Chad Ballay

CIS411-342N

Assignment 6-1

For this assignment I’ll approach this sequentially and as a set of imperative statements. Based on the writeup much of this will be items that they will have to implement and not items they have in place already.

**Chapter 3 - Audititing Entity-Level Controls, Step #14**

*Review and evaluate controls over remote access into the company’s network (such as VPN and dedicated external connections).*

* Vendors are allowed access to the site and computers without authorization or supervision.
* The network sits behind a gateway router and firewall. Antivirus is in use, but is not automatically updated across the company. Employees often work remotely and only use their login and password to gain access to the corporate systems.
* Each office has its own, decentralized wireless network connected to the production network.
* Password resets are done by giving out a generic password — *Chiefs2011*

Review the userid generation process. Establish that all users are given their own unique userid for access. Any multi user system accounts shall be flagged for review.

Review the password controls. Establish that aging, complexity, and reuse rules are in place. Test this by monitoring or intentionaly triggering these conditions to be attempted.

Review the remote access request process. By default accounts should not be given remote access. Establish this request process if it doesn’t exist.

Review communications around compromised access procedures and audit that they are periodically sent out and acknowledgement is required.

Establish that credentials can be revoked by request.

Establish that existing and new remote accounts are tied to internal employee as the owner. In the case of a vendor account this should be tied to budget line holder as the delegated owner.

Establish a yearly audit cycle for these accounts where the owner acknowledges the existence and the continuing need for these accounts.

Document the infrastructure in place for these connections. Establish a periodic review process to establish deficiencies in the tech stack.

**Chapter 5 – Auditing Data Centers and Disaster Recovery, Step #2**

*Research the data center location for environmental hazards and to determine the distance to emergency services.*

* The main office is located in a suburb neighborhood where physical security is not considered a concern.
* Recently, a number of PCs and office equipment has been stolen out of the office.
* There are 20 Windows 2008 servers in the main office, twelve of which are virtualized on three physical servers.

NOTE: The fact that they only reference the main site as being safe and that all sites contain hardware leads me to believe that the other sites are less safe. Since they all contain critical IT infrastructure they get rounded up into classified as data centers for some features.

Establish the annualized flood likelihood using FEMA for each of the four locations.

Within each location identify the nearest water sources such as bathrooms, sinks, fountains, pipes.

If able, migrate server hardware to rack mounted systems and elevate them as high as able to.

Establish the yearly process for reviewing a geolocation’s natural hazards.

Establish yearly process for surveying area around each site for environmental hazards. (Industrial site, transportation interchanges, socioeconomic indicators trend changes…)

For each of the hazards identified in the yearly review, establish likely emergency service response needed. Review contact mechanisms, establish expected response times, identify likely response levels. Create documentation for each site and replicate across all sites.

Review that multiple locked doors control physical access to datacenter rooms. If able the only physical access should be with user authentication either through electronic badge, biometric sensor, or some other multifactor authentication beyond physical key.

Identify if security gaurds are present and if so their shift logs should be audited routinely.

Routine audits of CCTV cameras of the door and inside the data center should be performed. These videos should have short duration at rest within Dalton Walton & Carlton before shipping to offsite, thirdparty vendor.