

Date	Version
08/05/2014	1.0

1.0 Policy Detail

1.1 Scope

That all Tier 1, or key Service Providers are required to show evidence of internal controls.

1.2 Purpose

RCL requires that their Tier 1, or key Service Providers provide evidence of audits conducted against their internal control environment. Typically an SSEA16 Type I or Type II report is preferred and acceptable. Other audit reports of the Service Provider's internal control environment might be accepted with approval from RCL IT Compliance. Foreign equivalents of an SSAE16 report will be accepted.

1.3 Definitions

1.3.1 Internal Controls

Is a process for assuring achievement of an organization's objectives in operational effectiveness and efficiency, reliable financial reporting, and compliance with laws, regulations and policies. A broad concept, internal control involves everything that controls risks to an organization.

1.3.2 SSAE16

Is an auditing statement issued by the Auditing Standards Board of the American Institute of Certified Public Accountants (AICPA). As of June 2011, the Statement on Standards for Attestation Engagements No. 16, Reporting on Controls at a Service Organization (SSAE16), replaced SAS 70.

1.3.3 SSAE16 SOC 1, Type I Report

Is technically known as a "*Report on Management's Description of a Service Organization's System and the Suitability of the Design of Controls*". A type I is a report on policies and procedures placed in operation as of a specified point in time. SSAE 16 type I reports evaluate the design effectiveness of a service provider's controls and then confirms that the controls have been placed in operation as of a specific date.

1.3.4 SSAE16 SOC 1, Type II Report

Is technically known as a "*Report on Management's Description of a Service Organization's System and the Suitability of the Design and Operating Effectiveness of Controls*". A type II is a report on policies and procedures placed in operation and tests of operating effectiveness for a period of time. SSAE 16 type II reports include the examination and confirmation steps involved in a type I examination plus include an evaluation of the operating effectiveness of the controls for a period of at least six consecutive calendar months. Most user organizations require their service provider to undergo the type II level examination for the greater level of assurance it provides.

1.3.5 Foreign Equivalents

For example (not an exhaustive list): The German equivalent report is known as an IDW PS 951. The United Kingdom report is known as an AAF 01/06. The Canadian report is known as a Section 5970. The Indian report is known as an AAS 24.

2.0 Exceptions

There may be Tier 1 Service Providers who have not chosen an Internal Control standard and therefore cannot be audited against a standard. This situation should only occur with very small companies that have limited products and/or services. These exceptions will be documented and presented to the Executive Vendor Governance Committee for review and approval.

3.0 Policy Administration and Governance

Policy May Be Modified at Any Time. RCL reserves the right to modify any provision of this Policy at any time without notice. Revisions will be effective when authorized parties have approved modifications to this Policy.

This policy must be reviewed by all of the parties below and approved by the CIO and Head of IT Vendor Management every 2 years.