COLLEGE OF CREATIVE INNOVATION

Programme

Diploma in Cloud Computing and Cyber Security
(120 Credits)

Course

CCC603: Cyber Security in Cloud
(Level 6, 30 Credits, Version 1.1)

Assessment Title

Practical Demonstration
(AWS Certified Security SCS-C02)
CCC603 | Assessment-5
(Individual Assesmsent)

Weighting within the course

50%

Objective:

The objective of this assessment is to demonstrate your ability to design, configure, and secure a cloud-based network architecture on AWS using best practices for cybersecurity and network security. You will implement services such as **Amazon VPC, EC2, Security Groups, Virtual Private Gateway, Customer Gateway, and Site-to-Site VPN, along with Libreswan for IPsec tunnelling,** to establish secure private connectivity between two AWS regions. By configuring, testing, and reflecting on the setup, you will showcase how AWS services can be used to replace traditional on-premises VPN hardware and deliver a resilient, encrypted communication channel between organisational networks.

Course Learning Outcomes (LOs) covered:

LO1: Implement robust cybersecurity measures within cloud computing environments to manage risks and preserve the safety and privacy of organisational assets.

LO2: Assess industry best practices when implementing organizational solutions for network security.

Qualification Graduate Profile Outcomes (GPOs) covered:

GPO3: Investigate and implement advanced network security solutions to protect and secure assets, troubleshoot, and mitigate threats and attacks, and to meet best practice and organisational requirements.

Assessment Tasks to Learning Outcome and GPOs Mapping:

LO	GPO	Task	Task Component	Weighting
LO 1	GPO3	**Task 1:** Secure VPC Setup and Architectural Design	**Activity 1.1:** Set up two isolated VPCs for SecureBank in Sydney (Organisation VPC) and Singapore (Customer VPC) with secure network configurations. **Activity 1.2:** Architectural Diagram Design	25%
LO 2	GPO3	**Task 2:** VPN Tunnel Configuration	**Activity 2.1:** Create VPN Gateways and Site-to-Site VPN **Activity 2.2:** Configure VPN on Singapore EC2	25%
LO 1	GPO3	**Task 3:** Secure Connectivity Testing	**Activity 3.1:** Step-by-Step Guide for Testing VPN Connectivity	25%
LO 1, LO2	GPO3	**Task 4:** Risk Mitigation, Best Practices & Report	**Activity 4.1:** Prepare a comprehensive technical report analysing the security, risk mitigation, and compliance considerations of the VPN deployment.	25%
			Total	100%

Recommended Tasks Completion Timeline:

Full Time Week	Part Time	Progress	Submission
Week 17	Week 33,34	Start working on the Assessment	
Week 18	Week 35,36	Complete Task 1, Task 2	
Week 19	Week 37,38	Complete Task 3	
Week 20	Week 39,40	Complete Task 4 and submit	Assessment due by Week 20 (Full Time) Assessment due by Week 40 (Part Time)

Grading:

The final grade will be determined by the score achieved in this assessment based on the following table. Should a second or third attempt be required, the maximum contribution toward the overall mark for the tasks that required a second or third assessment attempt is 50%. **A late submission is considered a second attempt, so the contribution will be capped at 50%.**

To pass this assessment, you must meet the requirements of each of the learning outcomes (irrespective of the numerical grade awarded).

Grade	Range
A	Meet all course requirements, range (80—100%)
B	Meet all course requirements, range (65—79%)
C	Meet all course requirements, range (50—64%)
D	Did not meet all course requirements, range (40—49%)
E	Did not meet all course requirements, mark range (0—39%)

Candidate's Assessment Instructions:

- This assessment is an **open-book activity**; you can use your course and review notes, and offline or online resources, such as textbooks or online journals.
- You can always ask your online tutor if you need further explanation if the instructions are unclear.
- Your work should not be plagiarised. Plagiarism includes copying material without acknowledging it, copying from another student, getting another person to help you with your assessment, using material from commercial essays or assignment services, or using AI to create the answers.
- The purpose of this assessment is to assess your knowledge. In the event Yoobee suspects collusion, this will be addressed. For more information on plagiarism, please refer to the Student Handbook.
- Submit your completed assessment online in the correct space provided.
- Marks and feedback will be returned within **15 working days** of the submission date.
- By completing and submitting an assessment, you are authenticating that the work is original and does not violate plagiarism or copyright law. Authenticity is checked where any breaches of academic integrity are suspected. Please refer to the Student Handbook for further information.

Submission Instructions:

Submit **one PDF report** document to the LMS by the specified due date.

Your report should:

- Include your name and ID number
- Include the AWS account login details, a cover page, and a report index for verification purposes in your report.
- Use a standard citation format if external sources are referenced.
- Clearly label tasks and subtasks, and Diagrams must be clear and labeled properly.
- Include screenshots of each practical step in sequence, naming and numbering the screenshots. Screenshots must display the relevant settings or outputs for each step.
- Include your answers to the assessment questions for each task, describing choices, configurations, and learned insights with an appropriate practical and theoretical understanding.
- Submission must be in PDF format only because other formats may cause issues with accessing screenshots.

Assessment Tasks: Scenario-Based Activity Design and Implementation (AWS)

Scenario:

You are working as a Cloud Security Engineer at **SecureBank Ltd,** a financial services company that needs to connect its head office VPC in Sydney (Organisation VPC) with its partner branch in Singapore (Customer VPC). For compliance and security, the connection must be private, encrypted, and follow best practices in line with industry standards.

Your task is to design, implement, and secure a **Site-to-Site VPN** between the two environments and demonstrate secure communication between the systems.

Note: Both your written report and task-specific explanations must comply **with APA style formatting requirements,** including accurate in-text citations and a complete reference list.

Task 1: Secure VPC Setup & Architectural Design (25%)

Activity 1.1: Set up two isolated VPCs for SecureBank in Sydney (Organisation VPC) and Singapore (Customer VPC) with secure network configurations.

- Create two VPCs:
    - SecureBank-Sydney-VPC (Organisation VPC)
    - SecureBank-Singapore-VPC (Customer VPC)
- Configure subnets, Internet Gateways, and Route Tables for each VPC.
- Launch EC2 Linux instances in both VPCs.
- Restrict access with security groups (least-privilege principle).

Activity 1.2: Architectural Diagram Design

- Design an architectural diagram of the SecureBank Site-to-Site setup showing:
    - Both VPCs (CIDR ranges)
    - Subnets, EC2 instances
    - VPN gateways (VGW, CGW)
    - Site-to-Site VPN tunnel

Deliverables:

- Detailed Step-by-Step Guide for Practical Implementation
- Screenshots of VPC setup, subnets, EC2, security group rules Include any additional screenshots that effectively demonstrate your outcomes.
- Your own well-labeled AWS architectural diagram of the solution.
- Brief explanation of how this design protects SecureBank assets in Minimum **500-word** limit **(+/- 10%)** allowed.

Task 2: VPN Tunnel Configuration (25%)

Activity 2.1: Create VPN Gateways and Site-to-Site VPN

- In Sydney VPC, create a Virtual Private Gateway (VGW).
- Identify the region and create a Customer Gateway (CGW).
- Configure a Site-to-Site VPN connection between gateways.

Activity 2.2: Configure VPN on Singapore EC2

- On Singapore EC2, install and configure Libreswan or any Linux EC2 for IPsec (edit ipsec.conf, aws-vpn.conf, aws-vpn. Secrets) as per VPN configuration file.
- vpn.conf file sample cmd’s

```
conn Tunnel1
  authby=secret
  auto=start
  left=%defaultroute # Assuming this is your local subnet, replace if needed
  leftid= As per your practical implementation
  right= As per your practical implementation
  type=tunnel
  ikelifetime=8h
  keylife=1h
  # Consider stronger options if supported by both sides:
  # phase2alg=aes256-gcm-sha256
  # ike=aes256-gcm-sha256
  # keyingtries=%forever
  keyexchange=ike
  leftsubnet= As per your practical implementation
  rightsubnet= As per your practical implementation
  dpddelay=10
  dpdtimeout=30
  dpdaction=restart_by_peer
```

Deliverables:

- Detailed Step-by-Step Guide for Practical Implementation
- Screenshot of VPN tunnel “UP” in AWS console, EC2, include any additional screenshots that effectively demonstrate your outcomes.
- Explanation of encryption methods (AES, IKE), Multiple Tunnelling and why they meet industry best practices in Minimum **500-word** limit **(+/- 10%)** allowed.

Task 3: Secure Connectivity Testing (25%)

Activity 3.1: Step-by-Step Guide for Testing VPN Connectivity

- Detailed Step-by-Step Guide for Practical Implementation
- From Sydney EC2, connect to Singapore EC2 using its private IP over VPN tunnel.
- Upload Singapore EC2’s private key file securely (e.g., WinSCP).
- Verify SSH access works only via private IP, not public IP.

Deliverables:

- Detailed Step-by-Step Guide for Practical Implementation
- Screenshot of SSH session over VPN tunnel and include any additional screenshots that effectively demonstrate your outcomes.
- Explain why SecureBank uses private IP communication for enhanced security in Minimum **500-word** limit **(+/- 10%)** allowed.

Task-4: Risk Mitigation, Best Practices & Report (25%)

Activity 4.1: Prepare a comprehensive technical report analysing the security, risk mitigation, and compliance considerations of the VPN deployment. The report should focus on managing risks and ensuring the safety and privacy of organizational assets.

The report must cover the following sections:

1. **Risk Identification**
   - Identify and describe at least three potential risks associated with the VPN setup.
     Examples include:
     - Weak or outdated encryption protocols
     - Exposed or leaked encryption keys
     - Routing misconfigurations or insecure traffic paths

2. **Mitigation Recommendations**
    - Provide actionable recommendations to address each identified risk.
      Examples include:
        - Implementing stronger ciphers and secure key management
        - Utilizing AWS CloudWatch for monitoring VPN health and anomalies
        - Enforcing IAM least-privilege policies for access control
3. **Alignment with Compliance Standards**
    - Explain how the VPN configuration aligns with recognized security frameworks and compliance standards, such as:
        - AWS Well-Architected Security Pillar
        - CIS Benchmarks
        - NIST Cybersecurity Framework
        - PCI-DSS requirements
4. **Summary of AWS Services Utilized**
    - Outline the AWS services leveraged to implement and secure the VPN, including:
        - VPC, Subnets, and EC2 instances
        - Virtual and Customer Gateways (VGW, CGW)
        - Site-to-Site VPN connections
        - Security Groups and IAM roles/policies
        - CloudWatch monitoring and alerts
5. **Architectural Diagram Reuse/Refinement**
    - Integrate and refine the diagram from Task 1 to visually demonstrate the secure VPN architecture, highlighting the placement of security controls and monitoring tools.

Deliverables:

- Well-structured written report in Minimum **1500-word** limit **(+/- 10%)**
- Clear mapping of AWS services used in the project

Marking Rubric

To pass this assessment, you must meet the requirements of each of the learning outcomes (irrespective of the numerical grade awarded).

Criterion		Evidence				
Task and Weightage		**A (80-100%)**	**B (65-79%)**	**C (50-64%)**	**D (40-49%)**	**E (0-39%**
Task 1: (LO1) Secure VPC Setup and Architectural Design **(25%)**	**Activity 1.1:** Set up two isolated VPCs for SecureBank in Sydney (Organisation VPC) and Singapore (Customer VPC) with secure network configurations. **Activity 1.2:** Architectural Diagram Design	Both VPCs correctly created with proper CIDR blocks; subnets, route tables, and IGWs correctly configured; EC2 instances launched; security groups follow least-privilege. clear, accurate architectural diagram with all components shown.	Most VPC components correctly created; minor misconfigurations in subnets, route tables, or security groups; EC2 instances mostly functional. Diagram mostly correct but minor omissions.	VPCs and subnets partially configured; some EC2 instances or security groups misconfigured Diagram incomplete or unclear.	Major misconfigurations in VPCs, subnets, or EC2; security groups not restrictive. Diagram missing or inaccurate.	VPC setup largely missing or incorrect; EC2 instances not launched. Or Incompelte Task. Diagram absent. Or Incompelte Task.
Task 2:(LO2) VPN Tunnel Configuration **(25%)**	**Activity 2.1:** Create VPN Gateways and Site-to-Site VPN **Activity 2.2:** Configure VPN on Singapore EC2	VGW and CGW correctly configured; Site-to-Site VPN connection established. EC2 VPN configuration correct; VPN tunnel shows “UP”; clear explanation of encryption, IKE, and multiple tunnels; meets best practices.	VPN connection mostly configured; minor errors in EC2 IPsec setup; tunnel “UP” but minor inconsistencies. Explanation mostly clear but missing some details	VPN partially configured; EC2 IPsec setup has errors. Tunnel may not show fully active; explanation incomplete.	VPN setup incomplete or mostly incorrect. Tunnel down; explanation lacks technical accuracy	VPN not configured; EC2 not set up. Or Incompelte Task. No functional VPN connection or explanation. Or Incompelte Task.
Task 3:(LO1) Secure Connectivity Testing **(25%)**	**Activity 3.1:** Step-by-Step Guide for Testing VPN Connectivity	Sydney EC2 connects to Singapore EC2 via private IP; SSH works; public IP access blocked; private key securely transferred; screenshots included detailed explanation of private IP usage and security.	Connectivity mostly successful; minor errors in SSH or key handling; screenshots included explanation mostly clear.	Partial connectivity; SSH may fail or use public IP; explanation incomplete; screenshots limited.	Connectivity mostly fails; private IP not used; screenshots missing; explanation inaccurate.	No testing done. no screenshots. no explanation. Or Incompelte Task.

Criterion		Evidence				
Task and Weightage		**A (80-100%)**	**B (65-79%)**	**C (50-64%)**	**D (40-49%)**	**E (0-39%**
Task 4: (LO1) (LO2) Risk Mitigation, Best Practices & Report **(25%)**	**Activity 4.1:** Prepare a comprehensive technical report analysing the security, risk mitigation, and compliance considerations of the VPN deployment.	Comprehensive technical report; identifies multiple risks; actionable mitigation recommendations; aligns with compliance standards; AWS services clearly mapped; refined architectural diagram included report well-structured, APA-compliant.	Report mostly complete; identifies some risks; mitigation suggestions mostly appropriate; compliance discussed; diagram present but minor omissions; APA mostly correct.	Report partially complete; few risks identified; mitigation vague; compliance discussion limited; diagram incomplete; APA issues present.	Report incomplete; minimal risk analysis; mitigation missing or unclear; compliance not addressed; diagram missing; APA issues significant.	Report largely missing; no risk analysis; mitigation absent; compliance not addressed; diagram absent; APA not followed. Or Incompelte Task.