Project Title: SecureCloud: End-to-End Cloud Security Implementation on GCP

1. Project Overview

Students will assume the role of a **Cloud Security Analyst** for a fictitious mid‑sized e‑commerce startup, **ShopNimbus**, migrating its web application and data services to Google Cloud Platform (GCP). Over 5 weeks, teams will design, implement, test, and document a comprehensive security posture applying all beginner‑level skills from the Google Cloud Cybersecurity Certificate.

2. Learning Objectives

1. **Apply foundational security principles** (confidentiality, integrity, availability) to cloud resources.
2. **Assess and manage risk** through threat modeling and control selection.
3. **Identify and mitigate common cloud threats** using IAM, VPC, and security scanning tools.
4. **Simulate incident detection & response** with Cloud Logging, Security Command Center, and automated alerting.
5. **Produce professional deliverables** (security design doc, incident report, readiness checklist) for a Cloud Security Analyst interview.

3. Project Scenario & Requirements

- **Background**: ShopNimbus offers an online store (Compute Engine + Cloud SQL) and a file‑sharing API (Cloud Storage + Cloud Functions). They require a secure, compliant deployment in us-central1.
- **Key Requirements**:
  - Enforce least‑privilege with IAM roles & service accounts.
  - Segment network tiers (public web tier, application tier, database tier).
  - Encrypt data at rest and in transit.
  - Implement automated vulnerability scanning and centralized logging.
  - Design an incident response plan with playbooks and notifications.

4. Project Breakdown by Module

Week	Module Covered	Deliverables
1	Introduction to Security Principles in Cloud Computing	- **Security Architecture Diagram** showing CIA triad controls - **Design Rationale** (1‑page)

2	Strategies for Cloud Security Risk Management	- **Risk Register**: identify ≥8 risks with likelihood & impact scores - **Mitigation Plan**
3	Cloud Security Risks: Identify and Protect Against Threats	- **IAM Policy Document**: custom roles & service account hierarchy - **Firewall Rules List**
4	Detect, Respond, and Recover from Cloud Cybersecurity Attacks	- **Logging & Monitoring Implementation**: Cloud Logging sinks, alerts - **Incident Playbook**
5	Put It All Together: Prepare for a Cloud Security Analyst Job	- **Final Report**: architecture, risk treatment, incident response - **Mock Interview Slides** (5 slides)

5. Detailed Task List

Week 1: Security Principles

1. **Draw** a 3-tier GCP architecture for ShopNimbus.
2. **Annotate** how each component meets Confidentiality, Integrity, Availability.
3. **Write** a 1-page justification of design choices.

Week 2: Risk Management

1. **Conduct** a mini threat modeling session (STRIDE) on your diagram.
2. **Populate** a risk register: risk description, likelihood (1–5), impact (1–5), overall score.
3. **Assign** controls: preventive, detective, corrective.

Week 3: Threat Identification & Protection

1. **Define** IAM roles: choose from predefined roles or create custom ones for Web Server, DB Admin, Security Auditor.
2. **Configure** Service Accounts with minimal scopes.
3. **Implement** VPC firewall rules: allow only HTTPS (TCP 443) to web tier; internal-only access to DB.
4. **Document** all policies in a readable table.

Week 4: Detection, Response & Recovery

1. **Enable** Cloud Logging and set up log sinks (e.g., to BigQuery).

2. **Create** Security Command Center findings for misconfigurations.
3. **Set up** an alerting policy in Cloud Monitoring to email or Pub/Sub on high‑severity events (e.g., repeated failed SSH).
4. **Draft** an incident response playbook: identification, containment, eradication, recovery, lessons‑learned.

Finally: Synthesis & Presentation

1. **Compile** a professional‑quality Final Report (max 10 pages) covering:
   - Architecture & security controls
   - Risk register & mitigation status
   - Monitoring & incident response procedures
2. **Prepare** a 5‑slide "Mock Interview" deck: highlight your role, key achievements, and how you'd answer typical interview questions about your project.
3. **Peer‑review** another team's report and provide constructive feedback.

6. Tools & Resources

- **GCP Free Tier** (Compute Engine, Cloud SQL, Cloud Functions, Cloud Storage)
- **Cloud Shell** & **Terraform** (optional) for IaC
- **Security Command Center**, **Cloud Logging**, **Cloud Monitoring**
- **Cloud IAM**, **VPC**, **Firewall Rules**, **KMS**
- **Risk Register Template** (provided as spreadsheet)
- **STRIDE Worksheet** (provided)

7. Evaluation Criteria

Criterion	**Weight**	**Description**
Design & Documentation	30%	Clarity of architecture diagram; thoroughness of design rationale
Risk Management	20%	Completeness & accuracy of risk register; feasibility of controls
Implementation Quality	25%	Correctness of IAM, firewall, logging, alerting configurations
Incident Response Plan	15%	Realism & clarity of playbook; coverage of all IR phases

Professionalism & Presentation	10%	Quality of final report and mock-interview slides

8. Timeline & Team Roles

- **Team Size**: 3–4 members
- **Milestones**: Deliverables due at end of each week (Sunday by 11:59 PM WAT)
- **Roles** (rotate weekly):
  - **Project Lead**: coordinates tasks, ensures deadlines
  - **Architect**: leads diagramming & design rationale
  - **Security Engineer**: implements IAM & network controls
  - **Monitoring Lead**: sets up logging, alerts, IR playbook

9. Submission & Presentation

- **Submit** via shared GitHub repo
- **Present** in a 15-minute demo session: live walkthrough of your secure environment + Q&A.