An organization that has decided to outsource its electronic records storage must do its due diligence in selecting a service provider (xSP) to ensure that its information will be managed appropriately throughout its life cycle. A critical aspect of this is investigating how potential xSPs will protect the information it is hosting.

The three following checklists from the technical report *Understanding Electronic Storage Technologies* (ARMA International TR 26-2014) will be invaluable tools for evaluating xSPs – and most of the checklist items would also be relevant for organizations wanting to evaluate how well they are protecting the records they store in house.

Readers should note that not all items in these checklists may be applicable to their organizations; careful consideration of their unique needs, requirements, and resources (i.e., timelines, personnel, and budgets) is essential.

Checklists for Evaluating Electronic Records Storage Protection

Checklist for Evaluating the xSP

Financial Stability

What is the ownership structure of the xSP (e.g., family-owned, sole proprietorship, partnership, or corporation)?

How many years has the xSP been in business?

How many years has the xSP been providing electronic records storage services?

If the xSP encounters financial difficulties, what legal agreements control the operation of the facility?

- Does bankruptcy trigger evacuation of all stored electronic records?
- Would a third party be enlisted to operate the facility?

xSPs' Providers

What electronic records storage services does the xSP subcontract?

Who are the subcontractors and where are they located?

Does the xSP own or lease the business's facilities such as the physical structure or real estate?

Could the real estate owner's bankruptcy or lienholders create a disruption in the conduct of business?

Are protection agreements in place should a utility company (e.g., communications services provider) fail to deliver on a contractual agreement?

If an energy crisis occurs that disrupts power or fuel availability, is a contingency plan in place that provides an alternative energy supply?

Checklist for Evaluating Electronic Records Security

Access Controls

How does the xSP prevent commingling of electronic records from various contracting organizations?

- What procedures are used to ensure xSP employees cannot release electronic records to the wrong contracting organization?

Are processes in place to secure electronic records from corruption, theft/intrusion, unauthorized access, and/or viruses?

What encryption methods are available and how are encryption keys stored?

What access controls are available?

What procedures exist for detecting security breaches?

What notification processes are in place (to alert the xSP and contracting organization) of potential security breaches (e.g., unusual usage patterns or unapproved configuration changes)?

What services are provided from entities located outside the United States?

What subcontractors or third parties have access to the contracting organization's electronic records?

- Is access encrypted and is it granted over the public network, a virtual private network (VPN), or via physical tape transfer?

Are all electronic records transmissions between the xSP and contracting organization performed in a secure (e.g., encrypted) manner?

- If a VPN is used, what entity is responsible for its maintenance?

Does the xSP have a robust firewall to prevent unauthorized external access?

How are audit trails tracking security-related activities managed?

System Issues

What are the critical points of system failure and how is redundancy ensured?

How is equipment slated for de-commissioning and previously used to transmit/store electronic records dispositioned?

Breach Response

If a security breach occurs (or is thwarted) while a backup is in process, what procedures are in place to avoid compromising backup operations?

In sophisticated attacks, secure lines can be diverted and backup mimicked. How would this situation be handled?

In the event of sabotage, can a remote command purge electronic records stored at the facility?

> Readers should note that not all items in these checklists may be applicable to their organizations; careful consideration … is essential.

Checklist for Evaluating Facility and Personnel – Safety and Security

Environmental Issues

Has an "Unacceptable Threat Matrix Identification" been performed?

Has the site been evaluated as outside of the 100-year flood plain?

- Are there issues that could change the flood risk at the site?

Is there proximity to nuclear power plants, chemical plants, pipelines, refineries, or other facilities that could create the need for a facility evacuation?

- Are underground storage tanks adjacent to the site?
- Could tanks create a contamination that would necessitate evacuation?
- Has a Phase III Environmental Hazard Risk Assessment been done?

Is the site in an area prone to civil unrest or high crime? (Lack of a secure neighborhood can affect the xSP's ability to retain a highly-skilled staff and maintain effective operations; criminal activity in the area can diminish employee morale and increase the xSP's insurance costs.)

Who are the adjacent tenants and landowners?

- Are there adjacent tenants that limit control and integrity of the site's ingress/egress?
- Is the site in an airport glide path where a crash or radar signals could interfere with electronic systems operation?

Does the site have security fencing, closed circuit television, motion sensors, and manned patrol or security guard monitors?

- Is there a security gate at the entrance to the site?

If applicable, has the security of fuel storage tanks been verified?

- Is there control fencing or are there buried units?
- Given the risk exposure, are the tanks of sufficient size? (Hurricanes or earthquakes can limit power supply for several weeks.)

How is the communication grid attached to the building (e.g., underground)?

How is traffic controlled?

- Could traffic patterns make the site difficult to reach in a threat (e.g., narrow and/or one-way streets)?
- Are there motor traffic set backs or barriers to limit vehicles proximity to the building?
- Are visitor and service vehicles searched for contraband?
- Can vehicles be inspected 150 feet or more away from the building?

How are parking areas secured?

- Are parking spaces assigned?
- Is there proper security lighting?
- Are there areas where trespassers could conceal themselves?

Are there multiple entry requirements with access controls such as photo identification badges, key cards and/or biometric interfaces?

Building Security

How is the building secured?

- Does the building design incorporate tiered levels of security such that there is lower to higher security as the data production and media storage areas are approached?
- Are there window barriers (burglar bars), security screens, or polycarbonate barriers?
- Is there visual control of delivery bays and entry doors?
- Is there minimal signage to avoid publicizing the existence of the building and its assets?
- Are dumpsters located away from the building?

What digital surveillance cameras and systems are in place?

- Are all entry doors, passageways, docks, delivery bays, foyers, and the entire server and data center area covered by digital cameras or closed circuit television with continuously monitored feeds?
- Is the digital camera feed set up to record locally and feed to a secure browser for remote monitoring? Or, is there monitoring via a mobile device such as a smartphone? (Remote feed or mobile device access could serve to assist fire fighters in responding efficiently to a threat.)
- Are the digital cameras equipped with motion sensors to respond to movement in secure areas? (These motion sensors can help firefighters locate staff trapped in the building during a fire.)
- Is digital video sent offsite to a remote recorder with dual copies available?

How is building access controlled?

- Are there access control levels with increasing rings of security and anti-passback (i.e., "in" must be followed by "out" before another "in" can be used)?
- Are there multiple entry requirements with access controls such as photo identification badges, key cards, and/or biometric interfaces?
- Is access also controlled by shift scheduling so that work hours are defined?

What are the procedures for ensuring the security of visitors to the building?

- Are there sign-in logs or a digital photo log?
- Are appropriately designated identification badges (e.g., color-coded tags worn in an externally-identifiable manner) issued to visitors?
- Are visitors escorted at all times while on-site?

Building Stability

Have the building's design and structure been assessed?

- What are the ratings for snow load, wind, water runoff, and ice storms?
- Is the facility grounded for lightning?
- Are window designs consistent with threat levels?
- Is the building rated for the proper seismic zone (I thru IV)?
- Is there base isolation for the data processing area?
- Are there prints on file with the original stamp and approvals?
- If the building is older than 15 years, has there been a licensed, professional inspection by a structural engineer with a review of existing wiring and light fixtures, and a review for contaminants, polychlorinated biphenyls (PCBs), or asbestos?
- Has the roof been inspected? Is there a water leak report or drainage inspection?
- Are walls floor-to-ceiling to prevent movement over the walls or through the heating, ventilation, and air

conditioning (HVAC) ductwork?
- Is the overall structure four-hour rated per the National Fire Protection Association (NFPA) standards for ground-supported structures?

Has there been a fire sprinkler inspection to evaluate water supply and source pressure as well as actual pressure available at heads?

Fire Protection

Has the building been assessed for fire hazards?

- Has there been a fire sprinkler inspection to evaluate water supply and source pressure as well as actual pressure available at heads? Have the pump systems been maintained?
- Is electrical wiring in conduit? Are ground fault or arc breakers used for critical area breaker panels?
- Are firewalls a vital part of the building design? Are fire stops used in wall penetrations? Are fire dampers in place to stop spread of smoke and fire and explosive gases?
- Is a fire marshal's inspection report on hand?
- Are the fire marshal and fire fighters familiar with the facility?
- Are hose seats defined in a fire fighter's plan of action?
- Are high security areas defined for early action suppression?
- Is a fire drill procedure in hand, allowing the evacuation of the building's occupants and the identification of a meeting area at evacuation?
- Is the fire department aware of media vaults and server vaults?
- Is the fire department aware that firefighters should not penetrate vault doors or server vault doors as it voids fire suppression control?
- Has the fire and casualty insurance carrier audited the facility for acceptability?
- Are there adjacent undeveloped, wooded areas that could pose a fire risk?
- Are staff smoking areas located a sufficient distance away from the building or media storage area?

Communications

What are the procedures for communication security?

- Are alarm signals sent by dual technology (FM and hardwire)?
- Is satellite telecommunication available to maintain connectivity during a utility outage, e.g., mobile satellite radios and repeaters?
- Are the communication lines monitored to avoid security risks and what is the procedure if a security breach occurs?
- If Wi-Fi is utilized, are appropriate security precautions implemented to safeguard communications transmissions originating inside the facility from possible detection by external entities?
- Are the wiring logs and design plans protected, with access limited to only authorized personnel?
- Is there radio frequency shielding or protection for server vaults?
- Are there rated cable trays for all wire entry points?
- Is the communication infrastructure located within rigid conduit within the facility?
- Are laptops and other mobile devices controlled through a mobile device management plan?
- Is there a call tree for communicating a change of security status?
- Will a fire alarm or security event trigger a breakdown in security?
- Are wireless local area networks secured? Is the information encrypted? To what level?
- Is the communication program designed so that the contracting organization and the xSP can easily remain in contact?
- Are there documented procedures for contact with community fire or police services?

Vaults

How secure is the vault structure?

- Is the secure vault chamber rated as Class 125 (UL 72) to protect the computer hardware, servers, switches, routers, and media?
- Is a secure vault door with a Class 125 (UL 72) fire rating and listing in place? Is the door labeled as such for audit assurance and documentation?
- Is the vault door equipped with a smoke- and heat-activated hydraulic closer to seal the vault door in the event of a fire?
- Is the door closer equipped to communicate with the internal clean agent fire suppression alarm panel as well as the building alarm panel to close the vault chamber during either alert status?
- Is the location of the vault capable of providing the ultimate security for the data chamber?
  - If the vault is located above grade, is the vault rated as six-sided for protection (per GSA Federal Specification AA-V-2737) from a fire below the server or data processing area?
  - Is the vault located above the level where flooding

could occur?
- Are the batteries for the uninterruptable power supply (UPS) system located within the vault?
- Is the vault located sufficiently away from elevator shafts, transformer or switch gear, or other equipment that delivers high electromagnetic interference?
- Are restroom or other plumbing-related facilities located so that they cannot create water or flooding hazards to the chamber?
- Is the vault optimally located to avoid the outside entrapment of radio frequencies or other information that could disclose data to a saboteur?
- Is the vault chamber equipped with a water-shield roof deck to avoid contamination from external firefighting activities, sprinkler activation, and water main breaks?
- Is the vault rated for water-shielding (per NFPA 220) if the data center is in a hurricane or tornado-prone region?
- Is the vault rated for Zone IV seismic protection (per NFPA 220) if the data center is in a seismic activity area?
- Is the vault rated for regional threats, e.g., termites, snow loads, high humidity, etc. (per NFPA 909)?
- Can a fire alarm, security alarm, or general evacuation order pose a particular threat by opening egress doors or circumventing access control?
- Is the vault chamber designed to secure itself upon each ingress or evacuation?
- Are portable extinguishers available near the vault for first responders?

Is the vault rated for regional threats, e.g., termites, snow loads, high humidity, etc. (per NFPA 909)?

What is the electrical design for the vault?
- Are the wire penetrations and cable trays rated for fire protection to the level of the vault chamber?
- Are the wire systems earth-grounded and fitted with the proper breaker switches?
- Is the electrical load sufficient for the load capacity?
- If the computer or switch equipment has been changed lately, has the chamber's load capability been re-evaluated for proper voltage?
- Are the vault penetrations completed with Class 125 (UL 72) fire-rated cable trays?
- Are the wiring harnesses, power circuits, and communication cables located above the servers to avoid flood contamination?
- Are the wiring systems set at ceiling level for ease of change out and to avoid extended downtime?
- Are wire management systems sufficient for future growth?
- Are communication fibers compliant with current industry standards?
- Are communication fibers Class IV (ISO/IEC 11801) or higher?

What are the environmental controls for the vault?
- Is the air conditioning facility a split system requiring through-wall coolant piping? (If so, these penetrations should be designed to avoid heat transfer from a fire.)
- Is the air conditioning system external to the chamber? (If so, the fire dampers should be of the same rating as the vault and designed to seal the duct opening by activation of heat or smoke detection.)
- Is the supply and return capability sufficient for the hardware loading?
- If the server equipment has been retrofitted after the initial vault install, is this chamber sufficiently cooled for the new heat loads?
- Is there a mechanical engineer's stamped drawing attesting to the proper cooling loads?
- Is there an environmental monitor providing online, real-time and historical vault status?
- In the event of a failure or alarm detection, is the environmental monitor set to report to a manager (via mobile phone, for instance) at all times?
- Is the vault chamber equipped with vapor barriers to prevent smoke and environmental contamination of the area?
- Is the vault equipped with an air-lock foyer to prevent dust and other contaminants?
- Are the man-trap foyer and the vault chamber entrance doors equipped with card or biometric access control?
- Is there a procedure for maintaining the cleanliness of the vault that will not compromise the integrity of the vault's security?
- Is air filtration accomplished with high efficiency particle arrester filters? (Ozone air cleaning may affect computer equipment and is a health concern for employees.)
- Is the vault chamber set up with closed loop technology to avoid contaminants?
- Are air intake vents for the vault area secure from sabotage?
- Is the roof area over the data chamber routinely main-

tained and designed to direct water leaks away from the vault area?
- Is the heat level within the server vault monitored?
- Are temperature and humidity displayed online for management control?
- Are environmental control systems designed to routinely and automatically communicate with managers?
- Have pest control features been incorporated into the data center structure's design (e.g., rodent and/or termite infestation prevention)?
- Is pest control part of the data center's ongoing maintenance program?
- Are there sealed slab and moisture barriers, as well as sealed windows?

Is there a clean agent suppression system for the vault?
- Is the clean agent suppression system designed for use with fragile electronic/computer equipment?
- Is it a "zero residue" clean agent suppression system?
- Are smoke, heat, and ionization detectors integrated into the system design?
- Is the system inspected and "green tagged" as safe for use?
- Has a complete scenario been run on the alarm panel, door closer interface, door closer, strobes, horn or alerting device, connection to the main building alarm, and alert to the community fire station?
- Does the alarm set off alerting devices outside the building to notify neighbors, if applicable?
- Are systems in a protected wiring loop?
- Is the building alarm an Underwriter's Laboratory Class A Central Station reporting type?
- Has the backup power system to the alarm panel been tested for battery life?
- Does the system present a risk to the servers or personnel at activated delivery?
- Is the system of high dielectric strength to avoid damaging computer hardware?
- Is the system equipped with an abort switch as well as a remote annunciator? (The remote annunciator allows the staff to check on the vault with sensors and camera video without opening the door and possibly defeating the design concentration required.)
- Is a Very Early Smoke Detection Apparatus (VESDA) system in place for early detection?
- Are the light fixtures dust and vapor resistant?

Personnel

What are the policies and procedures for personnel screening?
- Are background checks done for all personnel, both employees and non-employees?
- Are biometric and/or fingerprint records maintained?
- Is there a lie detector procedure?
- Is drug testing randomly conducted?

Are there personnel safety and security policies and procedures for employees as well as non-employees (e.g., janitorial or cafeteria vendors) who provide on-site services?

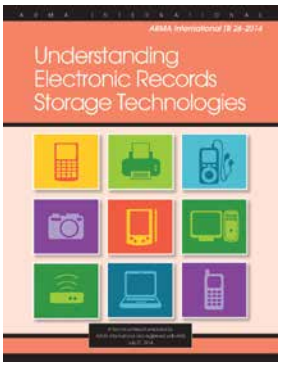
Outsourcing and Audits

Through an audit, the organization should determine the physical security, management capabilities, and processes available to protect the information within the xSP's electronic storage environment. The ongoing protection of the organization's information assets is a task that requires constant vigilance. Economic downturns can pressure xSPs to cut back on operations, especially back-office procedures that are not immediately visible or apparent.

As part of an audit, the organization may wish to review the xSP's history of responses to previous threats and security events or suggest conducting a mock drill. Ideally, the auditor should be able to review a "Threat-Risk Manual" developed by the xSP that indicates the response procedure for each type of event.

Well-developed, consistent response is the goal. The organization may need to change to a different xSP when audit findings reflect unacceptable performance levels or an unwillingness/inability to comply with industry standards benchmarked in the audit.

Read More About It



Understanding Electronic Storage Technologies (ARMA International TR 26-2014) is registered as a technical report with the American National Standards Institute. It includes a broad discussion of storage technologies and service offerings for electronic records, 10 checklists for evaluating service providers, and guidance for creating a request for proposal (RFP) document.

It may be purchased in hard copy or PDF format from the ARMA International online bookstore at *www.arma.org/bookstore*. **END**

This technical report was developed by an ARMA International Standards Development Program workgroup led by Kim Mayberry, CRM. She may be contacted via standards@armaintl.org. *See the complete list of team members on page 47.*