

GOVERNANCE DOCS

SOC 2 Trust Services Criteria

Gap Assessment Report

SOC 2 Trust Services Criteria

Brightline Payroll Cloud (sample)

The payroll SaaS platform, its production cloud environment and the customer support team, for the Security, Availability and Confidentiality criteria.

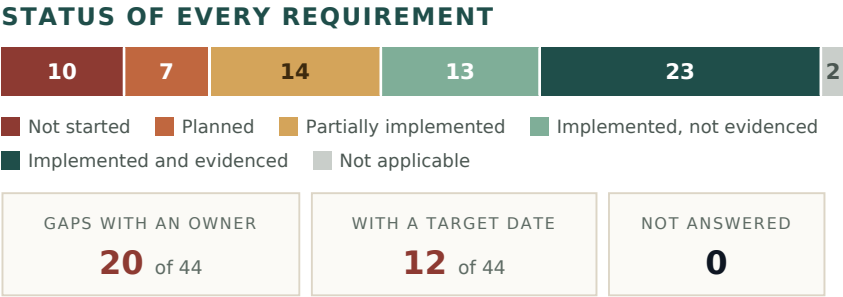
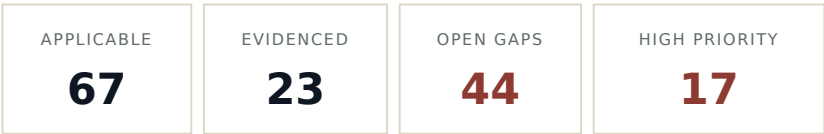
ASSESSED	25 September 2026
EDITION	2017 criteria, 2022 points of focus
IN SCOPE	69 requirements, 67 applicable
PROFILE	Technology, software and SaaS · 50 to 249 people
PREPARED BY	Governance Docs

CONTENTS

- 1 Executive summary
- 2 Readiness by area and where the next points come from
- 3 Remediation plan
- A About this report

Confidential. Prepared for Brightline Payroll Cloud (sample) from its own self-assessment; not independently verified by Governance Docs (see section A). Share on a need-to-know basis.

Where Brightline Payroll Cloud (sample) stands against SOC 2



WHAT THIS ASSESSMENT TELLS YOU

- Overall readiness is 61.9% against SOC 2 across 67 applicable controls. 23 of them are implemented and evidenced.
- Most open gaps: Privacy, with 15 at 50%. Strongest area: CC2 - Communication and information at 100%.
- 13 controls are operating but not evidenced. Collecting their records alone lifts the score to 66.8% (+4.9 points), the cheapest gain available.
- 17 gaps are high priority (not started or only planned); 6 of them are in Privacy.

DO THESE FIRST

	PRIORITY	ACTION	OWNER	START FROM
1	HIGH	Put an owner and date against the 6 high-priority gaps in Privacy	IT Manager	Information Security Policy
2	MEDIUM	Adopt and tailor the Information Security Policy, which closes 11 open gaps	To assign	Information Security Policy
3	LOW	Evidence the 13 controls that already operate (+4.9 points)	To assign	Records the controls already produce

Analysis and priorities

IN ONE SENTENCE

With a 61.9% score at Developing level, your immediate move is establishing control environment policies and assigning gap owners.

AI-assisted analysis, generated from the information the organization provided and checked automatically against the scores and findings in this report. It supports planning and is not an audit opinion; see "Basis of this report and limitation of liability".

FOR SENIOR MANAGEMENT AND THE BOARD

Our self-assessment shows an overall readiness score of 61.9%, placing us at level 2 of 4, or Developing. We have 44 open gaps, including 17 high priority gaps. Our primary exposures lie in control environment governance, logical access, and availability protections. External reviewers would identify material deficiencies in our oversight policies and recovery readiness. Management requests board endorsement of updated governance policies, formal delegation of authority, and support in directing department heads to allocate technical resources to clear unassigned gaps promptly.

WHERE YOU STAND

The organization currently stands at an overall score of 61.9%, placing it at readiness level 2 of 4, designated as Developing. Out of 69 total requirements, 67 are applicable and 44 remain open gaps. Among these open items, 17 are high priority gaps. Progress is under way with 23 requirements implemented and evidenced, 13 implemented without evidence, and 14 partially implemented. However, 10 requirements are not started and 7 are planned. Operational governance is limited, as only 20 gaps have an assigned owner and only 12 have target completion dates.

WHAT IT MEANS FOR THE ORGANIZATION

The assessment shows strong execution in operational controls such as risk assessment, change management, and risk mitigation, which all scored 100%. Conversely, significant weaknesses persist in foundational areas. Control environment scored 20% across 5 applicable controls, and availability scored 25%. Privacy presents 15 open gaps across 17 controls. This pattern indicates that day-to-day technical processes function, but formal governance, oversight structures, and documented policies are missing. Because material gaps exist, external auditors would uncover substantial deficiencies across control oversight, user access safeguards, and service continuity.

WHERE TO FOCUS FIRST

You should first target governance documentation and evidence collection. Assembling existing proof for controls already operating moves the score to 66.8%, while finishing partially implemented items advances readiness to 77.2%. Creating and ratifying an Information Security Policy is the single highest-leverage action, as it helps resolve 11 gaps. Immediate attention must also address high-priority control environment and access management items, specifically user registration and board oversight. Assigning accountable owners and explicit deadlines to all 44 open gaps will ensure sustained progress across operational teams.

1 · EXECUTIVE SUMMARY

PRIORITIES

	PRIORITY	WHY IT MATTERS	FIRST STEP	START FROM	WITHIN
1	Establish baseline control environment and governance policies CC1.1 Commitment to integrity and ethical values · CC1.2 Board independence and oversight · CC1.5 Accountability for control responsibilities	Without formal ethics, oversight, and accountability structures, auditors will find foundational governance deficiencies. These gaps prevent the organization from demonstrating management oversight and tone at the top.	Draft the Information Security Policy to establish reporting lines and governance responsibilities.	Information Security Policy SOC2 Toolkit - Premium Documentation Pack	30 DAYS
2	Strengthen user registration and logical access security CC6.2 User registration and authorisation · CC6.6 Logical access measures against external threats	Uncontrolled user provisioning and weak external threat controls leave critical systems vulnerable to unauthorized intrusion. Inadequate access administration represents a critical audit finding.	Review and update user provisioning workflows in accordance with the Access Control Policy.	Access Control Policy SOC2 Toolkit - Premium Documentation Pack	30 DAYS
3	Validate backup recovery infrastructure and disaster recovery plans A1.2 Environmental protections, backup and recovery infrastructure · A1.3 Testing recovery procedures	Untested recovery procedures and lack of documented backup safeguards threaten system uptime. Failure to verify restoration capabilities exposes the platform to prolonged outages.	Schedule an operational review of backup integrity against the Backup Policy.	Backup Policy SOC2 Toolkit - Premium Documentation Pack	60 DAYS
4	Formalize incident response procedures and event evaluation CC7.3 Evaluating security events · CC7.4 Incident response programme	Lacking formal incident evaluation procedures impairs rapid detection and containment of operational security threats. Clear documentation proves that security events are resolved systematically.	Standardize logging and event triage workflows using the Incident Response Procedure.	Incident Response Procedure SOC2 Toolkit - Premium Documentation Pack	60 DAYS
5	Implement vendor privacy and breach notification agreements P6.4 Third party privacy commitments · P6.5 Notification of third party unauthorised disclosure	Unregulated third-party data processing exposes personal records to unmonitored disclosure. Formal agreements ensure suppliers adhere to mandatory data breach reporting obligations.	Audit existing supplier contracts to incorporate standard terms from the Vendor Security Agreement.	Vendor Security Agreement SOC2 Toolkit - Premium Documentation Pack	90 DAYS

30 / 60 / 90-DAY ROADMAP**FIRST 30 DAYS**

- Assign accountable owners and completion deadlines to all 44 open assessment gaps.
- Adopt and publish the Information Security Policy to establish formal organizational governance.
- Enforce documented user registration procedures in alignment with the Access Control Policy.
- Collect and catalog evidentiary artifacts for the 13 controls currently running without documentation.

DAYS 31 TO 60

- Execute and document recovery test exercises in accordance with the Business Continuity Test Plan.
- Implement the Incident Response Procedure to evaluate and triage system security events.
- Finalize implementation across the 14 partially implemented controls to advance readiness.

DAYS 61 TO 90

- Issue the Vendor Security Agreement to all external subservice organizations and service providers.
- Formalize personal data amendment and breach notification procedures within privacy operations.
- Conduct a progress review against all applicable criteria to verify gap closure.

Maturity across the standard

Each bar shows how the requirements in one area break down by status, weakest on the left. The score is the average across applicable requirements; the chips count open gaps by priority.

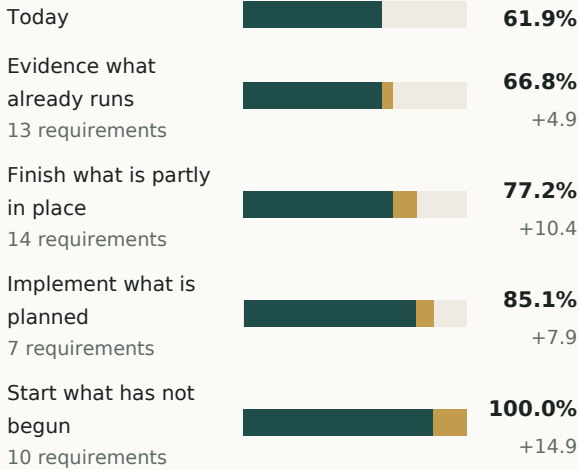
AREAS	STATUS MIX	SCORE	GAPS H · M · L		
Scope and report readiness	3 1 4	78%	0	3	1
CC1 - Control environment	3 1 1	20%	4	0	1
CC2 - Communication and information	2 1	100%	0	0	0
CC3 - Risk assessment	4	100%	0	0	0
CC4 - Monitoring activities	1 1	75%	0	1	0
CC5 - Control activities	1 2	83%	0	1	0
CC6 - Logical and physical access	1 2 3 1 1	47%	3	3	1
CC7 - System operations	1 2 2	75%	1	0	2
CC8 - Change management	1	100%	0	0	0
CC9 - Risk mitigation	2	100%	0	0	0
Availability	2 1	25%	2	0	1
Confidentiality	1 1	63%	0	1	1
Processing integrity	1 2 2	65%	1	2	0
Privacy	4 2 3 6 2	50%	6	3	6

Not started
Planned
Partially implemented
Implemented, not evidenced
Implemented and evidenced
Not applicable

Where the next points come from

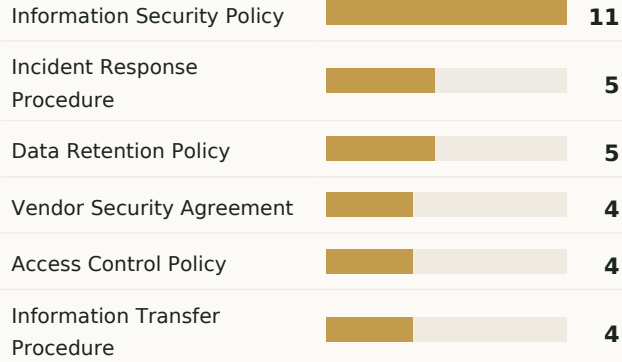
WHERE THE NEXT POINTS COME FROM

The score after each kind of work, cheapest first. Gold is what that step adds.



DOCUMENTS THAT CLOSE THE MOST GAPS

Each bar counts the open gaps that name the document as the way to close them.



All of these are in the SOC 2 Toolkit (56 documents).

Every open gap, grouped by what has to happen next

Work from the top. Requirements not yet started or only planned are the ones a certification auditor reaches first; the last group already operates and needs only its records.

HIGH Not started · 10

Start from a documented baseline: adopt and tailor the document named below, then put it into operation.

Ref	Requirement	Area	Owner · target	Closes it
CC1.1	Commitment to integrity and ethical values	CC1	Compliance Lead 4 Feb 2027	Acceptable Use Policy · Information Security Policy
CC1.2	Board independence and oversight	CC1	To assign	SOC2 - Project Highlight Report · Information Security Policy
CC1.5	Accountability for control responsibilities	CC1	HR Manager	Acceptable Use Policy · Information Security Policy
CC6.2	User registration and authorisation	CC6	To assign	Access Control Policy · Information Security Policy
A1.2	Environmental protections, backup and recovery infrastructure	Availability	HR Manager 10 Dec 2026	Backup Policy · Business Continuity Plan
A1.3	Testing recovery procedures	Availability	To assign	Business Continuity Test Plan · BCP Test Report
P5.2	Correction and amendment	Privacy	IT Manager	Information Security Policy
P6.2	Record of authorised disclosures	Privacy	To assign	Information Transfer Procedure
P6.4	Third party privacy commitments	Privacy	IT Manager 24 Dec 2026	Vendor Security Agreement · Cloud Services Security Policy
P6.5	Notification of third party unauthorised disclosure	Privacy	Operations Manager 4 Feb 2027	Vendor Security Agreement

HIGH Planned · 7

Move from plan to implementation. Assign an owner and a date, then put the control into operation.

Ref	Requirement	Area	Owner · target	Closes it
CC1.3	Structures, reporting lines and authority	CC1	IT Manager	Information Security Policy · Segregation of Duties Policy
CC6.5	Protections discontinued on disposal	CC6	Risk Manager 10 Dec 2026	Secure Data Disposal Policy · Removable Media Management Procedure
CC6.6	Logical access measures against external threats	CC6	IT Manager	Network Security Policy · Remote Working Policy +1 more
CC7.3	Evaluating security events	CC7	To assign	Security Incident Procedure · Incident Response Procedure
PI1.4	Outputs and delivery	Processing integrity	IT Manager 24 Dec 2026	Secure Development Policy · Access Control Policy

P1.1	Notice of privacy practices	Privacy	Compliance Lead 29 Oct 2026	Data Retention Policy · Information Security Policy
P6.3	Record of unauthorised disclosures	Privacy	HR Manager 21 Jan 2027	Security Incident Procedure · Incident Response Procedure

MEDIUM Partially implemented · 14

Extend the existing approach to the whole scope and apply it consistently, then evidence it.

Ref	Requirement	Area	Owner · target	Closes it
SC.1	Trust services categories in scope	Scope and report readiness	Operations Manager 12 Nov 2026	SOC2 - Project Initiation Document · SOC2 High Level Checklist
SC.7	Subservice organisations and carve-out	Scope and report readiness	Operations Manager 29 Oct 2026	Vendor Security Agreement · Cloud Services Security Policy
SC.8	Complementary user entity controls	Scope and report readiness	IT Manager 26 Nov 2026	SOC2 System Description Document
CC4.1	Ongoing and separate evaluations	CC4	Operations Manager 29 Oct 2026	SOC2 High Level Checklist · Vulnerability Assessment Procedure
CC5.3	Controls deployed through policies and procedures	CC5	Compliance Lead	Information Security Policy · Segregation of Duties Policy
CC6.1	Logical access security infrastructure	CC6	To assign	Access Control Policy · Cryptographic Policy +1 more
CC6.4	Physical access to facilities	CC6	To assign	Physical Security Policy · Secure Areas Policy
CC6.8	Preventing and detecting unauthorised software	CC6	IT Manager	Anti-Malware Policy · Configuration Management Procedure
C1.2	Disposal of confidential information	Confidentiality	Compliance Lead	Secure Data Disposal Policy · Data Retention Policy
PI1.2	System inputs	Processing integrity	To assign	Secure Coding Policy · Secure Development Policy
PI1.3	System processing	Processing integrity	To assign	Secure Development Policy · Log Monitoring Policy
P4.1	Limiting use to stated purposes	Privacy	To assign	Data Masking Policy · Information Security Classification Policy
P4.2	Retention of personal information	Privacy	Risk Manager	Data Retention Policy
P6.7	Accounting of personal information held	Privacy	To assign	Information Transfer Procedure

LOW Implemented, not evidenced · 13

Collect and file evidence an auditor can sample. The control is operating; what is missing is the record of it.

Ref	Requirement	Area	Owner · target	Closes it
SC.4	System description	Scope and report readiness	To assign	SOC2 System Description Document
CC1.4	Commitment to competence	CC1	To assign	Information Security Policy

CC6.7	Restricting transmission, movement and removal of information	CC6	To assign	Information Transfer Procedure · DLP Policy +2 more
CC7.4	Incident response programme	CC7	To assign	Incident Response Procedure · Security Incident Procedure
CC7.5	Incident recovery	CC7	To assign	Incident Response Procedure · Business Continuity Plan
A1.1	Capacity and usage monitoring	Availability	To assign	Log Monitoring Policy · Business Continuity Plan
C1.1	Identifying and maintaining confidential information	Confidentiality	To assign	Information Security Classification Policy · Information Security Labelling Procedure +1 more
P3.2	Explicit consent for sensitive personal information	Privacy	To assign	Data Retention Policy · Information Security Classification Policy
P4.3	Secure disposal of personal information	Privacy	To assign	Secure Data Disposal Policy · Backup Policy
P5.1	Access to stored personal information	Privacy	To assign	Information Security Policy
P6.1	Disclosure to third parties	Privacy	To assign	Vendor Security Agreement · Information Transfer Procedure
P6.6	Breach notification to affected individuals	Privacy	To assign	Incident Response Procedure · Security Incident Procedure
P8.1	Monitoring privacy compliance and complaints	Privacy	To assign	SOC2 High Level Checklist · Information Security Policy

How it was scored

STATUS WEIGHTS

Status	Weight	Meaning
■ Not started	0.00	No policy, process or activity exists for this requirement.
■ Planned	0.25	Approach agreed and scheduled, but nothing is in place yet.
■ Partially implemented	0.50	In place for part of the scope, or inconsistently applied.
■ Implemented, not evidenced	0.75	Operating as intended, but you could not prove it to an auditor today.
■ Implemented and evidenced	1.00	Operating as intended, with records an auditor can sample.
■ Not applicable	—	A justified exclusion. Removed from the score - record why in your notes.

READINESS LEVELS

1 • Initial (0%+)

Most requirements are not yet in place. Build the foundations before thinking about an audit.

2 • Developing (40%+)

The programme is under way, with material gaps an auditor would find.

3 • Established (65%+)

Most controls operate. Remaining work is closing specific gaps and evidencing what runs.

4 • Audit-ready (85%+)

Controls operate and are evidenced. Ready for an internal audit and a certification body.

WHAT THIS REPORT IS

BASIS OF THIS REPORT AND LIMITATION OF LIABILITY

This report is the output of a self-assessment. The scores, readiness levels, gaps, analysis and recommendations in this report are derived solely from the information entered by the organization, and have not been independently reviewed, verified, tested or audited by Governance Docs. Governance Docs did not conduct an independent assessment of the organization, its controls or its operations.

The accuracy and completeness of the results depend entirely on the accuracy and completeness of the information provided. Governance Docs gives no assurance, certification or audit opinion, and accepts no liability for any inaccuracy, omission or deviation arising from that information, or for any decision taken, or not taken, in reliance on this report.

The report, including any AI-assisted analysis, is provided for guidance and planning only. It does not constitute legal, regulatory or other professional advice, and it does not replace an independent assessment or a certification audit.

A control that is running but cannot be evidenced scores 0.75, not 1.00. Auditors sample records, not intentions. Closing that distance is usually the fastest route to a higher score.

All assessment questions and guidance are original wording by Governance Docs. Clause and control references are used as identifiers; no text from the standard is reproduced. You need your own licensed copy of the standard to implement it.

YOUR WORKBOOK

The Excel workbook that comes with this report follows the same sections and colours. Dashboard: sections 1 and 2, recalculated live. Assessment: every requirement; change a status and every score, chart and level updates. Remediation Plan: section 3, with owners, dates and progress since this report. How it was scored: this page.

Governance Docs · governancedocs.com