ABC Ltd - SOC 2 Readiness Assessment Case Study

ABC Ltd provides hosted platforms services using secure and reliable cloud technologies. ABC contacted the Accorp Partners in July 2020 as ABC had been asked by one of their US clients to undergo a SOC 2 Type 1 audit in line with the AICPA Trust Services Criteria. The AICPA Trust Services Criteria and the subsequent audit examines and reports on controls at a service organization relevant to security, availability, processing integrity, confidentiality and privacy.

Accorp Partners held an initial scoping call with ABC's Information Security Manager to establish the SOC 2 audit requirements. Following the scoping call it was decided that the Accorp Partners SOC 2 Readiness Assessment audit would be the service for the needs of ABC and help them prepare for a SOC 2 audit.

The Accorp Partners SOC 2 Readiness Assessment examines the organizations current level of compliance with the AICPA TSC requirements, examines the risks to the organization and provides a detailed report and roadmap on the current level of compliance and focuses areas that need to be addressed prior to a SOC 2 audit taking place. The contract agreement was signed off and the SOC 2 Readiness Assessment was conducted at remotely for ABC's head office in Manchester, July 2020.

The Readiness Assessment began with a detailed overview of the organization, its systems and services, IT infrastructure and internal functions. Interviews were conducted with the IT Security, Quality, and HR, IT and Development Managers and the Operations Director.

The following areas were reviewed during the readiness assessment:

- Audit scope to establish the boundaries of the audit and the internal and external interfaces and responsibilities
- The documented service or system description, which describes the services and products it provides and include information on the infrastructure, software, people, processes and data that support these services
- The applicability and scope of the 5 TSC's i.e. security, availability, processing integrity, confidentiality and privacy, relating to the risks to the organization
- Risk management and risk assessment
- Control selection, design and implementation
- Control monitoring and measurement

It was decided that 3 of the 5 TSC's would be included within the scope of the SOC 2 audit and these controls selected would adequately mitigate the risks to the organization. The security, availability and confidentiality were selected to mitigate the organizations risks.

Findings and recommendations were made during the Readiness Assessment as and when they were identified and discussed with the interviewees and the Senior Management Team.

The Readiness Assessment Report concluded that ABC did not meet the requirements of the AICPA TSC's at the time of the assessment and therefore would not meet the requirements of a SOC 2 Type 1 audit.

The following describes the high-level roadmap that was recommended that ABC should consider in its efforts to achieve compliance with the requirements of the SOC 2 TSC.

- Define the scope of the SOC audit
- Document the information security risk management framework and risk acceptance criteria
- Design and document controls (including definition of metrics, measures of effectiveness, records supporting operation, etc.)
- Produce a risk treatment plan and implement additional TSC controls/enhance existing controls
- Produce the required policy and procedural documentation
- Monitor and measure and evaluate control effectiveness
- Review metrics, reports, etc. to ensure controls remain effective
- Reassess risks on a regular and planned basis taking the effectiveness of controls into consideration and where necessary, design and implement additional controls or enhance existing controls
- Control monitoring and measurement should be an ongoing cyclical process.

After the readiness assessment, a detailed Readiness Assessment report was produced, and a follow up visit was carried out to present the findings to ABC's Senior Management Team. Accorp Partners are currently assisting ABC with their remediation work (advising on control design, reviewing the system description and conducting a SOC 2 pre audit) and have been referred to Accorp Partners' CPA audit partner who have agreed to carry out a SOC 2 Type 1 audit in February 2019.

Accorp Partners were very pleased to announce that ABC Ltd achieved their SOC 2 Type 1 audit report and are now working towards a SOC 2 Type 2 audit report which will provide their clients with the added level of assurance that a SOC 2 Type 2 audit report provides, as the CPA auditor examines and tests the effectiveness of the controls in place. Accorp Partners are proving ongoing assistance for ABC Ltd in their pursuit of the SOC 2 Type 2 audit report.