Pick one of the audit steps from Chapter 9 (Auditing Web Servers and Applications) and two of the audit steps from Chapter 15 (Auditing Applications). Describe the audit step and how you would conduct it for the case study company. Include specific procedures for performing and validating the audit step and any expected results. The procedures you use should be in your own words and not copied from the book. You may make assumptions, but should document those assumptions in your report. If you use references outside of the book, please cite those.

Chad Ballay

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

Assigment 7-2

June 9th, 2020

**Chapter 9 - Auditing Web Servers and Web Applications**

* *Verify the validity of any server certificates in use.*

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

Identify list of all Web Servers from scanning network or from existing IT asset list. (Nmap)

Verify with the help of the Web Server Support admins that any certificates are valid, are being used for their intended purpose, and have not been revoked. Certificate date ranges, public key, and metadata all should be valid. Discuss the certificate expiration and renewal process.

-OR-

There are several thirdparty solutions that manage the certificate lifecycle/verification process that the business may be using one. If so then verify the above items are being done within the tools. (CWS, Venafi, Tennable, etc….)

The Web Server Support admins will document the reporting process for ensuring that existing certificates are verified regularly. This includes validation checks for rebuilds, os patches, new deployments, and other Web Servers lifecycle events. The work product is report that can be audited periodically by methodically checking a subset of desktops for compliance vs the reported compliance.

**Chapter 15 - Auditing Applications**

* *If the same data is kept in multiple databases and/or systems, ensure that periodic sync processes are executed to detect any inconsistencies in the data.*
* *Ensure that users are automatically logged off from the application after a certain period of inactivity.*

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

Identify Business Process owners for the application. Alignment within this subset of employees will offer validation for relevance of data or applications.

For all data in a given application, the Applications Support area will document where and how they source that data.

For each data item, the business will review the relevance and validity of the data. They will work with the Applications Support area to establish access the lifecyclef of this data to ensure that the data being accessed is the correct source of truth.

During the previous analysis steps these lifecycles will be tracked to establish when multiple single sources of truth exists and which would be the applicable one to use.

Application Support area will review applications and identify any login points to the system. For each of these login points automated test should be created that continuously validates the status. Any discrepancies will have to be researched.

The maximum account login timespan will be defined in a company policy. Individual applications the use a shared login will have to document an exception to the company policy.