LiveRamp Security

As a recognized Acxiom Safe Haven, LiveRamp incorporates a holistic information security strategy focused on risk management and provides a secure, safe, and segmented environment for the processing of client's data. The security program incorporates the governance and insight at the executive and board levels and is based on ISO 27002-2013.

The defense-in-depth security solution includes:

Segmented Network

- Internet-facing DMZ bordered by Palo Alto stateful packet inspection firewalls.
- Network zone firewall borders include:
  - Intrusion detection and prevention system (IDS/IPS).
  - Data transfer and access logged, with logs monitored by dedicated team.

Dedicated Security Resource

- Key logs ingested into a security information and event management (SIEM) system for event monitoring and alerting.
- Security Operations Center (SOC) monitors the SIEM system.

Secure Data Transfer

- Data transfer via sftp; sftp server sits behind firewall.
- Upon upload, file is immediately copied over to internal server.
- Each client uploads to client-specific directory; authorized access only.

Data Processing Environment Controls

- Associates isolated by network zones from the data processing environment.
- Access restrictions:
  - Restricted user interface/application.
  - System administrator access restricted through a bastion host.
  - Access logs retained and stored in a centralized logging environment.
- Logical partition of client data; no co-mingling with other client's data.

Data Center Controls

- Multi-layered security including 24x7x365 on-premise personnel, biometrics, video surveillance and three layers of Network Operations Center monitoring.
- ITIL-based control environment validated for compliance against HIPAA, PCI DSS, and SOC (SOC2 and SOC3) framework
- Complies with Tier 2 architecture with single utility supply, multi-tenant and single threaded generators. Each has N+1 redundancy including UPS and backup generators.
- Tier 3 for critical power and HVAC.

Compliance Confirmation

- Third party quarterly vulnerability scanning and penetration testing of the Internet perimeter to PCI-DSS standards.
- Third party HP Fortify quarterly code scans.
- SOC2 Type II audit currently underway; report available February 2017.