RESKILLING LAB
DT-04 TRAINING & SELF-LEARNING PACK

CLOUD COMPUTING

From Digital User to Cloud Practitioner

Beginner → Intermediate | Recommended learning time: 30–50 hours
Expanded Learner Handbook | Version 1.0 | September 2026

How to Use This Handbook

DT-04 develops foundational cloud competence for employees, SME staff, VET learners, jobseekers and career changers. It combines cloud concepts with practical decision-making: selecting service models, organising cloud resources, managing identity and access, protecting data, planning backup and resilience, monitoring cost, and evaluating cloud services for an SME.

The handbook is vendor-neutral in its core theory. Microsoft Azure is used as an optional practical learning environment because it offers a structured beginner pathway, while the underlying concepts also apply to AWS, Google Cloud and other providers. Learners should use only authorised accounts and should understand pricing before creating chargeable resources.

1. Pathway Overview

Item	DT-04 Specification
Pathway	Cloud Computing
Target level	Beginner → Intermediate
Recommended workload	30–50 hours
Target groups	Employees; SME staff; VET learners; jobseekers; career changers; junior IT and digital staff
Entry requirements	Basic digital literacy and familiarity with web applications, files and user accounts
Possible target roles	Cloud Support Technician; Junior Cloud Practitioner; IT Support Specialist; Cloud-enabled Business Professional
Core learning environments	Vendor-neutral theory; optional Microsoft Learn/Azure guided practice
Main evidence	Cloud service inventory; service-model comparison; identity checklist; storage/backup plan; cloud risk register; cost estimate; capstone cloud adoption plan

1.1 Learning Outcomes

- Define cloud computing and explain its essential characteristics.
- Distinguish public, private, community and hybrid deployment concepts.
- Compare SaaS, PaaS and IaaS and explain how responsibility changes across them.
- Explain compute, storage, networking, databases and serverless services at a foundational level.
- Understand regions, availability zones, scalability, elasticity and high availability.
- Apply identity, MFA, least privilege and role-based access principles in cloud environments.
- Explain the shared responsibility model and identify responsibilities that remain with the customer.
- Recognise common cloud-security risks including misconfiguration, excessive permissions and exposed data.
- Plan basic backup, recovery, business-continuity and resilience requirements.
- Explain consumption-based pricing, cost drivers, budgets and basic FinOps practices.
- Assess cloud services for SME requirements including security, portability, support and vendor dependency.
- Describe basic cloud governance, logging, monitoring and compliance considerations.
- Create a practical cloud adoption and improvement plan for a small organisation.

1.2 Reference Framework

NIST SP 800-145 defines cloud computing through five essential characteristics, three service models and four deployment models. DT-04 uses this definition as its conceptual foundation. For practical progression, the current Microsoft Azure Fundamentals learning structure is used as an optional benchmark: cloud concepts; architecture and services; and management and governance.

Reference	Use in DT-04
NIST SP 800-145	Definition, essential characteristics, service models and deployment models.
Microsoft Azure Fundamentals / AZ-900	Optional beginner progression for cloud concepts, architecture, services, management and governance.
ENISA Cloud Security Guide for SMEs	SME-oriented cloud procurement, security risks, opportunities and provider questions.
NIST CSF 2.0	General cybersecurity risk-management context for cloud use.

2. Initial Skills Check

#	Statement	0 No	1 Partly	2 Yes
1	I can explain what makes a service a cloud service.	☐	☐	☐
2	I understand the difference between SaaS, PaaS and IaaS.	☐	☐	☐
3	I can explain public, private and hybrid cloud at a basic level.	☐	☐	☐
4	I understand what compute, storage and networking mean in cloud architecture.	☐	☐	☐
5	I can explain scalability and elasticity.	☐	☐	☐
6	I understand regions and availability zones.	☐	☐	☐
7	I can explain the shared responsibility model.	☐	☐	☐
8	I know why MFA and least privilege matter in cloud environments.	☐	☐	☐
9	I can identify common cloud misconfiguration risks.	☐	☐	☐
10	I understand basic cloud backup and recovery concepts.	☐	☐	☐
11	I can explain consumption-based pricing and common cost drivers.	☐	☐	☐
12	I can identify questions an SME should ask before selecting a cloud provider.	☐	☐	☐

Indicative formative interpretation: 0–8 Foundation needed; 9–16 Developing; 17–20 Functional; 21–24 Ready for intermediate practice.

3. What Is Cloud Computing?

Cloud computing is a model for obtaining configurable computing resources over a network on demand. Instead of purchasing and operating every server, storage device or software platform locally, an organisation can consume services provided from shared infrastructure and provision or release resources as requirements change.

NIST identifies five essential characteristics: on-demand self-service, broad network access, resource pooling, rapid elasticity and measured service. These characteristics distinguish cloud computing from

ordinary remote hosting. The user can obtain resources with limited provider interaction, access them through networks, share pooled infrastructure, scale capacity and consume services in a measurable way.

Cloud adoption changes both technology and operating models. Capital expenditure on owned hardware may shift toward operating expenditure based on consumption or subscription. Provisioning can become faster, but cost can also become less predictable if resources are created without governance.

For SMEs, cloud value often comes from access to capabilities that would otherwise require specialised infrastructure or staff. However, convenience does not remove the need for security, configuration, continuity planning, data governance or supplier management.

Practical Application

- Apply the concepts to a fictional 25-person SME using cloud email, shared files, accounting software, a website and remote work.
- Identify one business benefit, one technical risk, one governance risk and one cost consideration.
- Record one decision that should be made by management rather than left solely to a cloud provider.

4. Cloud Deployment Models

A public cloud is operated by a provider that offers services to multiple customers from shared infrastructure. Customers remain logically separated even though physical resources may be pooled. Public cloud provides rapid access to scale and broad service catalogues.

A private cloud is provisioned for exclusive use by one organisation. It may be operated internally or by a third party. Private cloud can provide greater control over architecture and location but usually requires more management capability.

A hybrid cloud combines distinct cloud or on-premises environments with integration or portability between them. Organisations may retain sensitive or legacy workloads locally while using public cloud for other services.

NIST also defines community cloud for exclusive use by a community of organisations with shared concerns. In practice, deployment decisions should be based on workload, regulation, security, cost, latency, integration and organisational capability rather than labels alone.

Practical Application

- Apply the concepts to a fictional 25-person SME using cloud email, shared files, accounting software, a website and remote work.
- Identify one business benefit, one technical risk, one governance risk and one cost consideration.
- Record one decision that should be made by management rather than left solely to a cloud provider.

5. SaaS, PaaS and IaaS

Software as a Service provides a complete application for users. Examples include cloud email, collaboration, CRM and accounting applications. The customer mainly manages users, data, configuration and appropriate use while the provider operates much of the underlying technology.

Platform as a Service provides a managed environment for developing or running applications without requiring the customer to manage the underlying physical infrastructure and usually not the operating system. The customer remains responsible for application logic, data, identities and relevant configuration.

Infrastructure as a Service provides virtualised compute, storage and networking. The provider manages physical infrastructure, while the customer takes greater responsibility for operating systems, applications, network configuration and workload security.

The service model affects required expertise. Moving from SaaS toward IaaS gives the customer greater flexibility and control but also greater operational responsibility. SMEs should not choose a lower-level service simply because it appears more technically powerful.

Practical Application

- Apply the concepts to a fictional 25-person SME using cloud email, shared files, accounting software, a website and remote work.
- Identify one business benefit, one technical risk, one governance risk and one cost consideration.
- Record one decision that should be made by management rather than left solely to a cloud provider.

6. Shared Responsibility in the Cloud

Cloud security is a shared responsibility between provider and customer. The exact boundary depends on the service. The provider generally secures physical datacentres, physical networks and hosts. Customer responsibility increases as the organisation moves from SaaS toward PaaS and IaaS.

Certain responsibilities remain important for customers across cloud models: customer data, user identities, access decisions, configuration choices and the security of devices under their control. A secure cloud platform can still be used insecurely through weak accounts, excessive permissions or public sharing.

Shared responsibility should be examined service by service rather than treated as a slogan. Contracts, configuration options, backup arrangements, logging and support models can differ even within the same provider.

Responsibility also applies to reliability. Providers may offer availability zones, replication and backup capabilities, but customers often need to select and configure them according to business requirements.

Practical Application

- Apply the concepts to a fictional 25-person SME using cloud email, shared files, accounting software, a website and remote work.
- Identify one business benefit, one technical risk, one governance risk and one cost consideration.
- Record one decision that should be made by management rather than left solely to a cloud provider.

7. Cloud Architecture: Regions, Zones and Resources

Cloud providers operate datacentres grouped into geographic regions. A region is a defined geographic area in which services are delivered. Organisations select regions based on latency, availability, service support, data-location requirements, cost and resilience.

Availability zones are physically separated locations within a region designed to reduce the chance that a single local failure affects all instances of a workload. Using zones can improve resilience, but applications must be designed and configured to benefit from them.

Cloud resources are manageable service instances such as virtual machines, databases, storage accounts or networks. Providers organise resources through accounts, subscriptions, projects, resource groups or similar structures. Good organisation supports ownership, permissions, cost allocation and lifecycle management.

Architecture should reflect business criticality. Not every workload needs multi-region design. The objective is to select resilience proportional to the impact of downtime.

Practical Application

- Apply the concepts to a fictional 25-person SME using cloud email, shared files, accounting software, a website and remote work.
- Identify one business benefit, one technical risk, one governance risk and one cost consideration.
- Record one decision that should be made by management rather than left solely to a cloud provider.

8. Compute Services and Virtualisation

Compute provides processing capacity for applications and workloads. Traditional cloud compute often uses virtual machines: software-defined computers with virtual CPU, memory, storage and networking running on shared physical hosts.

Virtualisation improves utilisation and isolation by allowing multiple virtual machines to operate on one physical server. Customers can choose operating systems and configurations but are responsible for managing those systems in IaaS.

Containers package an application with its dependencies while sharing more of the underlying operating system than a virtual machine. Containers can improve portability and deployment consistency, but orchestration and security introduce additional concepts.

Serverless computing allows developers to run code or functions without managing servers directly. The provider manages infrastructure scaling while the customer focuses on code, data and configuration. 'Serverless' does not mean that servers do not exist; it means the customer does not manage them directly.

Practical Application

- Apply the concepts to a fictional 25-person SME using cloud email, shared files, accounting software, a website and remote work.
- Identify one business benefit, one technical risk, one governance risk and one cost consideration.
- Record one decision that should be made by management rather than left solely to a cloud provider.

9. Cloud Storage

Cloud storage services provide durable storage for files, objects, disks, backups and other data. Different storage types are optimised for different access patterns. Object storage is widely used for documents, media, logs and data lakes; block storage commonly supports virtual-machine disks; file services provide shared hierarchical file access.

Storage design should consider performance, durability, availability, access frequency, retention and cost. Frequently accessed data may use a different storage tier from long-term archives.

Replication improves durability by maintaining additional copies, but replication is not identical to backup. If an authorised user deletes or corrupts replicated data, the change may also be replicated. Backup requires independent recovery points and retention appropriate to the business.

Public access settings are a major security consideration. Storage should be private by default unless there is a clear business requirement for public access.

Practical Application

- Apply the concepts to a fictional 25-person SME using cloud email, shared files, accounting software, a website and remote work.
- Identify one business benefit, one technical risk, one governance risk and one cost consideration.
- Record one decision that should be made by management rather than left solely to a cloud provider.

10. Cloud Networking

Cloud networking connects resources to one another, users and the internet. Core concepts include virtual networks, subnets, IP addressing, routing, firewalls, gateways, load balancing and private connectivity.

A virtual network creates a logically isolated network environment. Subnets divide it into smaller segments. Network-security rules control which traffic can flow between systems. Good design reduces unnecessary exposure.

Public endpoints are reachable from the internet; private endpoints restrict access through private network paths. Internet exposure should be deliberate, documented and protected.

Load balancers distribute traffic across multiple service instances and can improve availability and performance. Network design should be integrated with identity and application controls rather than treated as the only security boundary.

Practical Application

- Apply the concepts to a fictional 25-person SME using cloud email, shared files, accounting software, a website and remote work.
- Identify one business benefit, one technical risk, one governance risk and one cost consideration.
- Record one decision that should be made by management rather than left solely to a cloud provider.

11. Cloud Databases and Managed Data Services

Cloud databases can be delivered as managed services in which the provider handles much of the underlying infrastructure, patching and availability. Relational services support structured tables and SQL; NoSQL services support other data models and scalability patterns.

Managed databases reduce operational work but do not remove customer responsibility for access, data classification, query security, retention and application design.

Database selection should follow workload requirements: transaction consistency, query patterns, scale, latency, analytics needs and skills. Choosing a fashionable database without a clear requirement can increase complexity.

Backups, point-in-time recovery, replication and encryption capabilities should be reviewed explicitly. Default settings may not meet every business recovery objective.

Practical Application

- Apply the concepts to a fictional 25-person SME using cloud email, shared files, accounting software, a website and remote work.
- Identify one business benefit, one technical risk, one governance risk and one cost consideration.
- Record one decision that should be made by management rather than left solely to a cloud provider.

12. Scalability, Elasticity and Performance

Scalability is the ability to increase or decrease capacity to meet workload requirements. Vertical scaling changes the capacity of an individual resource; horizontal scaling changes the number of resource instances.

Elasticity is the ability to adjust resources dynamically as demand changes. Elastic services can reduce over-provisioning but require appropriate scaling rules and application design.

Performance is influenced by compute size, storage type, network latency, architecture, database design and application behaviour. Increasing resources is not always the most efficient solution; bottlenecks should be measured.

Cloud design balances performance, reliability and cost. A solution with maximum capacity at all times may be technically fast but financially inefficient.

Practical Application

- Apply the concepts to a fictional 25-person SME using cloud email, shared files, accounting software, a website and remote work.
- Identify one business benefit, one technical risk, one governance risk and one cost consideration.
- Record one decision that should be made by management rather than left solely to a cloud provider.

13. Availability, Reliability and Disaster Recovery

Availability is the proportion of time a service is accessible as required. Providers may publish service-level agreements, but an application can still fail because of customer configuration, software defects or dependencies outside the SLA.

Reliability is the ability of a workload to perform correctly and recover from failures. It depends on architecture, redundancy, monitoring, recovery procedures and operational discipline.

Recovery Time Objective defines the target time for restoring a service. Recovery Point Objective defines the acceptable amount of data loss measured in time. These business requirements should drive backup frequency and architecture.

Disaster recovery can use backup restoration, standby environments or active deployments across locations. More resilience usually increases cost and complexity, so the design should match business impact.

Practical Application

- Apply the concepts to a fictional 25-person SME using cloud email, shared files, accounting software, a website and remote work.
- Identify one business benefit, one technical risk, one governance risk and one cost consideration.
- Record one decision that should be made by management rather than left solely to a cloud provider.

14. Identity and Access Management

Identity is one of the most important cloud security boundaries. Cloud platforms use identity systems to authenticate users, applications and services and to determine what they may access.

Multi-factor authentication reduces dependence on passwords alone. Administrative accounts, email accounts and remote-access identities should receive particular protection.

Role-Based Access Control assigns permissions according to roles. Least privilege means granting only the permissions required for a task. Broad administrator rights increase both accidental and malicious risk.

Cloud environments also use service identities or managed identities for applications. Credentials embedded in scripts or configuration files should be avoided where secure identity mechanisms are available.

Practical Application

- Apply the concepts to a fictional 25-person SME using cloud email, shared files, accounting software, a website and remote work.
- Identify one business benefit, one technical risk, one governance risk and one cost consideration.
- Record one decision that should be made by management rather than left solely to a cloud provider.

15. Cloud Security and Common Misconfigurations

Many cloud incidents arise not because the provider's infrastructure failed, but because resources were configured insecurely. Common examples include public storage, exposed management interfaces, weak administrator accounts, excessive permissions and unmonitored access keys.

Defence in depth combines identity, network controls, endpoint security, encryption, logging, secure configuration and monitoring. No single control is sufficient.

Encryption should protect sensitive data in transit and at rest where appropriate. Key management is part of the security design; losing a key can make data unavailable, while uncontrolled key access weakens confidentiality.

Configuration baselines and automated policy checks can reduce drift. SMEs should begin with secure defaults and document exceptions.

Practical Application

- Apply the concepts to a fictional 25-person SME using cloud email, shared files, accounting software, a website and remote work.
- Identify one business benefit, one technical risk, one governance risk and one cost consideration.
- Record one decision that should be made by management rather than left solely to a cloud provider.

16. Monitoring, Logging and Cloud Operations

Cloud platforms generate logs and metrics that can show authentication events, resource changes, performance, network activity and application behaviour. Monitoring turns these signals into operational awareness.

Metrics are numerical measurements such as CPU usage, request count or latency. Logs contain event records. Alerts notify responsible people when defined conditions occur.

Operational monitoring should focus on business-relevant events, not only infrastructure. A service may be technically online while a critical transaction is failing.

Logs also support security investigations and accountability. Retention periods, access permissions and cost should be planned because high-volume logging can become expensive.

Practical Application

- Apply the concepts to a fictional 25-person SME using cloud email, shared files, accounting software, a website and remote work.
- Identify one business benefit, one technical risk, one governance risk and one cost consideration.
- Record one decision that should be made by management rather than left solely to a cloud provider.

17. Cloud Cost Management and FinOps Foundations

Cloud pricing is often consumption-based. Costs may arise from compute time, storage capacity, transactions, database tiers, network transfer, backup, monitoring and premium support. Resources that appear inexpensive individually can accumulate substantial monthly cost.

Cost management begins with visibility. Tags, labels, projects or resource groups can associate spending with owners, departments or services. Budgets and alerts can identify unexpected consumption.

Rightsizing means matching resource capacity to actual demand. Idle virtual machines, oversized databases, unattached disks and unnecessary retained snapshots are common sources of waste.

FinOps is a collaborative approach to cloud financial management in which technology, finance and business teams use timely cost information to make value-based decisions. Cost optimisation should not undermine required security or resilience.

Practical Application

- Apply the concepts to a fictional 25-person SME using cloud email, shared files, accounting software, a website and remote work.
- Identify one business benefit, one technical risk, one governance risk and one cost consideration.
- Record one decision that should be made by management rather than left solely to a cloud provider.

18. Cloud Governance and Resource Management

Cloud governance defines how resources may be created, configured, owned, monitored and retired. Without governance, rapid self-service can lead to inconsistent naming, unclear ownership, security gaps and uncontrolled cost.

A basic governance model includes account/subscription structure, naming standards, tagging, approved regions, identity rules, security baselines, budget controls, logging and lifecycle procedures.

Policy-as-code or platform policies can automatically enforce or audit configuration requirements. Even small organisations can benefit from simple preventive rules, such as prohibiting public storage unless approved.

Governance should enable responsible use rather than create unnecessary bureaucracy. The controls should be proportional to risk and understandable to users.

Practical Application

- Apply the concepts to a fictional 25-person SME using cloud email, shared files, accounting software, a website and remote work.
- Identify one business benefit, one technical risk, one governance risk and one cost consideration.
- Record one decision that should be made by management rather than left solely to a cloud provider.

19. Cloud Migration and Adoption for SMEs

Cloud migration should start with business objectives. Possible goals include reducing hardware management, improving remote access, increasing resilience, modernising applications or enabling new digital services.

Workloads can be retained, retired, rehosted, replatformed, refactored, repurchased as SaaS or replaced. Moving a poorly designed application unchanged to a virtual machine may provide limited cloud benefit.

An SME should inventory applications, data, dependencies, owners and criticality before migration. It should also identify internet connectivity requirements, licensing implications, skills gaps and exit options.

A pilot with a low-risk workload can build experience before critical systems are migrated. Success measures should include usability, performance, cost, security and support workload.

Practical Application

- Apply the concepts to a fictional 25-person SME using cloud email, shared files, accounting software, a website and remote work.
- Identify one business benefit, one technical risk, one governance risk and one cost consideration.
- Record one decision that should be made by management rather than left solely to a cloud provider.

20. Cloud Procurement, Vendor Risk and Lock-In

Cloud procurement is a technology and supplier-management decision. Organisations should evaluate service availability, security controls, support, contractual terms, data location, backup, portability, interoperability and incident notification.

Vendor lock-in occurs when moving to another provider becomes difficult because of proprietary services, data formats, architecture or commercial dependencies. Lock-in is not automatically unacceptable, but it should be understood and justified by the value obtained.

Exit planning should begin before procurement. Organisations should know how data can be exported, in what format, how long extraction may take, what it costs and how data will be deleted after termination.

ENISA's SME cloud-security guidance recommends that small organisations ask providers concrete security questions rather than relying only on general marketing claims.

Practical Application

- Apply the concepts to a fictional 25-person SME using cloud email, shared files, accounting software, a website and remote work.
- Identify one business benefit, one technical risk, one governance risk and one cost consideration.
- Record one decision that should be made by management rather than left solely to a cloud provider.

21. Data Protection, Compliance and Cloud Location

Cloud use can involve personal, confidential or regulated information. Organisations should understand what data is processed, for what purpose, where it may be stored or accessed, who can access it and what contractual safeguards apply.

Data residency refers to where data is stored, while data sovereignty concerns the legal regimes that may apply. Selecting a region can be relevant but does not by itself resolve every legal or contractual question.

Compliance is a shared organisational responsibility. A provider's certification can support assurance, but it does not automatically make the customer's workload compliant. Configuration and actual use remain important.

Retention and deletion requirements should be implemented across primary storage, backups, logs and exported copies where applicable.

Practical Application

- Apply the concepts to a fictional 25-person SME using cloud email, shared files, accounting software, a website and remote work.
- Identify one business benefit, one technical risk, one governance risk and one cost consideration.
- Record one decision that should be made by management rather than left solely to a cloud provider.

22. Cloud Collaboration and Digital Workplace

SaaS collaboration platforms combine email, file sharing, meetings, calendars and productivity applications. They can support flexible work but centralise large amounts of organisational information.

Sharing should follow least privilege. Public links, unrestricted external sharing and persistent guest access can expose data. Organisations should periodically review sharing and inactive accounts.

Version history, co-authoring and cloud storage improve productivity, but employees need clear rules for where official records should be stored and how sensitive documents should be shared.

Cloud collaboration security depends strongly on identity. MFA, conditional access where available, device security and rapid account offboarding are high-value controls.

Practical Application

- Apply the concepts to a fictional 25-person SME using cloud email, shared files, accounting software, a website and remote work.
- Identify one business benefit, one technical risk, one governance risk and one cost consideration.
- Record one decision that should be made by management rather than left solely to a cloud provider.

23. Emerging Cloud: Containers, Serverless, Edge and AI Services

Cloud platforms increasingly provide managed containers, serverless functions, AI services, data platforms and edge capabilities. These services allow organisations to build advanced systems without owning the underlying infrastructure.

Containers improve portability but introduce image, registry, orchestration and secret-management risks. Serverless reduces infrastructure management but requires secure code, permissions and event configuration.

Edge computing processes data closer to devices or users when latency, connectivity or local processing matters. Edge and cloud often operate together rather than as alternatives.

AI services extend the shared-responsibility concept. Organisations remain responsible for their data, identities, access and appropriate use even when the provider operates the model and infrastructure.

Practical Application

- Apply the concepts to a fictional 25-person SME using cloud email, shared files, accounting software, a website and remote work.
- Identify one business benefit, one technical risk, one governance risk and one cost consideration.
- Record one decision that should be made by management rather than left solely to a cloud provider.

24. Practical Lab Series

Lab	Focus	Task	Evidence
Lab 1	Cloud Service Inventory	Classify 12 organisational services as on-premises, SaaS, PaaS or IaaS.	Service inventory
Lab 2	Deployment Decision	Compare public, private and hybrid options for three SME workloads.	Decision matrix
Lab 3	Shared Responsibility	Map provider/customer responsibilities for SaaS, PaaS and IaaS scenarios.	Responsibility matrix
Lab 4	Cloud Architecture	Draw a simple architecture with users, identity, network, compute, storage and database.	Architecture diagram
Lab 5	Identity & Access	Review fictional users and roles; apply MFA and least privilege.	IAM checklist
Lab 6	Storage & Sharing	Classify data and define secure storage/sharing settings.	Storage policy
Lab 7	Backup & Recovery	Define backup frequency, RPO, RTO	Recovery plan

		and restore testing.	
Lab 8	Cost Estimation	Identify cost drivers and create a monthly budget estimate.	Cost worksheet
Lab 9	Cloud Security Review	Identify ten misconfigurations in a fictional cloud environment.	Risk register
Lab 10	Provider Assessment	Use a structured questionnaire to assess a cloud/SaaS supplier.	Supplier scorecard
Lab 11	Monitoring Plan	Define key logs, metrics, alerts and owners.	Monitoring matrix
Lab 12	Capstone	Create an SME cloud adoption and governance plan.	Portfolio + presentation

25. Shared Responsibility Practice Matrix

Area	**SaaS**	**PaaS**	**IaaS**
Physical datacentre	Provider	Provider	Provider
Physical network/hosts	Provider	Provider	Provider
Operating system	Provider	Provider	Customer
Application platform	Provider	Mostly provider	Customer
Application configuration	Customer/shared	Customer	Customer
Customer data	Customer	Customer	Customer
Identities/users	Customer	Customer	Customer
Access permissions	Customer	Customer	Customer
Client endpoints	Customer/shared	Customer	Customer
Workload architecture	Limited customer scope	Customer/shared	Customer

The matrix is an educational simplification. Actual responsibilities vary by service and contract; learners should review the provider's current documentation.

26. SME Cloud Provider Assessment Checklist

Question	**Evidence to request / review**
Where can our data be stored and processed?	Region options, contractual documentation
How is customer data isolated?	Architecture/security documentation
What MFA and access-control options exist?	Identity/security settings
What logging is available?	Audit and activity-log documentation
How are backups and recovery handled?	Backup scope, retention, restore process
What availability commitment applies?	Current SLA and exclusions
How are incidents communicated?	Incident-notification process
Can we export our data?	Export format, API, migration documentation
How is data deleted after termination?	Deletion/retention terms
Which certifications or assurance reports are available?	Current audit/certification evidence
What support level is included?	Support channels and response commitments
How can costs be monitored and limited?	Budgets, alerts, billing reports

27. SME Case Studies

Case 1 – File Server to Cloud Storage

A 15-person consultancy wants to replace an ageing office file server.

Task: Compare SaaS file collaboration with IaaS file-server hosting. Address identity, sharing, backup, migration, cost and user training.

Case 2 – Public Storage Exposure

A marketing team accidentally configures a storage location for public access.

Task: Identify immediate containment, logging, data-exposure assessment and preventive controls.

Case 3 – Rapid Growth

An e-commerce SME experiences seasonal traffic spikes.

Task: Explain scalability, elasticity, load balancing and cost controls appropriate to the scenario.

Case 4 – Cloud Outage

A critical SaaS application becomes unavailable for several hours.

Task: Identify business-continuity dependencies, alternative procedures and supplier questions.

Case 5 – Departing Employee

An employee leaves but retains access to cloud files through an old account and personal device.

Task: Design an offboarding process covering identity, sessions, shared links, devices and ownership.

Case 6 – Unexpected Bill

A development team leaves test resources running and monthly cloud cost triples.

Task: Design tagging, ownership, budget alerts, shutdown and review controls.

28. Capstone Project – SME Cloud Adoption Plan

Prepare a practical cloud adoption or cloud improvement plan for a fictional SME or an organisation for which you have explicit permission.

1. Organisation profile and business objectives.
2. Current IT/service inventory.
3. Workload classification and criticality.
4. Recommended deployment and service models.
5. High-level target cloud architecture.
6. Identity and access-management plan.
7. Data classification, storage and sharing rules.
8. Backup, RPO, RTO and recovery-testing plan.
9. Security and shared-responsibility matrix.
10. Supplier/procurement assessment.
11. Cost drivers, budget controls and ownership.

12. Monitoring and logging plan.
13. Migration phases and user-training needs.
14. Exit/portability considerations.
15. One-page management summary with five priority actions.

Capstone Assessment Rubric

Criterion	Weight
Business requirements and workload analysis	15%
Architecture and service-model selection	15%
Security and shared responsibility	20%
Identity, data and access governance	15%
Reliability, backup and recovery	10%
Cost and operational governance	10%
Supplier/exit considerations	5%
Feasibility, communication and evidence	10%

29. Final Knowledge Assessment

1. What are the five NIST cloud characteristics?

2. What are the three principal cloud service models?

3. Which model usually gives the customer the greatest infrastructure responsibility?

4. What is elasticity?

5. What is an availability zone?

6. Who remains responsible for customer data and identities in common cloud models?

7. Why is replication not the same as backup?

8. What does least privilege mean?

9. What is RTO?

10. What is RPO?

11. What is vendor lock-in?

12. Why can cloud costs become unexpectedly high?

Answer Key

1. On-demand self-service, broad network access, resource pooling, rapid elasticity and measured service.

2. SaaS, PaaS and IaaS.

3. IaaS.

4. The ability to adjust resources dynamically as demand changes.

5. A physically separated location within a cloud region designed to support resilience.

6. The customer retains important responsibility for data and identities.

7. Replicated deletion or corruption may propagate; backup preserves independent recovery points.

8. Grant only the permissions necessary for a legitimate role or task.

9. The target time to restore a service.

10. The acceptable amount of data loss measured in time.

11. Difficulty or cost in moving because of provider-specific technology, data formats or dependencies.

12. Consumption-based resources can accumulate cost when oversized, idle, retained or poorly governed.

30. Post-Training Skills Check and Reflection

Repeat the Initial Skills Check and compare the result with evidence from the practical labs and capstone.

- Which service model is most appropriate for your organisation's common workloads and why?
- Which cloud responsibility is most likely to be misunderstood by non-technical staff?
- Which identity control should be implemented first?
- What is your organisation's most important recovery requirement?
- Which cloud cost could become invisible without ownership and tagging?
- What additional learning do you need: administration, networking, security, DevOps, data or cloud architecture?

31. Career Transition Guide

Starting profile	Possible direction	Portfolio evidence
General digital user	Cloud-enabled Business Professional	Service inventory; secure-sharing checklist
Administrative / office staff	Cloud Collaboration / Support role	Identity, sharing and offboarding procedures
IT support	Cloud Support Technician	Architecture diagram; IAM review; monitoring plan
Junior technical learner	Junior Cloud Practitioner	Service-model labs; cost plan; cloud security review
SME manager	Cloud Adoption Coordinator	Provider assessment; governance and adoption plan
Cybersecurity learner	Cloud Security pathway	Shared responsibility; IAM; logging; configuration-risk register

32. Glossary

Term	Definition
Cloud Computing	On-demand network access to a shared pool of configurable computing resources.
SaaS	Software as a Service.
PaaS	Platform as a Service.

IaaS	Infrastructure as a Service.
Public Cloud	Cloud infrastructure offered for use by multiple customers.
Private Cloud	Cloud infrastructure provisioned for exclusive use by one organisation.
Hybrid Cloud	Use of distinct environments with integration or portability between them.
Region	A geographic area in which a cloud provider delivers services.
Availability Zone	A separated datacentre location within a region used for resilience.
Virtual Machine	A software-defined computer running on virtualised infrastructure.
Container	A packaged application environment sharing the host operating-system kernel.
Serverless	A model in which the provider manages server infrastructure while customers deploy code or functions.
Object Storage	Storage for data represented as objects with metadata and identifiers.
Virtual Network	A logically isolated cloud network.
Scalability	Ability to increase or decrease capacity.
Elasticity	Dynamic adjustment of capacity according to demand.
High Availability	Design aimed at maintaining service despite component failures.
RTO	Recovery Time Objective.
RPO	Recovery Point Objective.
IAM	Identity and Access Management.
RBAC	Role-Based Access Control.
Least Privilege	Granting only necessary permissions.
Shared Responsibility	Division of security/operational responsibilities between provider and customer.
SLA	Service Level Agreement.
FinOps	Collaborative cloud financial management focused on value and accountability.
Vendor Lock-In	Dependency that makes migration to another provider difficult or costly.
Data Residency	Geographic location where data is stored.
Cloud Governance	Policies and controls governing cloud resources, security, cost and lifecycle.

33. Curated Learning Resources

NIST SP 800-145 – The NIST Definition of Cloud Computing
https://csrc.nist.gov/pubs/sp/800/145/final
Primary reference for the five essential characteristics, three service models and four deployment models.

Microsoft Learn – Introduction to Cloud Infrastructure: Describe Cloud Concepts
https://learn.microsoft.com/en-us/learn/paths/azure-fundamentals/
Beginner learning path covering cloud concepts, deployment models and shared responsibility.

Microsoft Learn – Azure Fundamentals Certification
https://learn.microsoft.com/en-us/credentials/certifications/azure-fundamentals/
Optional progression toward a recognised foundational Azure credential.

Microsoft Learn – AZ-900 Study Guide
https://learn.microsoft.com/en-us/credentials/certifications/resources/study-guides/az-900
Current skills outline for cloud concepts, Azure architecture/services, management and governance.

Microsoft Learn – Shared Responsibility in the Cloud
https://learn.microsoft.com/en-us/azure/security/fundamentals/shared-responsibility
Detailed explanation of provider/customer responsibility across SaaS, PaaS and IaaS.

ENISA – Cloud Security Guide for SMEs
https://www.enisa.europa.eu/publications/cloud-security-guide-for-smes
SME-focused security risks, opportunities and questions for cloud providers.

NIST Cybersecurity Framework 2.0
https://www.nist.gov/cyberframework
Useful general risk-management framework for cloud governance and security.

AWS Skill Builder
https://skillbuilder.aws/
Optional provider-specific learning for AWS; verify current free/paid course and credential conditions.

Google Cloud Skills Boost
https://www.cloudskillsboost.google/
Optional provider-specific cloud learning; verify current access and credential conditions.

34. Certification and Progression

DT-04 should be presented as a ReskillingLab pathway completion record rather than as equivalent to a vendor certification. Learners who want a recognised vendor credential can continue with an appropriate provider-specific pathway.

- Microsoft Certified: Azure Fundamentals (AZ-900) is a relevant optional next step. Microsoft currently describes it as a beginner certification covering cloud concepts, Azure architecture/services, and management/governance.
- After fundamentals, learners can specialise in cloud administration, security, data, development, DevOps or architecture.
- AWS and Google Cloud also provide foundational learning and certification ecosystems; the appropriate choice should reflect the learner's target role and employer environment.
- Certification names, exam objectives, prices and availability can change and should be verified before ReskillingLab publishes them.

35. Suggested 30–50 Hour Delivery Plan

Component	Indicative hours
Orientation and initial skills check	2
Cloud fundamentals, deployment and service models	5
Architecture, compute, storage and networking	7
Databases, scalability and reliability	5
Identity, security and shared responsibility	6
Monitoring, governance and cost management	5
Migration, procurement and compliance	4
Practical labs and case studies	6
Capstone, assessment and reflection	5–10
Total (can be compressed to approximately 30 hours by reducing guided practice)	45–50 hours;

36. Trainer / Facilitator Notes

- Teach concepts before provider-specific interfaces.
- Use diagrams to show responsibility boundaries and architecture.
- Do not create chargeable cloud resources without clear learner authorisation and cost controls.
- Use fictional or non-sensitive data for cloud labs.
- Require learners to connect technical choices to business continuity, security and cost.
- Emphasise that provider security does not remove customer responsibility.
- Ask learners to document assumptions, owners and exit options in the capstone.
- Update certification and provider-specific information before each delivery.

37. References

Mell, P., & Grance, T. (2011). The NIST Definition of Cloud Computing. NIST Special Publication 800-145.

Microsoft Learn. (2026). Introduction to Cloud Infrastructure: Describe cloud concepts.

Microsoft Learn. (2026). Microsoft Certified: Azure Fundamentals.

Microsoft Learn. (2026). Study guide for Exam AZ-900: Microsoft Azure Fundamentals.

Microsoft Learn. (2026). Shared responsibility in the cloud.

European Union Agency for Cybersecurity (ENISA). (2015). Cloud Security Guide for SMEs.

National Institute of Standards and Technology. (2024). The NIST Cybersecurity Framework (CSF) 2.0.

38. Website Publishing Structure

For ReskillingLab, DT-04 should be published as modular content using a consistent interface: Learn | Practice | Check Your Understanding | Resources.

- Overview & Initial Skills Check
- Cloud Fundamentals
- Deployment Models
- SaaS, PaaS & IaaS
- Shared Responsibility
- Cloud Architecture
- Compute & Virtualisation
- Storage
- Networking
- Managed Databases
- Scalability & Performance
- Reliability & Disaster Recovery
- Identity & Access
- Cloud Security
- Monitoring & Operations
- Cost Management & FinOps
- Governance
- Cloud Migration

- Procurement & Vendor Risk
- Data Protection & Compliance
- Digital Workplace
- Emerging Cloud Services
- Labs & Cases
- Capstone
- Assessment
- Resources, Credentials & Glossary