

Example Service Organization, Inc.

Independent Service Auditor's Report on
Controls Relevant to Security, Availability and Confidentiality
(SOC 2[®] Type 2)

For the period **January 1, 2026, through June 30, 2026**

Example CPA Firm LLP
Certified Public Accountants

READ THIS BEFORE ANYTHING ELSE

This is not a real SOC 2 report. Example Service Organization, Inc. and Example CPA Firm LLP are fictional. No audit was performed, no CPA firm examined anything, and no opinion in this document is a real opinion. Every figure, control, test result and date was invented to illustrate structure.

It exists so that someone about to receive their first SOC 2 report knows what is coming, and so that someone reviewing a vendor's report knows where to look. The blue **Reader's note** boxes are the teaching layer and would never appear in a real report.

Do not present this document, or any part of it, to a customer, auditor or regulator as evidence of a completed audit. A real SOC 2 report is issued only by a licensed CPA firm that has performed the examination.

TABLE OF CONTENTS

Section I	Independent Service Auditor's Report	3
Section II	Management's Assertion	6
Section III	Description of the System	7
	Overview of services	7
	System components: infrastructure, software, people, procedures, data	7
	Subservice organizations and carve-outs	8
	Complementary subservice organization controls	8
	Complementary user entity controls	9
	Significant changes during the period	9
Section IV	Trust Services Criteria, Controls, Tests and Results	10
Section V	Other Information Provided by Management (unaudited)	13

READER'S NOTE 1: ORIENT FROM THE CONTENTS PAGE

No attestation standard fixes the order of these sections. This sample leads with the auditor's report, which is the common convention, but the AICPA and Cloud Security Alliance illustrative report puts management's assertion first. Any guide that tells you a section is "section 1" without qualification is guessing about the report in front of you. Find the contents page and work from that.

READER'S NOTE 2: WHAT THIS REPORT DOES NOT TELL YOU

Three criteria are in scope here: security, availability and confidentiality. Processing integrity and privacy are not. If you are buying this service on a commitment that depends on either (accurate transaction processing, or handling of personal data you are the controller of), this report does not cover it, however clean the opinion is.

SECTION I

INDEPENDENT SERVICE AUDITOR'S REPORT

To the Management of Example Service Organization, Inc.

Scope

We have examined Example Service Organization, Inc.'s ("the Company") accompanying description of its Example Data Platform system, in Section III, throughout the period January 1, 2026, to June 30, 2026, and the suitability of the design and operating effectiveness of the controls stated in the description throughout that period to provide reasonable assurance that the Company's service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability and confidentiality.

The Company uses a third-party cloud infrastructure provider (the subservice organization) to host the platform. The description in Section III indicates that complementary subservice organization controls, assumed in the design of the Company's controls, are necessary, along with the Company's controls, to provide reasonable assurance that the Company's service commitments and system requirements were achieved. The description presents the Company's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of the Company's controls. The description does not disclose the actual controls at the subservice organization. Our examination did not include the services provided by the subservice organization, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

The description also indicates that complementary user entity controls, assumed in the design of the Company's controls, are necessary, along with the Company's controls, to provide reasonable assurance that the Company's service commitments and system requirements were achieved. Our examination did not include such complementary user entity controls, and we have not evaluated the suitability of their design or operating effectiveness.

The information in Section V, Other Information Provided by Management, is presented by the Company's management to provide additional context. It has not been subjected to the procedures applied in the examination, and accordingly we express no opinion on it.

Service organization's responsibilities

The Company is responsible for its service commitments and system requirements, and for designing, implementing and operating effective controls to achieve them. The Company has provided the assertion in Section II. The Company is also responsible for preparing the description and for the completeness, accuracy and method of presentation of both the description and the assertion.

Service auditor's responsibilities

Our responsibility is to express an opinion on the matters described above, based on our examination. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform the examination to obtain reasonable assurance about whether, in all material respects, the description is presented in accordance with the applicable criteria and the controls stated in it were suitably designed and operated effectively throughout the period. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

We are required to be independent of the Company and to meet our other ethical responsibilities, in accordance with the relevant ethical requirements relating to the examination engagement.

Inherent limitations

The description is prepared to meet the common needs of a broad range of report users and may not include every aspect of the system that an individual user considers important to its own purposes. Because of their nature, controls may not always operate effectively to achieve the stated objectives. Also, the projection to future periods of any conclusions about the suitability of design or operating effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions, or that the degree of compliance with them may deteriorate.

READER'S NOTE 3: WHAT THE INHERENT-LIMITATIONS PARAGRAPH IS TELLING YOU

It is the auditor saying, in standard language, that this report describes a period that has already ended and makes no promise about today. That is why buyers treat a report as current for around twelve months, and why a material change to the vendor's systems can make a recent report stop covering what you buy, regardless of its date.

Description of tests of controls

The specific controls we tested, and the nature, timing and results of those tests, are presented in Section IV.

Opinion

In our opinion, in all material respects:

- a. the description presents the Example Data Platform system that was designed and implemented throughout the period January 1, 2026, to June 30, 2026, in accordance with the applicable criteria;
- b. the controls stated in the description were suitably designed throughout that period to provide reasonable assurance that the Company's service commitments and system requirements would be achieved based on the applicable trust services criteria, if the controls operated effectively throughout that period and if the subservice organization and user entities applied the complementary controls assumed in the design of the Company's controls throughout that period; and
- c. the controls stated in the description operated effectively throughout that period to provide reasonable assurance that the Company's service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary subservice organization controls and complementary user entity controls assumed in the design of the Company's controls operated effectively throughout that period.

READER'S NOTE 4: THIS IS AN UNQUALIFIED OPINION, AND THERE IS STILL AN EXCEPTION IN THE REPORT

The opinion above is the clean one. Section IV nonetheless records a deviation at control CC1.4 (see page 10). Reports use "deviation" and "exception" for the same thing: a test result showing a control did not operate as described.

The two are not in conflict. An exception is a per-test result, while the opinion is a judgment on the control system as a whole, in all material respects. Isolated deviations with a credible management response can sit inside a clean opinion. It is why "unqualified" is not the same as "nothing was found," and why the exceptions are worth reading even when the opinion looks fine.

Notice too the conditions in (b) and (c): the opinion holds only if the cloud provider runs the complementary subservice organization controls and your own company runs the complementary user entity controls. The auditor tested neither. Section III lists both.

Restricted use

This report, including the description of tests of controls and results in Section IV, is intended solely for the information and use of the Company, user entities of the Example Data Platform system during some or all of the period, and prospective user entities and their auditors and regulators who have sufficient knowledge and understanding of the matters set out in the report. It is not intended to be, and should not be, used by anyone other than these specified parties.

Example CPA Firm LLP (fictional firm, see cover)

Certified Public Accountants

Boston, Massachusetts

August 14, 2026

READER'S NOTE 5: WHO SIGNED IT

The report is only worth the firm behind it. Confirm the firm is a licensed CPA firm, ask for its current AICPA peer review report in writing, and check whether it has audited companies like the one you are assessing. A firm can be enrolled in the peer review program without having completed a review, and only a completed review tells you anything. This is the check buyers skip and then regret, because a report you accept becomes a report you are vouching for when your own customers ask.

Note the issuance date, August 14, against a period that ended June 30. Six weeks between period end and issuance is ordinary. It also means there is a stretch where the period has closed and the report does not yet exist, which is the gap a bridge letter covers.

SECTION II

MANAGEMENT'S ASSERTION

We have prepared the accompanying description of the Example Data Platform system in Section III throughout the period January 1, 2026, to June 30, 2026, based on the criteria for a description of a service organization's system set out in DC section 200. The description is intended to provide report users with information about the system that may be useful when assessing the risks arising from interactions with our system, particularly information about system controls that we have designed, implemented and operated to provide reasonable assurance that our service commitments and system requirements were achieved.

We use a subservice organization for cloud infrastructure. The description presents our controls and the types of complementary subservice organization controls assumed in the design of our controls, and does not include the actual controls at the subservice organization. The description also indicates that complementary user entity controls assumed in the design of our controls are necessary to achieve our service commitments and system requirements.

We confirm, to the best of our knowledge and belief, that:

- a. the description presents the system that was designed and implemented throughout the period in accordance with the applicable criteria;
- b. the controls stated in the description were suitably designed throughout the period to provide reasonable assurance that our service commitments and system requirements would be achieved based on the applicable trust services criteria, if the controls operated effectively and if the subservice organization and user entities applied the complementary controls assumed in the design of our controls throughout the period; and
- c. the controls stated in the description operated effectively throughout the period to provide reasonable assurance that our service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary subservice organization controls and complementary user entity controls assumed in the design of our controls operated effectively throughout the period.

We have disclosed in Section III the significant changes to the system during the period, and we are not aware of any other matters that would affect a report user's assessment of the system.

Signed on behalf of the management of Example Service Organization, Inc.

Chief Technology Officer

August 14, 2026

READER'S NOTE 6: WHO IS MAKING WHICH STATEMENT

Compare the wording here with Section I and you will see the two documents say nearly the same thing, signed by different parties. This section is the audited company asserting that its own description is accurate. Section I is an independent firm's opinion on that assertion. If you only read one, read the auditor's. If you read both, read them in that order: the assertion tells you what was claimed, and the opinion tells you whether the claim survived testing.

Note the second half of the last sentence: *we are not aware of any other matters*. Management is representing that the significant-changes disclosure in Section III is complete. That representation is what makes it worth reading.

DESCRIPTION OF THE SYSTEM

Overview of services

Example Service Organization, Inc. provides the Example Data Platform, a multi-tenant software-as-a-service application that ingests, stores and transforms operational data for customers in logistics and industrial services. Customers connect source systems to the platform through authenticated APIs, define transformation pipelines, and access results through a web application and a reporting API. The Company is headquartered in Boston, Massachusetts, with a development team in Lisbon, Portugal, and employed 84 people during the period.

The scope of this examination is the Example Data Platform production environment. **The Example Analytics product, released in April 2026, is not within the scope of this examination.**

READER'S NOTE 7: CONFIRM THE REPORT COVERS THE THING YOU ARE BUYING

That bolded sentence describes one of the most common ways a report turns out to be useless: it is a real report, with a clean opinion, about a different product. Check the overview of services against the product on your contract, and check the entity name against the entity you are contracting with. A report covering another product line, or a sibling legal entity, is a report about somebody else's controls.

System components

Infrastructure. The platform runs in a single public-cloud region, in a virtual private cloud segmented into public, application and data subnets. Production data stores are encrypted at rest using provider-managed keys. All external traffic terminates at a managed load balancer enforcing TLS 1.2 or higher.

Software. The application is a set of containerized services orchestrated by a managed Kubernetes service. Supporting tooling includes a source-control platform, a CI/CD pipeline, an identity provider providing single sign-on and multi-factor authentication, an endpoint management agent, a log aggregation service, a vulnerability scanner and a ticketing system.

People. Engineering (41), customer operations (18), security and compliance (4, reporting to the Chief Technology Officer), corporate functions (21). The Company engaged 6 contractors during the period, all of whom held access to non-production environments only.

Procedures. Documented policies cover information security, access control, change management, incident response, business continuity, vendor management, risk assessment and acceptable use. Policies are reviewed annually and acknowledged by all personnel on hire and after each material revision.

Data. Customer operational data, platform metadata, application and infrastructure logs, and personnel records supporting the control environment. Customer data is classified Confidential under the Company's data classification policy and is logically segregated by tenant identifier.

Subservice organizations

The Company uses one subservice organization within the scope of this description:

SUBSERVICE ORGANIZATION	FUNCTION	METHOD	HOW THE COMPANY MONITORS IT
Public-cloud infrastructure provider	Compute, storage, networking, managed database and key management for the production environment	Carve-out	The Company obtains and reviews the provider's SOC 2 Type 2 report annually, tracks the complementary user entity controls the provider identifies, and reviews the provider's published incident notices. Review is documented in the vendor management register.

Complementary subservice organization controls

The Company's controls were designed on the assumption that the subservice organization operates the following types of controls. They were not tested in this examination.

1. physical access to data centers housing the production environment is restricted to authorized personnel and monitored;
2. environmental protections at those data centers, including power, cooling and fire suppression, are maintained and monitored;
3. storage media are sanitized or destroyed before disposal; and
4. the managed database and key management services protect encryption keys and operate as the provider describes, including notifying customers of incidents affecting them.

READER'S NOTE 8: A CARVE-OUT LEAVES THE PROVIDER UNTESTED, AND THAT IS NORMAL

"Carve-out" means the provider's controls were excluded from testing. The Company's cloud host was not audited here; the auditor tested only the Company's controls, including how the Company monitors that host. The alternative method, "inclusive," folds the subservice organization into the examination and is less common.

Carve-outs are normal. What you are checking is whether the description still tells you what the provider does, which controls the Company assumes the provider runs (the list above), and how the Company monitors it. This one does all three. If a critical dependency is carved out and the description says nothing about oversight, that is the finding. And if your own risk assessment needs assurance over that provider, you have to go and read the provider's own report.

Complementary user entity controls

The Company's controls were designed on the assumption that user entities operate certain controls themselves. The controls stated in this description are not intended to provide, and do not provide, assurance over the following. User entities are responsible for:

1. provisioning, reviewing and deprovisioning their own administrator and end-user accounts within the platform, including prompt removal of access for departing personnel;
2. enforcing multi-factor authentication and password policy for their own identity provider where single sign-on is configured;
3. configuring tenant-level data retention, export and sharing settings in accordance with their own requirements;
4. protecting API credentials issued to them, and rotating those credentials in line with their own policy;
5. reviewing the access and audit logs the Company makes available to them for activity inconsistent with their expectations; and
6. notifying the Company promptly of any suspected compromise of their credentials or tenant data.

READER'S NOTE 9: THESE SIX ITEMS ARE YOUR JOB

This is the list most reviewers skip, and skipping it is how a clean report creates a false sense of coverage. The auditor's opinion in Section I is explicitly conditional on these being applied; reread clauses (b) and (c) on page 4. Nobody tested whether you do them.

The practical step: assign an owner on your side to each of the six before you accept the report, and check the list again at renewal, because vendors add to it as products change.

Significant changes during the period

The following changes to the system occurred during the period January 1, 2026, to June 30, 2026:

Primary data store migration (March 2026). The Company migrated the primary customer data store from a self-managed database cluster to the cloud provider's managed database service. The migration was executed under the change management process described above, with a documented rollback plan. Encryption at rest and tenant segregation were preserved. Access paths and monitoring were re-established and retested following cutover.

Identity provider consolidation (February 2026). Two legacy directories were consolidated into a single identity provider. All personnel accounts were re-provisioned and a full access review was performed at completion.

Security and compliance staffing (January 2026). A dedicated security and compliance function of four people was established, reporting to the Chief Technology Officer. Control ownership was reassigned accordingly.

The Company experienced no security incident during the period that resulted in unauthorized disclosure, alteration or loss of customer data, and met its published availability commitment of 99.9% monthly uptime in each month of the period.

READER'S NOTE 10: READ THE CHANGES AGAINST THE EXCEPTION

Three material changes in a six-month window is a lot of movement, and this is where a careful reviewer earns their keep. The staffing change in January reassigned control ownership; the exception in Section IV is a training control that failed in the first quarter. Those two facts are probably related, and management's response in Section V says so.

This is also the section to read for what is missing. A migration, acquisition, new subservice provider or failure to meet a service commitment all belong here, and management has asserted the list is complete. If you know of a change from a press release or your own account team that does not appear here, ask about it.

SECTION IV

TRUST SERVICES CRITERIA, CONTROLS, TESTS AND RESULTS

Tests of controls were performed throughout the period. Inquiry was performed for all controls and is not repeated in each row. Sample sizes reflect the population and control frequency. Extracted below is a representative selection; a complete report presents every control in scope.

CRITERION	CONTROL	TEST PERFORMED BY SERVICE AUDITOR	RESULT
CC1.1	A code of conduct is documented and acknowledged by all personnel on hire and annually thereafter.	Inspected the code of conduct. For a sample of 25 of 84 personnel, inspected acknowledgment records.	No deviations noted.
CC1.4	Personnel complete security awareness training within 30 days of hire and annually thereafter.	Inspected the training platform completion register. For a sample of 25 of 84 personnel, compared completion date against hire date and policy requirement.	Deviation noted. For 2 of 25 personnel sampled, both hired in January 2026, training was completed 47 and 52 days after hire, exceeding the 30-day policy requirement. Both completed training during the period. No other deviations noted. <i>See management's response in Section V.</i>
CC2.2	Information security policies are available to all personnel and reviewed at least annually by management.	Inspected the policy repository and the record of the most recent management review.	No deviations noted.
CC3.2	A risk assessment identifying threats to service commitments is performed at least annually and results are documented with treatment owners.	Inspected the risk assessment completed February 2026, the risk register, and evidence of treatment assignment.	No deviations noted.
CC6.1	Logical access to production systems requires unique credentials, single sign-on and multi-factor authentication.	Inspected identity provider configuration. For a sample of 25 of 47 users with production access, inspected enrollment records.	No deviations noted.

CRITERION	CONTROL	TEST PERFORMED BY SERVICE AUDITOR	RESULT
CC6.2	Access to production is approved by the system owner before provisioning, based on documented role.	For all 14 users provisioned during the period, inspected the access request ticket and approval.	No deviations noted.
CC6.2	Access is revoked within 1 business day of termination.	For all 9 personnel terminated during the period, compared the access revocation timestamp with the termination date.	No deviations noted.
CC6.3	Access to production systems is reviewed quarterly by the system owner, and changes are actioned within 10 business days.	For both quarterly reviews in the period, inspected the review record, reviewer, date, and tickets for actioned changes.	No deviations noted.
CC7.1	Infrastructure and application vulnerability scans are performed at least monthly and findings are remediated according to documented severity timelines.	Inspected scan output for all 6 months. For a sample of 15 findings, inspected remediation records against severity timeline.	No deviations noted.
CC7.2	Security events from production infrastructure and applications are logged centrally, retained for 12 months, and monitored with alerting to on-call personnel.	Inspected log aggregation configuration, retention setting and alert routing. For a sample of 5 alerts raised during the period, inspected triage records.	No deviations noted.
CC7.4	A documented incident response plan is maintained and exercised at least annually.	Inspected the plan and the record of the tabletop exercise conducted May 2026, including participants and findings.	No deviations noted.
CC8.1	Changes to production require peer review, successful automated testing, and documented approval before deployment.	For a sample of 25 of 1,180 production changes, inspected the pull request, peer approval, pipeline result and deployment record.	No deviations noted.
CC9.2	Vendors with access to customer data are risk-assessed before engagement and reviewed annually thereafter.	Inspected the vendor register. For a sample of 8 of 23 in-scope vendors, inspected the assessment record and most recent review.	No deviations noted.
A1.2	Production data is backed up daily, backups are encrypted, and restoration is tested at least annually.	Inspected backup configuration and encryption setting. Inspected the restoration test performed April 2026, including the restored dataset and validation record.	No deviations noted.

CRITERION	CONTROL	TEST PERFORMED BY SERVICE AUDITOR	RESULT
A1.3	A business continuity and disaster recovery plan is documented and tested at least annually.	Inspected the plan and the test record from April 2026.	No deviations noted.
C1.1	Confidential data is identified and protected in accordance with the data classification policy.	Inspected the classification policy, the data inventory, and encryption configuration for identified stores.	No deviations noted.
C1.2	Confidential data is retained and disposed of in accordance with documented commitments, including on termination of a customer agreement.	Inspected the retention schedule. For all 3 customer terminations during the period, inspected the deletion record and confirmation.	No deviations noted.

READER'S NOTE 11: HOW TO WEIGH THE ONE EXCEPTION

Four things decide how much a deviation matters, and all four are readable off the table above.

How many, out of how many. Two of twenty-five. One in forty reads differently from six in ten.

Which criterion. CC1.4 is security awareness training, a people control in the control-environment category. A deviation here is a different conversation from one at CC6.1, logical access, which is likely to be a control you directly rely on.

Whether it changed the opinion. It did not; Section I is unqualified. That is the auditor concluding the criteria were met in all material respects despite the deviation, and it is the strongest single signal available to you.

What management said. Section V is unaudited, but a response naming a root cause, an owner and a date reads very differently from one that restates the finding.

Note also what the sample sizes tell you. Where a population was small enough (9 terminations, 14 provisions, 3 customer terminations, 2 quarterly reviews), the auditor tested all of it. Where it was large, they sampled. A report showing tiny samples against large populations is worth a question.

A note about this sample. A deviation is included here because a spotless report cannot teach you how to read one. In practice, the reports companies circulate are almost always clean: across the eight real company reports we examined, every opinion was unqualified and not one recorded an exception. So treat the row above as instructive rather than typical, and treat a real report that does carry an exception as unusual to see rather than a warning sign.

SECTION V

OTHER INFORMATION PROVIDED BY MANAGEMENT

UNAUDITED

The information in this section is provided by the Company's management. It was not subjected to the procedures applied in the examination of the description, the suitability of control design, or operating effectiveness, and the service auditor expresses no opinion on it.

Management's response to the deviation noted at CC1.4

Finding. Two personnel hired in January 2026 completed security awareness training 47 and 52 days after their hire date, against a policy requirement of 30 days.

Root cause. Both hires were onboarded in the week the security and compliance function was established and control ownership was being reassigned from engineering management. Training assignment at that time was a manual step in the onboarding checklist, and the handover of that step was not completed. No automated reminder existed.

Corrective action taken. Training enrollment was automated from the identity provider on February 3, 2026, so an account creation now triggers enrollment without manual action. A weekly exception report of incomplete assignments is reviewed by the Security and Compliance Manager. Both individuals completed the training during the period.

Owner and date. Security and Compliance Manager; automation implemented February 3, 2026; first exception report reviewed February 10, 2026.

Recurrence prevention. The manual step has been removed from the onboarding checklist, and the exception report is a standing item in the monthly control review.

Planned initiatives

The Company expects to bring the Example Analytics product into the scope of its next examination, and to extend the examination period to twelve months, covering July 1, 2026, to June 30, 2027.

READER'S NOTE 12: UNAUDITED, AND STILL THE MOST INFORMATIVE PAGE IN THE REPORT

Nobody tested a word of this section. Read it as the company's own statement, and read it anyway: a management response that names a root cause, an owner, a date and a mechanism that prevents recurrence tells you more about how a vendor operates than a report with nothing in it. This one does, and it corroborates the January staffing change disclosed in Section III, which is the kind of internal consistency worth checking.

The planned-initiatives note also tells you something practical: next year's report will cover more than this one. The product currently excluded is coming in, and a six-month period is becoming twelve.

REMINDER

Example Service Organization, Inc. and Example CPA Firm LLP do not exist. No examination was performed and this document carries no assurance of any kind. It is a teaching illustration of the structure and language of a SOC 2 Type 2 report, and must not be presented to any third party as evidence of an audit.

A real report is issued only by a licensed CPA firm that performed the examination. There is no public library of genuine SOC 2 reports. They are confidential by design, and the routes to seeing a real one are the vendor's trust page or a direct request under NDA.

ILLUSTRATIVE SAMPLE: NOT A REAL REPORT