

ARE YOU AUDIT READY?



Any customer information that is accessed by, is resident at or is maintained by a records storage firm should be handled as confidential information in a secure facility protected against physical intrusion with the necessary detection equipment and systems. The right to audit (at your client's expense) your company's work processes to verify confidentiality can be built into the contract or service agreement.

If your client or prospective client should decide to audit your facility, you can expect the following areas to be of key concern:

- **SITE SECURITY** – The physical location of your facility can be an important consideration to the protection and access of a prospective client's property and to his or her comfort level. The protection of the facility and continued monitoring of challenges also are vital considerations. A prospective client may opt to visually inspect the storage site and the neighborhood as part of the qualification process.
- **FACILITY SAFETY AND SECURITY** – This area concerns the physical aspects of the facility that houses your firm's assets. Additionally, the prospective client may request information on building construction, access, remote and on-site monitors, the community and the disaster plan. The prospective client may conduct an analysis, and your company should be open to questions concerning security.
- **PERSONNEL SECURITY** – Personnel security depends upon having procedures in place with hiring parameters that include background checks, verification of skill and experience levels and bond requirements, if needed. Individual employee or company contract terms should specify required, as well as prohibited, conduct and remedies for security breaches. Policies and procedures for visitors and non-staff personnel similarly must be in place for the protection of all parties.

A prospective client may choose to review your response to previous threats and security events or may perform a mock drill.

Your company should provide the prospect with a "Threat-Risk Manual" that indicates response procedures for various events. Following mock testing and audits, the plan can be redesigned with corrective procedures to avoid future failures. A firm's overall plan should provide a decision tree that pinpoints responsibility for each task and, in the event of a missing element, a responsible manager who can replace this missing element in the process.

An organization not only bears responsibility to audit its information management service but also to change service providers when its current vendor is unwilling or unable to perform to the standards defined by the audit and its resulting findings.

Kevin S. Joerling, CRM, is senior manager of standards and records management for ARMA International, based in Lenexa, Kan. He can be reached at kjoerling@arma.org.

