al-nafi INTERNATIONAL COLLEGE

Diploma in

SYSOPS AND CLOUD ADVANCEMENT

Pearson

Endorsed by EduQual UK

ISACA Accredited Partner

EADL European Association for Distance Learning

Table of Contents

About the Diploma

The SysOps and Cloud Development Diploma is designed to provide hands-on training and practical expertise to learners in their job roles. The diploma includes AWS Solution Architecture, Microsoft Azure Administrator (Architect), Cloud Security Professional Course, Cloud Security Standards Review, and Information Systems Security Architecture Professional (ISSAP) Architecture Professional Review, which enable learners to automate repetitive tasks and gain expertise in cloud computing security architecture. In addition, the diploma focuses on developing learners' abilities to analyze, design, implement, and evaluate complex IT infrastructure and cloud-based systems, ensuring high availability, security, and performance. Upon completion, learners can pursue careers in SysOps, such as SysOps engineers, cloud architects, and system administrators, among others.

Our course material is designed to acquaint learners with various viewpoints on emerging technologies. The diploma aims to teach learners how to automate repetitive tasks and analyze, design, implement and evaluate complex IT infrastructure and cloud-based systems to ensure high availability, security, and performance. To prepare learners for job interviews, we provide internships, resume development, and interview coaching. Graduates of this diploma can pursue careers in SysOps, such as SysOps engineers, cloud architects, and system administrators within 3-6 months, enabling national or international job opportunities.

The SysOps and Cloud Development Diploma is supplemented with the contents of the Cloud Cyber Security Diploma, enabling learners to develop a more comprehensive understanding of emerging sciences and increase their employability with diversified knowledge.

Focusing on employability, the course uses open-source, vendor-agnostic content and provides students with recorded videos, hands-on practice, custom cloud labs, and assignments. Hands-on practice includes step-by-step guidance and interaction with trainers via communities, forums, and live classes.

Key Features of the Diploma

EduQual Globally Recognized Certificate

400+ hands-on cloud labs

Self-paced learning 5000+ hands-on projects

Job description learning

8X higher live interaction with live online classes by Industry experts

Student Communities

Resume building

Interview Preparation

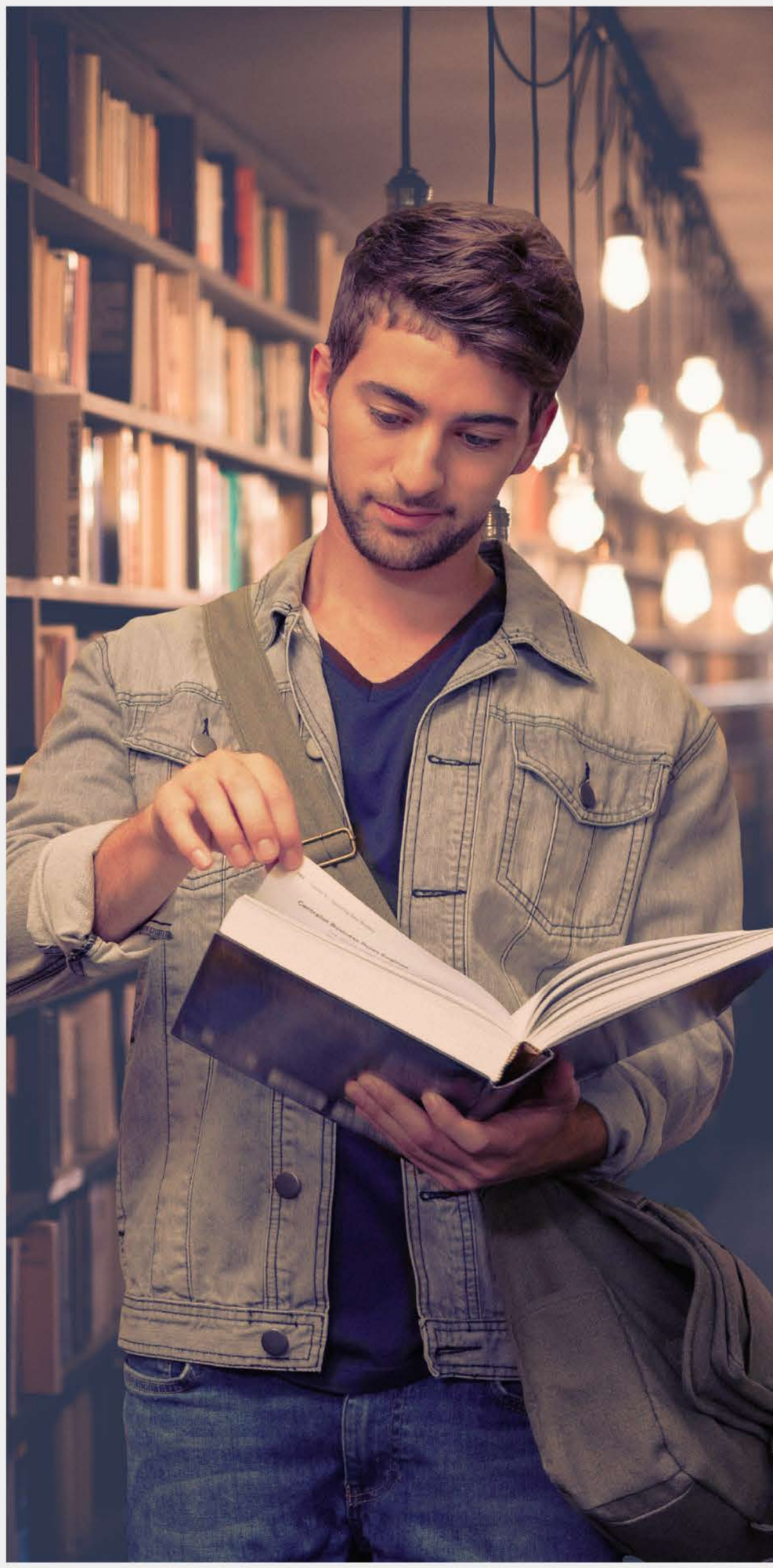
Internship Program

Global Undergraduate program eligibility

Gain full expertise in Cloud Environments with Cloud Playground's on-demand servers and specialized containers for labs

About our Diploma Program (Accredited by EduQual)

The SysOps and Cloud Development Diploma, accredited by EduQual, offers learners valuable knowledge and skills for pursuing careers in SysOps and cloud computing. EduQual is a globally recognized awarding organization that provides highly regarded qualifications that are respected by employers and academic institutions worldwide. The accreditation of the SysOps and Cloud Development Diploma attests to the program's dedication to maintaining high-quality standards and providing students with comprehensive training in cloud computing. This diploma is an excellent option for those seeking to improve their SysOps methodologies and cloud computing abilities while enhancing their career prospects in this rapidly changing sector. Additionally, since the diploma corresponds to Level 4 of the Regulated Qualifications Framework (RQF), graduates may be eligible for a first-year exemption in an undergraduate program upon successful completion of the course.



Upon completion of this diploma program, you will:

- Receive a Certificate from EduQual after completion of the diploma program.
- Eligible for Al Nafi Alumni membership

About Al Nafi

Al Nafi, the leading global e-Learning platform, offers rigorous and specialized training in emerging technologies and processes shaping the digital landscape. With a cost-effective, self-paced learning and time-efficient approach, we have served more than 300,000 learners, with numerous alumni excelling in Fortune 500 companies worldwide. Our customized programs are designed to help both individuals and organizations achieve their career and business objectives.

Program Eligibility Criteria & Application Process

To apply for the SysOps and Cloud Development Diploma at Eduqual Level 4, individuals who are interested will need to register for the diploma through the website. The provided link https://alnafi.com/tracks/sysops can be used by learners to complete their application.

Eligibility Criteria

To enrol in the SysOps and Cloud Development Diploma at Eduqual Level 4, there are no specific courses or academic prerequisites required. However, candidates must possess the following:

- A laptop or desktop computer that is in good working order
- A dependable internet connection
- Proficiency in using the internet and the ability to troubleshoot internet-related issues.

Application Process

After selecting the preferred payment plan, learners can begin their studies with ease as the application process comprises only three straightforward steps.

STEP 1
CHOOSE THE PAYMENT PLAN AND TYPE

Fill out the application form and choose your preferred payment plan, which includes options for monthly, quarterly, half-yearly, and annual payments.

STEP 2
SUBMIT THE APPLICATION PROCESS

With just one click, submit your application once you have chosen the payment method and plan.

STEP 3
ADMISSION

Once your payment method and plan have been verified, immediately begin your studies.

Connect with the

Support Operations

Center

Our dedicated support team is here to assist you with any questions or concerns you may have regarding the application process and related matters, 24/7. They can help you with inquiries regarding

- The application
- provide information on the interest-free student loan (if applicable)
- Clarify any confusion you have about the diploma program

Program Outcomes

Develop expertise in designing and deploying scalable, highly available, and fault-tolerant systems using AWS services and gain hands-on experience with AWS infrastructure. (AWS Solution Architecture)

Learn cloud security concepts, tools, and best practices to secure cloud-based infrastructure and protect sensitive data, including security governance, risk management, compliance, and threat detection and response. (Cloud Security Professional Course)

Understand the industry-recognized security standards and regulations, including ISO 27001/27002, NIST, CSA, and PCI DSS, and their implementation in cloud environments. (Cloud Security Standards Review)

Acquire the necessary knowledge and skills to design, implement, and maintain secure architectures for enterprise systems using the Information Systems Security Architecture Professional (ISSAP) framework. (ISSAP Architecture Professional Review)

Develop proficiency in administering, managing, and monitoring Microsoft Azure services and gain hands-on experience with Azure infrastructure and deployment models. (Microsoft Azure Administrator (Architect)

Who Should Enroll in this Program?

This SysOps and Cloud Advancement Diploma is designed for:

- School and university students looking to expand their knowledge, skills, and career opportunities
- Professionals in the industry who want to enhance their skills and advance their careers

This diploma program is suitable for individuals between the ages of 16 and 45 who are self-motivated and capable of studying independently. The diverse student body, composed of individuals from various industries and backgrounds, enriches class discussions and interactions.

The diploma prepares individuals for careers such as:

- AWS Solution Architect, AWS Cloud Architect, AWS Cloud Consultant
- Cloud Security Engineer, Cloud Security Analyst, Cloud Security Architect
- Cloud Security Consultant, Cloud Security Engineer, Cloud Security Analyst
- Information Security Architect, IT Security Manager, Security Analyst
- Microsoft Azure Administrator, Cloud Architect, Cloud Engineer
- Cybersecurity Analyst, Security Operations Center (SOC) Analyst
- Data Analyst, Data Scientist, Machine Learning Engineer
- SOC Engineer, Security Operations Center (SOC) Analyst
- Threat Hunting Engineer, Security Operations Center (SOC) Analyst
- Ethical Hacker, Incident Response Manager, Security Analyst
- Information Security Manager, Security Consultant, Security Auditor
- Data Analyst, Data Scientist, Machine Learning Engineer
- Data Analyst, Data Scientist, Machine Learning Engineer
- Job seeker, Professional looking to improve their LinkedIn profile

- Linux Administrator, System Administrator, DevOps Engineer
- Network Security Analyst, Penetration Tester, Ethical Hacker
- PCI DSS Compliance Auditor, Security Consultant, Compliance Officer
- Data Analyst, Data Scientist, Machine Learning Engineer
- Python Developer, Data Analyst, App Developer, Machine Learning Engineer
- Data Analyst, Data Scientist, Machine Learning Engineer
- DevOps Engineer, Cloud Engineer, Application Developer
- SCADA Security Analyst, Incident Response Manager, Cybersecurity Consultant
- SIEM Engineer, Security Operations Center (SOC) Analyst
- Data Analyst, Data Scientist, Machine Learning Engineer
- Vulnerability Assessment Specialist, Penetration Tester, Security Consultant

Important Features:

- No academic prerequisites required
- Only a reliable internet connection and a laptop/PC needed

Learning Path

1. AWS Solution Architecture
2. Cloud Security Professional Course
3. Cloud Security Standards Review
4. ISSAP Architecture Professional Review
5. Microsoft Azure Administrator (Architect)
6. Get ready and take the exam

EduQual Certificate

AWS Solution Architecture

The SysOps to CloudOps course aims to provide learners with comprehensive training and hands-on experience in AWS cloud computing, covering topics such as AWS models, features, VPC_IAM, networking, EC2, EBS, auto-scaling, S3, RDS, Route53, and more. By the end of the course, learners will be able to understand the fundamentals of cloud computing, implement and manage cloud-based systems, and automate repetitive tasks. Additionally, learners will have the knowledge and skills necessary to excel in job roles such as SysOps engineers, cloud architects, and system administrators.

Key Learning Objectives

- Understand the basics of cloud computing with AWS perspective, AWS free tier account set bill alerts, AWS regions, AZ basics of VPC_IAM budgets protect account using MFA.
- Learn about the management and identity access management (IAM) and create an IAM users group, IAM user sign-in, and practical 2 copy permission from existing users.
- Gain knowledge of the basics of networking, virtual private cloud (VPC), CIDR/IP range & subnet, subnet understanding & working on default VPC, and subnetting tool creating subnet in VPC.
- Learn about security group (SG), NACL network access control list, custom NACL associate NACL to subnet, EC2 instance families, launching EC2 instance, SG live practical, NACL live practical EC2 terminate.
- Understand EBS, EC2 pricing options, on-demand vs reserved instance, EC2 instance state, elastic IP EC2 termination protection, saving plan and use cases, spot instance use cases, and dedicated instances.
- Learn about ENI elastic network interface, placement groups, EBS snapshots, restoring EBS from 1AZ to another migration, EBS encryption, creating custom AMI, deregistering deleting AMI.

- Gain knowledge of application load balancer, auto-scaling, automating snapshots, S3, SNS integration with S3, setting up RDS prod HA, connecting RDS from the workbench, RDS failover-n setting up read replica for heavy workloads, RedShift, Kinesis, DynamoDB, Lambda, Route53 registering a domain, Route53 checking the health of your resource, Route53 route internet traffic A record, Route53 create a hosted zone for Godaddy, Route53 route internet traffic multi-value answer policy, Route53 route internet traffic weighted latency policy, Route53 route internet traffic geo-location failover policy CNAME alias record, alias record for S3 URL naked domain, CloudFront, CloudFront routing, cloud trail, 4_SQS, cloud formation, configuring VPN, configuring FortiGate firewall, IAM roles AD users integration, module 23-AD connect.

Course Curriculum

Lesson 1: AWS Demo | Think like an Architect:
Lesson 2: Start building on AWS using Free Tier
Lesson 3: AWS user creation & permission management
Lesson 4: Building your first Virtual Private Cloud (VPC)
Lesson 5: Architecting VPC as per customer
Lesson 6: Dive deep into Security Group and NACL
Lesson 7: Going down the Rabbit Hole Security Group and NACL
Lesson 8: How to write a letter for bill adjustments & reversal of charges
Lesson 9: Setting up NAT Instance inline with AWS documentation & AWS NAT Gateway
Lesson 10: VPC Peering Different Regions Amazon EBS
Lesson 11: EC2 Pricing Strategy with Reserved Instance
Lesson 12: EC2 Pricing Strategy with Saving Plans
Lesson 13: Placement Group Strategy
Lesson 14: Dive deep into EBS Encryption
Lesson 15: Building your own Amazon Machine Image
Lesson 16: Dive deep into Auto Scaling
Lesson 17: Automating Snapshots
Lesson 18: S3 Bucket creation versioning
Lesson 19: Building RDS cluster in Multi-AZ Prod setup
Lesson 20: Redshift Kinesis AWS Lambda DynamoDB
Lesson 21: Route 53
Lesson 22: CloudFront Cloud CloudFormation SQS Cloud Trail
Lesson 23: Connecting AWS VPC to On-Premises
Lesson 24: AD Connector for Streamlining Identity Management

Cloud Security Professional Course

The aim of this course is to provide learners with a comprehensive understanding of Cloud Computing and Security in a cloud environment. By the end of this course, learners will gain knowledge of the fundamental concepts, architecture, design, and security considerations of cloud computing. They will also be able to evaluate cloud service providers, understand the risks associated with cloud infrastructure and data security, and learn about secure software development life cycle processes. Additionally, learners will be familiar with identity and access management solutions, operational controls and standards, digital forensics, and legal, risk, and compliance issues in a cloud environment.

Key Learning Objectives

- Define cloud computing and its roles and responsibilities
- Understand key cloud computing characteristics and building block technologies
- Identify cloud service categories, deployment models, and shared considerations
- Recognize security concepts relevant to cloud computing and design principles of secure cloud computing
- Evaluate cloud service providers based on criteria and certifications
- Describe cloud data concepts, storage architectures, and data security technologies
- Understand data discovery, classification, and information rights management
- Learn about data retention, deletion, and archiving policies, auditability, traceability, and accountability of data events
- Identify cloud infrastructure components and secure data centre design principles
- Assess risks associated with cloud infrastructure and security controls
- Understand disaster recovery and business continuity strategies
- Advocate training and awareness for application security, including common pitfalls and vulnerabilities
- Describe the Secure Software Development Life Cycle (SDLC) process and cloud-specific risks
- Learn about threat modelling, secure coding practices, and software configuration management
- Understand cloud software assurance and validation and cloud application architecture
- Identify identity and access management solutions
- Understand the physical and logical infrastructure for the cloud environment and operate and maintain them

- Identify operational controls and standards, support digital forensics, and manage communication with relevant parties
- Learn about security operations, including security controls and monitoring, incident management, and vulnerability assessments
- Understand the configuration of host and guest operating system backup and restore functions and management plane
- Identify legal requirements and unique risks within the cloud environment, including privacy issues
- Understand the audit process, methodologies, and required adaptations for a cloud environment
- Learn about internal information security management and controls systems, specialized compliance requirements for highly-regulated industries, and implications of cloud to enterprise risk management
- Identify outsourcing and cloud contract design considerations, including vendor management, contract management, and supply-chain management.

Course Curriculum

Lesson 1: Cloud computing concepts
Lesson 2: Cloud reference architecture
Lesson 3: Security concepts relevant to cloud computing
Lesson 4: Design principles of secure cloud computing
Lesson 5: Evaluate cloud service providers
Lesson 6: Cloud data concepts
Lesson 7: Cloud data storage architectures
Lesson 8: Data security technologies and Strategies
Lesson 9: Data discovery
Lesson 10: Data classification
Lesson 11: Information Rights Management (IRM)
Lesson 12: Data retention, deletion, and archiving policies
Lesson 13: Auditability, traceability, and accountability of data events
Lesson 14: Cloud infrastructure components
Lesson 15: Secure data centre
Lesson 16: Risks associated with cloud infrastructure
Lesson 17: Security controls
Lesson 18: Disaster Recovery (DR) and Business Continuity (BC)
Lesson 19: Advocate training and awareness for application security
Lesson 20: Describe the Secure Software Development Life Cycle (SDLC) process

Lesson 21: Secure Software Development Life Cycle (SDLC)
Lesson 22: Cloud software assurance and validation
Lesson 23: Cloud application architecture
Lesson 24: Identity and Access Management (IAM) solutions
Lesson 25: Physical and logical infrastructure for cloud environment
Lesson 26: Operate and maintain physical and logical infrastructure for the cloud environment
Lesson 27: Operational controls and standards
Lesson 28: Support digital forensics
Lesson 29: Manage communication with relevant parties
Lesson 30: Security operations
Lesson 31: Legal Requirements and unique risks within the cloud environment
Lesson 32: Understand privacy issues
Lesson 33: Audit process, methodologies, and required adaptations for a cloud environment
Lesson 34: Implications of Cloud to enterprise risk management
Lesson 35: Understand outsourcing and cloud contract design

Cloud Security Standards Review

This course aims to provide a comprehensive understanding of cloud computing and security, covering various topics such as cloud architecture, infrastructure security, data security, and governance and compliance. Students will learn about different deployment and service models of cloud computing, essential characteristics of cloud computing, and shared responsibilities between cloud providers and customers. The course also covers best practices for securing cloud infrastructure, including software-defined networks, network security, and business continuity and disaster recovery planning. In addition, students will develop knowledge and skills in secure software development life cycle, testing and assessment, DevOps, and identity and access management. The course also addresses selecting a cloud provider, security as a service, incident response, Domain 14 considerations, and CCSK exam preparation. Upon completion of the course, students will be equipped with the knowledge and skills required to implement best practices in securing cloud computing environments and managing cloud security risks effectively.

Key Learning Objectives

- Understand the fundamental concepts of cloud computing including essential characteristics, service and deployment models, and shared responsibilities.
- Identify and implement best practices for securing cloud infrastructure including software-defined networks, network security, securing compute workloads, and business continuity and disaster recovery planning.
- Learn about governance and compliance in cloud computing including managing cloud security risks and legal issues in cloud computing.
- Gain an understanding of cloud data storage, encryption options, and data security lifecycle.
- Develop knowledge and skills in secure software development life cycle (SSDLC), testing and assessment, DevOps, and identity and access management.
- Learn about selecting a cloud provider, security as a service (SECaaS), incident response, Domain 14 considerations, and CCSK exam preparation.

Course Curriculum

Lesson 1: Introduction to Cloud Computing

Lesson 2: Introduction & Cloud Architecture

Lesson 3: Cloud Essential Characteristics

Lesson 4: Cloud Service Models

Lesson 5: Cloud Deployment Models

Lesson 6: Shared Responsibilities

Lesson 7: Module Introduction Unit

Lesson 8: Intro to Infrastructure Security for Cloud Computing

Lesson 9: Software-Defined Networks

Lesson 10: Cloud Network Security

Lesson 11: Securing Compute Workloads

Lesson 12: Management Plane Security

Lesson 13: BCDR

Lesson 14: Governance

Lesson 15: Managing Cloud Security Risk

Lesson 16: Legal Issues In Cloud Compliance

Lesson 17: Audit

Lesson 18: CSA Tools
Lesson 19: Module Introduction
Lesson 20: Cloud Data Storage
Lesson 21: Securing Data In The Cloud
Lesson 22: Encryption For IaaS
Lesson 23: Encryption For PaaS & SaaS
Lesson 24: Encryption Key Management
Lesson 25: Other Data Security Options
Lesson 26: Data Security Lifecycle
Lesson 27: Module Introduction
Lesson 28: Secure Software Development Life Cycle (SSDLC)
Lesson 29: Testing & Assessment
Lesson 30: DevOps
Lesson 31: Secure Operations
Lesson 32: Identity & Access Management Definitions
Lesson 33: IAM Standards
Lesson 34: IAM In Practice
Lesson 35: Module Introduction
Lesson 36: Selecting A Cloud Provider
Lesson 37: SECaaS Fundamentals
Lesson 38: SECaaS Categories
Lesson 39: Incident Response
Lesson 40: Domain 14 Considerations
Lesson 41: CCSK Exam Preparation

ISSAP Architecture Professional Review

The objective of this course is to equip students with the knowledge and skills necessary to design and implement a secure and resilient cloud infrastructure. By the end of the course, students will be able to determine legal, regulatory, organizational, and industry requirements, manage risk, and identify security architecture approaches. They will also be able to design infrastructure security requirements, secure shared services, integrate technical security controls, and design and integrate infrastructure monitoring. In addition, students will learn to design secure network and communication infrastructure, evaluate physical and environmental security requirements, and design identity and access control management solutions. The course also covers software development life cycle integration with application security architecture, proactive controls for applications, and security operations requirements gathering. Furthermore, students will learn to design information security monitoring, incident response management, Business Continuity (BC) and resiliency solutions. Finally, they will be able to validate Business Continuity Plan (BCP)/Disaster Recovery Plan (DRP) architecture.

Key Learning Objectives

- Determine legal, regulatory, organizational, and industry requirements, and manage risk.
- Identify security architecture approach and verify and validate the design, including functional acceptance testing and regression testing.
- Develop infrastructure security requirements and design defense-in-depth architecture.
- Secure shared services, integrate technical security controls, and design and integrate infrastructure monitoring.
- Design infrastructure cryptographic solutions and secure network and communication infrastructure, including VPNs, IPsec, and TLS.
- Evaluate physical and environmental security requirements and design identity management and access control management and lifecycle.
- Integrate Software Development Life Cycle (SDLC) with application security architecture and determine application security capability requirements and strategy.
- Identify common proactive controls for applications and gather security operations requirements.
- Design information security monitoring and incident response management.
- Design Business Continuity (BC) and resiliency solutions, and validate Business Continuity Plan (BCP)/Disaster Recovery Plan (DRP) architecture.am preparation.

Course Curriculum

Lesson 1: Determine legal, regulatory, organizational and industry requirements, Manage Risk, Identify security architecture approach, and Verify and validate design (e.g., Functional Acceptance Testing (FAT), regression).

Lesson 2: Develop infrastructure security requirements, Design defense-in-depth architecture, Secure shared services (e.g., wireless, e-mail, Voice over Internet Protocol (VoIP), Unified, Communications (UC), Domain Name System (DNS), Network Time Protocol (NTP)), Integrate technical security controls.

Lesson 3: Design and integrate infrastructure monitoring, Design infrastructure cryptographic solutions, Design secure network and communication infrastructure (e.g., Virtual Private Network (VPN), Internet Protocol Security (IPsec), Transport Layer Security (TLS)), and Evaluate physical and environmental security requirements.

Lesson 4: Design identity management and lifecycle, Design access control management and lifecycle, Design identity and access solutions, Integrate Software Development Life Cycle (SDLC) with application security architecture (e.g., Requirements Traceability Matrix (RTM), security architecture documentation, secure coding).

Lesson 5: Determine application security capability requirements and strategy (e.g., open source, Cloud Service Providers (CSP), Software as a Service (SaaS)/Infrastructure as a Service (IaaS)/ Platform as a Service (PaaS) environments), Identify common proactive controls for applications (e.g., Open Web Application Security Project (OWASP)).

Lesson 6: Gather security operations requirements (e.g., legal, compliance, organizational, and business requirements), Design information security monitoring (e.g., Security Information and Event Management (SIEM), insider threat, threat intelligence, user behaviour analytics, Incident Response (IR) procedures), Design Business Continuity (BC) and resiliency solutions, Validate Business Continuity Plan (BCP)/Disaster Recovery Plan (DRP) architecture, Design Incident Response (IR) management.

Microsoft Azure Administrator (Architect)

This course aims to provide a comprehensive understanding of various Azure cloud computing services and technologies. It covers the basics of cloud computing and Microsoft Azure, as well as specific topics such as identity and access management, virtual machines and networking, managed disks and images, cost management, backup and site recovery, load balancing and DNS, virtual machine scale sets, storage accounts, VPN/Express Route and Azure AD Connect, cloud migration, and Azure Bastion, Azure Automation, and Azure Monitor. By the end of the course, students will have a strong foundation in Azure.

Key Learning Objectives

- Understand the fundamentals of cloud computing and Microsoft Azure
- Learn to configure and manage Azure virtual machines, storage, and networking
- Understand the best practices for Azure cloud computing
- Gain an understanding of identity and access management (IAM)
- Learn to manage user accounts and implement multi-factor authentication
- Understand the best practices for IAM
- Learn to configure and manage Azure virtual machines and virtual machine networking
- Understand how to configure and manage Azure VPN/ExpressRoute and Azure AD Connect
- Understand the best practices for Azure virtual machines and networking
- Learn to configure and manage Azure virtual machine components, such as extensions and disks
- Understand the best practices for Azure virtual machine components
- Gain an understanding of Azure virtual machine routing and VNET peering
- Learn to configure and manage Azure virtual machine routing and VNET peering
- Understand the best practices for Azure virtual machine routing and VNET peering
- Learn to create and manage Azure-managed disks, images, and snapshots
- Understand the best practices for Azure-managed disks, images, and snapshots
- Gain an understanding of Azure cost management and billing optimization
- Learn to implement cost control, allocation, and chargeback
- Understand the best practices for Azure cost management

- Learn to plan and implement backup and recovery solutions in Azure
- Learn to implement Azure backup and site recovery
- Understand the best practices for Azure backup and site recovery
- Learn to plan and implement load-balancing solutions in Azure
- Learn to implement Azure traffic manager and DNS
- Understand the best practices for Azure load balancer, traffic manager, and DNS
- Learn to plan and implement Azure virtual machine scale sets
- Learn to implement load balancing and networking for virtual machine scale sets
- Understand the best practices for Azure virtual machine scale sets
- Learn to plan and implement Azure storage accounts
- Learn to implement blob storage, file storage, queue storage, and table storage
- Understand the best practices for Azure storage accounts
- Gain an understanding of Azure VPN and ExpressRoute
- Learn to plan and implement site-to-site VPNs and point-to-site VPNs
- Learn to integrate on-premises directories with Azure AD
- Understand the best practices for Azure VPN/ExpressRoute and Azure AD Connect
- Learn to plan and execute a cloud migration to Azure
- Understand how to assess on-premises infrastructure and select migration methods
- Understand the best practices for managing cloud migrations
- Learn to configure and manage Azure Bastion, Azure Automation, and Azure Monitor
- Understand how to automate workflows with Azure Automation and monitor Azure resources with Azure Monitor
- Understand the best practices for Azure Bastion, Azure Automation, and Azure Monitor

Course Curriculum

Lesson 1: Azure Cloud Computing Basics

Lesson 2: Identity and Access Management (IAM)

Lesson 3: Azure Virtual Machine and Networking

Lesson 4: Azure Virtual Machine Components

Lesson 5: Azure VM Routing and VNET Peering

Lesson 6: Azure Managed Disk, Image and Snapshot

Lesson 7: Azure Cost Management

Lesson 8: Azure Backup and Site Recovery

Lesson 9: Azure Load Balancer, Traffic Manger and DNS

Lesson 10: Azure Virtual Machine Scale Set

Lesson 11: Azure Storage Account

Lesson 12: Azure VPN/Express Route, Azure AD Connect

Lesson 13: Migration from On-Premises to Azure Clouds

Lesson 14: Azure Bastion, Azure Automation, Azure Monitor

Comprehensive Assessment Approach

Assessments are an essential component of any diploma course, and at our online and distance learning platform, we ensure that our students are evaluated thoroughly. Multiple choice questions (MCQs) will be the standard form of assessment across all diploma courses. However, for certain individual courses, students may be required to deliver an oral presentation or participate in an interview. Additionally, after completing the entire diploma course, students will be required to present an oral presentation, which will be mandatory. This approach allows us to evaluate our students comprehensively and helps them develop essential skills for their future careers.

EduQual Examinations:

Learners who are studying EduQual Level 3 and/or EduQual Level 4 diploma(s) will have to pay an examination fee as tabulated below.

Diploma	Total (£)
Diploma in Cloud Cyber Security (EduQual Level 3)	250*
DevOps and Cloud Advancement (EduQual Level 4)	250*
Diploma in SysOps and Cloud Advancement (EduQual Level 4)	250*
Diploma in Artificial Intelligence Advancement (EduQual Level 4)	250*

- **Learners will be required to pay the amount that is equal to the value of GBP (Great British Pound), and they should consult the current currency conversion rate to determine the amount in their local currency.**
- New learners must pay all examination fees of that respective diploma as soon as they are enrolled. Learners who are currently studying any advancement track can apply for a respective diploma by paying the examination fee of that respective diploma.
- Learners who successfully complete the EduQual Level 3 and/or Level 4 diplomas will be awarded a certificate by EduQual.
- Learners must provide accurate and up-to-date information during the application process as that information will be shared with the EduQual for awarding a certificate.
- Learners who paid full or yearly fees will get access to the full course contents of the diploma.

- Learners who paid half-yearly, quarterly, or monthly fees will get access to the course contents of the diploma as per the drip schedule defined in our LMS.
- All EduQual Level 3 and Level 4 diplomas will have content access for 12 months at most.
- Learners are responsible for ensuring that they have the necessary technology and resources to participate in the diploma.

Assessments For EduQual Level 3 and EduQual Level 4 Diplomas

- The learner must appear for the exam within 1 year after registration with EduQual. If they don't appear for the exam within 1 year they have to again submit the examination fees.
- Learners enrolled in the EduQual level 4 Diploma may choose to take the EduQual level 3 Diploma exam, which is available as an option for all EduQual level 4 Diploma students.
- Learners must submit all assessments and coursework on time and to the required standard as per the diploma.
- Learners must follow the guidelines for academic integrity and avoid plagiarism or other forms of academic misconduct.
- Learners must attend all required classes and complete all assessments and coursework on time.

- **Assessment Formats**

    - All customized courses in the diploma will include multiple-choice questions (MCQs) as part of the assessment.
    - Some courses may also include coding assignments where applicable.
    - The majority of courses will include oral presentations or interviews as part of the assessment.
    - There will be a comprehensive exam covering the material from all courses in the diploma.

- **Assessment Guidelines**

  - Learners must follow the guidelines for each type of assessment as provided by Al Nafi in the specific assessment.
  - Learners must complete all assessments honestly and to the best of their ability.
  - Learners are responsible for ensuring that their work is original and not plagiarized from any other source

- **Assessment Grading**

  - The grading system for each type of assessment will be clearly explained in the course materials.
  - Learners will be provided with feedback on their assessments and opportunities for improvement.
  - The final grade for each course will be based on a combination of assessments.

- **Oral Presentations/Interviews**

  - Learners will be assessed on their ability to communicate effectively and demonstrate subject knowledge during oral presentations or interviews.
  - The format and guidelines for oral presentations or interviews will be provided in the LMS.
  - Learners must prepare and rehearse their presentations or interviews to ensure they meet the required standard.

- **Coding Assignments**

  - Learners in courses that include coding assignments must demonstrate their ability to write code that meets the requirements of the assignment.
  - The coding assignments will be assessed based on factors such as functionality, readability, and efficiency.
  - Learners must adhere to coding best practices and avoid plagiarism.

- **Comprehensive Exam**

    - The comprehensive exam will cover material from all courses in the diploma.
    - The format and guidelines for the comprehensive exam will be provided in the LMS.
    - Learners must prepare and review all course materials in advance of the comprehensive exam.

- **Assessment Grading**

    - The comprehensive exam will cover material from all courses in the diploma.
    - The format and guidelines for the comprehensive exam will be provided in the LMS.
    - Learners must prepare and review all course materials in advance of the comprehensive exam.

- Al Nafi reserves the right to investigate and take action in cases of academic misconduct, including plagiarism or cheating.
- Learners who engage in academic misconduct may be subject to penalties, including a failing grade or expulsion from the diploma program.

- **Changes to Assessment Guidelines**

    - Al Nafi reserve the right to modify the assessment guidelines at any time.
    - Learners will be notified of any changes to the assessment guidelines via email or other communication channels.
    - Learners who do not agree to the modified assessment guidelines must inform support and may be subject to different assessment guidelines or cancellation of enrollment.

This track allows you to work in multiple industries

Features	
Accredited with EduQual	Yes
Access to Complete Course Content	Yes
Access to complete Hands On Labs	Yes
Resume Development	Yes
Interview Preparation	Yes
Internship Letter	Yes
Practice Exams	Yes
Live Sessions with Trainer	Yes
Multiple Languages	Yes

Career Opportunities for this Track:

The demand for DevOps has been on the rise in the last 3 years. This track will cover all the major tools and best practices that are used by DevOps engineers all over the world. Dive right in.

1

Cloud Network Engineer:

Average salary:
$90,000 per year

2

Cloud Automation Engineer:

Average salary:
$110,000 per year

3

Cloud Architect:

Average salary:
$135,000 per year

Our students are working all over the globe in fortune 500 companies

*Any third-party logos displayed in this booklet are the property of their respective companies.

Where Can I find more information?

UK Office Address.
167-169 Great Portland Street
5th Floor
London
WIW 5PF

Regional Office:
Pakistan: D-182, Block-7, Gulshan-e-Iqbal, Karachi, Sindh, Pakistan.

Contact Us:
+92-304-1110 400,
+1 (647) 680-0258 (WhatsApp)

Send Us Message
Support@alnafi.com

Visit:
www.alnafi.com