Chad Ballay

[CIS411-342N](https://cyberactive.bellevue.edu/webapps/blackboard/execute/courseMain?course_id=_493170_1)

Assigment 8

June 16th, 2020

**Chapter 13 - Auditing Virtualized Environments**

* *Evaluate the use of baseline templates and the security of guest virtual machines as appropriate to the scope of the audit.*

Identify the job roles of the IT staff that have Virtualization responsibilities. Alignment within this subset of employees will ensure that consistency in policy enforcement will be done.

Identify list of all Hypervisors from scanning network or from existing IT asset list.

For each Hypervisor establish the allowable mechanisms for building a system. Identify if the hypervisor software allows for administrator established limitations for allowable base image repositories.

Document the existing standard procedures used for building virtual machines. (If none then this deficiency will have to be addressed by Director level ownership.)

Every virtual machine must be built using an automated and repeatable process and gaps from this standard will be documented in detail.

The virtual machine lifecycle will be documented for identifying what is the standard operating procedures for rebuilding an existing virtual machine. (Care on whether an out of date image is selected and upgraded in place or if an updated image is selected.)

A recommendation should be made to strongly adopt Infrastructure As Code best practices.

**Chapter 16 - Auditing Cloud Computing and Outsourced Operations**

* *Review and evaluate the vendor’s physical security.*

Identify datacenter locations that cloud provider maintains that would be in scope for your business operations.

Within allowance from your vendor agreement, you will have to evaluate many details of their physical locations. If they are unwilling to allow onsite validation then proceed with evaluating the third party audit process for the following items.

Access to secure areas should be through the use of multifactor authentication. Badge reader, biometric scanner, keypad, etc…

Access to grounds of datacenter should incorporate layers of defense beginning with physical barriers like fences, no unmonitored building access, validated secure area access.

Physical area around the datacenter should have clear boundaries that are free of obstruction.

Logs of access to site should be detailed as to allow to identify identities.

Periodic penetration tests should be performed by multiple service providers to establish a variety of approaches. These should be documented and analyzed for additional learnings as well as to share with clients.