Service Organization Controls (SOC)

A SOC 2 report provides assurance that the service organization has deployed an effective control system to mitigate operational and compliance risks of its system. It addresses the System and Organization Controls (SOC) using Trust Services Criteria (TSC) for service organizations to apply and report on controls that may affect users of their service. A SOC 2 report demonstrates an independent Service Auditor's review of a service organization's application of criteria related to one or more of the TSC, which are: Security, Availability, Processing Integrity, Confidentiality and Privacy.

Trust Services are defined as a set of professional attestation and advisory services based on principles and criteria that address the risk and opportunities of IT-enabled systems and privacy programs. Trust Services principles and criteria are issued by AICPA and the Canadian Institute of Chartered Accountants (CICA). Trust Services Principles, Criteria, and Illustrations for Security, Availability, Processing Integrity, Confidentiality, and Privacy provides guidance when providing assurance services or advisory services (or both) on IT-enabled systems including electronic commerce (e-commerce) systems. It is particularly relevant when providing services related to security, availability, processing integrity, confidentiality and privacy.

The Trust Services principles and criteria are organized into four broad areas:

- **Policies**—The entity has defined and documented its policies relevant to the particular principle. (The term "policies" as used here refers to written statements that communicate management's intent, objectives, requirements, responsibilities and standards for a particular subject.)

- **Communication**—The entity has communicated its defined policies to responsible parties and authorized users of the system.

- **Procedures**—The entity has placed procedures in operation to achieve its principles in accordance with its defined policies.

- **Monitoring**—The entity monitors the system and takes action to maintain compliance with its defined policies.

The Trust Services introduce a list of criteria against which these four areas are evaluated to assess whether one or more of the following five principles, which were developed by AICPA and CICA for use by practitioners in the performance of trust services engagements, have been achieved:

- **Security**—The system is protected against unauthorized access (both physical and logical).

- **Availability**—The system is available for operation and use as committed or agreed.

- **Processing integrity**—System processing is complete, accurate, timely and authorized.

- **Confidentiality**—Information designated as confidential is protected as committed or agreed.

- **Privacy**—Personal information is collected, used, retained, disclosed and destroyed in conformity with the commitments in the entity's privacy notice and with criteria set forth in Generally Accepted Privacy Principles (GAPP) issued by AICPA and CICA.