



Diploma in **SysOps and Cloud Advancement**

EduQual Level 4 Endorsed Diploma

Learner Handbook
AL NAFI INTERNATIONAL COLLEGE
<https://alnafi.com>

Version: 1.0

© 2026 Al Nafi E-Learning Private Limited. All rights reserved.

Table of Contents

1. About the Diploma	4
2. Key Features of the Diploma	4
3. About the Diploma Program Endorsed by EduQual	5
4. About Al Nafi International College	5
5. Program Eligibility Criteria and Application Process	6
5.1. Eligibility Criteria	6
5.2. Application Process	6
6. Connect with the Support Operations Center	7
7. Program Outcomes	7
8. Who Should Enroll in this Program?	8
9. Learning Path	9
10. Assessment Information	9
10.1. Assessment Overview	9
Assessment Components	10
10.2. Al Razzaq Lab Assignments (70% weightage in overall Grade)	10
What Are They?	10
How Are They Graded?	10
What If You Need to Resubmit?	11
10.3. Multiple Choice Questions (15% of Your Grade)	11
Assessment Format	11
Attempts and Scoring	11
Diploma Program Access Period	12
10.4. English Language Exam (15% of Your Grade)	12
Mandatory Requirement	12
Submission Requirements	12
Verification and Compliance	12
Why Is This Required?	12
10.5. Al Razzaq Labs Program Access	13
Prerequisites for Lab Access	13
Lab Components	13
Additional Features and Support	13
10.6. Grading Criteria	14
Grade Boundaries	14
Example Calculation	
For a student:	14
Example: Overall Grade Calculation	15
Quick Reference Table	16
10.7. Academic Integrity	17
Violation Response	17
10.8. Support for Students	17
10.9. Accessibility and Reasonable Adjustments	18
10.10. Appeals Process	18

Complete Course Units (12 Units)	18
Unit 1: Linux Deep Dive	18
Unit 2: Python Deep Dive	19
Unit 3: Red Hat Enterprise Linux (RHEL)	19
Unit 4: Certified Information Systems Security Professional (CISSP)	20
Unit 5: AWS Solutions Architect	21
Unit 6: Certified Cloud Security Professional (CCSP)	22
Unit 7: Information Systems Security Architecture Professional (ISSAP)	23
Unit 8: Microsoft Azure Administrator (AZ-104)	24
Unit 9: Certificate of Cloud Security Knowledge (CCSK)	25
Unit 10: Certified AI-Enhanced Industrial Automation and SCADA Systems Engineer (CAIASE)	26
Unit 11: LinkedIn Course for Job Seekers	27
Unit 12: IELTS Academic and General Training	27
COPYRIGHT NOTICE	28
Unauthorized Use Prohibited	28

1. About the Diploma

The Diploma in SysOps and Cloud Development is designed to provide hands-on training and practical expertise to learners in their job roles. The comprehensive curriculum encompasses a wide array of critical domains: Cloud Infrastructure (AWS Solutions Architect, Microsoft Azure Administrator), Advanced Cybersecurity (CISSP, CCSK, CCSP, and ISSAP Architecture Professional Review), Operating Systems & Automation (Red Hat Enterprise Linux and Linux Deep Dive), and Foundational Programming (Python Deep Dive). Additionally, to bridge the gap between traditional IT and industrial environments, we include AI-Enhanced Industrial Automation and SCADA Systems (CAIASE). Recognizing that technical skills alone are not enough, the diploma also integrates a specialized LinkedIn Course for Job Seekers and an IELTS Training module to enhance global communication, personal branding, and career prospects.

This robust structure enables learners to automate repetitive tasks and gain comprehensive expertise in cloud computing security architecture, system administration, industrial control systems, and secure software development. In addition, the diploma focuses on developing learners' abilities to analyze, design, implement, and evaluate complex IT infrastructure, cloud-based systems, and hybrid industrial networks, ensuring high availability, security, and performance. Upon completion, learners can pursue careers in SysOps, such as SysOps engineers, cloud architects, system administrators, and security specialists.

Our course material is designed to acquaint learners with various viewpoints on emerging technologies across these 12 specialized units. The diploma aims to teach learners how to automate repetitive tasks and analyze, design, implement, and evaluate complex IT infrastructure, cloud-based systems, and secure architectures 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, cloud engineering, cybersecurity, and IT administration within 3-6 months, enabling national or international job opportunities.

The SysOps and Cloud Development Diploma is supplemented with the 6 units of the Cloud Cyber Security Diploma, creating a powerful synergy between operational excellence and security frameworks. This integration enables learners to develop a more comprehensive understanding of emerging sciences, covering everything from infrastructure deployment and automation to identity management, cryptography, incident response, and compliance, ultimately increasing their employability with diversified, future-ready 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 across all core units. Hands-on practice includes step-by-step guidance and interaction with trainers via communities, forums, and live classes, ensuring learners are fully equipped to tackle real-world challenges from day one.

2. Key Features of the Diploma

- EduQual endorsement, a globally recognised qualification.
- Nearly 1400 hours of hands-on cloud labs integrated across all units
- Delivered through Self-paced online and distance learning.
- Job description-led learning aligned with industry roles

- 8X higher live interaction through live online classes conducted by industry experts
- Vibrant student communities for peer support and networking
- Professional resume building and Internship programme eligibility services through Al Razzaq Program
- Undergraduate programme progression pathways
- Gain full expertise in Cloud Environments with Cloud Playground's on-demand servers and specialised containers for every lab scenario

3. About the Diploma Program Endorsed by EduQual

The Diploma in SysOps and Cloud Advancement, endorsed by EduQual, holds significant value for those seeking careers in cloud computing and DevOps. As a globally recognized awarding organization, EduQual provides top-tier qualifications that are widely respected by employers and academic institutions worldwide. The endorsement of the SysOps and Cloud diploma demonstrates the program's commitment to upholding high-quality standards and providing students with comprehensive training in cloud computing. This diploma is an excellent option for individuals looking to improve their SysOps methodologies and cloud computing abilities while enhancing their career opportunities in this rapidly changing sector. Moreover, 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, students will:

- Receive one Certificate and one transcript of EduQual diploma after completion of the program.
- Eligible for Al Nafi Alumni membership and admission in second year Bachelor's Degree programs
- Apply for jobs based upon the skills of the student does not want to take admission

4. About Al Nafi International College

Al Nafi International College, 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 diploma programs are designed to help both students, professionals and organizations achieve their career and business objectives.

5. Program Eligibility Criteria and Application Process

To apply for the SysOps and Cloud Advancement 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/courses/diploma-in-sysops-and-cloud> can be used by learners to complete their application.

To enrol in this diploma, individuals just need to have studied up to at least grade 12, or hold a Level 3 qualification – for example Intermediate, A Level, IB diploma, a Pearson BTEC Level 3, or any equivalent qualification.

5.1. Eligibility Criteria

To enrol in this diploma, individuals just need to have studied up to at least grade 12, or hold a Level 3 qualification – for example Intermediate, A Level, IB diploma, a Pearson BTEC Level 3, or any equivalent qualification. In addition, all learners must possess the following:

- A laptop with an average specification 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.

5.2. 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

COMPLETE KYS VERIFICATION

After payment, complete the KYS form and upload your previous qualification documents for verification. Course access will only be provided after the KYS verification process is completed successfully.

STEP 4

ADMISSION

Once your KYS have been completed and verified, immediately begin your studies. Access to the student portal might take 24 to 48 hours to verify. If there are issues in accessing the Al Nafi student portal then learners should connect with support through call, message on the number given on the website. Or either through email at support@alnafi.com

6. 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 course and labs and assessments.
- Guide about job aspects
- Guide about admission by using this diploma.
- clarify any confusion you have about the diploma program.

7. Program Outcomes

- Design secure, resilient, high-performance, and cost-optimized cloud architectures, implement robust identity and access management controls, and evaluate deployment strategies for scalable infrastructure. (AWS Solutions Architect)
- Manage Azure identities, governance, storage, compute resources, and virtual networking, implement comprehensive monitoring solutions, and administer cloud environments effectively. (Microsoft Azure Administrator (AZ-104))
- Analyze feasibility, define system requirements, design industrial architectures, develop HMI and SCADA configurations, deploy field projects, and manage lifecycles for AI-enhanced industrial automation and control systems. (Certified AI-Enhanced Industrial Automation and SCADA Systems Engineer (CAIASE))
- Apply cloud governance and risk management frameworks, implement security controls across infrastructure, workloads, and data, and execute incident response strategies in cloud environments. (Certificate of Cloud Security Knowledge (CCSK))
- Design secure cloud architectures, protect data across its lifecycle, secure platforms and applications, manage security operations, and address legal, risk, and compliance requirements. (Certified Cloud Security Professional (CCSP))
- Design access control methodologies and secure network architectures, implement cryptographic solutions and PKI, analyze security frameworks, and plan business continuity, disaster recovery, and physical security strategies. (Information Systems Security Architecture Professional (ISSAP))
- Install, configure, and administer Linux systems, manage packages and networking, implement security hardening and firewalls, automate administrative tasks with Bash scripting, and monitor system performance. (Linux Deep Dive)
- Administer Red Hat Enterprise Linux systems, manage software packages using DNF, configure advanced storage and networking, enforce SELinux security policies, and implement virtualization, containerization, and automation strategies. (Red Hat Enterprise Linux (RHEL))

- Design Python solutions using core syntax, data structures, object-oriented programming, and modular packages; develop web applications and RESTful APIs; perform data analysis; and apply AI-powered tools for code optimization. (Python Deep Dive)
- Apply security governance principles, manage enterprise risk and compliance, implement cryptographic and network security controls, manage identity and access, conduct security assessments, and respond to incidents effectively. (Certified Information Systems Security Professional (CISSP))
- Design a professional LinkedIn presence, apply personal branding and content marketing strategies, implement targeted networking techniques, and identify hidden job market opportunities in the global emerging technology sector. (LinkedIn Course for Job Seekers)
- Analyze and apply advanced reading, listening, writing, and speaking strategies to achieve a high band score in the IELTS examination for academic and professional environments. (IELTS Training)

8. Who Should Enroll in this Program?

This SysOps diploma is designed for:

- School, College and university students looking to gain admissions in second year of Bachelor's degree globally and expand their knowledge, skills, and career opportunities as well.
- Individuals looking to learn job based skills and secure employment globally.
- 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

9. Learning Path

1. Linux Deep Dive
2. Python Deep Dive
3. Red Hat Enterprise Linux (RHEL)
4. Certified Information System Security Professional (CISSP)
5. AWS Solution Architecture
6. Certified Cloud Security Professional (CCSP)
7. Information Systems Security Architecture Professional (ISSAP)
8. Microsoft Azure Administrator (Architect)
9. Certificate of Cloud Security Knowledge (CCSK)
10. Certified AI-Enhanced Industrial Automation and SCADA Systems Engineer (CAIASE)
11. LinkedIn Course for Job Seekers
12. IELTS Academic and General Training
13. Pass all MCQs and all AI Razzaq part 1 labs given for the diploma
14. Achieve a 6.5 band or more in IELTS for UKVI
15. Attain EduQual Certificate.

10. Assessment Information

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. This section outlines the assessment framework specifically designed for students who enroll in their EduQual diploma programs from July 2026 onwards.

10.1. Assessment Overview

Student assessments are designed to provide practical, skills-based learning experiences that reflect real-world vocational requirements across emerging technology domains.

Assessment Components

Assessment Component	Weightage	Passing Percentage Requirement
AI Razzaq Lab Assignments(part 1 only)	70%	Minimum 40%
Multiple Choice Questions (MCQs)	15%	Minimum 40%
English Language Exam	15%	Minimum IELTS 6.5 or Duolingo 115–120

Important: You must achieve a minimum of 40% in each of the AI Razzaq Lab Assignments(part 1) and MCQs exam to qualify for diploma completion. Students will have to pay for IELTS for UKVI on their own. The fee is not included in the diploma fee.

10.2. AI Razzaq Lab Assignments (70% weightage in overall Grade)

What Are They?

AI Razzaq Lab Assignments are practical, hands-on tasks divided into three phases:

Phase	Description
Basic Phase	Foundational tasks introducing core concepts and tools
Intermediate Phase	Integrated tasks requiring application of skills in scenario-based contexts
Advanced Phase	Complex, multi-step tasks simulating real-world problem-solving

These assignments are customized based on your chosen emerging technology domain (e.g., AIOps, DevSysOps, DevOps, SysOps, Cloud Advancement).

How Are They Graded?

- Assignments are submitted via the student portal.
- Graded using AI-augmented assessment tools.
- Students receive real-time feedback on their performance
- Final scores are recorded as a percentage

What If You Need to Resubmit?

Scenario	Process
----------	---------

First failure	You may resubmit once within 30 days of receiving your result
Second failure	You must repeat the unit with full attendance and reassessment of all phases
Lab access expires before completion	You must renew access as per the Course Access Policy
Lab assessments incomplete within two years	£100 reassessment fee applies

10.3. Multiple Choice Questions (15% of Your Grade)

Assessment Format

- Each MCQ carries 1 mark
- No negative marking for incorrect answers
- Questions include:
 - Knowledge-based
 - Scenario-based
 - Job-based
 - Critical Thinking
 - Application-based

Attempts and Scoring

Feature	Detail
Attempts	Unlimited attempts within your program access period
Final Score	Average of all attempts that meet or exceed the passing grade
Passing Requirement	Minimum 40%
Requirement	You must pass each individual assessment bank (20 MCQs each)

Diploma Program Access Period

Diploma Level	Access Period
EduQual Level 3 & 4	12 months (in total)

EduQual Level 5	15 months (in total)
EduQual Level 6	18 months (in total)

Note: If you fail to complete all MCQ assessments within your program access period, you must renew access as per the Course Access Policy.

10.4. English Language Exam (15% of Your Grade)

Mandatory Requirement

You must appear for IELTS for UKVI and score a 6.5 band or more to complete the minimum requirements of the exam.

Submission Requirements

You must submit:

- Official score report (verified link or Test Report Form)
- Valid identification matching test records
- Test date (must be within 2 years)
- Registered email used for the test

All submissions must be uploaded via the AI Nafi Student Portal or verified directly through official providers.

Verification and Compliance

AI Nafi International College reserves the right to verify scores with official test providers.

Non-compliance or falsification will result in academic disciplinary action and possible program suspension or termination.

Why Is This Required?

Submission of a valid English proficiency score is required for:

- Program completion and diploma issuance
- Participation in AI Razzaq Program (employment pathways)
- Eligibility for international university admissions or work based opportunities

If you do not meet the minimum requirement, you must retake the test until the required benchmark is achieved and participate in mandatory live classes of IELTS happening weekly.

10.5. AI Razzaq Labs Program Access

Prerequisites for Lab Access

Access to AI Razzaq Labs requires completion of:

1. Enrollment in an eligible EduQual diploma program (Levels 3 to 6)

2. Know Your Student (KYS) Form submission, capturing:
 - Academic background
 - Career goals
 - Geographic preferences
 - Industry focus
3. Engagement with the program as per your selected study plan (monthly, quarterly, annual)

Lab Components

Component	Description
Course-Linked Labs	Embedded and mandatory labs directly tied to your diploma coursework
KYS-Based Personalized Labs	Customized labs tailored to your individual career and skill profile

Additional Features and Support

Every learner will benefit from:

Feature	Description
AI-Driven Internship Guidance	Personalized internship recommendations and preparation
Resume Building	ATS scoring and career coaching
Interview Preparation	AI-powered voice interview practice (coming soon)
GitHub Integration	Portfolio building and code repository integration
Skill Certification Badges	Recognition of completed competencies
Global Career Forum	Access to networking and opportunities
University Admission Assistance	Support for university applications worldwide
Visa and Work Permit Support	Assistance for 70+ countries and G20 nations
Post-Employment Services	30, 60, and 90-day post-employment support
Job Placement	Placement assistance with Fortune 500 and global companies

10.6. Grading Criteria

Final grade is determined by applying the weightage of each assessment component to the scores a student achieves. Each component's score is multiplied by its respective weightage, and the results are summed to calculate your overall grade.

Grades are awarded based on absolute grading criteria, meaning the final grade depends solely on the performance against the predefined percentage thresholds, rather than being compared to other students.

Grade Boundaries

Grade	Percentage Range
A*	90% and above
A	80% – 89%
B	70% – 79%
C	60% – 69%
D	50% – 59%
U	Below 50%

Example Calculation

For a student:

Component	Score Achieved	Weightage	Weighted Score
Lab Assignments	75%	× 70%	= 52.5%
MCQs	60%	× 15%	= 9.0%
English Exam	65%	× 15%	= 9.75%
Final Grade			71.25%

A final score of 71.25% would correspond to a Grade B.

IELTS Band Score to Percentage Conversion

The IELTS test does not have a direct, official percentage conversion. However, for the purpose of diploma, the minimum requirement is Band 6.5, and any score above 6.5 is considered as meeting and exceeding the requirement.

What Does a Band 7 Mean?

A Band 7 indicates a student is a “Good User” of English. According to IELTS:

“You have an operational command of the language, though with occasional inaccuracies, inappropriacies and misunderstandings in some situations. You generally handle complex language well and understand detailed reasoning.”

How Is Band 7 Treated for Diploma?

For English Language Exam component (15% of overall grade), the scoring works as follows:

IELTS Band	Status	Percentage Equivalent (for grading purposes)
Below 6.5	Fail	0% – Does not meet the minimum requirement
6.5	Pass (Minimum)	50%
7.0	Pass (Good)	Approximately 75%
7.5	Pass (Very Good)	Approximately 85%
8.0+	Pass (Excellent)	100%

How English Score Affects Final Grade

Since the English Exam contributes 15% to overall grade, here is how a Band 7 (≈75%) contributes:

Component	Student Score	Weightage	Weighted Contribution
English Exam	75%	× 15%	= 11.25% (out of 15%)

Example: Overall Grade Calculation

Component	Your Score	Weightage	Weighted Score
Lab Assignments	70%	× 70%	= 49.00%
MCQs	60%	× 15%	= 9.00%
English Exam	75% (Band 7)	× 15%	= 11.25%
Final Grade	C		69.25%

A final score of 69.25% would correspond to a Grade C.

Quick Reference Table

IELTS Band	Interpretation	Approx. Percentage	Weighted Contribution (15%)
6.5	Minimum Pass	50%	7.5%
7.0	Good User	75%	11.25%
7.5	Very Good User	85%	12.75%
8.0+	Excellent User	100%	15.00%

Note: The percentage equivalents above are used only for the purpose of calculating your overall diploma grade. They do not represent an official IELTS percentage conversion, as IELTS does not provide one. Any score of 6.5 or above satisfies the English proficiency requirement for your diploma.

10.7. Academic Integrity

To maintain academic integrity, the following practices are strictly prohibited:

Prohibited Practice	Description
Use of Automated Tools	Employing bots, scripts, or unauthorized software to answer MCQs or manipulate assessment platforms

Undisclosed AI-Generated Work	Passing off AI-created content as original work without proper acknowledgment or authorization
Unauthorized Assistance	Using prohibited tools, devices, or receiving help during practical exams

Violation Response

If suspected malpractice is detected:

1. Student will be formally informed in writing
2. A panel will review the evidence
3. Student will have the opportunity to respond
4. If confirmed, student may be banned from retaking the assessment and may be disqualified from the diploma program

10.8. Support for Students

The college provides comprehensive support to help students succeed:

Support Type	Description
Academic Integrity Workshops	Sessions on plagiarism prevention and ethical assessment practices
Counseling and Advising	Guidance on academic challenges and career planning
Detailed Feedback	Constructive feedback on assessments to guide improvement
AI Usage Guidance	Resources on responsible AI usage in academic work
Technical Support	Assistance with platform and technical issues via live chat or email

10.9. Accessibility and Reasonable Adjustments

The college is committed to ensuring equal access to assessments. If students have documented disabilities or special needs, they may request reasonable adjustments, including:

- Extra time
- Alternative formats
- Assistive technology
- Modified lab environments

Submit requests to: academics@alnaf.com

Timeline: At least 7 working days before the scheduled assessment with supporting documentation.

10.10. Appeals Process

If any student believes an assessment decision is unfair:

Step	Timeline	Action
Informal Review	Within 10 working days of receiving results	Contact academics@alnaf.com
Formal Appeal	Within 14 working days of informal response	Submit formal appeal with supporting evidence
Acknowledgment	Within 3 working days	Appeal is acknowledged and assigned for review
Final Decision	Within 15 working days	Impartial panel issues final written decision

Complete Course Units (12 Units)

Unit 1: Linux Deep Dive

Unit Objectives:

- Build comprehensive Linux system administration skills
- Master installation, configuration, and management
- Develop security, networking, and monitoring expertise
- Learn automation and high availability concepts

Unit Curriculum:

- Introduction and installation (virtual environment, custom partitions, hardening)
- Basic configuration (system architecture, commands, file systems, permissions)
- Bash shell scripting
- Package management with YUM/DNF
- Advanced Linux configuration (single-user mode, run levels, performance reporting)
- Linux networking (DHCP, static/dynamic IP, DNS, routing)
- Advanced disk management (partitions, LVM, file systems)
- Linux services (SSH, NFS, Samba, NTP, cron)
- Linux security (firewalld, iptables, rkhunter)
- Web, MySQL, and Squid server configuration
- High availability (bonding, teaming, failover, load balancing)

- Linux monitoring (Nagios, NRPE, Docker monitoring)
 - AI-powered automation and optimization
-

Unit 2: Python Deep Dive

Unit Objectives:

- Build deep, professional Python programming skills
- Master OOP, data structures, and advanced features
- Develop web applications, APIs, and data solutions
- Implement testing, debugging, and best practices

Unit Curriculum:

- Introduction to Python environment and setup
 - Basic syntax and operations
 - Data structures (lists, tuples, dictionaries, sets, strings)
 - Modules and packages
 - Object-Oriented Programming (classes, inheritance, polymorphism)
 - Advanced topics (decorators, generators, context managers)
 - Working with data (CSV, JSON, databases, Pandas)
 - Web development (Flask, Django, RESTful APIs)
 - Testing and debugging (unit tests, TDD)
 - Concurrency and parallelism (threading, multiprocessing, asyncio)
 - Network programming (sockets, client-server)
 - Advanced libraries and tools (regex, logging, argparse)
 - Best practices and design patterns (PEP 8)
 - Python 3.13 new features
 - Capstone project
-

Unit 3: Red Hat Enterprise Linux (RHEL)

Unit Objectives:

- Install, configure, and manage Red Hat Enterprise Linux systems
- Implement security, networking, and storage solutions
- Master automation with Shell and Ansible
- Manage containers and virtualization

Unit Curriculum:

- RHEL 9 overview and architecture
- Installation and initial setup
- Linux fundamentals and shell
- Software management with DNF/YUM
- User and access control
- Storage and file systems
- Networking and remote access
- Security and SELinux
- Monitoring and performance
- Automation with Shell and Ansible

- Containers and Podman
- Virtualization and high availability

Unit 4: Certified Information Systems Security Professional (CISSP)

Unit Objectives:

- Prepare learners for the CISSP certification exam
- Master all domains of the CISSP Common Body of Knowledge
- Develop expertise in security governance, risk management, and operations
- Build comprehensive understanding of security technologies and practices

Unit Curriculum:

- Security governance through principles and policies
- Personnel security and risk management concepts
- Business continuity planning
- Laws, regulations, and compliance
- Protecting security of assets
- Cryptography and symmetric key algorithms
- PKI and cryptographic applications
- Security models, design, and capabilities
- Security vulnerabilities, threats, and countermeasures
- Physical security requirements
- Secure network architecture and components
- Secure communications and network attacks
- Managing identity and authentication
- Controlling and monitoring access
- Security assessment and testing
- Managing security operations
- Preventing and responding to incidents
- Disaster recovery planning
- Investigations and ethics
- Software development security
- Malicious code and application attacks

Unit 5: AWS Solutions Architect

Unit Objectives:

- Design secure access controls to AWS resources using IAM, MFA, and federated access.
- Architect resilient, highly available, and fault-tolerant systems across multiple Availability Zones.
- Optimize high-performance storage, compute, and database solutions for scalable cloud workloads.
- Implement cost-effective architectures by selecting appropriate pricing models and storage lifecycles.

- Evaluate and apply security best practices for VPC, encryption, and incident response.

Unit Outline:

- **Module 1: Design Secure Architectures** – Secure access to AWS resources, IAM fundamentals, users, groups, roles, policies, MFA best practices, STS and role switching, cross-account and federated access, AWS SSO, Control Tower and SCPs, resource-based policies, VPC security basics, security groups, NACLs, route tables, public/private subnet design, NAT gateways, bastion hosts, AWS Shield and WAF, AWS Secrets Manager, VPN and Direct Connect, data encryption in transit and at rest, ACM and TLS, encryption key management, backup, replication, DR planning, regulatory compliance.
- **Module 2: Design Resilient Architectures** – Scalable and loosely coupled architectures, event-driven, microservices, and multi-tier patterns, horizontal and vertical scaling strategies, loose coupling techniques, containers and serverless architectures, selecting compute/storage/networking/database services, high availability concepts and AWS service choices, fault tolerance across AZs and regions, infrastructure automation (Auto Scaling, CloudFormation), monitoring and health checks, data durability strategies, DR planning and AWS DR solutions, modernizing legacy applications.
- **Module 3: Design High-Performance Architectures** – Amazon S3, EBS, and EFS features and use cases, hybrid storage architectures, storage scalability and optimization, decoupling workloads, Auto Scaling metrics and triggers, EC2 instance types and sizes, compute alternatives (on-demand, reserved, spot, serverless), Amazon RDS, Aurora, DynamoDB performance features, read replicas and caching strategies, capacity planning, database engine selection, global/hybrid/multi-tier network architectures, CloudFront and Global Accelerator, load balancing options, network resource placement, data lakes, Kinesis, Data Firehose, data transfer and transformation services, visualization and analytics.
- **Module 4: AWS Cost Optimization** – Storage class selection and lifecycle policies (S3 Standard, Glacier, etc.), Cost Explorer, Budgets, optimizing storage size and access frequency, cost-effective backup and archiving, data migration services and cost considerations, pricing models and instance purchase options, cost-effective Auto Scaling and load balancing, selecting instance families for budget efficiency, balancing performance and cost.
- **Module 5: Design Cost-Effective Architectures** – Database backup and retention cost optimization, cost-effective database engines and services, replication and capacity planning cost management, efficient database migration, cost-effective network topologies, NAT gateway and VPN cost optimization, network routing and peering for cost reduction, CDN usage and edge caching strategies, monitoring network costs and optimizing bandwidth usage.

Unit 6: Certified Cloud Security Professional (CCSP)

Unit Objectives:

- Design secure cloud architectures and understand design requirements.
- Protect cloud data across its lifecycle using classification, encryption, and DLP strategies.

- Secure cloud platforms, infrastructure, and applications against threats.
- Manage cloud security operations, monitoring, and incident response.
- Address legal, risk, and compliance requirements for cloud environments.

Unit Outline:

- Domain 1: Cloud Concepts, Architecture and Design – Cloud characteristics, business requirements, cloud evolution, vernacular and models, service and deployment models, roles and responsibilities, virtualization, encryption, auditing and compliance, design requirements, business requirements analysis, security considerations for IaaS, PaaS, SaaS, design principles for protecting sensitive data.
- Domain 2: Cloud Data Security – Data classification, inventory and discovery, data lifecycle, jurisdictional requirements, Information Rights Management (IRM), data retention, audit, destruction, cloud data lifecycle (create, store, use, share, archive, destroy), cloud storage architectures (volume, object, databases, CDNs), foundational security strategies (encryption, masking, tokenization, SIEM, DLP).
- Domain 3: Cloud Platform & Infrastructure Security – Shared cloud platform risks and responsibilities, risks by deployment and service model, virtualization threats and countermeasures, Disaster Recovery and Business Continuity, foundations of managed services, shared responsibilities by service type, shared administration of OS and middleware, data access responsibilities, shared monitoring and testing.
- Domain 4: Cloud Application Security – Training and awareness, cloud-secure SDLC, configuration management, ISO/IEC 27034-1 standards, Identity and Access Management (IAM), identity repositories, SSO, federated identity, federation standards, MFA, cloud application architecture (APIs, tenancy, cryptography, sandboxing), application assurance and validation, threat modeling, software security testing, API management, securing open-source software.
- Domain 5: Cloud Security Operations – Physical/logical operations, facilities and redundancy, virtualization and storage operations, physical and logical isolation, Security Operations Center (SOC), continuous monitoring, incident management, monitoring and capacity management, change and configuration management, release management, IT Service Management (ITSM), Business Continuity and Disaster Recovery (BC/DR).
- Domain 6: Legal, Risk and Compliance – Legal requirements and unique risks, legal concepts, US and international laws, privacy laws, information security management systems (ISMS), eDiscovery, forensic requirements, forensic data collection, audit processes and methodologies, virtualization and audit scope, gap analysis, types of audit reports, AICPA reports, impact of diverse jurisdictions, enterprise risk management, risk management frameworks, contracts and SLAs, supply chain and vendor management, CSA STAR, common criteria.

Unit 7: Information Systems Security Architecture Professional (ISSAP)

Unit Objectives:

- Design access control methodologies and implement authentication, authorization, and accounting systems.

- Architect secure communication networks and protect against network attacks.
- Implement cryptographic solutions, PKI, and key management strategies.
- Analyze security architecture frameworks and conduct risk-based design validation.
- Plan business continuity, disaster recovery, and physical security strategies.

Unit Outline:

- Domain 1: Access Control Systems & Methodology – Access control concepts (DAC, MAC, nondiscretionary), least privilege, separation of duties, authentication, authorization, and accounting (AAA), centralized, decentralized, and federated access control, directories and identity management, access control administration, database access, group-based, role-based, task-based access control, biometric authentication tools, design validation and testing strategies.
- Domain 2: Communications & Network Security – Voice and facsimile communications, VoIP architecture and security, circuit-switched vs packet-switched networks, network architecture, redundancy and availability, internet vs intranet vs extranet, perimeter controls, firewalls, IDS/IPS, SIEM, wireless network security (WPA, WPA2, 802.11i), anti-malware solutions, application and transport layer security, SSL/TLS, VPNs and tunneling protocols (IPSec, L2TP), network security design considerations, cross-domain risks, penetration testing, vulnerability assessment.
- Domain 3: Cryptography – Cryptographic principles and applications, symmetric and asymmetric cryptosystems, block cipher modes, stream ciphers, hash functions, digital signatures, key management lifecycle, key creation, distribution, storage, rotation, revocation, escrow, backup and recovery, Public Key Infrastructure (PKI), certificates, certificate authorities, trust models, certificate chains and revocation, CRLs, OCSP, cross-certification, bridge CA, cryptographic design validation, attack models (brute force, side-channel, cryptanalytic), risk-based cryptographic architecture.
- Domain 4: Security Architecture Analysis – Risk analysis, types of risk, quantifying cyber risks, attack vectors, threat actors, vulnerabilities, product assurance evaluation criteria, Common Criteria (CC), Evaluation Assurance Levels (EALs), ISO/IEC 27000 series, Capability Maturity Model (CMMI), architecture frameworks (DoDAF, Zachman), system security engineering methodologies, design validation techniques, security certification, peer reviews.
- Domain 5: Business Continuity Planning (BCP) & Disaster Recovery Planning (DRP) – Planning phases and deliverables, natural and human-made risks, Business Impact Analysis (BIA), protecting electronic data, remote replication, backup strategies, selecting recovery strategies, recovery objectives (RTO/RPO), cost-benefit analysis, documenting the plan, step-by-step DR planning (information gathering, plan development, testing, ongoing maintenance).
- Domain 6: Physical Security Considerations – Physical security risks, unauthorized access, facility risk, restricted work areas, protection plans, evacuation drills, incident response, design validation, penetration tests, access control violation monitoring.

Unit 8: Microsoft Azure Administrator (AZ-104)

Unit Objectives:

- Manage Azure subscriptions, resource groups, and governance policies.

- Implement identity management, role-based access control (RBAC), and hybrid identities using Azure AD.
- Deploy, configure, and manage Azure compute resources, including VMs and containers.
- Design and secure virtual networking infrastructure with VNet, NSGs, and load balancers.
- Monitor resources, configure backups, and implement disaster recovery solutions.

Unit Outline:

- Module 1: Introduction to Microsoft Azure – Azure overview, global infrastructure, regions and availability zones, resource groups and subscriptions, Azure services overview, compute, storage, networking, and databases.
- Module 2: Manage Azure Identities and Governance – Azure Active Directory (Azure AD), users and groups, roles and RBAC, Azure AD Connect and hybrid identities, password hash sync, pass-through authentication, federation, subscriptions and resource governance, Azure Policies, resource locks, tags, and blueprints.
- Module 3: Implement and Manage Storage – Azure Storage Accounts, blob, file, queue, and table storage, secure and manage storage, Shared Access Signatures (SAS), access keys, firewalls, and encryption, configure Azure Files and Azure Blob Storage, Azure File Sync, lifecycle management, data tiering, import/export data, AzCopy, Azure Import/Export Service.
- Module 4: Deploy and Manage Azure Compute Resources – Virtual Machines (VMs), creating and configuring VMs, availability sets and availability zones, automate VM deployments, ARM Templates, Azure Bicep, Cloud Shell, VM backups and monitoring, Azure Backup, Log Analytics, VM Insights, Azure App Services and containers, App Service Plans, Container Instances, Container Registry.
- Module 5: Configure and Manage Virtual Networking – Virtual Network fundamentals, subnets, IP addressing, network interfaces, NSGs, ASGs, route tables, Azure DNS and name resolution, Azure DNS zones, private DNS, VNet Peering, VPN Gateway, ExpressRoute, Azure Load Balancer, Application Gateway, Traffic Manager, Network Watcher, Connection Monitor, NSG Flow Logs.
- Module 6: Monitor and Maintain Azure Resources – Azure Monitor, alerts, metrics, diagnostic settings, Log Analytics and workbooks, KQL (Kusto Query Language), insights, Recovery Services Vaults, Azure Site Recovery, Azure Automation Accounts, runbooks, Logic Apps.

Unit 9: Certificate of Cloud Security Knowledge (CCSK)

Unit Objectives:

- Define cloud computing concepts, deployment models, and service models.
- Apply cloud governance strategies, risk management, and compliance frameworks.
- Secure cloud infrastructure, networks, workloads, and data using shared responsibility models.
- Implement identity and access management, security monitoring, and incident response.
- Evaluate related technologies such as Zero Trust, AI, and SASE for cloud security.

Unit Outline:

- Domain 1: Cloud Computing Concepts & Architecture – Defining cloud computing, abstraction and orchestration, essential characteristics, cloud service models (IaaS, PaaS, SaaS), cloud deployment models, CSA Enterprise Architecture Model, shared security responsibility model.
- Domain 2: Cloud Governance and Strategies – Cloud governance, governance hierarchy, aligning with requirements and standards, consulting with stakeholders, cloud security frameworks, Cloud Controls Matrix (CCM), CSA STAR Registry, policies.
- Domain 3: Risk, Audit and Compliance – Cloud risk management, cloud risks, corporate risk management strategy, risk assessment and treatment, assessing cloud services, business requests, review CSP documentation, compliance and audit, jurisdictions, privacy laws and regulations, compliance inheritance, artifacts of compliance, GRC tools and technologies.
- Domain 4: Organization Management – Organization hierarchy models, capabilities within a CSP, building hierarchy, managing organization-level security, identity provider and user/group/role mappings, shared services, hybrid and multi-cloud deployments, tooling and staffing.
- Domain 5: Identity and Access Management – How IAM is different in the cloud, fundamental terms, federation, common federation standards, federated identity management, managing users and identities.
- Domain 6: Security Monitoring – Cloud monitoring, logs and events, posture management, management plane logs, service and application logs, resource logs, cloud-native tools, telemetry sources, collection architectures, log storage and retention, cascading log architecture, AI for security monitoring.
- Domain 7: Infrastructure & Networking – Cloud infrastructure security techniques, CSP infrastructure responsibilities, infrastructure resilience, cloud network fundamentals, SDN-based components, cloud connectivity, preventative and detective security measures, Infrastructure as Code (IaC), Zero Trust, Software Defined Perimeter (SDP), ZTNA, SASE.
- Domain 8: Cloud Workload Security – Types of cloud workloads, securing virtual machines, challenges and mitigations, secure VM images, snapshots, securing containers, container image creation and networking, container orchestration security, runtime protection, securing serverless and FaaS, IAM for serverless, securing AI workloads.
- Domain 9: Data Security – Cloud storage primer (object, block, database), data classification, IAM, access policies, encryption and key management, DLP, cloud data encryption at rest, application level encryption, key management strategies (client-side, server-side, customer-managed), KMS, Data Security Posture Management (DSPM).
- Domain 10: Application Security – Secure Development Lifecycle (SSDLC), threat modeling, pre-deployment and post-deployment testing, architecture's role in security, identity and access management for applications, secrets management, DevOps and DevSecOps, CI/CD pipelines, WAFs and API gateways.
- Domain 11: Incident Response & Resilience – Incident response lifecycle, preparation, detection and analysis, cloud system forensics, container and serverless forensics, containment, eradication, recovery, post-incident analysis.
- Domain 12: Related Technologies & Strategies – Zero Trust technical objectives and pillars, Zero Trust and cloud security, AI workloads and cloud security intersection.

Unit 10: Certified AI-Enhanced Industrial Automation and SCADA Systems Engineer (CAIASE)

Unit Objectives:

- Conduct feasibility analysis and cost-benefit assessments for industrial automation projects.
- Analyze operational requirements and design SCADA and control system architectures.
- Develop HMI systems, database reporting, and control configurations for industrial processes.
- Implement safety, security, and compliance measures for cyber-physical systems.
- Deploy, test, and manage industrial automation systems throughout their lifecycle with AI integration.

Unit Outline:

- Domain 1: Feasibility Analysis – Define preliminary scope, techniques for identifying automation opportunities, basics of processes and equipment, control and information technologies, value analysis methods, performing cost/benefit analysis, technical studies, risk assessments, control strategies, justification analyses, lifecycle costs, ROI and NPV models, Lean Six Sigma, stakeholder acceptance, AI-powered predictive analytics and financial modeling.
- Domain 2: Requirement Analysis – Collaborate with stakeholders, define design requirements, applicable codes and standards, data analysis tools, interview techniques, consensus building, analyze technical approaches, control elements (sensors, instruments, actuators, HMIs), develop basis of design, network architecture, safety and regulatory compliance, cost estimation, documentation, AI-enabled optimization and smart control.
- Domain 3: System Architecture and Design – Safety, hazard, security, and compliance analyses, electrical and industry-specific standards (NEC, ISA62443), instrument selection, programming languages (IEC 61131), data requirements and flow analysis, communication media and protocols (Ethernet, Devicenet, Fieldbus), functional descriptions, testing requirements, simulation tools, detailed design, procurement, documentation and user manuals, AI-driven standardization and compliance automation.
- Domain 4: Software Development and Configuration – Develop HMI systems, report configurations, tag definition schemes, alarm configuration, database and reporting functions, control configurations and programs, P&IDs, PFDs, memory addressing, data transfer methodologies, network protocols, system interfaces, implement safety and security systems, stakeholder and peer reviews, acceptance testing (FAT), AI-enhanced HMI design and automated testing.
- Domain 5: Project Deployment – Physical inspections of installed equipment, construction documentation, discrepancy reporting, site acceptance testing (SAT), test safety and security systems, operational testing, control loop tuning, troubleshooting and root-cause analysis, facilitate system turnover, training and handover, AI-powered automated inspection and performance validation.

- Domain 6: Lifecycle Management – Conduct periodic inspections, provide technical support, analyze training needs, deliver training on safe and secure operation, monitor system performance, continuous improvement and optimization, document lessons learned, manage system licenses and updates, evaluate spare parts availability, perform maintenance, backups, and recovery planning, facilitate management of change (MOC), AI-driven predictive maintenance and intelligent disaster recovery.
-

Unit 11: LinkedIn Course for Job Seekers

Unit Objectives:

- Enable learners to effectively use LinkedIn for job searching and freelancing opportunities
- Develop skills in personal branding and content marketing on LinkedIn
- Build professional networks and identify hidden job markets
- Create an optimized LinkedIn profile that attracts recruiters and clients

Unit Curriculum:

- Understanding LinkedIn's ecosystem for job search and freelancing
 - Branding as a subject matter expert and thought leader
 - Content and keyword targeting strategies
 - About Summary optimization and content relevance
 - Networking and identifying the hidden job market
 - LinkedIn Marketplace for freelancers
 - Tools for targeting global emerging technology opportunities
 - Q&A live sessions with LinkedIn coach
 - Toolkits, worksheets, and best practice guides
-

Unit 12: IELTS Academic and General Training

Unit Objectives:

- Prepare students for the IELTS examination
- Improve reading, writing, listening, and speaking skills
- Develop strategies for attempting each section of the IELTS test
- Build confidence in English language usage for academic and general contexts

Unit Curriculum:

- Reading for gist, scanning details, and in-depth reading
 - Listening for gist, important details, and deeper meanings
 - Writing cohesive essays (argumentative, descriptive, discursive)
 - Letter writing and academic analysis of graphs, charts, and tables
 - Speaking fluently in work-based and academic scenarios
 - Everyday conversation skills in English
 - Test-taking strategies and exam techniques
-

COPYRIGHT NOTICE

This document, including all content, text, images, graphics, logos, and course materials, is the exclusive property of ALNAFI E-LEARNING (PRIVATE) LIMITED.

Unauthorized Use Prohibited

No part of this document may be reproduced, stored in a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise) without the prior written permission of the College.

Permitted Use

This document is provided for informational and educational purposes only. You may view, download, and print this document for personal, non-commercial use, provided that:

- All copyright and proprietary notices are retained.
 - The content is not modified or altered in any way.
-

Where Can I find more information?

UK Office Address:

167-169 Great Portland Street 5th Floor London W1W 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**

