

The Security Gauntlet - A Design Review Challenge

Assignment - 1

Syed Aquib R .

Security Fundamentals for Cloud

Table of Contents

[Detailed Instructions, Timelines, Deliverables & Grading: 2](#_Toc179493612)

[Objective: 2](#_Toc179493613)

[1. Teams & Assets: 2](#_Toc179493614)

[2. Role Assignments: 2](#_Toc179493615)

[3. Analyzing the System Design: 3](#_Toc179493616)

[4. Deliverables: 3](#_Toc179493617)

[A. Video Presentation (10-15 Minutes): 3](#_Toc179493618)

[B. Individual Reflection (1-2 Paragraphs): 4](#_Toc179493619)

[5. Timeline and Milestones: 4](#_Toc179493620)

[6. Tools and Resources: 4](#_Toc179493621)

[7. Grading Criteria - 20 Points: 4](#_Toc179493622)

[8. Peer Review: 5](#_Toc179493623)

# Detailed Instructions, Timelines, Deliverables & Grading:

## Objective:

In this group assignment, your team will critically evaluate a system design from a security perspective. Each team member will take on a specific role related to cloud security and analyze the system from that role’s perspective. The goal is to identify security risks, propose mitigations, and present your findings in a recorded video.

You will:

* Apply security principles to assess a cloud-based system design.
* Practice collaboration and communication to deliver a cohesive design review.
* Present your findings through a recorded video and engage in peer review.

## 1. Teams & Assets:

**(The list of Teams & Assets Distribution are attached separately)**

## 2. Role Assignments:

Each team member will take on a specialized role to focus on a specific area of cloud security during the review. Your role dictates your perspective and the specific security aspects you will need to evaluate in the system design.

**Core Roles** (every team will have these):

1. **Cloud Security Architect**: Evaluate the overall security strategy and architecture of the system. Focus on industry best practices, misconfigurations, and risk mitigation.
2. **Cloud DevOps Engineer**: Review the security of automation tools, CI/CD pipelines, and infrastructure-as-code. Focus on potential vulnerabilities in deployment scripts, configuration, and containers.
3. **Cloud Penetration Tester**: Approach the design with an attacker’s mindset. Identify weak points in the system that could be exploited, such as misconfigurations, privilege escalations, or unauthorized access.
4. **Cloud Compliance Officer**: Ensure the system complies with relevant regulations and data privacy standards (e.g., GDPR, HIPAA). Focus on legal and compliance risks.
5. **Research and Innovation Lead:** This student would be responsible for exploring new ideas, researching best practices, and identifying innovative approaches related to the project or topic. They would keep the team informed about the latest trends and potential improvements. This role encourages critical thinking and staying up-to-date with advancements in the field.

**Specialized Roles** (teams will have one or more of these):

1. **Identity and Access Management (IAM) Specialist**: Focus on authentication and authorization policies. Evaluate user provisioning, privilege escalation risks, and identity federation mechanisms.
2. **Data Protection Officer**: Review data encryption, data loss prevention, and data classification. Ensure the system protects data from unauthorized access or misuse.
3. **Incident Response Specialist**: Analyze the design’s incident detection and response capabilities. Ensure logging, monitoring, and alerting are sufficient to handle potential breaches.
4. **Cloud Network Security Engineer**: Review the system’s network security, focusing on firewalls, segmentation, and traffic filtering. Ensure the network is adequately secured.
5. **Documentation and Reporting Specialist:** This student would be in charge of documenting the project's progress, methodologies, findings, and any challenges encountered. They would also be responsible for compiling reports and ensuring that all relevant information is clearly and accurately recorded. This role emphasizes organization, attention to detail, and clear communication through writing.

## 3. Analyzing the System Design:

Once roles are assigned, your task is to analyze the system based on your role. Consider the following when reviewing the system:

* **What are the main security risks or vulnerabilities** in the system related to your role?
* **How could these risks be exploited**? (For example, as the Penetration Tester, think like an attacker.)
* **What mitigation strategies** can be applied to resolve these issues or reduce risk?
* **How does the system** adhere to or deviate from cloud security best practices (e.g., CIS Benchmarks, NIST CSF)?
* **Are there any regulatory compliance concerns** based on the nature of the system (e.g., handling personal data)?

## 4. Deliverables:

### A. Video Presentation (10-15 Minutes):

Your team will submit a recorded video presenting your security analysis. The video should be clear and professional, covering the following sections:

1. **Introduction**:
   * Introduce the system and briefly explain the context (assets you are evaluating).
   * Give a high-level overview of the system's security posture.
2. **Role-Specific Analysis** (Focus on Security Risks and Mitigations):
   * Each team member will present their analysis based on their assigned role.
   * For each role, describe the potential risks, vulnerabilities, and improvements.
   * Provide evidence from the design assets to support your analysis.
3. **Suggested Security Improvements**:
   * Summarize the main areas for improvement based on the findings from each role.
   * Highlight practical strategies for making the system more secure.
4. **Conclusion**:
   * Reflect on the team's overall findings and the importance of a secure design in cloud systems.

### B. Individual Reflection (1-2 Paragraphs):

Each team member must submit a short reflection on their contribution to the project. Address the following:

* **What you learned** about your specific area of cloud security.
* **How your role contributed** to the overall security of the system.
* **Challenges** you faced during the assignment.

## 5. Timeline and Milestones:

To ensure timely progress, I have outlined specific deadlines for your team:

* **Week 1 (7th to 13th Apr)**: Asset and role assignment completed. Start your research and initial analysis.
* **Week 2 (14th to 20th Apr)**: Draft security findings for your role submitted to the group. Use this week for team discussions and collaboration.
* **Week 3 (21st to 27th Apr)**: Peer review session. During this session, you will watch and provide feedback on team’s video.
* **Week 4 (28th to 4th May)**: Final video presentation submitted by **3rd May 2025**.

## 6. Tools and Resources:

* **Collaboration Tools**: Use shared documents (e.g., Google Docs, Microsoft OneDrive) to collaborate on your analysis and presentation.
* **Presentation Tools**: You can use any video recording tool (e.g., PowerPoint with recording, & Microsoft Teams) to create your video.
* **Reference Materials**: Use cloud security best practices, compliance frameworks (e.g., NIST CSF, GDPR), and class materials to inform your analysis.

## 7. Grading Criteria - 20 Points:

Your assignment will be graded on the following:

1. **Understanding of Security Principles (35% - 7 points)**: Did the team demonstrate a solid understanding of security risks and best practices based on their assigned roles?
2. **Critical Thinking and Analysis (25% - 5 points)**: Did the analysis reflect depth, considering both obvious and less visible vulnerabilities? Were mitigation strategies well-reasoned?
3. **Presentation Quality (20% - 4 points)**: Was the presentation clear, professional, and well-organized? Did each team member contribute effectively?
4. **Collaboration and Teamwork (10% - 2 points)**: How well did the team work together? Was there a cohesive flow to the presentation?
5. **Reflection (10% - 2 points)**: Did each individual provide thoughtful reflections on their learning and contribution?

## 8. Peer Review:

After the video submissions, each team will review their team's video. You are expected to:

* Watch the video in its entirety.
* Provide constructive feedback based on the clarity, depth of analysis, and suggested improvements.