Internal Audit Report IA-2026-07

IT General Controls Review — Merchandising and Finance Platforms

Beaumont Retail Group plc | Fieldwork: April 13 – May 29, 2026 | Draft issued: June 8, 2026 | Final issued: June 22, 2026
Chief Audit Executive: R. Ntuli | Engagement lead: F. Delacroix | Executive sponsor: Group CIO

Overall opinion

PARTIALLY EFFECTIVE

The control environment over the in-scope platforms (Oracle Retail merchandising, Workday Financials, and the nightly integration layer) is partially effective. Controls over change management are well designed and operated consistently. However, one high-rated finding on privileged access to the integration middleware and two medium-rated findings on joiner-mover-leaver processing and backup restoration testing require remediation before reliance can be placed on the environment for the FY2026 external audit.

We raised four findings: one high, two medium, and one low. Management has accepted all findings and agreed remediation dates; none were disputed. Two advisory observations on logging retention and password-vault onboarding were communicated separately to the CISO and are not reproduced here. Follow-up testing is scheduled for the week of October 12, 2026.

Ratings legend

High	Fundamental control weakness with realistic potential for material financial, regulatory, or operational impact. Remediation expected within 90 days; reported to the Audit Committee individually.
Medium	Control weakness that undermines an individual control objective but is partially compensated elsewhere. Remediation expected within 180 days.
Low	Isolated exception or improvement opportunity with limited impact. Tracked by management; verified at the next cyclical review.

Findings register

Ref	Finding	Rating	Owner	Agreed date
F-01	Shared privileged account on integration middleware with no session attribution	High	Head of Integration Services	30 Sep 2026
F-02	Leaver access not revoked within SLA for 9 of 45 sampled leavers	Medium	IT Service Delivery Manager	31 Oct 2026
F-03	Backup restoration tests not performed for two of six tier-1 databases in the last 12 months	Medium	Head of Infrastructure	30 Nov 2026
F-04	Emergency change records missing retrospective approval in 3 of 28 sampled changes	Low	Change Manager	31 Aug 2026

Finding F-01 — Shared privileged account on integration middleware (High)

Observation

The nightly integration layer that moves sales, inventory, and journal data between Oracle Retail and Workday runs under a single shared administrator account (SVC_INTADM). The password is known to at least seven engineers, is stored in a team OneNote page, and was last rotated in November 2024. Session logs record only the account name, so individual actions cannot be attributed. During fieldwork we observed the account used interactively to modify a production mapping table without a change ticket.

Risk

Unattributable privileged activity defeats segregation-of-duties monitoring over the financial data pipeline. An erroneous or malicious mapping change could misstate revenue or inventory in Workday with no forensic trail, and the shared credential materially widens the impact of a single compromised workstation.

Recommendation

Replace interactive use of SVC_INTADM with named accounts brokered through the privileged access management (PAM) platform; convert the service account to non-interactive with a vault-managed, auto-rotated credential; and enable command-level session recording for all middleware administration.

Management response

Agreed. PAM onboarding for the integration estate was already scoped under project Sentinel; we will accelerate it. Interactive logons for SVC_INTADM will be disabled by August 14, named-account brokering live by September 18, and session recording enabled by September 30. Owner: Head of Integration Services. Due: September 30, 2026.

Finding F-02 — Leaver access revocation outside SLA (Medium)

Observation

Group policy requires logical access to be revoked within one business day of an employee's leaving date. For 9 of 45 leavers sampled between January and April 2026, at least one in-scope system account remained active beyond the SLA; the longest exception was 26 calendar days (a store-operations analyst with read access to Oracle Retail). None of the nine accounts showed post-termination logon activity.

Risk

Dormant accounts of former employees are a common initial-access vector and may breach the group's ISO 27001 certification commitments (control A.5.18). Impact is partially mitigated by single sign-on deactivation, which blocked interactive access for 7 of the 9 exceptions.

Management response

Agreed. The HR-to-IAM feed will be extended to cover the two directly-provisioned legacy systems that caused the exceptions, with automated revocation and a daily reconciliation report to the service desk. Owner: IT Service Delivery Manager. Due: October 31, 2026.

Finding F-03 — Backup restoration testing gaps (Medium)

Restoration tests were not performed within the required 12-month cycle for two of six tier-1 databases (the Oracle Retail price-management schema and the integration staging database). Backup jobs themselves completed successfully with a 99.4% success rate, but untested backups provide limited recovery assurance. Management agreed to complete restoration tests for both databases by August 28 and to add restoration-test evidence to the monthly infrastructure KPI pack from September. Owner: Head of Infrastructure. Due: November 30, 2026 (full cycle re-baseline).

Finding F-04 — Emergency change retrospective approvals (Low)

Three of 28 sampled emergency changes lacked the retrospective CAB approval required within five business days, though all three had valid incident references and peer-reviewed implementation notes. The change-management tool will be configured to auto-escalate unapproved emergency records after three days. Owner: Change Manager. Due: August 31, 2026.

This report is prepared for the Audit Committee and management of Beaumont Retail Group plc under the Internal Audit Charter approved March 2025. Our work was performed in conformance with the IIA Global Internal Audit Standards and does not constitute an audit under ISA (UK). Sample sizes and methodology are described in Appendix A of the full report.