GRC Team Handover Plan – Trimester Handover to Incoming Team

Author: Rohan Batra
Team: Governance, Risk, and Compliance (GRC)
Organisation: Redback Operations

Objective

This handover plan is intended to provide the incoming Governance, Risk, and Compliance (GRC) team with clear direction on the work completed during the current trimester, along with priorities and recommendations for the next phase. This document summarises key deliverables, lessons learned, and actionable next steps to ensure continuity and progression of Redback's cybersecurity and compliance posture.

---

1. Key Projects Completed This Trimester

Essential Eight (E8) Workstream:

- Conducted multiple Essential Eight Maturity Level 1 (ML1) assessments across Redback's internal teams (Blue Team, Infrastructure Team, Data Warehouse, Project Orion and Ethics Team).
- Developed and presented a comprehensive Essential Eight proposal and strategic recommendations to Redback's Senior Leadership.
- Created detailed E8 assessment checklists aligned with ACSC guidance to standardise evaluations.
- Coordinated and delivered a board-level presentation to communicate the findings and maturity level insights.

Policy & Governance:

- Drafted and submitted an updated Redback Cybersecurity Audit Policy (v1), which is now adopted.
- Collaboratively reviewed and revised ISMS policies focused on access control, incident management, compliance monitoring, cryptography, and endpoint protection.
- Developed a master ISMS policy and detailed policy safeguard documents.
- Updated and pushed revised policies to GitHub for documentation and future reference.

Roles & Responsibilities Audit:

- Conducted interviews with Blue Team and Infrastructure Team leads to clarify and define cybersecurity responsibilities.
- Identified overlaps in monitoring, data recovery, and escalation processes.

Commented [KB1]: @ROHAN BATRA Also assessed Data Warehouse and Project Orion

Commented [RB2R1]: Done

- Documented current gaps and proposed coordination improvements such as shared storyboards and joint charters.

Risk Management:

- Developed an initial risk register template and presentation to support the future implementation of structured risk tracking.

---

2. Recommendations for Incoming Team

a) Continue the Essential Eight Assessments

- Review the completed E8 maturity assessments and checklist outputs.
- Presentations are available which can be used to educate the incoming team members who are not aware with what essential eight is.
- Consider re-assessing select teams to evaluate changes since last trimester.
- To provide other teams with the time to implement our recommendations, consider re-assessing during Trimester 1 2026 at the earliest.
- Explore moving toward Maturity Level 2 where feasible.
- Use findings to guide technical recommendations to other teams (e.g. patching cycles, MFA, backups).
- We also recommend transitioning to a SOE (standard operating environment).

b) Expand Policy Management Stream

- Finalise review and implementation of the ISMS policies submitted this trimester.
- Identify additional outdated or missing policies (use GitHub audit trail).
- Establish a quarterly schedule for policy reviews and updates.

c) Operationalise the Risk Register

- Review the risk register template created this trimester.
- Begin populating it with real risks identified through E8 assessments and team audits.
- Establish ownership and update cycles.

d) Improve Team Coordination and Escalation Paths

- Review the documented audit of Blue and Infra team responsibilities.
- Ensure that unclear escalation processes are resolved.
- Propose a unified security operations communication channel for inter-team collaboration.

---

3. Tools & Resources to Use

- **Essential Eight Checklists**: Located in the GitHub repo (Redback-cyber), use these for consistent maturity assessments.

Commented [KB3]: @ROHAN BATRA I'd say explicitly call out that E8 assessments should wait until the other teams have had time to implement recommendations, so T1 2026 at the earliest

Commented [RB4R3]: Done

Commented [KB5]: @ROHAN BATRA Probably worth explicitly highlighting the recommendation to transition to a Standard Operating Environment (SOE) VM

Commented [KB6]: @ROHAN BATRA I think we need to add a recommendation to future GRC teams to build out an escalation framework so that compliance/risk management is taken seriously by projects

Commented [KB7]: @ROHAN BATRA Bit of a left-field one here, but I think we should consider if GRC truly comes under Cyber Security or not - there's a whole conversation to be had about bringing Infra, DW, Ethics, and GRC into a separate overarching team much like CS currently is - this would mimic the way a real organisation functions in that CS tends to be separate from all the other various Infra elements

Commented [RB8R7]: I say we leave that for Ben to decide, don't think that is something we can help much with

- **Redback Cybersecurity Audit Policy v1**: This defines how internal audits should be structured.
- **ISMS Policy Drafts**: Use the GitHub version history to see proposed and implemented changes.
- **Audit Reports & Gap Analyses**: Refer to existing reports as a basis for continued improvement. (available on GitHub)
- **GitHub Documentation Folder**: All final versions of policies, assessments, and planning documents are pushed here. (Redback-cyber)

---

4. Collaboration & Workflow

- Hold weekly internal team meetings to plan deliverables, rotate roles, and share findings.
- Maintain Agile principles for iterative delivery.
- Use GitHub and Microsoft planner (or other task tools) for documentation and progress tracking.
- Maintain consistent communication with Ben for approvals and direction.

---

5. Engage with Other Project Teams

One of the GRC team's ongoing responsibilities is to proactively engage with other project teams within Redback Operations to support Essential Eight maturity tracking and overall compliance with the GRC framework. This collaboration is not passive—it involves initiating conversations, identifying opportunities to assist, and offering targeted support.

Key Responsibilities:

- **Conduct regular audits** across key control areas (e.g., backups, MFA, PAM), according to a defined audit schedule. These audits serve as operational evidence to inform Essential Eight assessments.
- **Support Essential Eight assessments**, which are conducted every 1–2 years or as needed when significant operational changes occur (e.g., new projects, organizational shifts). These assessments determine the current Maturity Level.
- **Initiate cross-team support**, by actively reaching out to project teams to understand current security challenges, offer guidance, and provide training where necessary.
- **Identify emerging risks or gaps**, especially in new initiatives or projects where compliance or security controls might be insufficient.

Maintaining strong, intentional relationships with project teams will ensure the GRC team is seen as a proactive partner, fostering a unified and secure operational environment.

Commented [KB9]: @ROHAN BATRA Pet peeve of mine - I despise Trello with a passion, but beyond that, most of Redback is working on MS Teams, Planner, etc., so I think it's better if we recommend future GRC teams to stick with that unless Redback changes it's default. Reason is that GRC will need heavy cross-team collaboration, so it will cause less friction if handled on the same platform

Commented [KB10]: @ROHAN BATRA I feel like this section needs work. A few notes:

- We need to be clear that E8 does not involve any audits, rather the E8 assessments are to be done once every 1-2 years as operational demands arise (e.g. new projects spun up, changes to org structure, etc.), and are designed solely to confirm which Maturity Level we are operating at.
- Audits are separate, but related. We should be doing audits every so often based on what is being audited (e.g., backup schedules might be audited each trimester, but PAM might be audited once a year), and these audits should help serve as evidence for the E8 assessments (e.g., we point to MFA audit as evidence that MFA is being adhered to)
- We need to work on inter-team communication more actively; we should be regularly meeting with the other teams to see how they are going, if they need support, etc. You've mentioned something along those lines, but I think it's worth being explicit about our intentionality in the process - it's not "we're here if you need us", it's "Hey, we're here and we have capacity, what can we do to help?"

Commented [RB11R10]: Done

6. Suggested Roadmap for Incoming Trimester

Week	Priority Item
1	Allocate GRC team members to specific streams (Infra, Dev, Ethics, etc.). Schedule intro meetings with each project team to offer support and understand needs.
2–3	Begin targeted **audits** (e.g., backup processes, user access reviews). Start populating and launching the **risk register** with identified issues from each stream.
4–5	Collate audit findings, update GRC documentation (e.g., controls matrix), and begin drafting improvements to existing policies (e.g., Audit Policy v2).
6–8	Conduct **company-wide Essential Eight assessments** using data collected from audits and team engagements. Clarify maturity levels and gaps.
9–10	Finalise policy improvements, prepare **board-level summary** slides, and draft the **handover package** for the next trimester (including updated risk register, E8 progress, and audit trail).

Conclusion

This trimester marked significant strides in maturing Redback's GRC program. With foundational work done across the Essential Eight, policy management, and internal audit structure, the next team is well-positioned to continue Redback's cybersecurity enhancement. The focus should now shift toward operationalising these frameworks, improving communication with technical teams, and expanding oversight through practical tools like the risk register.

Commented [KB12]: @ROHAN BATRA I think it's best to parallelise the workload:

week 1 should be allocating team members to specific streams
Weeks 2 and 3 involve audits right off the bat, risk register, etc.
Weeks 4 and 5 involve collating, updating, etc.,
Weeks 6 - 8 would be company-wide E8 assessments
Weeks 9 and 10 are reporting, creating recommendations, handover, etc.

Basically, shift what we did a few weeks earlier, and explicitly parallelise the tasks from the beginning

Commented [RB13R12]: Done