Koala Freight Pty Ltd: Information Security Risk Assessment

Version	1.0
Date	5 November 2026
Assessor	Darvin Patel, Information Security Lead
Scope	Customer portal, dispatch and billing platform, AWS and Azure environments, Microsoft 365, company endpoints and key vendors
Method	Risk score = Likelihood × Impact, rated before treatment

Portfolio exercise: Koala Freight Pty Ltd is a fictional company. Where a risk cites a dashboard finding, it comes from the synthetic Koala Freight Powerpipe compliance run on 1 November 2026, not from a real environment.

Rating key

Likelihood (1–5)	Impact (1–5)	Risk score = L × I
1 Rare · 2 Unlikely · 3 Possible · 4 Likely · 5 Almost certain	1 Minor · 2 Limited · 3 Moderate · 4 Major · 5 Severe	1–6 Low · 7–14 Medium · 15–25 High

Risk register

ID	Area	Risk description	L	I	Score	Rating	Treatment	Owner
R-01	Access offboarding	Departing staff, contractors and carrier users keep access to Microsoft 365, the customer portal admin console or AWS because leaver notifications from managers and HR are late or missed, and there is no single list of accounts per person.	3	4	12	Medium	**Mitigate:** HR system triggers an offboarding ticket on the last day; IT disables single sign-on within one business day; quarterly access review signed off by managers; carrier portal accounts expire after 90 days without use.	IT and Security Lead
R-02	Ransomware and backup restore	Ransomware encrypts laptops and file shares, or an attacker with stolen admin credentials deletes cloud data. Backups exist but have never been fully restored, so recovery time is unknown and dispatch could stop for days.	3	5	15	High	**Mitigate:** immutable, separately administered backups (AWS Backup vault lock); documented restore runbook; full restore test of the portal database every six months with the time recorded; ransomware tabletop exercise annually. **Transfer:** review cyber insurance cover for business interruption.	Head of Engineering

ID	Area	Risk description	L	I	Score	Rating	Treatment	Owner
R-03	MFA gaps	Some accounts can sign in without MFA: legacy authentication to Microsoft 365, a service account used for carrier integrations and internal admin functions on the customer portal. A phished password gives direct access.	4	4	16	High	**Mitigate:** Entra ID Conditional Access requiring MFA for all users and blocking legacy authentication; replace the shared service account with scoped API keys stored in a secrets manager; MFA on the portal admin console; monthly report of accounts without MFA.	IT and Security Lead
R-04	Open cloud storage and network rules	An S3 bucket or Azure storage container holding proof-of-delivery documents is made public by mistake, or a network security group allows RDP or SSH from the internet, exposing customer data or servers.	3	4	12	Medium	**Mitigate:** S3 Block Public Access at account level and Azure policy denying public blob access; NSG rules reviewed in change control; weekly CIS Benchmark checks with alarms sent to the engineering channel; remote admin through a bastion with single sign-on.	Cloud Platform Lead
R-05	Vendor SaaS	A breach or long outage at a critical SaaS vendor (route optimisation, payroll or the support ticketing tool) exposes Koala Freight data or stops operations, and the contract gives no breach notification or exit terms.	3	3	9	Medium	**Mitigate:** vendor register ranked by data and criticality; security questionnaire or ISO/IEC 27001 / SOC 2 evidence before onboarding critical vendors; contract clauses for 72-hour breach notification and data return. **Transfer:** confirm insurance and contractual liability for vendor-caused incidents.	Operations Manager
R-06	Patch lag (Essential Eight)	Operating system and application patches are applied inconsistently, and some devices run unsupported versions. In the synthetic dashboard run, *Patch operating systems* had the most alarms of any Essential Eight strategy (10). Unpatched devices are a common ransomware entry point and would fail Essential Eight Maturity Level One.	4	4	16	High	**Mitigate:** automated patching through device management with two-week deadline (48 hours for critical or exploited vulnerabilities); replace unsupported operating systems; weekly patch compliance report tracked against Essential Eight ML1.	IT and Security Lead
R-07	Privileged access	Engineers use everyday accounts with standing administrator rights in AWS, Azure and on laptops. If one of these accounts is compromised, an attacker gains full control of production and can disable logging.	2	5	10	Medium	**Mitigate:** separate admin accounts not used for email or browsing; just-in-time elevation through AWS IAM Identity Center and Entra Privileged Identity Management; remove local admin from standard users; quarterly privileged access review; root and global admin kept for break-glass with alerts on use.	Head of Engineering

ID	Area	Risk description	L	I	Score	Rating	Treatment	Owner
R-08	Third-party data sharing	Consignee names, addresses and phone numbers are emailed to subcontracted carriers in spreadsheets, so personal information sits in mailboxes Koala Freight does not control and could trigger a notifiable data breach.	2	3	6	Low	**Mitigate:** move carrier job details into the driver app so spreadsheets are no longer emailed; data sharing clause in carrier agreements covering use, retention and breach notification; share only the fields carriers need.	Operations Manager

Treatment options: **Mitigate** (reduce it), **Accept** (live with it), **Transfer** (insure or outsource it) or **Avoid** (stop the activity).

Summary

Rating	Count	Risks
High (15–25)	3	R-02 Ransomware and backup restore, R-03 MFA gaps, R-06 Patch lag
Medium (7–14)	4	R-01 Access offboarding, R-04 Open cloud storage and network rules, R-05 Vendor SaaS, R-07 Privileged access
Low (1–6)	1	R-08 Third-party data sharing

The three High risks share a theme: they are the controls attackers most often exploit in ransomware incidents, and they line up with Essential Eight strategies (multi-factor authentication, patch operating systems and applications, regular backups). They are the first priority for the next quarter. All risks are reviewed quarterly by the Information Security Lead and reported to the Board, and are re-scored after treatment to record residual risk.