ABS has put up their new guidelines for Outsourced Service Providers (OSPs) servicing Financial Institutions on their website. These guidelines outline minimum standards and controls that OSPs, including their relevant subcontractors, are required to have. The OSPs are required to be audited against these guidelines by external auditor once a year.

On IT infrastructure, the guidelines cover a number of areas ranging from data access control, physical security of Data Centre to Network & System security and incident response and recovery. The extensive list can be found

GENERAL INFORMATION TECHNOLOGY (IT) CONTROLS

(a) Logical Security - provide reasonable assurance that logical access to programs, data, and operating system software is restricted to authorised personnel within the OSP.

(b) Physical Security - restrict physical access to Data Centre/Controlled (DC) areas and have put in place environmental controls to protect the IT assets hosted at its data centres.

(c) Change Management - reasonable assurance that the OSP documents and approves all changes to the system software and network components.

(d) Incident Management - reasonable assurance that the OSP resolves all system and network processing issues in a timely manner.

(e) Backup and Disaster Recovery - reasonable assurance that the OSP's business and information systems recovery and continuity plans are documented, approved, tested and maintained. Backups are performed and securely stored.

(f) Network & System Security and Monitoring - reasonable assurance that the OSP's systems and network controls are implemented based on FIs' business needs.

(g) Security Incident Response - reasonable assurance that appropriate personnel within the OSP are contacted and immediate action is taken in response to a security incident.

(h) System Vulnerability Assessments - reasonable assurance that the OSP performs regular system vulnerability assessment and penetration testing on environments with FIs' customer information.

(i) Technology Refresh Management - reasonable assurance that the OSP maintains up-to-date software and hardware components used in the production and disaster recovery environment.