Executive Summary

In March 2015, Ovum was engaged by the ACCC to conduct a review of Telstra's Information Security Remediation (ISR) program to ensure that its IT systems were compliant with the information security obligations in its Structural Separation Undertaking (SSU).

Since commencing the project, the scope has been extended to take into account an additional Internal Due Diligence (IDD) review by Telstra (which commenced in July 2015). As a result, Ovum's project for the ACCC has been split into two phases:

- Phase 1: Review Telstra's ISR program and a sample of 8 IT systems; and
- Phase 2: Review Telstra's IDD review and a sample of 6 IT systems.

ISR Program

Telstra's ISR program has been a large scale program of work which included:

- The remediation of 42 IT systems.
- The implementation of a Compliance Management Framework (CMF).
- A dedicated remediation program team with involvement of up to 100 business analysts, project managers and subject matter experts from business units across Telstra.
- Three years of project implementation time.

In structuring the remediation project model, Telstra implemented a clear reporting structure with Director level program accountability and with appropriate senior management governance through tiered internal oversight. Progress reports were delivered to the ACCC on a monthly basis.

In approaching the remediation, Telstra applied a 3 stage gating model across each of the IT systems to address the remediation issues (identification, assessment and treatment phases). Testing of the remediation involved three layers of testing (vendor tests, remediation program tests and legal verification tests).
In addition to the remediation of the 42 IT systems, Telstra also built a Compliance Management Framework to help embed its SSU responsibilities across the company through changes in system and product development processes and staff training.

In assessing the design and implementation of the program, Ovum considers that it was well resourced and structured to meet the task of a large scale IT change program. The implementation of a Compliance Management Framework was also a positive initiative which should help ensure a continued focus on SSU compliance.

Ovum conducted a review of 8 IT systems which had gone through Telstra's ISR program. The review included a system briefing from Telstra (covering the issues identified and the remediation strategy) and physical testing of the system (using a selection of test scenarios) for a number of key systems used frequently by Telstra Retail staff.

Overall, Ovum was satisfied with the range of tests conducted, the data input options and the customer cases used in the review. However, 3 issues were identified in 3 of the 8 IT systems under review. These issues were reported by Telstra in its confidential reporting to the ACCC.

In each case, Telstra has now remediated the issue and Ovum has verified the remediation.

IDD Review

Following the initial Ovum/ACCC review of Telstra's ISR program, Telstra commenced an Internal Due Diligence (IDD) project to review the systems remediated in the ISR program. The purpose of the IDD review project was to "conduct a systematic and thorough review of the reported systems remediated in the ISR program and which RBU staff have access to", in order to ensure wholesale

customer information could not be accessed by the RBU staff. As a result, Telstra reviewed 24 of the original 42 ISR program IT systems over a 9 week period.

In structuring the IDD review, Telstra again implemented a clear reporting and appropriate corporate governance model with senior management oversight.
Whilst the approach in the ISR program was to identify, assess and treat SSU compliance for each IT system, the IDD review employed a “break testing” approach in order to look for any remaining vulnerable areas/scenarios. As a result Telstra developed a test case library of business rules for use across all IT systems and then matched these with the IT system menu options to create a test scenario. In addition, while the business analysts selected to run the tests had system experience they were not involved in the original system testing in order to provide “a fresh set of eyes” to the testing.

Of the 24 systems tested, Telstra reported a subset of remaining potential SSU issues in 4 systems.

Ovum has reviewed the test summaries for the 4 systems and an additional 2 systems which had no issues, concluding that:

- Given the ISR program focussed on the remediation and testing of identified issues and the IDD review applied a “break testing” approach, Ovum accepts that the issues arising from the IDD review would not necessarily have been the focus of the ISR program tests. In this regard, the “break testing” approach of the IDD review proved to be a positive way to re-test the systems.
- Given the IDD review test cases were not necessarily normal RBU use cases and would have involved the RBU user using the system in a manner which did not necessarily reflect its day to day use, Ovum also accepts that they would have been difficult to generate in practice and therefore unlikely to have been picked up by the CMF. However, if those exceptions had arisen then the CMF should have been able to identify the issues through staff awareness and self-reporting processes.

Based on the review of the ISR and IDD documentation, Telstra briefings, and given that the majority of test cases were successful, Ovum considers that Telstra has applied an appropriate level of due diligence in conducting (and instigating) the ISR and IDD programs.

Whilst there may be other issues which have not yet come to light, it is likely that those issues (if they exist) will relate to more obscure aspects of the various IT systems or customer scenarios which are not part of the day to day operations of the systems. We therefore expect that Telstra’s Compliance Management Framework should be able to deal with these issues if they appear.

Summary and Recommendation

For the last 4 years, the ACCC has relied on self-reporting and remediation activities by Telstra. Ovum’s review has shown that Telstra’s approach to remediation has been appropriate for such a large scale program of work. The issues found during the review were self-reported by Telstra and either remediated or are in the process of being remediated. In addition the majority of tests in both the IDD and ISR programs passed successfully.

As a result we would recommend that the ACCC continue to rely on Telstra’s self-reporting mechanisms and that the implementation of Telstra’s Compliance Management Framework should either:

- Prevent new issues from arising (given the SSU compliance framework is now built into new product development or IT changes); or
- Allow the reporting of new issues as they arise (through compliance checks and company training).