Security Operations and Management

Incident response

Customers need to be notified when an issue, incident, or breach has occurred and the impact to environment or to their data. Issues, incidents and data breaches should be communicated by the Provider to all affected Customers in a timely manner.
Customers should also consider whether their Provider requires all Customers to immediately notify the Provider of potential breaches in their environments, allowing the Provider to respond more quickly to contain the breach and minimize its impact to other Customers.
Based on the type of cloud service category used –relating to facilitating the storage, processing or transmitting of cardholder data each phase of the incident response life cycle is affected at a different level.
Notification processes and timelines should be included in SLAs, and incident response plans should include notification requirements.

Customers should contractually require data breach notification from their Providers in clear and clear-cut language, taking into consideration the need to comply with local and global Regulatory/breach laws, data privacy, security incident management and breach notification requirements.

Forensics Investigation

Incident investigation may involve consideration of legal and jurisdiction requirements, and these requirements should be included in SLAs or operational agreements.

The potential for Customer data to be captured by third parties during a breach investigation should also be clearly understood.

Forensic functionality should be specified in service level objectives (SLOs) incorporated into the SLA between the Customer and the Provider. SLOs may include requirements for notification, identification, preservation and access to potential evidence sources.
Customers and law enforcement agencies require, and rely on Providers for, forensics support, and these obligations varies depending upon cloud service category as noted below.

In software as a service, the capability for forensics is dependent upon the Provider’s support, as Customers have no control over the Provider’s environment. Forensics examiners may need to rely on high-level application logs available from the SaaS application. SLOs may include evidence sources such as logs from applications.

In platform as a service, the capability for forensics is shared between Customers and Providers. Customers control the Developed and hosted software application, and hence control forensics capability within the application, automatic logging to an external log server can be configured to capture the applicable audit trail. However, since the actual operation of the application is within

the Provider’s controlled infrastructure, Customers must clearly identify Providers' responsibilities with respect to forensics investigation. SLOs may include evidence sources such as logs from the application, web, and database server, guest OS/host, portal, network capture, billing and management portal.

In an infrastructure as a service, the capability for forensics is shared between Customers and Providers. Customers have greater control over the range of potential evidence sources; however, some essential data only exists with Providers and under their control. Customers must clearly identify Providers' responsibilities with respect to forensics investigation. SLOs may include evidence sources such as logs from the cloud network perimeter, DNS servers, virtual machine monitor, APIs, host OS, and network capture, billing and management portal.

Revision #1
Created 6 October 2025 09:41:51 by RISA
Updated 6 October 2025 09:43:31 by RISA