to-restore measurement.
Evidence Reviewed	Restoration test log entries for the 10 sampled records.
Exception Identified	The secondary reporting database lacked a documented restoration test for Q2 2026; restoration testing evidence for Q1 and Q3 2026 for that database was present and successful.
Root Cause	The restoration testing schedule for the secondary reporting database is coordinated separately from the primary production databases and was affected by a resourcing gap during a Q2 2026 platform migration project.
Risk / Business Impact	The absence of a single quarter's restoration test for a secondary, non-primary database limits assurance of recoverability for that specific quarter, while the broader restoration testing program for primary production data stores was evidenced as operating consistently.
Likelihood / Impact / Residual Risk	**Unlikely** (Likelihood) | **Moderate** (Impact) | Residual: **Low**
Evidence Reference	*EV-014, EV-015 (Illustrative Evidence Reference — No Actual Client Evidence)*
Recommendation	Consolidate restoration testing scheduling for all in-scope databases, including secondary and reporting data stores, under a single centrally tracked quarterly calendar with completion sign-off required from the Backup & Infrastructure Manager.
Management Response	*Agreed. The Q2 2026 restoration test gap for the secondary reporting database has been remediated with a completed test in Q3 2026, and restoration testing scheduling has been consolidated.*
Owner / Target Date / Status	**Backup & Infrastructure Manager** | 31 Oct 2026 | **Open**
Retest Requirement	*Retest recommended: confirm consistent quarterly restoration test evidence across all in-scope databases in the subsequent assessment period.*

SOC2-ENC-011 — Confidential Data Classification Enforcement Gap	**LOW**
Trust Services Criteria: C1.1 — Confidentiality: Identification and Maintenance of Confidential Information	**Illustrative Assessment Status: Partially Effective**
Control Objective	Data classified as Confidential under the Data Classification Policy is labeled and handled consistently with its classification tier, including restricted access and approved storage locations.

Criteria	ApexCloud's Data Classification Policy requires that documents and data repositories containing Confidential-tier customer or business information be labeled accordingly and stored only in approved, access-restricted repositories.
Condition	A sample review of internal collaboration-platform repositories identified 2 of 18 sampled shared folders containing Confidential-tier business documents (customer contract summaries) that were not labeled per policy and had broader internal access than the policy-defined minimum.
Testing Procedure	Selected a sample of internal shared repositories reasonably likely to contain Confidential-tier information based on folder naming and department ownership; inspected folder-level access permissions and document labeling against the Data Classification Policy.
Population / Sample Selected	18 internal shared repositories judgmentally selected from the Sales, Legal, and Customer Success functions.
Evidence Expected	Confidential-tier labeling on applicable documents and repository access restricted to the defined minimum-necessary group for each sampled repository.
Evidence Reviewed	Repository access-control listings and a sample of document metadata/labeling for the 18 sampled repositories.
Exception Identified	2 of 18 sampled repositories contained unlabeled Confidential-tier documents accessible to a broader internal group (all Sales department members) than the policy-defined minimum (the account team assigned to the applicable customer).
Root Cause	Data classification labeling and repository access provisioning are performed manually by content owners without a technical control (such as automated data-loss-prevention labeling) enforcing consistency.
Risk / Business Impact	Broader-than-intended internal access to Confidential-tier contract information increases the risk of unintended internal disclosure, though the exposure identified was limited to internal personnel rather than external parties.
Likelihood / Impact / Residual Risk	**Unlikely** (Likelihood) | **Minor** (Impact) | Residual: **Low**
Evidence Reference	*EV-022, EV-023 (Illustrative Evidence Reference — No Actual Client Evidence)*
Recommendation	Evaluate and implement automated data-classification labeling and access-restriction tooling for collaboration-platform repositories identified as likely to contain Confidential-tier information, prioritized by department risk.
Management Response	*Agreed. Access to the 2 identified repositories has been restricted to the appropriate account teams, and ApexCloud will evaluate automated classification tooling for broader rollout.*
Owner / Target Date / Status	**Data Governance Lead** | 31 Jan 2027 | **Open**
Retest Requirement	*Retest recommended in the subsequent assessment period once automated tooling evaluation is complete.*

SOC2-MON-012 — Control Monitoring Review Documentation Inconsistent	**LOW**
Trust Services Criteria: CC4.1 — Monitoring Activities	**Illustrative Assessment Status: Partially Effective**
Control Objective	Management performs and documents periodic reviews of key control performance metrics (access reviews, change management, vulnerability management, and incident response) to identify and remediate control deficiencies on an ongoing basis.
Criteria	ApexCloud's Control Monitoring Program requires a documented monthly management review of key control metrics, with meeting minutes retained showing metrics discussed, issues identified, and follow-up actions assigned.
Condition	Of 8 monthly control monitoring review cycles sampled, minutes were retained for 6; 2 cycles had confirmed meeting occurrence (calendar invite and attendee list) but no retained minutes documenting the substance of the review.
Testing Procedure	Requested control monitoring review minutes for a sample of monthly cycles within the assessment period; corroborated meeting occurrence via calendar records where minutes were not located.
Population / Sample Selected	8 of the monthly control monitoring review cycles within the assessment period.
Evidence Expected	Retained minutes for each monthly review documenting the metrics presented, any deficiencies identified, and assigned follow-up actions.
Evidence Reviewed	Meeting minutes and calendar corroboration for the 8 sampled cycles.
Exception Identified	2 of 8 sampled cycles had confirmed meeting occurrence but no retained minutes documenting review substance.
Root Cause	Minutes are taken manually by a rotating note-taker without a standardized template or a defined secondary owner responsible for confirming minutes are finalized and archived.
Risk / Business Impact	The absence of documented substance for 2 review cycles limits the evidentiary trail for those specific months, while calendar corroboration and consistent documentation for the remaining 6 sampled cycles indicate the underlying review activity is occurring.
Likelihood / Impact / Residual Risk	**Rare** (Likelihood) | **Minor** (Impact) | Residual: **Low**
Evidence Reference	*EV-027, EV-030 (Illustrative Evidence Reference — No Actual Client Evidence)*
Recommendation	Adopt a standardized control monitoring review minutes template with a designated secondary owner accountable for confirming minutes are finalized and archived to the compliance evidence repository within 5 business days of each review.
Management Response	*Agreed. A standardized minutes template and designated secondary owner have been assigned effective September 2026.*
Owner / Target Date / Status	**GRC Program Manager** | 30 Sep 2026 | **Open**
Retest Requirement	*Retest recommended: sample subsequent monthly cycles to confirm consistent minutes retention under the new process.*

SOC2-DR-013 — Business Continuity Contact Validation Not Fully Evidenced	**LOW**
Trust Services Criteria: A1.3 — Availability: Recovery Plan Testing and Maintenance	**Illustrative Assessment Status: Partially Effective**
Control Objective	The Business Continuity Plan's emergency contact roster (incident commanders, executive escalation contacts, and key vendor contacts) is validated for currency on a defined cadence.
Criteria	ApexCloud's Business Continuity Plan requires semi-annual validation of the emergency contact roster, with confirmation from each listed individual retained as evidence.
Condition	The emergency contact roster was updated during the assessment period, but documented confirmation from each listed individual (as opposed to a general roster update by the BCP owner) was evidenced for the primary incident-commander tier only; secondary and vendor-contact tiers lacked individual confirmation evidence.
Testing Procedure	Requested the current emergency contact roster and the semi-annual validation evidence; inspected confirmation records for a sample of listed individuals across each contact tier.
Population / Sample Selected	All 3 contact tiers defined in the Business Continuity Plan (primary incident commanders, secondary escalation contacts, and key vendor contacts).
Evidence Expected	Individual confirmation (e.g., an acknowledgement email or signed attestation) from each listed contact within each semi-annual validation cycle.
Evidence Reviewed	Roster update records and individual confirmation evidence for the primary incident-commander tier.
Exception Identified	Individual confirmation evidence for the secondary escalation and key vendor contact tiers was not located; the roster itself had been updated by the BCP owner based on organizational-chart changes rather than direct confirmation from each listed contact.
Root Cause	The semi-annual validation process is not standardized across all three contact tiers, with only the primary tier subject to a formal individual-confirmation workflow.
Risk / Business Impact	Reduced assurance that secondary and vendor emergency contacts remain current increases the risk of delayed escalation during an actual continuity event, though the primary incident-commander tier — the first point of escalation — was confirmed current.
Likelihood / Impact / Residual Risk	**Rare** (Likelihood) | **Minor** (Impact) | Residual: **Low**
Evidence Reference	*EV-028 (Illustrative Evidence Reference — No Actual Client Evidence)*
Recommendation	Extend the individual-confirmation validation workflow already used for the primary incident-commander tier to the secondary escalation and vendor contact tiers.
Management Response	*Agreed. The individual-confirmation workflow will be extended to all contact tiers beginning the next semi-annual validation cycle.*
Owner / Target Date / Status	**Business Continuity Lead** | 31 Dec 2026 | **Open**
Retest Requirement	*Retest recommended: confirm individual confirmation evidence exists across all three contact tiers in the subsequent validation cycle.*

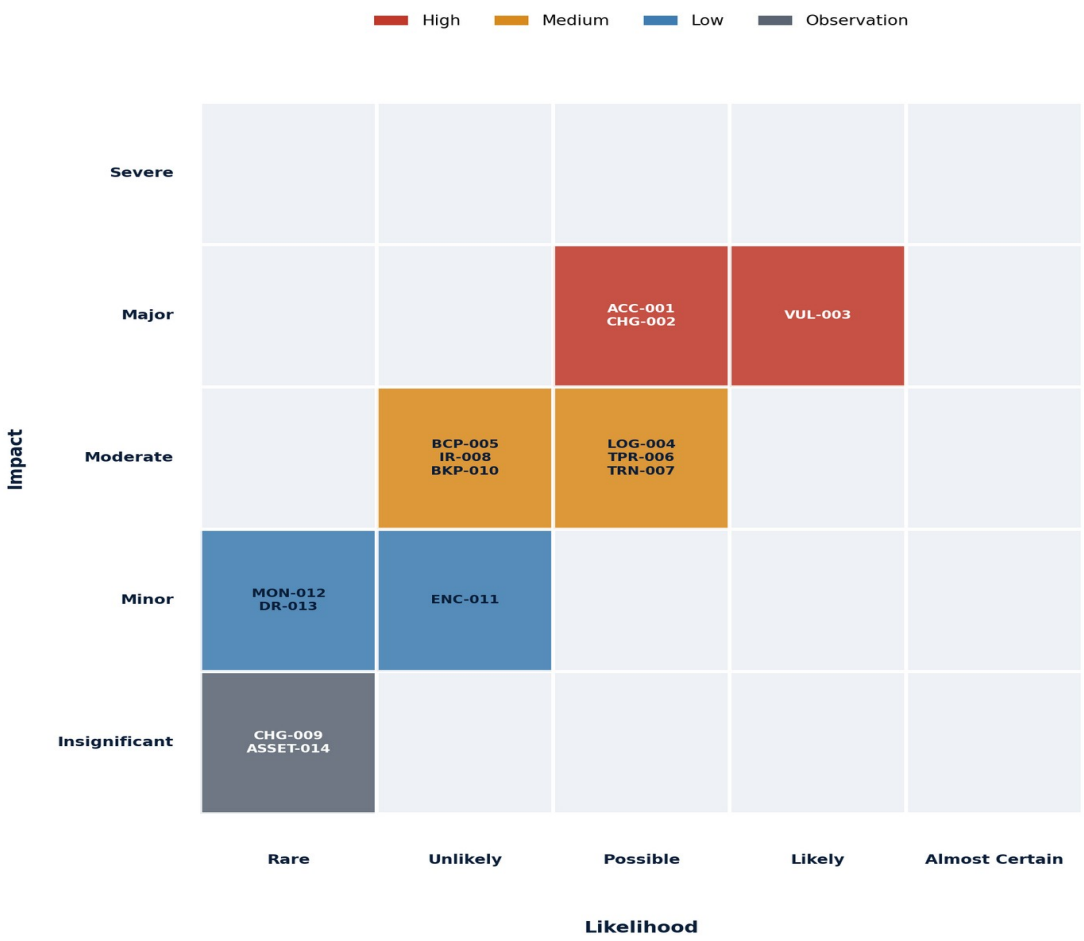
SOC2-CHG-009 — Change Approval Evidence Missing for Sampled Tickets	**OBSERVATION**
Trust Services Criteria: CC8.1 — Change Management	**Illustrative Assessment Status: Effective**
Control Objective	Standard and normal production changes receive documented technical review and approval from an individual independent of the change author prior to deployment.
Criteria	ApexCloud's Change Management Policy requires a peer code review and a separate deployment approval, both evidenced in the change ticket, prior to any production deployment.
Condition	Of the 8 standard/normal change tickets sampled (excluding the 4 emergency changes addressed under SOC2-CHG-002), 1 ticket showed evidence of peer code review but the deployment approval field was completed retroactively, shortly after the production deployment timestamp rather than immediately before it.
Testing Procedure	Inspected each sampled change ticket for requestor identity, peer code review approval, independent deployment approval, and correlation of the approval timestamp to the deployment timestamp in the CI/CD pipeline log.
Population / Sample Selected	8 of 340 standard/normal change-management tickets logged during the assessment period (in addition to the 4 emergency changes sampled separately).
Evidence Expected	A peer code review approval and a separately recorded deployment approval, both timestamped prior to the corresponding CI/CD deployment event.
Evidence Reviewed	Change tickets, pull-request review records, and CI/CD deployment logs for the 8 sampled tickets.
Exception Identified	No control exception is asserted; this is a forward-looking observation. 1 of 8 sampled tickets had a recorded peer code review but the deployment approval field was completed shortly after, rather than strictly prior to, the CI/CD deployment timestamp; the change itself was properly reviewed and authorized.
Root Cause	The CI/CD pipeline does not currently enforce a hard gate requiring a recorded deployment approval prior to allowing a production deployment to proceed for this deployment pathway, relying instead on process expectation.
Risk / Business Impact	This single, already-reviewed instance did not result in an unauthorized or unreviewed change reaching production, but represents an opportunity to harden the deployment pathway with a system-enforced gate rather than a process-only control.

Likelihood / Impact / Residual Risk	**Rare** (Likelihood) | **Insignificant** (Impact) | Residual: **Low**
Evidence Reference	*EV-012 (Illustrative Evidence Reference — No Actual Client Evidence)*
Recommendation	Implement a CI/CD pipeline gate that blocks production deployment until a deployment approval is recorded by an individual independent of the code author, consistent with the control already enforced for the primary deployment pathway.
Management Response	*Agreed. ApexCloud will extend the existing deployment-approval pipeline gate to the affected deployment pathway as a forward-looking hardening measure.*
Owner / Target Date / Status	**Engineering Director, Platform** | 15 Dec 2026 | **Open**
Retest Requirement	*No formal retest required; recommended for review during the subsequent assessment cycle.*

SOC2-ASSET-014 — Cloud Asset Inventory Reconciliation Opportunity	**OBSERVATION**
Trust Services Criteria: Not directly applicable — Informational	**Illustrative Assessment Status: Effective**
Control Objective	The cloud asset inventory reflects the current population of provisioned infrastructure resources to support accurate scoping of access, monitoring, and vulnerability management activities.
Criteria	A complete and current cloud asset inventory is not itself a discrete SOC 2 requirement, but supports the effective operation of several Security common criteria, including logical access boundary definition (CC6.1) and vulnerability detection scope (CC7.1).
Condition	A comparison of the central cloud asset inventory against a live AWS resource export identified a small number of short-lived analytics-environment compute resources that were provisioned via automated scaling but not yet reflected in the central inventory at the time of comparison.
Testing Procedure	Compared the central asset inventory export to a point-in-time AWS Resource Explorer export and reconciled discrepancies.
Population / Sample Selected	Full population comparison (not a statistical sample) between the central asset inventory and the live cloud resource export as of the comparison date.
Evidence Expected	Full reconciliation between the central asset inventory and the live cloud resource population.
Evidence Reviewed	Central asset inventory export and AWS Resource Explorer export as of the comparison date.
Exception Identified	No control exception is asserted; this is a forward-looking observation. A small number of ephemeral, auto-scaled analytics resources were not yet reflected in the central inventory at the comparison point-in-time.
Root Cause	Auto-scaling resource provisioning in the analytics environment does not currently trigger an automatic registration event in the central asset inventory.
Risk / Business Impact	This gap did not result in an unmonitored or unprotected asset in this fictional sample, but represents an opportunity to strengthen inventory completeness ahead of anticipated future assurance-framework expectations around asset inventory currency.
Likelihood / Impact / Residual Risk	**Rare** (Likelihood) | **Insignificant** (Impact) | Residual: **Low**
Evidence Reference	*EV-023, EV-024 (Illustrative Evidence Reference — No Actual Client Evidence)*
Recommendation	Implement automated asset-inventory registration for auto-scaled analytics resources at provisioning time, and periodically reconcile the central inventory against live cloud resource exports.
Management Response	*Agreed. Automated registration will be implemented for the analytics environment, with periodic reconciliation performed going forward.*
Owner / Target Date / Status	**Cloud Infrastructure Lead** | 31 Dec 2026 | **Open**
Retest Requirement	*No formal retest required; recommended for review during the subsequent assessment cycle.*

32 RISK HEATMAP

The 5×5 risk matrix below maps all 14 fictional findings and observations from this sample assessment by Likelihood and Impact, consistent with the rating methodology introduced in Section 14. Likelihood ranges from Rare to Almost Certain; Impact ranges from Insignificant to Severe. Cell shading reflects the highest severity finding mapped to that cell.



Illustrative 5×5 Risk Heatmap — Fictional Findings, Mapped by Likelihood × Impact

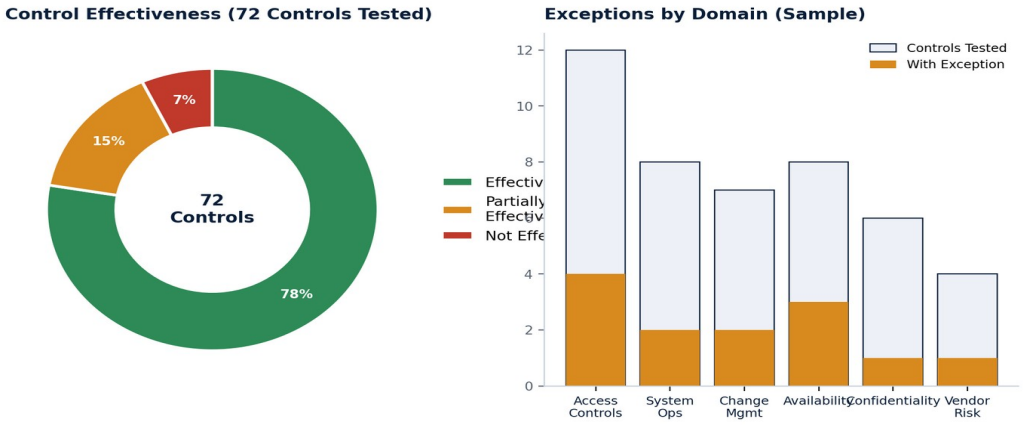
How to Read the Heatmap

- Upper-right cells (higher likelihood, higher impact) represent the fictional findings warranting the most urgent remediation attention, led by SOC2-VUL-003 in the Likely / Major cell.
- Lower-left cells represent lower-urgency observations, several of which are reported as forward-looking hardening or documentation-currency notes rather than direct control exceptions.
- The heatmap is a visualization aid; the authoritative severity rating for each finding is presented in Section 31 (Detailed Control Exceptions & Findings) and Section 39 (Finding Register).

33 TYPE II OPERATING EFFECTIVENESS SUMMARY

This section consolidates the Type II-style operating-effectiveness conclusion for all 72 illustrative controls tested in this fictional sample assessment, organized by domain. An 'Effective' conclusion indicates the sampled evidence supported consistent operation throughout the assessment period; 'Partially Effective' indicates the control operated as designed for the majority of the sample with one or more documented exceptions; 'Not Effective' indicates the sampled exception rate or nature was sufficient that the control cannot be concluded as operating consistently across the period.

Fictional Type II Operating Effectiveness Summary — Illustrative Data Only



Fictional Type II Operating Effectiveness Summary — Illustrative Data Only

Effectiveness by Domain

Domain	Tested	Effective	Partially Eff.	Not Eff.	Eff. %
Control Environment	6	5	1	0	83%
Risk Assessment	5	3	0	2	60%
Communication & Information	4	4	0	0	100%
Monitoring Activities	4	3	1	0	75%
Logical & Physical Access Controls	12	11	0	1	92%
System Operations	8	5	2	1	63%
Change Management	7	6	0	1	86%
Risk Mitigation	4	3	1	0	75%
Availability	8	5	3	0	63%
Confidentiality	6	4	2	0	67%
Vendor & Third-Party Risk	4	4	0	0	100%
Security Awareness & Workforce	4	3	1	0	75%
TOTAL	72	56	11	5	78%

Type II Conclusion (Illustrative)

Across the 72 illustrative controls tested, 56 (78%) are concluded Effective, 11 (15%) Partially Effective, and 5 (7%) Not Effective for this fictional sample assessment period. This distribution supports the report's overall illustrative status of PARTIALLY EFFECTIVE: ApexCloud's simulated control environment is concluded sound in design and largely effective in operation, with a defined, addressable set of Type II-style exceptions concentrated in privileged access governance, emergency-change documentation, and vulnerability exception governance that should be remediated and retested before ApexCloud engages an independent service auditor for an actual SOC 2 Type II examination.

34 90-DAY REMEDIATION ROADMAP

The fictional remediation roadmap below sequences remediation activity across a 90-day window, prioritizing the high-severity sample findings for early closure ahead of an actual independent SOC 2 Type II examination. All dates and timelines shown are illustrative.

Illustrative 90-Day Remediation Roadmap — Fictional Timeline

0–30 Days

- Begin remediation of privileged access governance across cloud, container, and database tiers (SOC2-ACC-001).
- Implement automated SLA-breach flagging and escalation for emergency-change retroactive approval and post-implementation review (SOC2-CHG-002).
- Automate exception-register triggering from vulnerability SLA-threshold breach, with mandatory Security Leadership Team sign-off (SOC2-VUL-003).

31–60 Days

- Formalize SOC staffing contingency for holiday/reduced-coverage periods and enable automated SLA-breach alerting for alert triage (SOC2-LOG-004).
- Complete outstanding High-risk vendor reassessments and enable automated reassessment-due reminders (SOC2-TPR-006).
- Reduce the LMS manager-escalation threshold for overdue training completions and add completion metrics to monthly reporting (SOC2-TRN-007).
- Schedule and deliver the data-breach and availability-scenario tabletop exercises (SOC2-IR-008).

61–90 Days

- Complete disaster recovery testing for the two previously untested business-critical services and reconcile the DR testing calendar (SOC2-BCP-005).
- Consolidate backup restoration testing scheduling under a single centrally tracked calendar (SOC2-BKP-010).
- Extend individual-confirmation validation to all business continuity contact tiers (SOC2-DR-013).
- Evaluate automated data-classification labeling tooling and complete the control-monitoring minutes template rollout (SOC2-ENC-011, SOC2-MON-012).
- Complete a full retest cycle across all 2026 findings ahead of engaging an independent service auditor for an actual SOC 2 Type II examination.

35 MANAGEMENT ACTION PLAN

ApexCloud's fictional management team has reviewed and formally accepted each sample finding below, with defined ownership and target remediation dates. This table is synchronized with the Detailed Control Exceptions & Findings section (Section 31) and the Finding Register (Section 39).

Finding ID	Management Response	Owner	Target Date	Priority	Status
SOC2-ACC-001	Agreed. ApexCloud will extend its existing IAM governance platform to cover all privileged account populations, including Kubernetes cluster-admin and database superuser roles, with attestation workflows enforced beginning Q4 2026.	IAM Program Manager	31 Oct 2026	Priority 1	Open
SOC2-CHG-002	Agreed. ApexCloud will implement automated SLA tracking and escalation for emergency-change approval and post-implementation review within the ITSM platform.	Engineering Director, Platform	15 Nov 2026	Priority 1	Open
SOC2-VUL-003	Agreed. ApexCloud will integrate automated SLA-threshold alerting between the vulnerability management platform and the exception register, with mandatory Security Leadership Team approval prior to SLA deferral.	Vulnerability Management Lead	30 Nov 2026	Priority 1	Open
SOC2-LOG-004	Agreed. ApexCloud will formalize SOC on-call and holiday staffing coverage and enable automated SLA-breach notifications.	SOC Manager	15 Nov 2026	Priority 2	Open
SOC2-BCP-005	Agreed. Recovery tests for the analytics/reporting and customer notification services will be scheduled and completed, with the testing calendar reconciled against the service-classification register going forward.	Backup & Infrastructure Manager	15 Dec 2026	Priority 2	Open
SOC2-TPR-006	Agreed. ApexCloud will enable automated reassessment reminders and complete outstanding reassessments for the 4 identified vendors.	Third-Party Risk Manager	31 Dec 2026	Priority 2	Open
SOC2-TRN-007	Agreed. ApexCloud will reduce the escalation threshold and add training completion metrics to the monthly security reporting package.	Training & Awareness Lead	30 Nov 2026	Priority 2	Open
SOC2-IR-008	Agreed. The October 2026 availability-scenario exercise remains scheduled, and a data-breach scenario exercise will be added to the Q1 2027 calendar; future exercise scheduling will be aligned to the assessment period.	Incident Response Manager	31 Mar 2027	Priority 2	Open
SOC2-BKP-010	Agreed. The Q2 2026 restoration test gap for the secondary reporting database has been remediated with a completed test in Q3 2026, and restoration testing scheduling has been consolidated.	Backup & Infrastructure Manager	31 Oct 2026	Priority 2	Open
SOC2-ENC-011	Agreed. Access to the 2 identified repositories has been restricted to the appropriate account teams, and ApexCloud will evaluate automated classification tooling for broader rollout.	Data Governance Lead	31 Jan 2027	Priority 3	Open
SOC2-MON-012	Agreed. A standardized minutes template and designated secondary owner have been assigned effective September 2026.	GRC Program Manager	30 Sep 2026	Priority 3	Open
SOC2-DR-013	Agreed. The individual-confirmation workflow will be extended to all contact tiers beginning the next semi-annual validation cycle.	Business Continuity Lead	31 Dec 2026	Priority 3	Open
SOC2-CHG-009	Agreed. ApexCloud will extend the existing deployment-approval pipeline gate to the affected deployment pathway as a forward-looking hardening measure.	Engineering Director, Platform	15 Dec 2026	Priority 4	Open
SOC2-ASSET-014	Agreed. Automated registration will be implemented for the analytics environment, with periodic reconciliation performed going forward.	Cloud Infrastructure Lead	31 Dec 2026	Priority 4	Open

36 FINAL ASSESSMENT & CONCLUSION

Based on the fictional evidence and simulated Type II-style testing described in this report, ApexCloud Technologies, Inc.'s environment is presented with an overall Illustrative Assessment Status of PARTIALLY EFFECTIVE for demonstration purposes.

This status is illustrative only. It is not an official SOC 2 opinion, attestation, certification, or independent service auditor's report of any kind.

Executive Conclusion

This fictional assessment demonstrates that ApexCloud maintains a mature foundational Security, Availability, and Confidentiality control program: a strong identity architecture with MFA enforcement, centralized SIEM monitoring, mature vulnerability identification coverage, a documented and exercised incident response program, a sound cloud security baseline, an immutable and encrypted backup architecture, and a structured vendor governance framework. Material fictional improvement opportunities exist around the completeness and consistency of privileged access recertification evidence, emergency-change documentation discipline, vulnerability exception governance, disaster recovery test coverage, vendor reassessment timeliness, and Type II evidence-retention practices more broadly.

None of the fictional findings in this report indicate an absent control program; rather, they reflect documentation, consistency, and evidence-retention gaps within an otherwise well-designed program — the pattern TMG Security would

expect to identify and help remediate during a readiness engagement conducted ahead of an organization's first, or a subsequent, independent SOC 2 Type II examination. ApexCloud requires remediation of the identified findings, particularly the three high-severity items, before engaging an independent service auditor for an actual SOC 2 Type II examination.

Strengths (Fictional)

- Strong identity architecture with centralized SSO and MFA enforcement across administrative and primary platform access.
- Centralized SIEM providing consistent security event monitoring coverage across infrastructure, application, and endpoint layers.
- Mature vulnerability identification program with continuous automated scanning coverage.
- Documented, exercised incident response plan with defined severity classification.
- Strong cloud security baseline, including infrastructure-as-code peer review and CSPM scanning.
- Immutable, encrypted backup architecture with a defined restoration testing program.
- Structured vendor governance framework with risk-tiered onboarding due diligence.

Improvement Areas (Fictional)

- Privileged access recertification evidence retention across cloud, container, and database tiers.
- Emergency-change documentation discipline (retroactive approval and post-implementation review).
- Vulnerability exception governance and risk-acceptance documentation.
- Disaster recovery testing coverage for newly classified business-critical services.
- Vendor reassessment timeliness for High risk-tier vendors.
- Incident response tabletop exercise scenario-class coverage within each assessment period.
- Backup restoration evidence completeness across all in-scope databases.

This conclusion, and every figure, finding, and status referenced above, is entirely fictional and constructed for demonstration purposes only. It does not describe the security, availability, or confidentiality posture of any real organization, and does not constitute a SOC 2 report, SOC 2 certification, attestation opinion, or independent service auditor's report.

37 EVIDENCE REGISTER

ILLUSTRATIVE EVIDENCE REFERENCE — NO ACTUAL CLIENT EVIDENCE

The register below lists every fictional evidence reference (EV-xxx) cited throughout this sample report. Each item is an illustrative placeholder used solely to demonstrate TMG Security's evidence referencing convention; no actual ApexCloud documents, configurations, or artifacts were collected, reviewed, or retained.

Reference	Evidence Description	Type	Illustrative Owner
EV-001	Information Security Policy	Policy	CISO
EV-002	Risk Register	Risk Assessment	GRC Program Manager
EV-003	Access Control Policy	Policy	IAM Program Manager
EV-004	Privileged Access Review Records	Access Records	IAM Program Manager
EV-005	User Termination Records	Access Records	IAM Program Manager
EV-006	MFA Configuration Export	Configuration Export	IAM Program Manager
EV-007	SIEM Monitoring & Alert Triage Records	Monitoring Records	SOC Manager
EV-008	Incident Response Plan	Program Records	Incident Response Manager
EV-009	Incident & Tabletop Exercise Records	Program Records	Incident Response Manager
EV-010	Vulnerability Scan Reports	Scan Report	Vulnerability Management Lead
EV-011	Patch / Exception Management Records	Operational Records	Vulnerability Management Lead
EV-012	Change Management Tickets	Change Records	Engineering Director, Platform
EV-013	Emergency Change Records	Change Records	Engineering Director, Platform
EV-014	Backup Configuration & Job Reports	Operational Records	Backup & Infrastructure Manager
EV-015	Restoration Test Records	Test Report	Backup & Infrastructure Manager
EV-016	Disaster Recovery Plan	Program Records	Backup & Infrastructure Manager
EV-017	DR / BCP Test Records	Test Report	Backup & Infrastructure Manager
EV-018	Vendor Risk Register	Register	Third-Party Risk Manager
EV-019	Vendor Risk Assessments & Questionnaires	Assessment Records	Third-Party Risk Manager
EV-020	Security Awareness Training Records	Training Records	Training & Awareness Lead
EV-021	Encryption Standard	Standard / Configuration	IT Endpoint Security Lead
EV-022	Data Classification Policy	Policy	Data Governance Lead
EV-023	Asset Inventory Export	Register	Cloud Infrastructure Lead
EV-024	Cloud Configuration & CSPM Records	Configuration Export	Cloud Infrastructure Lead
EV-025	Penetration Test Summary	Test Report	CISO
EV-026	Security Monitoring & Metrics Reports	Monitoring Records	SOC Manager
EV-027	Management / Control Monitoring Review Minutes	Governance Records	GRC Program Manager
EV-028	Business Continuity Contact Roster & Validation Records	Program Records	Business Continuity Lead
EV-029	Access Recertification Reports	Access Records	IAM Program Manager
EV-030	Control Monitoring Review Records	Governance Records	GRC Program Manager

38 CONTROL TESTING REGISTER

This register presents the full illustrative Type II-style testing model applied to a representative sample of controls, including population definition, sample selection, testing frequency, evidence type, test procedure, result, exception, and conclusion. All populations, samples, and results are fictional and provided to demonstrate TMG Security's Type II testing documentation convention.

Quarterly Privileged Access Review	Not Effective
Population	All privileged accounts (AWS IAM, Kubernetes cluster-admin, database superuser) active during the assessment period.
Sample Selected	8 quarterly/monthly review instances across selected systems.
Testing Frequency	Monthly (cloud/DB tiers) / Quarterly (aggregate program review)

Evidence Type	Review tracker, exported account listing, reviewer attestation
Test Procedure	Verify reviewer assignment, review completion, evidence of approval, and remediation of identified exceptions.
Result	5 of 8 samples effective; 3 exceptions (no retained reviewer attestation).
Exception	Yes — see SOC2-ACC-001

User Termination — Timely Access Revocation	**Effective**
Population	All workforce terminations during the assessment period.
Sample Selected	25 terminated-user records.
Testing Frequency	Event-driven (per termination)
Evidence Type	HR termination record, access revocation timestamp
Test Procedure	Compare HR-recorded termination date/time to system access revocation timestamp across all in-scope systems for each sampled termination.
Result	25 of 25 samples effective; access revoked within the same business day in all sampled cases.
Exception	No

Change Management — Peer Review & Deployment Approval	**Partially Effective**
Population	All standard/normal production change tickets during the assessment period.
Sample Selected	12 change-management tickets (8 standard/normal, 4 emergency).
Testing Frequency	Event-driven (per change)
Evidence Type	Change ticket, pull-request review, CI/CD deployment log
Test Procedure	Inspect each ticket for peer code review, independent deployment approval, and correlation of approval timestamp to deployment timestamp.
Result	11 of 12 samples effective; 1 observation (retroactive approval timestamp) and 2 exceptions within the emergency-change subset.
Exception	Yes — see SOC2-CHG-002, SOC2-CHG-009

Vulnerability Remediation SLA & Exception Governance	**Not Effective**
Population	All Critical/High vulnerability findings identified during the assessment period.
Sample Selected	6 monthly vulnerability remediation cycles.
Testing Frequency	Continuous scanning / monthly cycle review
Evidence Type	Scan report, remediation tracker, exception/risk-acceptance register
Test Procedure	Identify SLA-exceeding findings within each sampled cycle and confirm a corresponding documented exception record.
Result	4 of 9 SLA-exceeding findings had a documented exception; 5 did not.
Exception	Yes — see SOC2-VUL-003

Backup Restoration Testing	**Partially Effective**
Population	All in-scope production databases supporting business-critical services.
Sample Selected	10 backup restoration evidence records across 3 quarters.
Testing Frequency	Quarterly
Evidence Type	Restoration test log, test outcome record
Test Procedure	Confirm a documented, successful restoration test exists for each in-scope database each quarter.
Result	8 of 10 samples effective; 2 samples (one database, one quarter) lacked restoration test evidence.
Exception	Yes — see SOC2-BKP-010

Security Awareness Training Completion	**Partially Effective**
Population	All active workforce members with system access.
Sample Selected	20 security awareness completion records.
Testing Frequency	Annual
Evidence Type	LMS completion record, escalation log
Test Procedure	Confirm on-time completion or, where late, evidence of an escalation notice.
Result	17 of 20 samples effective; 3 samples completed late with no escalation notice recorded.
Exception	Yes — see SOC2-TRN-007

Vendor Risk Reassessment (High / Critical Risk Vendors)	Partially Effective
Population	All active High and Critical risk-tier vendors.
Sample Selected	15 vendor risk assessments.
Testing Frequency	Annual
Evidence Type	Vendor risk register entry, reassessment record, SOC report review
Test Procedure	Compare current reassessment completion date to the prior assessment date against the 12-month policy target.
Result	11 of 15 samples effective; 4 High-risk vendors reassessed 14–19 months after the prior cycle.
Exception	Yes — see SOC2-TPR-006

SIEM High-Priority Alert Triage	Partially Effective
Population	All high-priority SIEM alerts generated during the assessment period.
Sample Selected	10 weekly triage periods (35-week population).
Testing Frequency	Daily triage / weekly sample review
Evidence Type	SIEM alert export, SOC ticketing disposition record
Test Procedure	Confirm each high-priority alert generated during the sampled week has a documented disposition within one business day.
Result	7 of 10 weeks fully effective; 3 weeks contained delayed dispositions (14 alerts, 2–4 business days).
Exception	Yes — see SOC2-LOG-004

Incident Response Tabletop Exercise Coverage	Partially Effective
Population	All tabletop/simulation exercises conducted during the assessment period.
Sample Selected	Full population — 1 exercise conducted within the assessment period.
Testing Frequency	Annual (per incident severity class)
Evidence Type	After-action report
Test Procedure	Compare exercise scenario coverage against the three incident severity classes defined in the Incident Response Plan.
Result	1 of 3 required scenario classes exercised and evidenced within the assessment period.
Exception	Yes — see SOC2-IR-008

Disaster Recovery Testing (Business-Critical Services)	Partially Effective
Population	All services classified as business-critical.
Sample Selected	Full population — 5 business-critical services.
Testing Frequency	Annual (full failover) / Quarterly (tabletop)
Evidence Type	DR test plan, execution record, results summary
Test Procedure	Confirm a completed, documented recovery test exists for each business-critical service within the assessment period.
Result	3 of 5 services evidenced; 2 services (added to the critical inventory mid-period) lacked test evidence.
Exception	Yes — see SOC2-BCP-005

MFA Enforcement — Administrative & Customer-Facing Access	Effective
Population	All administrative console and primary platform accounts.
Sample Selected	Full population reviewed via configuration export; corroborated with 12 individual account walkthroughs.
Testing Frequency	Continuous (policy-enforced)
Evidence Type	IdP/MFA configuration export
Test Procedure	Confirm MFA is enforced at the identity-provider and conditional-access-policy level for all in-scope account populations.
Result	12 of 12 samples effective.
Exception	No

Control Monitoring — Monthly Management Review	Partially Effective
Population	All monthly control monitoring review cycles during the assessment period.
Sample Selected	8 monthly review cycles.
Testing Frequency	Monthly

Evidence Type	Meeting minutes, calendar record
Test Procedure	Confirm retained minutes documenting metrics discussed, issues identified, and follow-up actions assigned.
Result	6 of 8 samples effective; 2 samples had confirmed occurrence but no retained minutes.
Exception	Yes — see SOC2-MON-012

39 FINDING REGISTER

Illustrative Assessment Status reflects the sampled control condition underlying each finding; Remediation Status reflects fictional tracking of the corrective action itself. Both are synchronized with Section 30, Section 31, and Section 35.

ID	Title	Severity	TSC Reference	Illustrative Assessment Status	Remediation Status
SOC2-ACC-001	Privileged Access Review Evidence Not Consistently Retained	HIGH	CC6.2 / CC6.3	Not Effective	Open
SOC2-CHG-002	Emergency Change Documentation Incomplete	HIGH	CC8.1	Not Effective	Open
SOC2-VUL-003	Vulnerability Remediation Exceptions Not Consistently Governed	HIGH	CC7.1	Not Effective	Open
SOC2-LOG-004	Security Event Review Evidence Inconsistent	MEDIUM	CC7.2	Partially Effective	Open
SOC2-BCP-005	Disaster Recovery Testing Coverage Gap	MEDIUM	A1.2 / A1.3	Partially Effective	Open
SOC2-TPR-006	Vendor Risk Reassessment Evidence Delayed	MEDIUM	CC9.2	Partially Effective	Open
SOC2-TRN-007	Security Awareness Completion Tracking Gap	MEDIUM	CC1.4	Partially Effective	Open
SOC2-IR-008	Incident Response Exercise Documentation Incomplete	MEDIUM	CC7.3 / CC7.4	Partially Effective	Open
SOC2-CHG-009	Change Approval Evidence Missing for Sampled Tickets	OBSERVATION	CC8.1	Effective	Open
SOC2-BKP-010	Backup Restoration Evidence Not Available for All Critical Services	MEDIUM	A1.2	Partially Effective	Open
SOC2-ENC-011	Confidential Data Classification Enforcement Gap	LOW	C1.1	Partially Effective	Open
SOC2-MON-012	Control Monitoring Review Documentation Inconsistent	LOW	CC4.1	Partially Effective	Open
SOC2-DR-013	Business Continuity Contact Validation Not Fully Evidenced	LOW	A1.3	Partially Effective	Open
SOC2-ASSET-014	Cloud Asset Inventory Reconciliation Opportunity	OBSERVATION	Not directly applicable	Effective	Open

40 SOC 2 CONTROL MATRIX

The matrix below maps all 72 illustrative controls tested in this sample assessment to their Trust Services Criteria reference, domain, control objective, owner, frequency, evidence, illustrative operating effectiveness, related finding, and recommended action.

TSC Ref.	Domain	Control Description	Operating Effectiveness	Evid.	Finding	Recommended Action
CC1.1 CE-01	Control Environment	Code of Conduct is documented, distributed, and acknowledged annually by all workforce members.	Effective	EV-001	—	Maintain current acknowledgement tracking.
CC1.2 CE-02	Control Environment	Executive leadership reviews the security and compliance program at least quarterly.	Effective	EV-027	—	Maintain current governance review cadence.
CC1.3 CE-03	Control Environment	Security roles, responsibilities, and reporting lines are documented in the organizational chart and security RACI.	Effective	EV-001	—	Maintain current documentation.
CC1.4 CE-04	Control Environment	Workforce members complete annual security awareness training and role-based training as applicable.	Partially Effective	EV-020	SOC2-TRN-007	Reduce escalation threshold; add completion metrics to monthly reporting.
CC1.5 CE-05	Control Environment	Individual control ownership is assigned and tracked in the GRC platform for each in-scope control.	Effective	EV-002	—	Maintain current ownership tracking.
CC1.2 CE-06	Control Environment	Documented control narratives are reviewed and updated when the underlying process materially changes.	Effective	EV-002	—	Add narrative-review step to workflow-tooling change process.
CC3.1 RA-CTRL-01	Risk Assessment	Annual enterprise risk assessment identifies threats and vulnerabilities relevant to Security, Availability, and Confidentiality commitments.	Effective	EV-002	—	Maintain current risk assessment cadence.
CC3.2 RA-CTRL-02	Risk Assessment	Identified risks are rated for likelihood and impact, including consideration of fraud risk factors.	Effective	EV-002	—	Maintain current risk rating methodology.
CC3.3 RA-CTRL-03	Risk Assessment	Significant changes to the business or IT environment trigger a documented reassessment of related risks.	Not Effective	EV-002	—	Formalize trigger criteria and evidence retention for change-driven reassessment; 2 of 5 sampled significant changes lacked a documented reassessment during the assessment period.
CC3.4 RA-CTRL-04	Risk Assessment	Vendors and subservice organizations are risk-classified and reassessed on a defined cadence.	Not Effective	EV-018	SOC2-TPR-006	Implement automated reassessment-due reminders; this control angle (timely trigger of the reassessment cycle) is addressed together with SOC2-TPR-006.
CC3.2 RA-CTRL-05	Risk Assessment	The enterprise risk register is maintained and reviewed by the Security Leadership Team.	Effective	EV-002	—	Maintain current review cadence.
CC2.1 CI-01	Communication & Information	Security policies and objectives are communicated to the workforce via the policy portal and onboarding process.	Effective	EV-001	—	Maintain current communication channels.
CC2.2 CI-02	Communication & Information	Individual security responsibilities are communicated through role-based training and policy acknowledgement.	Effective	EV-020	—	Maintain current process.
CC2.3 CI-03	Communication & Information	Security commitments and incident notification procedures are communicated to customers via the Trust Center and customer agreements.	Effective	EV-008	—	Maintain current external communication channels.
CC2.1 CI-04	Communication & Information	A confidential channel exists for reporting suspected security or ethics concerns.	Effective	EV-001	—	Maintain current reporting channel.
CC4.1 MON-01	Monitoring Activities	Management performs and documents monthly control monitoring reviews.	Partially Effective	EV-027	SOC2-MON-012	Adopt standardized minutes template with designated secondary owner.
CC4.1 MON-02	Monitoring Activities	Key security metrics (alerts, vulnerabilities, training, changes) are compiled and reviewed monthly.	Effective	EV-026	—	Maintain current metrics reporting.
CC4.2 MON-03	Monitoring Activities	Identified control deficiencies are tracked to remediation with assigned owners and target dates.	Effective	EV-002	—	Maintain current tracking process.
CC4.1 MON-04	Monitoring Activities	An independent penetration test of the production environment is performed annually.	Effective	EV-025	—	Maintain current annual testing cadence.
CC6.1 AC-01	Logical & Physical Access Controls	Network and system boundaries are defined and access is restricted via security groups, IAM policy, and network segmentation.	Effective	EV-024	—	Maintain current boundary controls.
CC6.1 AC-02	Logical & Physical Access Controls	A central inventory of cloud infrastructure assets supports access and monitoring scoping.	Effective	EV-023	SOC2-ASSET-014	Implement automated registration for auto-scaled resources.
CC6.2 AC-03	Logical & Physical Access Controls	New access requests require documented manager and system-owner approval prior to provisioning.	Effective	EV-003	—	Maintain current provisioning workflow.
CC6.2 AC-04	Logical & Physical Access Controls	Access is revoked across all in-scope systems within one business day of a workforce termination.	Effective	EV-005	—	Maintain current termination workflow.
CC6.3 AC-05	Logical & Physical Access Controls	Standard user access is reviewed quarterly by system owners.	Effective	EV-029	—	Maintain current review cadence.
CC6.3 AC-06	Logical & Physical Access Controls	Privileged/administrative access across cloud,	Not Effective	EV-004	SOC2-ACC-001	Migrate privileged access

TSC Ref.	Domain	Control Description	Operating Effectiveness	Evid.	Finding	Recommended Action
		container, and database tiers is reviewed on a recurring basis with retained evidence.				recertification into centralized IAM governance platform.
CC6.6 AC-07	Logical & Physical Access Controls	MFA is enforced for administrative consoles, the primary platform, and remote access.	Effective	EV-006	—	Maintain current MFA enforcement.
CC6.6 AC-08	Logical & Physical Access Controls	Data in transit between customers, the application, and backend services is encrypted using current TLS standards.	Effective	EV-021	—	Maintain current transmission security controls.
CC6.7 AC-09	Logical & Physical Access Controls	Outbound data transmission from production environments is restricted to approved endpoints and monitored.	Effective	EV-024	—	Maintain current egress controls.
CC6.8 AC-10	Logical & Physical Access Controls	EDR is deployed on all managed workforce endpoints with centralized alerting.	Effective	EV-007	—	Maintain current EDR coverage.
CC6.4 AC-11	Logical & Physical Access Controls	Badge-based access control and visitor logging are enforced at the Austin, TX corporate office.	Effective	EV-023	—	Maintain current physical access controls.
CC6.5 AC-12	Logical & Physical Access Controls	Decommissioned physical media and hardware are securely disposed of or wiped in accordance with the Data Classification Policy.	Effective	EV-022	—	Maintain current disposal procedures.
CC7.1 OPS-01	System Operations	Automated vulnerability scanning covers cloud infrastructure, container images, and internet-facing endpoints.	Effective	EV-010	—	Maintain current scanning coverage.
CC7.1 OPS-02	System Operations	SLA-exceeding vulnerability findings are routed through a documented risk-acceptance process.	Not Effective	EV-011	SOC2-VUL-003	Automate exception-register triggering from SLA-threshold breach.
CC7.2 OPS-03	System Operations	SIEM aggregates security-relevant logs and generates alerts for anomalous activity.	Effective	EV-007	—	Maintain current monitoring coverage.
CC7.2 OPS-04	System Operations	High-priority alerts are triaged and dispositioned within one business day.	Partially Effective	EV-007	SOC2-LOG-004	Formalize SOC staffing contingency for reduced-coverage periods.
CC7.3 OPS-05	System Operations	Security incidents are classified, triaged, and responded to per the Incident Response Plan.	Effective	EV-008	—	Maintain current incident response process.
CC7.3 OPS-06	System Operations	The Incident Response Plan is exercised annually across all defined incident severity classes.	Partially Effective	EV-009	SOC2-IR-008	Realign exercise calendar to assessment-period scenario coverage.
CC7.4 OPS-07	System Operations	Post-incident review documents root cause, remediation, and lessons learned for all classified incidents.	Effective	EV-009	—	Maintain current post-incident review process.
CC7.5 OPS-08	System Operations	Infrastructure capacity and application performance are continuously monitored with alerting on defined thresholds.	Effective	EV-026	—	Maintain current capacity monitoring.
CC8.1 CHG-01	Change Management	Production code changes require documented peer code review prior to merge.	Effective	EV-012	—	Maintain current peer review requirement.
CC8.1 CHG-02	Change Management	Production deployments require an independent approval separate from the code author.	Effective	EV-012	SOC2-CHG-009	Extend CI/CD pipeline approval gate to all deployment pathways (forward-looking hardening observation).
CC8.1 CHG-03	Change Management	Emergency changes receive documented retroactive approval within 2 business days.	Not Effective	EV-013	SOC2-CHG-002	Automate SLA-breach flagging and escalation for emergency changes.
CC8.1 CHG-04	Change Management	Changes are tested in a non-production environment prior to production deployment.	Effective	EV-012	—	Maintain current testing requirements.
CC8.1 CHG-05	Change Management	Production deployment credentials are restricted from the general engineering population.	Effective	EV-012	—	Maintain current access restriction.
CC8.1 CHG-06	Change Management	Documented rollback procedures exist and are tested for critical services.	Effective	EV-012	—	Maintain current rollback testing.
CC8.1 CHG-07	Change Management	Infrastructure changes deployed via IaC templates require peer review prior to apply.	Effective	EV-024	—	Maintain current IaC review requirement.
CC9.1 RM-01	Risk Mitigation	Identified availability and business-disruption risks have documented mitigation or transfer strategies.	Effective	EV-002	—	Maintain current risk treatment documentation.
CC9.2 RM-02	Risk Mitigation	New vendors undergo security due diligence, including SOC report review where applicable, prior to onboarding.	Effective	EV-019	—	Maintain current onboarding due diligence.
CC9.2 RM-03	Risk Mitigation	High and Critical risk-tier vendors are reassessed annually.	Partially Effective	EV-018	SOC2-TPR-006	Implement automated reassessment-due reminders.
CC9.2 RM-04	Risk Mitigation	Vendor access and data-sharing arrangements are terminated upon contract end.	Effective	EV-018	—	Maintain current offboarding process.
A1.1 AV-01	Availability	Infrastructure capacity is planned and monitored against forecasted demand.	Effective	EV-026	—	Maintain current capacity planning process.
A1.1 AV-02	Availability	Production infrastructure is deployed across multiple availability zones with automated failover.	Effective	EV-024	—	Maintain current redundancy architecture.
A1.1 AV-03	Availability	Service availability is continuously monitored against internal SLA commitments.	Effective	EV-026	—	Maintain current SLA monitoring.
A1.2 AV-04	Availability	Production data is backed up on a defined schedule with encryption at rest.	Effective	EV-014	—	Maintain current backup schedule.
A1.2 AV-05	Availability	Backup restoration is tested quarterly for in-scope production databases.	Partially Effective	EV-015	SOC2-BKP-010	Consolidate restoration testing scheduling under a single calendar.
A1.3 AV-06	Availability	The Disaster Recovery Plan is reviewed and updated at least annually.	Effective	EV-016	—	Maintain current DR plan review cadence.
A1.3 AV-07	Availability	Business-critical services undergo full or tabletop DR testing on a defined cadence.	Partially Effective	EV-017	SOC2-BCP-005	Update DR testing calendar to reflect current business-

TSC Ref.	Domain	Control Description	Operating Effectiveness	Evid.	Finding	Recommended Action
						critical inventory.
A1.3 AV-08	Availability	Emergency contact rosters are validated semi-annually across all defined tiers.	Partially Effective	EV-028	SOC2-DR-013	Extend individual-confirmation workflow to all contact tiers.
C1.1 CF-01	Confidentiality	Confidential-tier data is identified and labeled consistent with the Data Classification Policy.	Partially Effective	EV-022	SOC2-ENC-011	Evaluate automated classification labeling and access-restriction tooling.
C1.1 CF-02	Confidentiality	Repositories containing Confidential-tier data are restricted to the minimum-necessary access group.	Partially Effective	EV-022	SOC2-ENC-011	Restrict access on identified over-permissioned repositories.
C1.2 CF-03	Confidentiality	Confidential-tier data stores are encrypted at rest using a current, industry-standard algorithm.	Effective	EV-021	—	Maintain current encryption standard.
C1.2 CF-04	Confidentiality	Confidential data is securely deleted or the underlying storage sanitized at the end of its defined retention period.	Effective	EV-022	—	Maintain current disposal procedures.
C1.2 CF-05	Confidentiality	Workforce members and vendors with access to Confidential data execute confidentiality/NDA agreements.	Effective	EV-001	—	Maintain current agreement execution process.
C1.1 CF-06	Confidentiality	DLP monitoring is applied to email and endpoint egress channels for Confidential-tier data patterns.	Effective	EV-021	—	Maintain current DLP monitoring coverage.
CC9.2 TPR-01	Vendor & Third-Party Risk	Vendors are classified by risk tier at onboarding based on data access and service criticality.	Effective	EV-018	—	Maintain current classification methodology.
CC9.2 TPR-02	Vendor & Third-Party Risk	SOC reports or equivalent assurance artifacts are reviewed for Critical-risk subservice organizations.	Effective	EV-019	—	Maintain current assurance-review process.
CC9.2 TPR-03	Vendor & Third-Party Risk	Vendor contracts include security, confidentiality, and incident-notification requirements.	Effective	EV-018	—	Maintain current contract requirements.
CC9.2 TPR-04	Vendor & Third-Party Risk	Vendor contracts require timely notification of security incidents affecting ApexCloud data.	Effective	EV-018	—	Maintain current notification requirements.
CC1.4 TRN-01	Security Awareness & Workforce	New hires complete security awareness training as part of onboarding, prior to system access.	Effective	EV-020	—	Maintain current onboarding training requirement.
CC1.4 TRN-02	Security Awareness & Workforce	All workforce members complete annual security awareness refresher training.	Partially Effective	EV-020	SOC2-TRN-007	Reduce manager-escalation threshold for overdue completions.
CC1.4 TRN-03	Security Awareness & Workforce	Simulated phishing exercises are conducted periodically with individual results tracked.	Effective	EV-020	—	Maintain current phishing simulation cadence.
CC1.4 TRN-04	Security Awareness & Workforce	Engineering and administrative personnel complete role-based security training (e.g., secure coding, cloud security).	Effective	EV-020	—	Maintain current role-based training program.

41 MANAGEMENT ASSERTION & RESPONSIBILITY

MANAGEMENT ASSERTION — ILLUSTRATIVE ONLY

Role of Management's Assertion in an Actual SOC 2 Examination

In an actual SOC 2 examination, management of the service organization is responsible for preparing the system description and for asserting, in writing, that the description fairly presents the system and that the controls were suitably designed (Type I) and operated effectively (Type II) throughout the specified period. The independent service auditor then plans and performs procedures to obtain reasonable assurance about whether management's assertion is fairly stated, and issues an opinion accordingly. TMG Security, in the preparation of this fictional sample, is not ApexCloud's management and has not obtained or relied upon an actual management assertion.

Illustrative Fictional Assertion (For Demonstration Only)

For demonstration purposes only, the following illustrates the general form and content a management assertion might take in an actual engagement. This text is fictional, is not signed or issued by any real party, and does not constitute an actual assertion:

> *"We have prepared the accompanying description of ApexCloud Technologies, Inc.'s [system name] system throughout the period 01 January 2026 to 31 August 2026 (description) based on the criteria for a description of a service organization's system in the AICPA's Description Criteria. We confirm, to the best of our knowledge and belief, that the description fairly presents the system throughout the period, and that the controls stated in the description were suitably designed and operated effectively throughout the period to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria."*
>
> **— Fictional / Illustrative Text Only. Not Signed. Not an Actual Management Assertion.**

TMG Security's Role in This Sample

Throughout this sample engagement, TMG Security acted in the fictional capacity of a readiness assessor — the role an organization typically engages before its own management prepares an actual system description and assertion for submission to an independent service auditor. TMG Security did not, and does not in an actual readiness engagement, sign, issue, or attest to a management assertion on behalf of any client.

42 REGULATORY / FRAMEWORK WATCH — 2026

FORWARD-LOOKING AWARENESS — NOT A CHANGE TO CURRENT SOC 2 CRITERIA

SOC 2 Framework Stability

SOC 2 is based on the AICPA Trust Services Criteria, which are periodically updated by the AICPA's Assurance Services Executive Committee (ASEC) but do not change on the frequent cycle seen in some regulatory frameworks. This report is based on the 2017 Trust Services Criteria with the 2022 revised Points of Focus, the version in standard use for SOC 2 examinations as of this report's date. This section does not propose or imply any new SOC 2 requirement; it identifies broader assurance, cybersecurity, privacy, cloud, and AI-governance trends that organizations in ApexCloud's position should monitor for their potential future relevance.

Forward-Looking Considerations (Not Current Criteria)

Evolving Cybersecurity Expectations	Customers and cyber-insurers increasingly expect evidence of MFA everywhere, EDR coverage, and tested incident response beyond baseline SOC 2 criteria — worth tracking even though not a formal SOC 2 requirement.
AI Governance & Data Use	As SaaS platforms adopt AI/ML features, customers are beginning to request disclosure of AI-related data handling and model-governance practices in due-diligence questionnaires, though this is not currently a distinct Trust Services Criterion.
Privacy Criterion Adoption	Some organizations are proactively adding the Privacy Trust Services Category to their SOC 2 scope as customer data-protection expectations increase, even where not strictly required by current criteria.
Continuous Controls Monitoring	Automated, continuous control monitoring tooling is becoming a common readiness practice ahead of Type II examinations, reducing reliance on point-in-time evidence collection.
Subservice Organization Transparency	Customers are increasingly requesting more granular subservice organization risk disclosure (the inclusive method) rather than the carve-out method, a trend worth monitoring for future system description scoping.

These forward-looking considerations are presented for awareness and future-readiness purposes only. They are NOT current SOC 2 Trust Services Criteria and are NOT scored as part of the current-state assessment in this sample report.

43 ASSESSMENT LIMITATIONS

This entire report — including its scope, methodology, evidence, testing results, findings, and conclusions — is a fictional construct created solely to demonstrate TMG Security's report structure, Type II testing methodology, and reporting standards. The following limitations apply specifically to this sample document and distinguish it from an actual SOC 2 engagement deliverable:

- ApexCloud Technologies, Inc. is a fictional organization. It does not correspond to any real company, and no real entity was assessed in the production of this document.
- No production environment, system, or network of any kind was accessed, scanned, or tested in the creation of this report.
- No real customer data or confidential business information was accessed at any point in the production of this document.
- No actual policies or evidence were collected. All evidence references (EV-xxx) are illustrative placeholders only.
- No actual penetration testing was performed.
- No actual vulnerability scanning was performed.

- No actual interviews occurred; all interviews and control walkthroughs referenced in this report are simulated.
- No actual security incident occurred; the tabletop exercise scenarios in Section 26 and Section 27 are entirely fictional.
- No actual independent SOC 2 examination, audit, or attestation engagement occurred.
- Findings, evidence references, testing results, sample selections, dates, control statuses, and management responses are fictional and illustrative.
- Risk ratings and Type II effectiveness conclusions are illustrative and do not reflect any actual assessment outcome.
- This document does not constitute a SOC 2 report, SOC 2 certification, attestation opinion, or independent service auditor's report.
- This document does not constitute an AICPA-recognized examination of any kind.
- This document does not constitute legal, accounting, or professional assurance advice.
- This document does not establish actual SOC 2 compliance or readiness for any organization.
- An actual SOC 2 Type II examination and attestation report must be performed and issued by an appropriately qualified independent service auditor in accordance with applicable AICPA professional standards, and actual readiness depends on the organization's specific facts, systems, controls, and evidence.

44 GLOSSARY

SOC 2	System and Organization Controls 2 — an AICPA attestation reporting framework addressing a service organization's controls relevant to security, availability, processing integrity, confidentiality, and/or privacy.
Type I	A SOC 2 report addressing the suitability of control design as of a specific point in time.
Type II	A SOC 2 report addressing the suitability of control design and the operating effectiveness of controls over a specified period.
Trust Services Criteria (TSC)	The AICPA criteria framework (2017, with 2022 revised Points of Focus) underlying SOC 2 examinations, comprising Security, Availability, Processing Integrity, Confidentiality, and Privacy.
Common Criteria (CC)	The nine criteria categories (CC1–CC9) that make up the mandatory Security criterion, applicable to every SOC 2 examination.
Subservice Organization	A third-party vendor whose services are part of the system being examined (e.g., a cloud hosting provider).
Carve-Out Method	A system description approach that excludes a subservice organization's controls from the description and the auditor's testing.
Inclusive Method	A system description approach that includes a subservice organization's controls within the description and the auditor's testing.
Complementary User Entity Controls (CUECs)	Controls the service organization assumes its customers will implement, necessary to achieve certain service commitments.
Population	The complete set of transactions or instances of a control's operation during the assessment period, from which a test sample is drawn.
Exception	An instance in a tested sample where a control did not operate exactly as designed.
MFA	Multi-Factor Authentication — authentication requiring two or more independent verification factors.
SIEM	Security Information and Event Management — a platform for centralized log aggregation, correlation, and alerting.
EDR	Endpoint Detection and Response — technology that monitors and responds to threats on endpoint devices.
RBAC	Role-Based Access Control — an access model that assigns permissions based on defined roles.
RTO	Recovery Time Objective — the targeted duration within which a system or service must be restored after a disruption.
RPO	Recovery Point Objective — the maximum acceptable amount of data loss, measured in time, following a disruption.
CI/CD	Continuous Integration / Continuous Deployment — the automated pipeline used to build, test, and deploy software changes.
GRC	Governance, Risk, and Compliance — the discipline and tooling used to manage organizational risk and regulatory/contractual compliance.
ITSM	IT Service Management — the platform and practices used to manage change, incident, and access-request workflows.
NPRM	Notice of Proposed Rulemaking — used in this report's Regulatory Watch section to refer generally to proposed (not final) regulatory changes relevant to organizations' broader compliance posture.

45 CONTACT & DISCLAIMER

Cybersecurity | SOC | VAPT | GRC | MDR | Compliance Solutions | Corporate Trainings

Web: www.tmgsec.com **Email:** security@tmgsec.com
USA Office: 117 South Lexington Street, STE 100, Harrisonville, MO 64701
Support: support@tmgsec.com | **Phone:** +1 (816) 793-1929
WhatsApp: +1 (480) 680-0342

Final Disclaimer

FICTIONAL SAMPLE REPORT — NOT AN ACTUAL SOC 2 ATTESTATION

This document was created by TMG Security solely to demonstrate assessment methodology, Type II testing approach, and professional reporting standards. ApexCloud Technologies, Inc. is fictional. No actual SOC 2 examination, audit, certification, attestation, or independent service auditor's report was performed or issued.