

ITEM 6.5.2 | RISKS

One of the major risks with cloud computing involves the accessibility of data/services upon termination of the hosting agreement due to formatting or proprietary storage protocols implemented by the vendor. Care should be given to ensure the data is returned in the same format in which it was migrated. Security and integrity of the court data may be at risk when a contracted cloud service provider, who is also responsible for data security, is storing the data outside the monitoring capability of court/clerk staff. Care must be taken to ensure the security and integrity of court data and services. Security audits and reviews should be conducted preferably by an external, third-party entity. Security breaches should be properly and immediately reported to the Trial Court Administrator, Chief Judge, and the Chief Information Security Officer at the Office of the State Courts Administrator.

Because Service Level Agreements ("SLA's") can change often and with short notice, a plan must be in place to monitor and audit the impact that such changes to agreements could have and mitigate their impact.

