Koala Freight Pty Ltd: NIST CSF 2.0 Gap Summary

Version 1.0, 5 November 2026. Prepared by Darvin Patel. Portfolio exercise: Koala Freight Pty Ltd is fictional. Koala Freight holds no ISO/IEC 27001 certification and has not had a formal Essential Eight assessment; the overlaps below show where work would count towards both.

Function	Current state	Biggest gap	Next control	Overlap (Essential Eight / ISO 27001:2022)
Govern (GV)	An information security policy (KF-POL-001) and a first risk register now exist, with a named policy owner. Risk appetite and security roles are not yet formally approved by the Board.	No agreed risk appetite or regular Board reporting, so security spend is reactive.	Board-approved risk appetite statement and a quarterly security and risk report to the Board.	ISO clauses 5 (Leadership) and 6.1 (risk assessment and treatment); Annex A 5.1 (policies), 5.19–5.22 (supplier security). Essential Eight has no governance strategy, so this sits outside it.
Identify (ID)	Cloud accounts are known, but there is no single asset inventory covering laptops, SaaS tools and data stores. Risks are assessed for the first time in this pack.	Incomplete inventory of assets and of where personal information is held.	Maintained asset and data inventory (cloud, endpoints, SaaS) with an owner and classification for each item.	ISO Annex A 5.9 (inventory of assets), 5.12 (classification). Supports every Essential Eight strategy, because you cannot patch or harden what you have not listed.
Protect (PR)	Single sign-on and MFA cover most users; laptops are managed and encrypted. The synthetic dashboard run still shows MFA, patching and admin privilege alarms.	Patch lag and standing administrator rights (risks R-06 and R-07).	Automated patching to Essential Eight ML1 timeframes, plus removal of local admin and just-in-time cloud admin.	Essential Eight: patch applications, patch operating systems, restrict administrative privileges, MFA, application control, macros, user application hardening. ISO Annex A 5.15–5.18 (access), 8.2 (privileged access), 8.5 (secure authentication), 8.8 (technical vulnerabilities).
Detect (DE)	AWS CloudTrail and Microsoft 365 audit logs are on, and a weekly CIS / Essential Eight compliance check runs on the dashboard. Nobody is assigned to review security alerts.	Logs are collected but not monitored, so a compromise could go unnoticed for weeks.	Alert rules for high-risk events (root or global admin sign-in, logging disabled, impossible travel) routed to an on-call owner, with a weekly review.	ISO Annex A 8.15 (logging), 8.16 (monitoring activities). Essential Eight ML1 does not require centralised logging.
Respond (RS)	Staff know to report incidents to the service desk. There is no written incident response plan or breach assessment process.	No tested plan for deciding whether an incident is a notifiable data breach or for telling customers within contract timeframes.	Incident Response Plan with roles, contact list, NDB assessment steps and customer notification templates, tested in an annual tabletop exercise.	ISO Annex A 5.24–5.28 (incident management and evidence). Essential Eight does not cover incident response.
Recover (RC)	Daily backups run for the portal database and file storage. A full restore has never been tested.	Unknown recovery time after ransomware (risk R-02).	Immutable backups and a six-monthly full restore test with measured recovery time against an agreed target.	Essential Eight: regular backups (including restore testing and protecting backups from modification). ISO Annex A 8.13 (information backup), 5.30 (ICT readiness for business continuity).

Priorities for the next 90 days: close the three High risks (MFA, patching, backup restore), which sit in Protect and Recover and map directly to Essential Eight ML1; then approve a risk appetite (Govern) and write the incident response plan (Respond). This is a self-assessment against the CSF Functions only; Tiers and target Profiles would be set once the Board agrees risk appetite.