HorseInsure Pty Ltd
Level 12, 45 Pitt Street, Sydney NSW 2000

ABN 41 209 837 156

INTERNAL AUDIT REPORT

Access Control, Incident Management & Change Management

Report Reference: AUD-001
Audit Period: 14 - 18 October 2025
Report Date: 25 October 2025
Audit Team: Angela Torres (Compliance Manager), Jennifer Walsh (Meridian Assurance Pty Ltd)

EXECUTIVE SUMMARY

This internal audit was conducted during 14-18 October 2025 to assess the effectiveness of HorseInsure's information security controls across access control, incident management and change management processes. The audit was conducted in accordance with the organisation's audit plan and examined policies, procedures, system configurations and supporting documentation. Three major findings were identified relating to incomplete quarterly access reviews, undocumented emergency change procedures and inadequately assessed third-party suppliers. Three minor findings were also noted in training records and documentation. Two observations for improvement have been raised. Overall, the control environment is largely adequate, but remediation of major findings is required.

FINDINGS SUMMARY

Severity	Count	Status
Major	3	Remediation Required
Minor	3	Remediation Recommended
Observation	2	Continuous Improvement

MAJOR FINDING 1: Incomplete Quarterly Access Reviews

Finding ID: AUD-001-MJ-001

Area: Access Control

Description:

Quarterly access reviews for active user accounts across critical systems (EquiClaim, EquiPolicy, EquiQuote, Azure AD) have not been completed for Q3 2025 (July-September). Our review found that the last completed access review was for Q2 2025 (completed 30 June 2025). The Q3 review was due 30 September 2025 but has not been conducted. This represents a control breakdown in user access governance.

Evidence:

- Access Review Log - Q3 2025 marked as 'Not Commenced'
- Email trail showing Q3 review was scheduled for 20 September but cancelled
- System audit logs showing 12 user deactivations not formally reviewed in Q3
- Interviews with Sarah Williams (Head of IT) confirming resource constraints

Risk Rating: MAJOR

Risk Impact: Unauthorised or obsolete user accounts may retain access to sensitive systems containing customer horse insurance data and claims information.

Recommendation:

- Complete Q3 2025 access review immediately with documented sign-off
- Establish dedicated resource or allocate existing resource to prevent future delays
- Implement automated reminders 2 weeks prior to review due dates
- Consider quarterly access review checklist to ensure completeness

Management Response:

Agreed. We acknowledge the delay in Q3 access review. Sarah Williams will prioritise completion of Q3 review by 30 November 2025. We will review resource allocation for IT governance activities. However, we believe the risk is mitigated by the fact that deactivated accounts are disabled in Azure AD automatically after 90 days of inactivity.

Target Completion Date: 30 November 2025

Owner: Sarah Williams, Head of IT

MAJOR FINDING 2: Emergency Change Process Not Documented

Finding ID: AUD-001-MJ-002

Area: Change Management

Description:

The Change Management Policy (v2.1, approved June 2024) defines a standard change process requiring 5 business days advance notice and documented approval. However, no formal emergency change procedure exists for critical security patches or system outages requiring immediate remediation. Review of 2025 change logs identified 7 changes categorised as 'emergency' but implemented without documented approvals or impact assessments. Examples include: (1) security patches to claims system on 12 March, (2) database failover configuration on 5 August, (3) Azure AD policy update on 18 September.

Evidence:

- Change Management Policy v2.1 (no emergency procedure section)
- Change request tickets #2025-0847, #2025-1263, #2025-1524, #2025-1687 marked 'Emergency' but no approval evidence
- Interview with Sarah Williams and Marcus Lee (IT Security Analyst) confirming ad-hoc emergency processes
- Network change logs showing 7 unscheduled changes in 2025

Risk Rating: MAJOR

Risk Impact: Undocumented emergency changes increase risk of unintended system disruptions, loss of audit trail, and inability to demonstrate change control compliance to regulators.

Recommendation:

- Develop and document formal Emergency Change Procedure defining scope, approval authority, notification requirements and post-implementation review
- Establish emergency change committee with representatives from IT, Security and Operations
- Implement weekly review of all emergency changes for post-implementation assessment
- Train IT staff on new emergency change process

Management Response:

We agree this requires formal documentation. David Chen will work with Sarah Williams to develop an Emergency Change Procedure by 15 January 2026. We note that emergency changes to date have been necessary to maintain system availability and data security.

Target Completion Date: 15 January 2026

Owner: David Chen, CIO/CISO

MAJOR FINDING 3: Third-Party Suppliers Without Security Assessments

Finding ID: AUD-001-MJ-003

Area: Supplier Management / Access Control

Description:

Review of active supplier agreements identified three suppliers providing IT services or accessing company systems without documented security assessments: (1) ABC Printing Pty Ltd - provides document management services for policy documents with access to file server, (2) QuickFix IT Support Pty Ltd - remote access to claims system for technical support, (3) Regional IT Services - manages network infrastructure at Dubbo and Scone offices. No evidence of security questionnaires, risk assessments or contractual security obligations were found for any of these suppliers.

Evidence:

- Supplier register (Salesforce) listing 47 active suppliers, 3 with no security assessment recorded
- Supplier agreements for ABC Printing, QuickFix IT Support and Regional IT Services lacking security clauses
- Interview with Sarah Williams confirming assessments not performed
- System access logs showing active accounts for all three suppliers with documented access rights

Risk Rating: MAJOR

Risk Impact: Unvetted suppliers with system access create risk of data breach, non-compliance with insurance regulations (ASIC, APRA), and liability exposure for customer data compromise.

Recommendation:

- Immediately conduct security assessments for three identified suppliers
- Establish baseline supplier security questionnaire (align with ISO 27001 Annex A.15)
- Update supplier agreements to include security obligations
- Establish quarterly supplier risk assessment review schedule
- Consider third-party risk scoring model (e.g., based on access level and data sensitivity)

Management Response:

Acknowledged. Angela Torres will conduct security assessments of the three identified suppliers. We expect to have questionnaires completed by suppliers by end of November 2025, though we note that ABC Printing has been operating with document access for 3 years without incident.

Target Completion Date: 30 November 2025

Owner: Angela Torres, Compliance Manager

MINOR FINDING 1: Incomplete Incident Response Training Records

Finding ID: AUD-001-MN-001

Description:

Training records for incident response team members were not consistently documented. Some staff indicated they received training but no formal record exists.

Risk Rating: MINOR

Recommendation: Implement centralised training tracking system for all security-related training.

Management Response:

James O'Brien will audit training records and update documentation.

Target Completion Date: 31 December 2025

MINOR FINDING 2: System Security Standards Documentation Gaps

Finding ID: AUD-001-MN-002

Description:

Documentation for system security standards (SAP Finance, Salesforce) lacks current review dates and sign-off evidence. Documentation appears outdated.

Risk Rating: MINOR

Recommendation: Schedule quarterly review and update of system security standards documentation with formal sign-off.

Management Response:

Sarah Williams to establish quarterly review schedule for system security standards. Initial review to be completed by 15 January 2026.

Target Completion Date: 15 January 2026

MINOR FINDING 3: Backup Restoration Testing Records

Finding ID: AUD-001-MN-003

Description:

Documentation of backup restoration testing for critical systems shows gaps in 2025. Testing was performed but not formally recorded.

Risk Rating: MINOR

Recommendation: Implement standardised backup testing checklist and maintain centralised log of all restoration tests.

Management Response:

Liam Foster will establish backup testing log and ensure all tests are documented going forward.

Target Completion Date: 31 December 2025

OBSERVATIONS AND OPPORTUNITIES FOR IMPROVEMENT

Observation 1: Access Request Approval Timeliness

Review of access request processing times shows 85% are completed within target 5 business days, but 15% exceed targets due to approver unavailability. Consider implementing automated escalation or backup approver designation.

Observation 2: Incident Reporting Awareness

Staff interviews suggest moderate awareness of security incident reporting procedures, but awareness could be enhanced through more frequent reminders and refresher training. Current training is delivered at induction only.

CONCLUSION

This audit identified areas requiring remediation, particularly around access review timeliness, emergency change procedures and supplier security assessments. Management has committed to addressing major findings by specified target dates. The audit team will conduct follow-up assessment in Q1 2026 to verify remediation effectiveness.

Report Prepared By:

Angela Torres
Compliance Manager
HorseInsure Pty Ltd
Date: 25 October 2025

Supporting Auditor:

Jennifer Walsh
Meridian Assurance Pty Ltd
Date: 25 October 2025