CyberLaw and Cloud Security FINAL Practical

Practical Directions: To complete your final practical, you will be asked to address the compliance requirements for a particular scenario and let this influence on how you will assess risks and apply security in your cloud environment. For this practical, you will identify relevant security standards, deploy security capabilities, and assess your controls. You will then produce a security report based on the following instructions and requirements:

FINAL PART 1 (250 points) – Midterm Carryover

Taking into consideration, the recommendations you made to the bank in the midterm practical, the IT representative has decided to adopt your recommendations and include an OFAC check for all international and domestic wire transfer and ACH transactions. However, they decided to implement a custom, lower cost solution rather than subscribing to Jack Henry's solutions exclusively.

The bank selected a small product to perform the OFAC checks and manage the overall wire process due to cost and restrictions with Jack Henry. The design presented to you includes data and workload integration within the wire process. The solution will work for both FAIM and ISO wires which just recently went into effect on March 10, 2025. You advised against the complexity for security and resiliency purposes. However, the bank received an incentive from this Credit Union product company that is now designing solutions for small banks, CuTech.. The architecture diagram is presented to you and it includes sending data to the AWS CuTech private cloud instance set up for your client. The platform includes a custom landing zone hosting the CuTech application and a database. The process and data flow diagram are also presented to you. All FAIM and ISO wire data is included in the scope of the integration. Data will be sent bi-directionally to this new platform. You review the solution and determine that it may also require some security governance and are back on the clock.

Your client is now asking you to advise on how to best apply continuous security monitoring and assessments to this custom cloud platform. Your solution will be translated into business requirements and passed to CuTech for adoption. You research the problem and determine that the company should enable some core security services that allow the company to monitor the environment against select regulatory compliance requirements.

To complete this portion of the FINAL, you will identify the core security monitoring services to enable and identify any applicable security frameworks or conformance packs that should be adopted.

Ensure you add enough context so that your client and CuTech understand these. Your client bank is CuTech's first banking client so they will also benefit from your extraordinary intellect.

Format: Presentation

Content Requirements for full grading consideration.

1) List the service,
2) provide a description and how it benefits the use case
3) provide a high level overview of how this would be configured and implemented for the use case

4) provide a proposed shared responsibility model for these services between the bank and CuTech

Key considerations: What conformance/compliance monitoring should be enabled and how will findings be managed and resolved. What other security recommendations would you make?

FINAL PART 2 (500 points)

This is the cloud security portion of the FINAL. To complete this section you will perform the following in your personal cloud platform:

1) **Budget (100 points):** You will give a final budget report for the costs of the services for this class. This can be a one-page summary or a cloud native report.
2) **AWS Inspector (100 points):** You will identify 2 vulnerabilities and resolve them. The following is required to satisfy this section of the FINAL.
    a. Include a breakdown of the vulnerabilities you are targeting (CVE, score, severity, risk)
    b. Include your analysis for resolving these vulnerabilities (prioritization – why these first?, impact – what systems/services are affected if these not resolved? , efficiency – what is the expected level of effort to address these vulnerabilities?, recommendation – how do you recommend these vulnerabilities should be addressed?)
    c. Include a screenshot of the vulnerabilities prior to resolution
    d. Include a screenshot of the vulnerabilities after resolution
    e. Requirement: At least 2 vulnerabilities should be resolved for full credit.
3) **AWS Config (100 points):** You will identify 2 noncompliant rules and resolve them. The following is required to satisfy this section of the FINAL.
    a. Include a breakdown of the rules you are targeting (service, severity, risk)
    b. Include your analysis for remediating these rules (prioritization – why these first?, impact – what systems/services are affected if these not resolved? , efficiency – what is the expected level of effort to achieve compliance, recommendation – how do you recommend these compliance rules should be addressed?)
    c. Include a screenshot of the noncompliant rules prior to remediation
    d. Include a screenshot of the rules following remediation
    e. Requirement: At least 2 noncompliant rules should be resolved for full credit.
4) **AWS Security Hub (100 points):** You will identify 2 failed checks/control findings and resolve them. The following is required to satisfy this section of the FINAL.
    a. Include a breakdown of the control findings you are targeting (service, severity, risk)
    b. Include your analysis for remediating these control findings (prioritization – why these first?, impact – what systems/services are affected if these not resolved? , efficiency – what is the expected level of effort to achieve compliance, recommendation – how do you recommend these control findings should be addressed?)
    c. Include a screenshot of the failed security checks prior to remediation
    d. Include a screenshot of the passed security check s following remediation

    e. Requirement: At least 2 failed security checks should be resolved for full credit. You are not permitted to use resolved checks where scan automation was causing the failure. Only checks that resulted in a control finding.

5) **AWS Audit Manager (100 points):** You will identify 2 failed findings and resolve them. The following is required to satisfy this section of the FINAL.
    a. **Scope:** categories for findings that you may use for this portion of the practical include Compliance check and Configuration data findings. User activity and Manual are considered out of scope.
    b. Include a breakdown of the findings you are targeting (service, severity, risk)
    c. Include your analysis for remediating these findings (**integration** – what services does AWS Audit Manager use to evaluate these findings?, prioritization – why these first?, impact – what systems/services are affected if these not resolved? , efficiency – what is the expected level of effort to achieve compliance, recommendation – how do you recommend these findings should be addressed?)
    d. Include a screenshot of the noncompliant findings prior to remediation
    e. Include a screenshot of compliance following remediation
6) Requirement: At least 2 noncompliant findings should be resolved for full credit.

Suppression is not a valid resolution for any of the above sections.

OPTIONAL - FINAL PART 3 (250 bonus points)

This is a bonus cloud security portion of the FINAL. To complete this section you will perform the following in your personal cloud platform:

You will compliance monitoring in your personal cloud platform based ion the work you conducted in PART 1 of the FINAL. Once you have enabled the appropriate services/checks, you will perform the following for full grading consideration:

You will resolved one additional compliance violation in each of the following using the same approach to PART 2 of the FINAL. For credit, the noncompliant rule/finding/check MUST be unique to this use case. This means that it is NOT a finding for other conformance packs or pre-defined frameworks. To complete this portion of the exam, simply resolve 1 unique compliance findings for:

1) Security Hub (50 POINTS)
2) AWS Config (50 POINTS)
3) AWS Audit Manager (50 POINTS)

For Inspector extra credit, you will enable CIS scans and resolve 1 unique vulnerability/benchmark failure for full grading consideration.

TOTAL POSSIBLE POINTS with EXTRA CREDIT: 1000 points