Executive Summary

Essential Eight Maturity-Level 1 Review (Trimester 1 2025)

Introduction

Redback Operations undertook its first formal Essential Eight (E8) assessment across five active student teams: Data Warehousing (DW), Blue, Infrastructure, Ethics, and Project 4 (Orion), during May 2025. The review showed a large gap between the smaller well-governed practices embedded in the DW virtual machine and the ad-hoc, device-of-choice approach that dominates the wider organisation. There are two main drivers of this disparity:

Rapid student turnover
Each cohort participates for only one or two trimesters, leaving little room to design, implement and embed long-term cyber-hygiene controls. As a result, successive years "roll with the punches" rather than progressing a roadmap of uplift.

Fragmented development environments.
Most work occurs on personal devices or occasionally on Deakin hardware. This single factor blocks at least five of the eight ML1 controls (application control, application patching, OS patching, user-application hardening, and backup validation).

What is working

The limited successes observed derive from either central university services or one-off efforts by motivated teams:

Restrict Administrative Privileges:
The DW VM inherits Deakin Active Directory, granular JIRA-based approvals and container isolation, meeting every ML1-Restrict Admin test except those undermined by shared home directories and a manual quarterly review process.

Identity and MFA:
Blue Team systems rely on Entra ID for least-privilege access and duo-layer MFA, achieving Level 2 for those two controls despite operating on unmanaged hosts.

University foundations:
Deakin's federated authentication, VPN gating and on-premise infrastructure provide a ready-made security backbone that Redback can piggy-back.

Why those gains are not enough

Outside the DW team, the organisation lacks a patch cycle, tested backups, application allow-listing, macro policies and hardened baselines. Infrastructure leads confirm VM patching is "ad-hoc" with some legacy images still online, MFA is only "partly" enforced on VMs, and no encrypted or verified backups exist. Meanwhile, Ethics and Project 4 teams work exclusively on personal hardware with no formal control framework. In short, Redback cannot claim organisation-wide ML1 while the

majority of student code is written in environments the organisation neither owns nor governs.

Principal risk

The uncontrolled nature of personal devices constitutes the programme's highest cyber risk. It leaves administrators blind to unpatched software, rogue extensions, and data exfiltration paths, and it prevents any realistic attempt to uplift the organisation to achieve E8 Maturity at any level.

Strategic recommendation

To break this cycle the programme should standardise on an Infrastructure-managed "Redback Dev VM" image and mandate its use from Week 1 of every trimester. A centrally hosted, snapshot-protected VM can embed:

- Entra ID sign-in with mandatory MFA;
- An allow-listed software catalogue and Wazuh enforcement policies;
- Weekly automated OS and third-party patching;
- Scheduled OneDrive backups validated by the Infrastructure team.

This single initiative directly lifts five stalled E8 controls and gives the Blue and GRC teams a stable platform for future hardening.

Uplift Roadmap

Build and internal testing (T2 2025)
Infrastructure to create the standard image and verify E8 baselines.

Pilot with one or two project teams (T3 2025)
Lower enrolments make this an ideal trial-run period. Feedback loops into image refinement.

Full roll-out (T1 2026)
Every student receives Dev VM access at the beginning of Trimester and participates in an induction designed to familiarise them with the environment; de-provisioning scripts clean up at trimester's end.

Ownership rests primarily with Infrastructure (build, patch, backup), supported by Blue Team (monitoring) and GRC (policy, induction content). Progress should be reviewed at the next scheduled E8 reassessment in 2026.

Final Thoughts

Redback's security story begins the moment a new student signs in. Give them a safe, consistent workspace from day one and most of the rest of the controls fall into place. A shared Dev VM, hooked into the university's identity and backup services, is the fastest and clearest path to reaching – and keeping – Essential Eight Maturity Level 1.