Meridian Payroll Services Limited

Independent Service Auditor’s Report on Controls at a Service Organisation Relevant to User Entities’ Internal Control over Financial Reporting (SOC 1® Type II)

For the period 1 October 2025 to 30 September 2026

FICTIONAL SAMPLE. Meridian Payroll Services Limited, Harlow & Finch LLP and every individual, date and finding in this document are invented for product demonstration. This is not an audit opinion and describes no real organisation.

Section 1 — Independent Service Auditor’s Opinion

We have examined Meridian Payroll Services Limited’s description of its Payroll Processing System throughout the period 1 October 2025 to 30 September 2026, and the suitability of the design and operating effectiveness of controls to achieve the related control objectives stated in the description.

In our opinion, in all material respects, **except for the matters described in the Basis for Qualified Opinion paragraph below**, the description fairly presents the system that was designed and implemented throughout the period, and the controls were suitably designed and operated effectively throughout the period.

Basis for Qualified Opinion

Control 4.2 (removal of logical access within one business day of termination) did not operate effectively throughout the period. For 6 of 25 terminations selected, access was removed between 4 and 34 calendar days after the termination date. Accordingly, control objective 4 was not achieved throughout the period.

Section 2 — Management’s Assertion

Management of Meridian Payroll Services Limited is responsible for preparing the description and its assertion, including the completeness, accuracy and method of presentation of both.

Section 3 — Description of the System

Meridian processes payroll for approximately 240 user entities across the United Kingdom and Ireland. The system comprises the Meridian Payroll Engine (a hosted application), a payments gateway integration with two clearing banks, and a customer portal used by user entity payroll administrators. The application is hosted in two availability zones of a public cloud provider; the provider is a subservice organisation and the **carve-out method** has been used.

Subservice organisation controls are therefore **not** included in the scope of this report. User entities are responsible for evaluating the cloud provider’s own SOC 2 report.

Section 4 — Control Objectives, Controls, Tests and Results

Tests of operating effectiveness were performed on populations covering the full period unless otherwise stated. Sampling was attribute-based, with sample sizes determined by control frequency.

Ref	Control	Test performed	Result
1.1	Logical access to the Payroll Engine requires unique named credentials and multi-factor authentication. Shared accounts are prohibited.	Inspected the user listing for all 412 accounts as at 30 Sep 2026; inspected MFA enforcement policy; tested 25 accounts for MFA enrolment.	No exceptions.
1.2	Privileged (administrator) access is restricted to members of the Platform Operations team and is reviewed quarterly by the Head of Operations.	Inspected all four quarterly reviews; re-performed the Q2 review against the underlying role assignment extract.	No exceptions.
2.1	Changes to the Payroll Engine are approved by the Change Advisory Board before deployment to production.	Selected 40 of 613 production changes; inspected CAB approval records.	One exception. Change CHG-2026-0411 (an emergency tax-table correction on 6 April 2026) was deployed before approval and approved retrospectively 2 days later. Management confirmed the emergency change procedure was followed and the change was reviewed by a second engineer at deployment.
2.2	Developers cannot deploy to production. Deployment is performed by the release pipeline using a service principal.	Inspected pipeline configuration; inspected production deployment logs for the full period for any deployment not originating from the pipeline.	No exceptions. Population tested was 100% (613 deployments).
3.1	Payroll calculation results are reconciled to input files by an operator independent of data entry, and exceptions are cleared before payment.	Selected 25 of 2,880 payroll runs; inspected reconciliation and exception clearance.	No exceptions.
3.2	Bank payment files are transmitted over an encrypted channel and are hash-verified by the receiving bank before execution.	Inspected transmission configuration; inspected hash verification confirmations for 25 selected payment files.	No exceptions.
4.1	New joiner access is provisioned only on receipt of an approved access request from an authorised approver at the user entity.	Selected 25 of 96 joiners; inspected approved access requests.	No exceptions.
4.2	Logical access is removed within one business day of notification of termination.	Selected 25 of 88 leavers; compared access removal timestamps to termination dates.	**Exception.** 6 of 25 removals occurred between 4 and 34 calendar days after termination. Four of the six accounts showed no authentication activity after the termination date; two showed activity on the day following termination, which management attributes to the individuals completing handover.
5.1	Backups of the payroll database are taken daily and restoration is tested annually.	Inspected the backup schedule and the 12 March 2026 restoration test.	No exceptions.

Section 5 — Complementary User Entity Controls (CUECs)

The controls at Meridian were designed on the assumption that certain controls are implemented by user entities. This report does not extend to those controls, and the control objectives stated in Section 4 can be achieved only if they are in place and operating.

CUEC-1. User entities are responsible for notifying Meridian of employee terminations on the day the termination takes effect.

CUEC-2. User entities are responsible for maintaining a current list of individuals authorised to approve access requests and payroll changes, and for notifying Meridian of changes to that list within five business days.

CUEC-3. User entities are responsible for reviewing the payroll register produced by Meridian before authorising payment, and for reporting discrepancies within two business days.

CUEC-4. User entities are responsible for the security of credentials issued to their payroll administrators, including prohibiting credential sharing.

CUEC-5. User entities are responsible for evaluating the SOC 2 report of the cloud hosting provider, whose controls are carved out of this report.

CUEC-6. User entities are responsible for reconciling amounts debited by their bank to the payment file totals reported by Meridian.

Section 6 — Other Information Provided by Management (Unaudited)

Management has begun an automated joiner-mover-leaver integration with user entity HR systems, targeted for completion in Q2 2027, intended to address the matter described in control 4.2. This information has not been subjected to the procedures applied in the examination.

Harlow & Finch LLP · Chartered Accountants · London · 14 November 2026