YASSI

WHITEPAPER

SOC 1 TYPE II & SOC 2 TYPE II

TOP SECURITY DATA PROTECTION STANDARDS

Understanding SOC 1 and SOC 2 Type II Reports: Why Every Data Provider Should Have One

An educational guide for security, compliance, audit, and procurement teams.

PUBLISHED BY YOTTA AUTOMATED SOFTWARE SOLUTIONS, INC. (YASSI) AUGUST 2026

CONTENTS

01 Executive Summary

Independent attestation has become the common language of third-party assurance. It is also one of the most frequently misread documents in the vendor review process.

Organizations that purchase data services are increasingly expected to demonstrate that they have evaluated the security posture of the providers they rely on. In practice, that evaluation often comes down to two artifacts: a security questionnaire completed by the provider, and an attestation report the reviewer receives but rarely has time to read closely. The questionnaire is self-reported. The report is independent, but it is also technical, scope-limited, and easy to misread in either direction, as either a guarantee or a formality.

This paper is written for the security, compliance, audit, and procurement professionals on the receiving end of that process. It explains what System and Organization Controls (SOC) reporting is, what the different report types are designed to answer, what an auditor's opinion does and does not establish, and how to read a report closely enough to reach a documented conclusion.

It also explains why Yotta Automated Software Solutions (YASSI) maintains both a SOC 1 Type II and a SOC 2 Type II report instead of one or the other. The two reports answer genuinely different questions, for different audiences, and neither substitutes for the other. Section 4 develops that reasoning in full. YASSI's 2026 examinations of both reports were completed with no exceptions noted, and the company maintains an annual examination cycle it intends to continue in 2027 and onward.

Three points frame everything that follows:

1. A SOC report is documented evidence, not a warranty. It reflects an independent examination of specified controls, over a stated period, against stated criteria.
2. Scope and period are more informative than the conclusion. Two reports can reach the same conclusion and differ substantially in what they actually cover. The reviewer's work is in the scope section.
3. The report assumes the customer does its part. Nearly every SOC 2 report identifies controls the customer is expected to operate, and Section 6 explains why those pages deserve closer attention than they typically get.

02 Third-Party Risk Has Outpaced Third-Party Verification

The case for rigorous provider review no longer rests on argument. It rests on published data, and that data has moved sharply in one direction.

48%

of confirmed breaches involved a third party — up roughly 60% over the prior year.

23%

of third-party organizations had fully remediated missing MFA on cloud accounts.

SOURCE: VERIZON, 2026 DATA BREACH INVESTIGATIONS REPORT

Verizon's 2026 Data Breach Investigations Report, drawn from more than 22,000 confirmed breaches across 145 countries, found that third parties were involved in 48 percent of breaches. That is an increase of roughly 60 percent over the prior year, which had itself roughly doubled from the year before. Across three reporting cycles, third-party involvement moved from a meaningful minority of breaches to nearly half of them. The same report found that only 23 percent of third-party organizations had fully remediated missing multi-factor authentication on cloud accounts, indicating that exposure in the provider layer is not only common but slow to close.

Two observations follow for anyone responsible for provider review. The first is that an organization's effective perimeter now includes the control environments of its providers, whether or not the organization has visibility into them. The second is that the harder problem is not identifying risk but verifying that it was addressed, which is the difference between asking a provider a question and examining whether the provider's controls operated.

REVIEW IS INCREASINGLY EXPECTED TO BE DOCUMENTED

Across regulated industries, expectations around provider oversight have shifted from informal comfort to review that leaves a record. Many organizations now operate under contractual, customer, insurer, or internal audit expectations to select providers capable of maintaining appropriate safeguards, to address those safeguards in their agreements, and to reassess providers periodically based on the risk they present.

The practical consequence is that a reviewer's assessment often has to be documented well enough to be shown to someone else: an internal audit function, an external auditor, or a customer conducting its own review. That standard of proof is difficult to satisfy with a self-completed questionnaire alone. Organizations should look to their own advisors and regulators for the specific requirements that apply to them.

FOR MANY CUSTOMERS, THIS IS ALREADY A REGULATORY OBLIGATION

For many of the organizations that rely on data like YASSI's, including lenders, finance companies, servicers, and insurers, provider oversight is not only prudent risk management; for many, it is already a standing legal requirement. The FTC's GLBA Safeguards Rule (16 C.F.R. Part 314) requires financial institutions under its jurisdiction to take reasonable steps to select and retain service providers capable of maintaining appropriate safeguards, to require those safeguards by contract, and to periodically reassess providers based on the risk they present. Separately, the NAIC Insurance Data Security Model Law has been adopted in some form by a majority of states and imposes a parallel obligation on insurance licensees to oversee the security practices of their third-party service providers. Where either framework applies, the review this paper describes is not a best practice layered on top of existing compliance work; it is the record that shows that compliance work actually happened. Organizations should confirm with their own counsel or compliance function which requirements apply to their specific charter, license, and states of operation.

WHAT QUESTIONNAIRES DO WELL, AND WHERE THEY STOP

Security questionnaires, including standardized instruments such as the Cloud Security Alliance CAIQ and the Shared Assessments SIG, remain useful. They are efficient, they can be tailored to the specific risk a provider presents, and they surface topics a general-purpose report may not cover. What they cannot do is provide independent verification. A questionnaire records what an organization says about itself, at the time it was completed, in language the organization chose.

An attestation examination is designed to close part of that gap. An independent licensed CPA firm examines whether specified controls were suitably designed and, in a Type II engagement, whether they operated effectively over a defined period, and documents the tests performed and the results obtained. That is a different and more durable form of evidence. It is not a substitute for the reviewer's own judgment.

03 What a SOC Report Is

SOC stands for System and Organization Controls. The framework is maintained by the American Institute of Certified Public Accountants (AICPA). A SOC engagement is an attestation examination performed by an independent licensed CPA firm under AICPA attestation standards. The auditor examines management's description of a system and management's assertion about the controls in that system, tests those controls, and reports the results.

Three report families are in common use, and they are not interchangeable:

- SOC 1 addresses controls at a service organization that are relevant to its customers' internal control over financial reporting. Its intended audience is the customer and the customer's financial statement auditor.
- SOC 2 addresses controls relevant to the Trust Services Criteria: security, availability, processing integrity, confidentiality, and privacy. Its intended audience is management, customers, and other parties with sufficient knowledge of the system.
- SOC 3 covers the same subject matter as SOC 2 but is a general-use summary. It omits the detailed description of tests and results, which makes it suitable for public distribution and insufficient for substantive review.

THE TRUST SERVICES CRITERIA

A SOC 2 examination is performed against one or more of five criteria categories. Security is included in every engagement.

CRITERIA	WHAT IT ADDRESSES	TYPICAL RELEVANCE
Security	Protection of information and systems against unauthorized access, use, or modification.	Always in scope for SOC 2.
Availability	Whether the system is available for operation and use as committed or agreed.	Relevant where customers depend on uptime or real-time delivery.
Processing Integrity	Whether processing is complete, valid, accurate, timely, and authorized.	Relevant where the output informs a downstream decision.
Confidentiality	Protection of information designated as confidential.	Relevant where the data carries contractual or regulatory restrictions.
Privacy	Collection, use, retention, disclosure, and disposal of personal information.	Relevant where personal information is handled on behalf of individuals.

Table 1. The five Trust Services Criteria categories. Covering more categories is not automatically stronger.

TYPE I AND TYPE II

The distinction between report types matters more than the distinction between criteria. A Type I report addresses whether controls were suitably designed as of a single specified date. A Type II report addresses whether those controls were suitably designed and whether they operated effectively throughout a specified period, commonly three to twelve months, and includes the auditor's description of the tests performed and the results obtained.

Design assurance without operating assurance answers only half the question, because a control can be well designed and inconsistently performed. For that reason, a Type II report covering a period of reasonable length is generally the appropriate expectation for a provider handling sensitive data, and a Type I report is best understood as an interim milestone, typically a first-year engagement, not a settled state.

THE CONCLUSION, AND WHAT "NO EXCEPTIONS NOTED" MEANS

The auditor reports one of four conclusions: unqualified, meaning the auditor concluded the description is fairly presented and the controls were suitably designed and operated effectively; qualified, meaning that conclusion holds except for specified matters; adverse, meaning it does not hold; or a disclaimer, meaning the auditor was unable to form an opinion. The conclusion appears in the independent service auditor's report and should be read in full, not summarized.

Within the detailed test results, the auditor records whether each test identified a deviation. Where no deviations were identified, the report states that no exceptions were noted. It means the tests the auditor performed, on the controls within the defined scope, during the defined period, did not identify deviations. It is bounded by scope, by period, and by sampling, because attestation testing is generally performed on a sample basis, not on every instance. A result of no exceptions noted is a meaningful and non-trivial outcome. It is not a statement that no risk remains or that no incident will occur.

WHAT A SOC REPORT DOES NOT ESTABLISH

A few things are true regardless of the report's conclusion:

- A SOC engagement produces a report containing an independent auditor's conclusion. There is no governing body that issues a SOC credential, and no license or authorization to operate results from the process.

- It is not pass or fail. A report with exceptions noted does not automatically describe an unacceptable provider, and a report with none is not automatically sufficient for a given reviewer's purpose.

- It is not a general-use document. SOC 1 and SOC 2 reports are restricted-use reports, ordinarily provided to specified parties under a confidentiality agreement. A provider that declines to post a full report publicly is following the framework, not withholding information.

- It is not perpetual. Every report covers a historical period that has already closed by the time a reviewer reads it.

04 Why Two Reports: SOC 1 Type II and SOC 2 Type II

SOC 1 and SOC 2 are not tiers of the same assurance. They answer different questions, for different audiences, and neither substitutes for the other.

This point gets lost most often in provider conversations, and it's why YASSI maintains both reports. A SOC 2 examination asks whether the controls in a system are suitably designed and operating effectively with respect to security and, where in scope, availability, processing integrity, confidentiality, and privacy. A SOC 1 examination asks a narrower and quite different question: whether the controls at the service organization that are relevant to its customers' internal control over financial reporting are suitably designed and operating effectively.

	SOC 1 TYPE II	SOC 2 TYPE II
Question answered	Are controls relevant to customers' financial reporting suitably designed and operating effectively?	Are controls relevant to the Trust Services Criteria suitably designed and operating effectively?
Criteria used	Control objectives defined by management, relevant to internal control over financial reporting.	AICPA Trust Services Criteria: security, plus any additional categories in scope.
Primary audience	Customer management and the customer's financial statement auditor.	Customer security, compliance, risk, and procurement functions.
Typical reason requested	The provider's processing is an input to a financially significant process at the customer.	The provider stores, processes, or transmits sensitive or regulated data.
What it does not address	Security and confidentiality of the data itself.	The customer's financial reporting control environment.

Table 2. SOC 1 and SOC 2 compared. They may draw on overlapping control environments, but they do not provide overlapping assurance.

WHY A REAL-TIME DATA PROVIDER CAN SIT IN BOTH PATHWAYS

Most service organizations reasonably need only one of these reports. Maintaining both is a scope decision driven by the shape of an organization's risk, not a measure of quality and not a claim that one approach is better than another. YASSI's decision reflects two characteristics of the services it provides.

The first is the nature of the data. Personal information contained in state motor vehicle records is subject to the federal Driver's Privacy Protection Act (18 U.S.C. § 2721 et seq.) and to the terms of the data-exchange agreements state agencies establish with the organizations authorized to receive it. Access control, permitted-use governance, logging, and confidentiality are therefore central design considerations, not general good practice. That is SOC 2 subject matter.

The second is where the output lands. Vehicle, title, registration, and lien data delivered through an API is consumed inside customer processes at lenders, finance companies, servicers, and insurers: processes such as collateral identification, lien status verification, portfolio monitoring, and underwriting and claims workflows. Where a customer process of that kind contributes to amounts or disclosures in the customer's financial statements, the customer's external auditor has a question about the provider's control environment that security assurance alone does not answer.

SOC 2 addresses whether the data is protected. SOC 1 gives the customer's auditor a basis for evaluating the controls surrounding how that data reached them. A provider positioned between sensitive source records on one side and financially significant customer processes on the other encounters both questions, and answering only one of them leaves a reviewer with real work still to do.

WHY TYPE II FOR BOTH, AND THE INTERVAL BETWEEN REPORTS

Both of YASSI's reports are Type II for the reason described in Section 3: design assurance alone does not establish that controls operated. Each is examined on an annual cycle. A practical limitation applies to every provider, however: a Type II report covers a historical period that ends before the reviewer reads it, leaving an interval between the end of the examination period and the present date.

The customary way to address that interval is a bridge letter, sometimes called a gap letter, in which management represents whether there have been material changes to the control environment since the period end. A bridge letter is useful and standard practice. It is also management's representation rather than an audited product, and a reviewer should treat it accordingly: as a statement of continuity from the provider, not as an extension of the auditor's conclusion. Where the interval is long or the risk is high, the appropriate step is to ask when the next examination period ends.

05 How Data Sensitivity Changes the Review

Not all sensitive data carries the same expectations. Where data is subject to restrictions on who may receive it and for what purposes, the review question changes: it is no longer only whether the data is protected from outsiders, but whether the provider can demonstrate that access and use were governed and recorded. That shifts several control areas from background hygiene to primary subject matter.

CONTROL AREAS THAT WARRANT SPECIFIC ATTENTION

For providers handling data subject to use restrictions, a reviewer should expect the description of the system to address the following in specific rather than generic terms:

- Customer eligibility and onboarding: how the provider determines that a customer is entitled to receive the data before access is granted, rather than treating onboarding as a commercial step.
- Permitted-use governance: how the permitted purpose for a request is established, constrained, and enforced at the point of access.
- Access control and credential management: how access is provisioned, reviewed, and removed, and how API credentials are issued and protected.
- Logging and retention: what is recorded about each request and recipient, how long those records are retained, and how they can be produced when requested.
- Onward disclosure controls: how obligations are addressed with customers who may themselves provide data to others.

WHY AVAILABILITY AND PROCESSING INTEGRITY ARE NOT SECONDARY

In a real-time delivery model, criteria that reviewers sometimes treat as optional carry direct consequences. If a response is delayed, a decision at the customer is delayed or made without the data. If a record is returned incompletely or matched to the wrong vehicle or lienholder, the customer may act on it. Where the output informs a lending, underwriting, titling, or servicing decision, timeliness and accuracy of processing are properties of the control environment that a reviewer should confirm are within the scope of the examination rather than assume.

06 Reading a SOC 2 Type II Report

A SOC 2 Type II report is typically organized into recognizable sections. Knowing what each contains lets a reviewer allocate attention deliberately instead of reading front to back and running out of time in the detail.

SECTION	CONTENTS	WHAT TO DO WITH IT
Independent service auditor's report	The auditor's conclusion, the scope, the period, and the criteria applied.	Read it in full. Confirm the conclusion, the exact period, and the criteria in scope.
Management's assertion	Management's statement about the description and the controls.	Note what management is and is not asserting, and over what boundary.
Description of the system	Services, system boundaries, infrastructure, people, processes, subservice organizations, and CUECs.	Defines what was examined. Confirm the services purchased are inside the boundary.
Criteria, controls, tests & results	Each control, the auditor's test procedures, and the results, including any exceptions noted.	The substantive section. Read the tests relevant to your risk, not only the results column.
Other information (if present)	Supplemental material provided by management, outside the auditor's conclusion.	Useful context. Do not treat it as audited.

Table 3. Sections of a typical SOC 2 Type II report. Ordering and titles vary somewhat between firms.

FIVE CHECKS THAT DO MOST OF THE WORK

Scope. Confirm the report's boundary includes the specific product being purchased — the most common review error.

Period. Check both the length and recency of the examination period.

Exceptions. Read them, don't just count them — design vs. operation, significance, and remediation matter.

CUECs. Nearly every report assumes controls the customer performs — commonly the least-read pages, and among the most consequential.

Subservice organizations. Carved-out organizations may need their own reports reviewed separately.

Scope. A report can legitimately cover a subset of a provider's services, systems, or locations. The most common review error is accepting a report whose boundary does not include the specific product being purchased. Confirm the match explicitly.

Period. Check both the length and the recency of the examination period. A short first-year period provides less evidence of consistent operation than a full twelve months, and a report whose period ended some time ago should prompt a question about the current cycle.

Exceptions and management responses. Where exceptions are noted, read them instead of just counting them. What matters is whether the deviation was in design or in operation, how significant it was, whether it affects a control being relied on, and what remediation management described.

Complementary user entity controls. Nearly every report identifies controls the report assumes the customer will perform: managing user provisioning and deprovisioning, protecting credentials and API keys, configuring permissions appropriately, reviewing access logs, and restricting requests to permitted purposes.

Subservice organizations. Providers rely on other providers. A report will treat those relationships using either the carve-out method, which excludes the subservice organization's controls and identifies the complementary controls expected of it, or the inclusive method, which brings them inside the examination.

A NOTE ON THE AUDITOR

Because a SOC report is an attestation product, the firm issuing it matters. Confirm that the report was issued by an independent licensed CPA firm.

07 A Review Framework: Questions to Ask Any Data Provider

The following questions are written to be applied to any provider of sensitive data services, including YASSI, directly in a provider review workflow. None requires the reviewer to be an auditor, and each produces an answer that can be documented.

AREA	QUESTION	WHY IT MATTERS
Report type	Do you maintain a SOC 2 Type II? A SOC 1 Type II? Which, and why those?	A provider should explain its scope decision in terms of its own risk profile.
Period	What period does the current report cover, and when does the next period end?	Establishes recency and whether coverage is continuous.
Criteria	Which Trust Services Criteria categories are in scope, and why were others excluded?	Confirms the report addresses the risks being assessed.
Boundary	Is the specific service or API being purchased inside the described system boundary?	The most common and most consequential scope mismatch.
Results	Were any exceptions noted, and what remediation was performed?	Substance matters more than the count.
Customer obligations	What CUECs does the report assume the customer operates?	Determines whether the assurance holds on the customer side.
Subservice providers	Which subservice organizations are carved out, and can their reports be reviewed?	Reveals dependencies outside the examination.
Continuity	Is a bridge letter available covering the interval since the period end?	Standard practice; note that it is unaudited.
Data governance	How are customer eligibility, permitted use, logging, and retention governed?	Central where data carries use restrictions.
Incident terms	What are the provider's incident notification commitments, and how do they align with the customer's own obligations?	Notification expectations vary considerably between agreements.

Table 4. A provider-neutral review framework, intended to be applied consistently across a vendor portfolio.

WHEN THE REPORT ISN'T A CURRENT, UNQUALIFIED TYPE II

The framework above assumes the straightforward case: a current, unqualified SOC 2 Type II report. Reviewers will also encounter other situations, and each calls for a specific next step rather than a single pass or fail judgment:

- No report exists yet. Ask whether a readiness assessment or Type I engagement is underway, and treat the timeline to a completed Type II as part of the risk decision, not a reason to stop the conversation.

- Only a Type I is available. As Section 3 notes, this is the expected state for a first-year engagement. Confirm that a Type II covering a full period is in progress and ask when it will be issued.

- The opinion is qualified. Read the specific matters excepted, not just the label. Determine whether the excepted control is one your organization actually relies on, and evaluate the remediation management described.

- The opinion is adverse or a disclaimer. Treat this as a substantive finding that warrants escalation through your own risk process, not a basis for continuing the relationship on the report alone.

None of these outcomes is disqualifying on its own. Each is simply more information for the reviewer to weigh before reaching a conclusion.

08 Conclusion: Raising the Standard

Independent attestation is the most useful instrument available for making third-party control environments legible to the people who have to rely on them. Read as intended, as evidence of an independent examination of defined controls over a defined period, it allows a security or compliance function to reach a conclusion and show its work. Read as a guarantee, it does a disservice to reviewers with real decisions to make.

The clearest conclusion to draw from the trend described in Section 2 is not simply that buyers should ask harder questions. It is that the number of organizations able to answer those questions with verifiable, independently examined evidence needs to grow.

THE CALL TO ACTION

If your organization provides data, software, or processing services that others depend on, the most useful step available is to obtain your own SOC 2 Type II report. Ask every provider in your portfolio for a current report, and apply the framework in Section 7 to your whole portfolio, not just to new vendors.

Request the reports

Reviewers who would like to evaluate YASSI's reports against the framework in Section 7 can request them directly at trust.yassi.com, subject to a mutual confidentiality agreement. Both 2026 examinations were completed with no exceptions noted.

ABOUT YASSI

Yotta Automated Software Solutions, Inc. (YASSI) provides real-time vehicle, title, registration, and lien data to organizations in the automotive, financial services, insurance, and government sectors. Information about the company's security and compliance program, and requests for its attestation reports, are handled through the Trust Center at trust.yassi.com.

Notice

This document is provided for general informational and educational purposes only. It does not constitute legal, regulatory, audit, accounting, or compliance advice, and it should not be relied upon as a substitute for advice from qualified professional advisors regarding a specific situation. Descriptions of SOC reporting, the Trust Services Criteria, and attestation practice are summaries provided for orientation and are necessarily incomplete; the authoritative sources are the applicable professional standards themselves, which are subject to change. Third-party research is described as published by its author and has not been independently verified.

Statements regarding YASSI's attestation reports are descriptive summaries. The reports themselves (including their scope, the periods covered, the criteria applied, the description of the system, the complementary user entity controls, and the independent service auditor's conclusion) are the sole authoritative statement of their contents and are available to eligible parties subject to a confidentiality agreement. A result of no exceptions noted in a completed examination is a statement about the tests performed by the auditor within a defined scope and period; it is not a credential, a warranty, a guarantee of future performance, or a representation that no risk or incident exists or will occur.

Nothing in this document is intended to characterize the internal control over financial reporting of any customer, to indicate that any customer may rely on YASSI's controls in place of its own, or to substitute for the procedures a customer or its auditor determines to be necessary.

Statements about future examination activity, including any intention to continue an annual examination cycle, describe present intent only. Future examinations have not been performed, and no representation is made as to their scope, timing, or outcome. Nothing in this document creates any contractual commitment, representation, or warranty, or modifies any agreement between YASSI and any party. This document reflects the views of YASSI and not those of any auditor, standard-setting body, or third party. Third-party names and marks referenced in this document are the property of their respective owners.

Glossary of Terms

TERM	WHAT IT MEANS
SOC	System and Organization Controls, the AICPA attestation framework this paper is about.
AICPA	American Institute of Certified Public Accountants, the body that sets the attestation standards under which SOC examinations are performed.
Trust Services Criteria (TSC)	The five categories a SOC 2 examination can be measured against: security, availability, processing integrity, confidentiality, and privacy. Security is always in scope.
Type I / Type II	Type I addresses whether controls were suitably designed as of one date. Type II addresses design and whether controls operated effectively over a period, commonly three to twelve months.
No exceptions noted	The auditor's finding that none of the tests performed, on the controls within the defined scope and period, identified a deviation. It is bounded by scope, period, and sampling.
CUECs	Complementary user entity controls: controls the report identifies as the customer's responsibility to operate, such as managing user access or protecting API credentials.
Carve-out / inclusive method	How a report treats a subservice organization: carve-out excludes its controls from the examination; inclusive brings them inside it.
Bridge letter (gap letter)	Management's representation that there have been no material changes to the control environment between the end of the examination period and the present date. It is a management statement, not an audited product.

References

- American Institute of Certified Public Accountants, Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy.
- American Institute of Certified Public Accountants, attestation standards applicable to examination engagements.
- Driver's Privacy Protection Act of 1994, 18 U.S.C. § 2721 et seq.
- Federal Trade Commission, Standards for Safeguarding Customer Information (GLBA Safeguards Rule), 16 C.F.R. Part 314.
- National Association of Insurance Commissioners, Insurance Data Security Model Law (MDL-668).
- Verizon, 2026 Data Breach Investigations Report (19th ed.).