

Big Four Australian Bank: Privileged Access Management Roadmap and Operating Model

Role: Engagement Partner, Technology Strategy and Cyber

A major Australian bank had invested in a leading platform to control privileged access, the powerful administrator accounts that can change systems, data and security settings across the enterprise. However, without a mandated strategy, standard or policy, adoption was inconsistent. The implementation faced stability and support issues, integration work remained outstanding, and reliance on legacy in house tools persisted. Audit findings and two formal risk treatment plans required the bank to close these gaps within a defined timeframe.

With a new privileged access strategy endorsed, the bank engaged us to turn it into an executable plan. Working with the enterprise architecture, technology service management and IT security operations teams, we were asked to define what controls were required in practice, how to get there, and how the service should be run and enforced once in place.

Key areas of focus included:

- Facilitated workshops with each privileged access stakeholder group to define the required use cases for Windows and Unix platforms
- A use case model describing the actors, system boundaries, controls and data involved in each privileged scenario
- Gap analysis between the current implementation and the strategic end state, rather than simply migrating legacy processes to a new tool
- A two year implementation roadmap aligned to the horizons in the bank's strategy and its network segmentation programme

- Remediation of gaps in technology capability, capacity, currency and resilience
- A revised operational support model to sustain the service and enforce mandatory use across the organisation

The work combined our experience of privileged access practices at other institutions with the bank's existing and planned processes, giving stakeholders a common baseline and accelerating agreement on the target state.

The outcome was an agreed set of privileged access controls, a sequenced roadmap that directly addressed the open audit findings and risk treatment plans, and a sustainable operating model that made the bank's privileged access platform the mandatory control across its technology estate.

For more information about this case or to discuss how similar cyber and technology risk programmes could be applied in your organisation, please contact me at marco@marcociobo.com or visit www.marcociobo.com.