IT Service Delivery And Support Week Eight - Data Center

IT Auditing and Cyber Security

Fall 2016

Instructor: Liang Yao

Data Center & Operations Audit

* Data Center 101
* Facility-Based Controls
  * Physical security
  * HVAC
  * Fire Suppression System
  * Power Source
* Data Center Operations
  * Security
  * Roles and Responsibilities of Data Center Personal
  * Segregation of Duty of Data Center Personal
  * Emergency and Disaster Response
  * Facility and Equipment Maintenance
  * Data Center Capacity Planning
  * Data Center

Data Center & Operations Audit

* Data Center 101 – "*A **data center** or **computer centre** (also **datacenter**) is a facility used to house computer systems and associated components, such as telecommunications and storage systems. It generally includes redundant or backup power supplies, redundant data communications connections, environmental controls (e.g., air conditioning, fire suppression) and security devices. Large data centers are industrial scale operations using as much electricity as a small town and sometimes are a significant source of air pollution in the form of diesel exhaust*." - Wikipedia

Data Center & Operations Audit

Physical Security and Access Control

* **Build on the right spot.** Be sure the building is some distance from headquarters (20 miles is typical) and at least 100 feet from the main road. Bad neighbors: airports, chemical facilities, power plants. Bad news: earthquake fault lines and (as we've seen all too clearly this year) areas prone to hurricanes and floods. And scrap the "data center" sign.
* **2. Have redundant utilities.** Data centers need two sources for utilities, such as electricity, water, voice and data. Trace electricity sources back to two separate substations and water back to two different main lines. Lines should be underground and should come into different areas of the building, with water separate from other utilities. Use the data center's anticipated power usage as leverage for getting the electric company to accommodate the building's special needs.

Data Center & Operations Audit

Physical Security and Access Control

* **Pay attention to walls.** Foot-thick concrete is a cheap and effective barrier against the elements and explosive devices. For extra security, use walls lined with Kevlar.
* **Avoid windows.** Think warehouse, not office building. If you must have windows, limit them to the break room or administrative area, and use bomb-resistant laminated glass.
* **Use landscaping for protection.** Trees, boulders and gulleys can hide the building from passing cars, obscure security devices (like fences), and also help keep vehicles from getting too close. Oh, and they look nice too.
* **Keep a 100-foot buffer zone around the site.** Where landscaping does not protect the building from vehicles, use crash-proof barriers instead. Bollard planters are less conspicuous and more attractive than other devices.

Data Center & Operations Audit

Physical Security and Access Control

* **Use retractable crash barriers at vehicle entry points.** Control access to the parking lot and loading dock with a staffed guard station that operates the retractable bollards. Use a raised gate and a green light as visual cues that the bollards are down and the driver can go forward. In situations when extra security is needed, have the barriers left up by default, and lowered only when someone has permission to pass through.
* **Plan for bomb detection.** For data centers that are especially sensitive or likely targets, have guards use mirrors to check underneath vehicles for explosives, or provide portable bomb-sniffing devices. You can respond to a raised threat by increasing the number of vehicles you check perhaps by checking employee vehicles as well as visitors and delivery trucks.
* **Limit entry points.** Control access to the building by establishing one main entrance, plus a back one for the loading dock. This keeps costs down too.

Data Center & Operations Audit

Physical Security and Access Control

* **Make fire doors exit only.** For exits required by fire codes, install doors that don't have handles on the outside. When any of these doors is opened, a loud alarm should sound and trigger a response from the security command center.
* **Use plenty of cameras.** Surveillance cameras should be installed around the perimeter of the building, at all entrances and exits, and at every access point throughout the building. A combination of motion-detection devices, low-light cameras, pan-tilt-zoom cameras and standard fixed cameras is ideal. Footage should be digitally recorded and stored offsite.
* **Protect the building's machinery.** Keep the mechanical area of the building, which houses environmental systems and uninterruptible power supplies, strictly off limits. If generators are outside, use concrete walls to secure the area. For both areas, make sure all contractors and repair crews are accompanied by an employee at all times.

Data Center & Operations Audit

Physical Security and Access Control

* **Plan for secure air handling.** Make sure the heating, ventilating and air-conditioning systems can be set to recirculate air rather than drawing in air from the outside. This could help protect people and equipment if there were some kind of biological or chemical attack or heavy smoke spreading from a nearby fire. For added security, put devices in place to monitor the air for chemical, biological or radiological contaminant.
* **Ensure nothing can hide in the walls and ceilings.** In secure areas of the data center, make sure internal walls run from the slab ceiling all the way to subflooring where wiring is typically housed. Also make sure drop-down ceilings don't provide hidden access points.
* **Use two-factor authentication.** Biometric identification is becoming standard for access to sensitive areas of data centers, with hand geometry or fingerprint scanners usually considered less invasive than retinal scanning. In other areas, you may be able to get away with less-expensive access cards.

Data Center & Operations Audit

Physical Security and Access Control

- **Harden the core with security layers.** Anyone entering the most secure part of the data center will have been authenticated at least three times, including:
  - At the outer door. Don't forget you'll need a way for visitors to buzz the front desk.
  - At the inner door. Separates visitor area from general employee area.
  - At the entrance to the "data" part of the data center. Typically, this is the layer that has the strictest "positive control," meaning no piggybacking allowed.
    - A floor-to-ceiling turnstile. If someone tries to sneak in behind an authenticated user, the door gently revolves in the reverse direction. (In case of a fire, the walls of the turnstile flatten to allow quick egress.)
    - A "mantrap." Provides alternate access for equipment and for persons with disabilities. This consists of two separate doors with an airlock in between. Only one door can be opened at a time, and authentication is needed for both doors.
  - At the door to an individual computer processing room. This is for the room where actual servers, mainframes or other critical IT equipment is located. Provide access only on an as-needed basis, and segment these rooms as much as possible in order to control and track access.

Data Center & Operations Audit

Physical Security and Access Control

* **Watch the exits too.** Monitor entrance and exit—not only for the main facility but for more sensitive areas of the facility as well. It'll help you keep track of who was where when. It also helps with building evacuation if there's a fire.
* **Prohibit food in the computer rooms.** Provide a common area where people can eat without getting food on computer equipment.
* Install visitor rest rooms. Make sure to include bathrooms for use by visitors and delivery people who don't have access to the secure parts of the building.

    * Source: csoonline.com **19 Ways to Build Physical Security into a Data Center**

Data Center & Operations Audit

Data Center & Operations Audit

* Facility Based Controls:
  * Access Control Systems
    * Security Booth
    * ID Check (Card-key, Biometric)
    * Turnstile & Man Trap
    * Visitors (?)
  * Alarm Systems
    * Burglar Alarm
    * Fire Alarm
    * Water Alarm
    * Humidity Alarm
    * Power Fluctuation Alarm
    * Chemical or Gas Alarm
  * Tools used to send alerts: e.g. WatchDog

Data Center & Operations Audit

* Facility Based Controls:
  * Fire Suppression Systems
    * Water Based System (Wet-pipe, Dry-pipe,)
    * Gas Based System (Halon vs. FM200)
  * Power
    * Redundant Power Feeds (connect to more than one power grid)
    * Ground to Earth (to carry power away from critical equipment during fault condition)
    * Power Conditioning (to flatten out harmful spike and sags in current)
    * Battery Backups
    * Power Generator

Data Center & Operations Audit

* Facility Based Controls:
  * HVAC
    * Heating
    * Ventilation
    * Air Condition
  * Capacity and Redundancy
  * Monitoring
  * Network Connectivity
    * Redundant Internet and WAN connections using different carriers
  * Lease and Contract – Renew and Expiration

Data Center & Operations Audit

* Threats to Data Centers
  * Natural Disaster (flooding, earthquakes, fire)
  * Man-Made Threats (terrorist attack, riot, theft)
  * Environmental Hazards (heat or humidity)
  * Loss of utilities (Black out, Brown out)

* Auditor's Concerns
  * Physical Access Control (Preventive & Detective)
  * System and Facility Monitoring
  * Equipment Maintenance Record (HVAC, UPS, Generator, etc.)
  * Emergency Responding

Data Center & Operations Audit

* Data Center Operations
  * Roles and Responsibilities
  * Segregation of Duties
    * E.g. developers vs. Operations
  * Capacity Planning and Monitoring
  * Emergency Procedures to address reasonably anticipated threats (DR/BCP)
  * Training and Education of Data Center Personnel
  * Information Asset Disposal

IT Operations

Understanding IT Operation Environment

* Hardware Inventory
* Software Inventory
* Network Topologies and Diagrams
* Data Flow and Business Processes Diagrams
* IT Operation Strategy

FFIEC IT Examination Ops Handbook (pg. 5 -6)

IT Operations

Risk Assessment

* Internal and external risks
  * Improper implementation and deployment
  * Lack of capacity planning
  * Interdependency issues
  * Security breach
* Risks associated with individual platforms, systems and processes
* The quality and quantity of controls
  * Policies and procedures
  * Environmental controls
  * Preventive maintenance
  * Physical security
  * Logical security
  * Change management
  * Information controls
  * User Support/help desk
  * Job scheduling
  * Event management, etc.

FFIEC IT Examination Ops Handbook (pg. 10 -27)

IT Operations

Risk Monitoring and Reporting

* Performance Monitoring
* Capacity Planning
* Control Self-Assessment

FFIEC IT Examination Ops Handbook (pg. 27, 29)

Sample Control Objectives and Testing Procedures

* Define the audit scope
* IT operations oversight
* Board and senior management's risk appetite
* Understanding the IT Ops environment
* Access the controls that mitigate the Ops risks
* HR
* Data storage and backup
* Telecommunication
* Program management program

FFIEC IT Examination Ops Handbook (pg. 29, 35)