

Glossary

The following glossary defines the core terminology used throughout this book. Definitions are written to stand alone: each explains what a term means, why it matters to a Trusted Advisor, and, where relevant, how Azure implements the underlying concept. This edition has been audited against the final text of Chapters 1-22: unused entries were reviewed, missing high-frequency terms were added, and every definition has been checked for consistent British English.

A

Access Control

The set of policies, mechanisms and administrative practices used to determine who or what may access a resource, and under what conditions. In modern enterprise architecture, access control shifts from static, network-based permissions toward continuous, identity-based evaluation informed by user, device, and session risk.

Acquisition Integration

The structured process of bringing an acquired company's identity, applications, data and infrastructure into an enterprise's existing platform, sequenced to protect security and business continuity from day zero through full integration.

Active Directory

Microsoft's directory service for on-premises identity and access management, providing authentication and authorisation for users, computers and other resources within a Windows-based network. Hybrid identity architectures synchronise or federate Active Directory with Microsoft Entra ID to extend a single identity across on-premises and cloud environments.

Active-Active

A resilience architecture in which two or more sites simultaneously process live traffic, so that the failure of one site is designed to minimise or avoid service interruption because the other instances are already processing live traffic. Contrasted with active-passive, where a standby site remains idle until called upon.

Active-Passive

A resilience architecture in which a standby site or system remains idle, ready to take over should the primary site fail. Simpler and cheaper to operate than active-active, but recovery still requires a failover event.

ADR (Architecture Decision Record)

A structured document that captures a significant architectural decision, the context in which it was made, the alternatives considered, the rationale for the chosen approach and the resulting consequences. ADRs provide organisational memory and support governance throughout the lifecycle of an enterprise architecture.

Agility

The capacity of an organisation to sense change and respond with speed and confidence, without sacrificing control. In cloud transformation, agility is created deliberately through governance, automation and platform design rather than assumed as a natural side effect of migration.

AIOps

The application of artificial intelligence and machine learning to IT operations data, used to reduce alert noise, correlate related signals and surface the events that genuinely require human attention. AIOps supports the shift from reactive monitoring to proactive, predictive operations.

AKS (Azure Kubernetes Service)

Microsoft's managed Kubernetes offering, which removes the operational burden of control-plane management and provides a foundation for containerised, microservice-based workloads. AKS is frequently the substrate for internal developer platforms built under a platform engineering operating model.

Anti-pattern

A commonly repeated approach that appears reasonable but produces poor outcomes in practice. Naming anti-patterns explicitly — such as lift-and-shift without rationalisation, or governance applied only after go-live — helps organisations recognise and avoid them before they cause damage.

Application Portfolio Rationalisation

The structured process of assessing every application in a digital estate against business value and technical fitness, in order to decide whether it should be retired, retained, rehosted, replatformed, refactored, rearchitected or replaced.

Application Security Group

An Azure networking construct that groups virtual machines by application role, allowing network security rules to be defined in terms of application structure rather than individual IP addresses.

Architecture Decision Rights

The explicit allocation of authority to make, and be accountable for, architectural decisions at a given scope. Clear decision rights prevent both central-team bottlenecks and uncontrolled decentralisation.

Architecture Principles

A concise set of enduring rules that guide technology and design decisions across an enterprise, independent of any single project. Effective principles are specific enough to be testable, not so generic that they permit any decision.

Architecture Review Board

A governance body, typically cross-functional, responsible for reviewing significant architectural decisions, approving exceptions to standards and maintaining the coherence of the enterprise architecture over time.

Assessment Toolkit

A structured set of scored questionnaires used to evaluate an organisation's maturity across dimensions such as cloud readiness, security and governance, providing an evidence-based starting point for investment decisions.

Assume Breach

A Zero Trust design principle that treats compromise as inevitable and focuses architecture on limiting blast radius, accelerating detection and enabling rapid containment, rather than relying solely on prevention.

Attack Surface

The complete set of points at which an unauthorised actor could attempt to gain access to or extract data from an

environment. Reducing attack surface is a continuous architectural discipline, not a one-time project.

Automation

The use of technology to perform tasks with minimal human intervention, ranging from Infrastructure as Code deployments to automated incident response. Automation increases consistency and speed but requires safeguards, evidence and rollback capability to remain trustworthy.

Availability Zone

A physically separate location within an Azure region, each with independent power, cooling, and networking, designed to improve resilience against localised datacentre failures.

Azure Advisor

A free Azure service that analyses resource configuration and usage to provide personalised recommendations across cost, security, reliability, operational excellence, and performance.

Azure Firewall

A managed, cloud-native network security service that provides centralised traffic filtering and threat intelligence for workloads connected to a hub-and-spoke or Virtual WAN topology.

Azure Landing Zone

A scalable Azure environment and architectural foundation that establishes governance, security, networking, identity and operational capabilities for secure and repeatable workload deployment. See Chapter 7 for the complete architectural treatment.

Azure Policy

A governance service that enforces organisational standards and assesses compliance at scale, allowing rules to be defined once and applied automatically across the estate.

Azure Virtual Desktop

A desktop and application virtualisation service that delivers Windows experiences from Azure, enabling secure access to corporate applications without extending the network perimeter to unmanaged devices.

Azure Well-Architected Framework

Microsoft's guidance for evaluating workloads against five pillars: reliability, security, cost optimisation, operational excellence, and performance efficiency.

B**Backup Immutability**

A property of backup storage that prevents deletion or alteration for a defined retention period, protecting recovery data from both accidental loss and deliberate tampering during a ransomware event.

Blast Radius

The extent of impact that a single failure, compromise or misconfiguration can cause. Segmentation, both in network and identity design, exists primarily to reduce blast radius.

Blue-Green Deployment

A release technique that maintains two identical production environments, allowing traffic to be switched instantly between them and rolled back with minimal risk if a new release fails.

Board Readiness

The state of being able to present a technology transformation to a board of directors in the language of risk, value and confidence, with a clear decision requested rather than a status update delivered.

Budget Owner

The individual accountable for a specific area of cloud spend, responsible for justifying, monitoring and optimising consumption within their domain under a FinOps operating model.

Business Capability

A stable organisational ability that delivers measurable business value independently of organisational structure or technology implementation. Capabilities change far more slowly than the systems and teams that deliver them, making them a durable basis for architecture.

Business Case

A structured argument that explains why an investment should be made, what value it will create, and what would

happen if the investment were not made. A credible business case addresses cost, risk, time to value, and opportunity cost together.

Business Continuity

The organisational capability to continue delivering critical products and services during and after a disruptive event, encompassing people, process, and technology, not technology alone.

Business Continuity Operating Model

The ongoing governance structure — roles, cadence, testing schedule and reporting — through which an organisation sustains its resilience capability after the initial investment in disaster recovery architecture.

Business Continuity Plan

A documented set of procedures describing how an organisation will maintain or resume critical functions during and after a disruption, tested regularly rather than filed and forgotten.

Business Impact Analysis

A structured assessment of the operational and financial consequences of a disruption to specific business processes, used to prioritise recovery investment and inform recovery priorities, RTO/RPO and continuity investment.

Business Service

A business-facing service or capability whose continuity, performance and recovery matter directly to customers, employees, operations or revenue. Trusted Advisors design resilience around business services rather than around isolated infrastructure components.

Business Value

The measurable benefit an investment delivers to an organisation, typically expressed through cost reduction, risk reduction, revenue growth, agility or strategic optionality. Business value, not technical elegance, is the currency in which a Trusted Advisor speaks.

C

Capacity Planning

The practice of forecasting future resource requirements based on business growth and consumption trends, avoiding both costly over-provisioning and disruptive under-provisioning.

Change Management

The discipline of preparing, equipping and supporting individuals and teams to adopt new ways of working. Technical transformation without change management routinely fails to realise its intended value.

Chaos Engineering

The practice of deliberately injecting failure into a system in a controlled way to validate that resilience mechanisms work as designed, rather than assuming they do.

Chargeback

A FinOps practice of billing internal business units directly for their actual cloud consumption, creating financial accountability at the point of consumption.

Cloud Adoption Framework (CAF)

Microsoft's structured guidance for planning, governing and managing cloud adoption through defined methodologies, governance disciplines, and operating models. See Chapter 4 for its application as an enterprise operating model rather than a technical checklist.

Cloud Adoption Strategy

The documented rationale, motivations and business outcomes that justify an organisation's decision to adopt cloud technology, forming the foundation on which a migration plan is built.

Cloud Centre of Excellence (CCoE)

A cross-functional leadership and enablement team established to accelerate cloud adoption by defining standards, providing reusable patterns and supporting delivery teams, rather than acting as a gatekeeper.

Cloud Operating Model

The combination of governance, decision rights, platform services, financial management and organisational

structure through which an enterprise runs its cloud estate on an ongoing basis, distinct from the one-time act of migration.

Cognitive Load

The mental effort required of a team to understand and operate a system. Platform engineering exists partly to reduce cognitive load, allowing application teams to focus on business logic rather than infrastructure mechanics.

Commitment-Based Discount

A cloud pricing model in which a customer commits to a certain level of usage or spend in exchange for a reduced rate, requiring active management to avoid over-commitment.

Compliance as Code

The practice of expressing regulatory and policy requirements as automatically enforced and continuously assessed technical controls, reducing reliance on manual, point-in-time evidence gathering.

Compliance by Design

An approach in which regulatory and policy requirements are embedded into architecture and delivery pipelines from the outset, rather than validated retrospectively before an audit.

Conditional Access

A Microsoft Entra ID capability that evaluates signals such as user risk, device compliance and location to make real-time access decisions, forming the policy engine of a Zero Trust architecture.

Configuration Drift

The gradual divergence of a system's actual configuration from its intended, documented state, typically caused by manual changes outside of an Infrastructure as Code pipeline.

Continuous Compliance

An operating discipline in which compliance evidence is collected and controls are assessed continuously, rather than assembled manually in the weeks before an audit.

Continuous Deployment

A software delivery practice in which every change that passes automated testing is released to production automatically, requiring mature automated testing and rollback capability.

Cost Avoidance

Value created by preventing future expenses that would otherwise have been incurred, such as a hardware refresh or a data-centre lease renewal, distinct from cost reduction against a current baseline.

Cost Governance

The set of policies, controls and accountability structures that ensure cloud spending remains visible, justified, and aligned with business value, rather than growing unmanaged.

Cost Transparency

The degree to which cloud spending is visible and attributable to the business units, products or capabilities that generate it, a prerequisite for financial accountability.

Cross-Functional Team

A team composed of members with different functional expertise — development, security, operations, finance — organised around a shared outcome rather than a shared reporting line.

Cutover

The defined point at which a migrated workload is switched from its legacy environment to its new platform and begins serving live business traffic. A well-governed cutover includes rollback criteria agreed before the switch is made.

Cyber Resilience

The ability of an organisation to prepare for, respond to and recover from cyberattacks while continuing to deliver its critical functions, extending beyond prevention alone.

D**Cyber Recovery**

The disciplined restoration of trusted business services after a cyber incident, including validated backup integrity, clean administrative access, isolated recovery

environments, security investigation, data validation and controlled reconnection. Cyber recovery differs from conventional disaster recovery because replicated corruption or malicious change must not be restored blindly.

Data Classification

The practice of categorising data according to its sensitivity and business value, enabling proportionate security controls to be applied rather than a single uniform standard across all data.

Data Governance

The system of policies, roles, standards and controls through which an organisation ensures the quality, availability, integrity and security of its data assets across their lifecycle.

Data Loss Prevention (DLP)

A set of tools and policies designed to detect and prevent the unauthorised transmission or exposure of sensitive data outside of approved boundaries.

Data Residency

The physical or jurisdictional location in which data is stored, which may be constrained by regulation, contractual obligation or corporate policy independent of technical convenience.

Datacentre Exit

The structured programme of migrating or decommissioning workloads from a physical datacentre, typically tied to a lease expiry or a strategic decision to leave owned infrastructure, and requiring its own governance, milestones and funding distinct from the underlying application migrations.

Decision Model

A structured method for evaluating options, comparing trade-offs and reaching a documented, defensible conclusion, typically used when stakeholders hold differing priorities.

Decommissioning

The formal, controlled retirement of an application, system or piece of infrastructure, including data retention decisions, dependency validation, and stakeholder sign-off.

Defence in Depth

A security strategy that layers multiple, independent controls — identity, network, application, data and operational — so that the failure of any single control does not result in compromise.

Dependency Mapping

The process of identifying and documenting the technical and business relationships between applications, data stores and infrastructure, used to sequence migration safely and avoid unplanned outages.

Dependency Visualisation

The graphical representation of relationships between applications, services and infrastructure, used to make hidden technical debt and migration risk visible to decision-makers.

Deployment Pipeline

An automated sequence of build, test and release stages that moves a change from source code to production, providing consistency, speed, and auditability.

Digital Estate

The complete inventory of an organisation's applications, infrastructure, data, and dependencies, maintained as a living register rather than a static, point-in-time spreadsheet.

Digital Transformation

The process of using digital technology to create new, or modify existing, business processes, culture and customer experiences in order to meet changing business and market requirements.

Disaster Recovery

The set of technical and operational measures used to restore systems, data and services following a disruptive event, measured against defined recovery time and recovery point objectives.

Discovery Workshop

A structured, facilitated session used early in an engagement to surface an organisation's true objectives, constraints and concerns, forming the foundation for a credible business case.

DNS Private Resolver

An Azure service that enables hybrid DNS resolution between on-premises networks and Azure private DNS zones, a critical and frequently underestimated component of private connectivity architecture.

E**Enterprise Architecture**

The discipline of aligning business strategy, organisational capabilities, information, applications and technology to enable sustainable transformation and long-term business value.

Enterprise Risk Management

The organisation-wide discipline of identifying, assessing and responding to risks that could affect the achievement of strategic objectives, of which cyber and technology risk form one component.

Escalation Path

A predefined route by which an issue is raised to progressively senior decision-makers when it cannot be resolved at the level at which it was first identified.

Estate Modernisation

The coordinated programme of rationalising, migrating and rearchitecting an organisation's application and infrastructure estate to remove constraints and enable future capability.

Executive Alignment

A condition in which senior leaders share a sufficiently common understanding of objectives, priorities and trade-offs that decisions can be made and sustained without repeated renegotiation.

Executive Dashboard

A summarised, outcome-oriented view of transformation progress and risk designed for senior leadership, distinct from the detailed operational dashboards used by delivery teams.

Executive Sponsor

A senior leader who holds visible, personal accountability for a transformation's success and actively removes

organisational obstacles, distinct from a delivery lead who manages day-to-day execution.

Exit Strategy

A documented plan for how an organisation would migrate away from a given technology, vendor or platform if required, reducing strategic lock-in risk.

ExpressRoute

A private, dedicated network connection between an organisation's premises and Microsoft's cloud services, offering more predictable latency and reliability than a typical internet-based connection.

F**Feature Flag**

A configuration mechanism that allows functionality to be enabled or disabled without a new deployment, supporting safer releases and controlled rollout.

Federated Identity

An identity architecture in which authentication is delegated to a trusted external identity provider rather than managed directly, commonly used for business-to-business collaboration.

Federated Operating Model

An organisational design that combines central strategy, tooling and standards with local operational autonomy, used where global consistency and local context both matter, such as security operations across multiple countries.

Financial Accountability

The condition in which the individuals who consume a resource are also responsible for justifying and managing its cost, a foundational FinOps principle.

FinOps

An operational framework that enables organisations to maximise business value from cloud investments through financial accountability, transparency and continuous optimisation, organised around the phases of Inform, Optimise, and Operate.

FinOps Foundation

The vendor-neutral organisation that maintains and publishes the FinOps Framework, a widely adopted standard for cloud financial management practice.

G**GDPR**

The General Data Protection Regulation, the European Union's framework for data protection and privacy, which requires organisations to apply risk-based security of processing and to demonstrate accountability for personal data.

Golden Path

A well-supported, opinionated route through a platform that makes the secure and compliant way of working also the easiest way of working, reducing the need for teams to make risky decisions alone.

Governance

The system of policies, decision rights and accountability structures through which an organisation directs and controls its technology estate. Effective governance enables innovation by providing clear boundaries, rather than obstructing it through unclear or excessive control.

Governance as an Operating System

A framing of governance as the continuously running set of automated policies and controls that every workload inherits, rather than a periodic review activity performed after deployment.

Governance Checklist

A structured list of conditions that must be satisfied before a decision, deployment or exception is approved, used to make governance consistent and auditable.

Governance Erosion

The gradual weakening of governance standards through the accumulation of undocumented or unreviewed exceptions, each individually reasonable but collectively undermining control.

Guardrail

An automated control that constrains what can be deployed or configured within an environment, designed to make the secure and compliant path also the easiest path.

H**Hub-and-Spoke**

A network topology that centralises shared connectivity and security services in a hub, while isolating workloads in spoke networks connected through peering, reducing blast radius and duplication of shared services.

Hybrid Identity

An identity architecture that synchronises or federates on-premises directory services with a cloud identity provider such as Microsoft Entra ID, enabling a single identity to govern access across environments during a multi-year transformation.

Hypercare

A defined period of heightened monitoring and support immediately following a migration or major change, during which issues are resolved with priority before the team returns to standard operations.

I**Identity as the New Perimeter**

A framing that reflects the shift of enterprise security from network boundaries towards identity verification as a primary control point across cloud, hybrid and remote-working environments.

Identity Governance

The automation of identity lifecycle processes — joiners, movers, leavers, access reviews and entitlement management — reducing administrative effort and security risk compared with manual processes.

Immutable Backup

See Backup Immutability.

Immutable Infrastructure

An approach in which servers and environments are never modified after deployment; changes are made by deploying

a new, replacement instance, improving consistency and auditability.

Incident Command

The structure and authority established during a significant incident to make rapid decisions, coordinate response and communicate with stakeholders under pressure.

Incident Management

The process of restoring normal service operation as quickly as possible following a disruption, prioritising speed of recovery over root-cause analysis, which is addressed separately through problem management.

Incident Response

The coordinated process of detecting, containing, eradicating and recovering from a security incident, combining technology, documented process, and executive decision-making authority.

Independent Assurance

Review or audit activity performed by a party independent of the team responsible for a control, providing objective confirmation that the control operates as intended.

Infrastructure as Code (IaC)

The practice of defining and provisioning infrastructure through machine-readable configuration files rather than manual processes, enabling repeatable, testable, and auditable deployments.

Innovation Enablement

The dimension of business value concerned with new capabilities that become possible only because of a technology investment, distinct from cost or risk-focused value.

Internal Developer Platform

A self-service layer built by a platform engineering team that provides application teams with golden paths, reusable modules and automated deployment capability, reducing the cognitive load of operating on the underlying cloud platform directly.

Interview Mastery

The ability to communicate architectural judgement clearly under questioning, explaining decisions, alternatives,

trade-offs, assumptions and measurable outcomes rather than simply recalling technical facts.

IP Address Management (IPAM)

The planning, tracking and governance of IP address allocation across an enterprise network, essential to preventing overlapping ranges that complicate connectivity and future mergers.

J**Just-Enough Administration (JEA)**

A security capability that constrains administrative access to the specific commands and resources required for a task, reducing the privilege available to any single administrative session.

Just-in-Time Access (JIT)

An access model in which elevated permissions are granted only for a limited, requested time window rather than persistently, reducing the standing attack surface created by always-on privileged accounts.

K**Key Vault**

A cloud service for securely storing and managing secrets, encryption keys and certificates, removing the need to embed credentials directly in application code or configuration.

KPI (Key Performance Indicator)

A measurable value used to evaluate progress against a defined objective. Effective transformation KPIs are tied to business outcomes, not merely to technical completion milestones.

L**Landing Zone**

See Azure Landing Zone.

Landing Zone Accelerator

A pre-built, opinionated implementation of Azure landing zone architecture, reducing the time required to establish a governed and standardised foundation from first principles.

Latency

The time delay between a request and its response, a critical design consideration for factory operations, real-time analytics and any workload sensitive to network distance from Azure regions.

Leadership Alignment

See Executive Alignment.

Least Privilege

A security principle under which every identity is granted only the minimum access required to perform its function, reducing both the attack surface and the potential impact of a compromised account.

Legacy Application

An application built on outdated technology, architecture or practices that constrains an organisation's ability to change, scale or secure it, independent of how critical the application remains to the business.

Legacy Modernisation

See Modernisation.

Lessons Learned

A structured reflection conducted after a project, incident or programme phase, intended to improve future performance rather than assign blame.

Lift and Shift

A migration approach that moves a workload to the cloud with minimal modification, prioritising migration speed over architectural improvement. Appropriate for some workloads, but a poor default strategy when applied indiscriminately across an entire estate.

Lift, Rationalise and Shift

A migration approach that applies a lightweight rationalisation pass before migration, avoiding both the risk of unmodified lift-and-shift and the delay of full rearchitecture.

Long-Term Support (LTS)

A vendor commitment to provide updates and security patches for a specified extended period, a key consideration when assessing technical debt and platform currency.

M

Managed Identity

An automatically managed identity in Microsoft Entra ID that applications can use to authenticate to cloud services without embedding credentials in code or configuration.

Management Group

An Azure construct that allows governance conditions, such as policy and access control, to be applied consistently across multiple subscriptions through a hierarchical structure.

Material Risk

Risk of sufficient financial, operational, regulatory, strategic or reputational significance to require explicit leadership attention, ownership or acceptance. Trusted Advisors distinguish material enterprise exposure from technical issues that can be managed operationally.

Maturity Model

A structured framework that describes stages of organisational capability, from ad hoc to optimised, used to benchmark current state and plan improvement.

Mean Time to Detect (MTTD)

The average time elapsed between the occurrence of a security or operational event and its detection, a primary indicator of monitoring and detection engineering effectiveness.

Mean Time to Restore (MTTR)

The average time elapsed between the detection of an incident and the restoration of normal service, a primary indicator of incident response and recovery effectiveness.

Mergers and Acquisitions (M&A) Integration Playbook

A standardised, repeatable methodology for integrating an acquired company's technology estate, designed to reduce uncertainty, protect continuity and accelerate integration.

Microsegmentation

The practice of dividing a network into small, tightly controlled zones, limiting lateral movement in the event of a compromise beyond what traditional perimeter segmentation achieves.

Microsoft Entra ID

Microsoft's cloud-based identity and access management service, providing authentication, single sign-on and Conditional Access across cloud, on-premises and software-as-a-service applications. Formerly known as Azure Active Directory.

Microsoft Sentinel

Microsoft's cloud-native security information and event management (SIEM) and security orchestration (SOAR) service, used to collect, detect, investigate and respond to threats across an enterprise estate.

Migration Factory

A repeatable, standardised operating model for executing application migrations at scale, treating migration as an industrialised process rather than a series of bespoke projects.

Migration Wave

A defined, sequenced group of workloads migrated together, planned according to business priority, technical dependency and risk rather than convenience.

Minimum Viable Platform

The smallest set of platform capabilities required to safely onboard the first production workloads, expanded iteratively based on demonstrated demand rather than built exhaustively upfront.

Modernisation

The disciplined removal of technical and architectural constraints from an application or platform, distinct from the pursuit of newer technology for its own sake.

Multi-Factor Authentication (MFA)

An authentication method that requires two or more independent forms of verification, substantially reducing the risk of credential-based compromise compared with passwords alone.

Multi-Region

An architecture that distributes workloads across two or more Azure regions to meet resilience, latency or data-residency requirements. Each additional region adds complexity to routing, data replication and DNS, so the

decision should be driven by a documented business requirement rather than default caution.

N

Network Security Group (NSG)

An Azure construct that filters network traffic to and from resources within a virtual network, providing a further layer of segmentation beyond centralised firewalling.

NIS2 Directive

European Union legislation establishing cybersecurity risk-management and incident-reporting obligations for entities within its scope, covering areas including incident handling, business continuity, supply-chain security, and access control.

NIST Cybersecurity Framework

A voluntary framework, now in version 2.0, that organises cybersecurity outcomes into six functions: Govern, Identify, Protect, Detect, Respond, and Recover.

Non-Functional Requirement

A requirement that specifies how a system should behave, such as availability, performance or security, rather than what it should do, often the deciding factor in architectural trade-offs.

O

Observability

The capability to understand the internal state of a system from its external outputs — logs, metrics and traces — enabling teams to diagnose novel problems rather than only detect anticipated ones. Observability precedes and enables effective monitoring.

Operating Model

The way an organisation structures people, process, governance and technology to deliver its strategy on an ongoing basis. Cloud is an operating model, not a destination — the migration ends, but the operating model must keep working.

Operational Excellence

One of the pillars of the Azure Well-Architected Framework, concerned with the processes that keep a system running effectively in production.

Operational Technology (OT)

The hardware and software used to detect or cause changes in physical industrial processes, such as manufacturing control systems, which require security approaches distinct from traditional information technology.

Opportunity Cost

The value forgone by choosing one course of action over the best available alternative, an essential but frequently omitted consideration in technology business cases.

Organisational Change Management

See Change Management.

Outcome-Based Metric

A measure of success defined in terms of business result, such as revenue enabled or risk reduced, rather than technical activity completed.

P**Performance Efficiency**

One of the pillars of the Azure Well-Architected Framework, concerned with a workload's ability to scale to meet demand efficiently.

Platform Engineering

A discipline that treats the internal cloud platform as a product, providing self-service capability, golden paths and reusable modules to application teams, measured by developer experience and business outcome rather than control retained.

Playbook

A documented, repeatable sequence of actions for responding to a known scenario, reducing reliance on improvisation under pressure.

Policy as Code

The practice of defining governance rules in machine-readable format so they can be version-controlled, tested and automatically enforced, rather than documented as prose and applied manually.

Post-Incident Review

A structured analysis conducted after an incident to establish root cause and identify improvements, conducted without attributing blame to individuals.

Principle of Least Privilege

See Least Privilege.

Private Endpoint

A network interface that connects privately to a supported Azure service, removing the need for that service to be exposed to the public internet.

Private Link

The Azure capability that enables private endpoints, allowing traffic to a supported service to remain entirely within the Microsoft backbone network.

Privileged Identity Management (PIM)

A Microsoft Entra ID capability that enables just-in-time, time-bound and approval-gated activation of privileged roles, reducing the standing risk of always-on administrative access.

Product Backlog

A prioritised list of work items for a product or platform, maintained transparently so that stakeholders can see what is planned and why.

Product Owner

The individual accountable for defining and prioritising the backlog of a product or platform, representing the interests of its users and the business value it is intended to deliver.

Product Vision

A concise statement of the intended future value and purpose of a product or platform, used to align stakeholders and guide prioritisation decisions.

Product-Oriented Platform Engineering

An approach to platform engineering in which the internal platform is managed with the same rigour as an external product, including a documented vision, defined personas, a transparent backlog, and measured adoption.

Q**Quality Attribute**

See Non-Functional Requirement.

R**Ransomware**

Malicious software that encrypts an organisation's data and demands payment for its release, defended against primarily through identity hygiene, segmentation, and tested, immutable backups.

Rationalisation

The process of assessing an application portfolio and deciding, workload by workload, whether to retire, retain, rehost, replatform, refactor, rearchitect or replace each application.

Readiness Assessment

See Assessment Toolkit.

Recovery Point Objective (RPO)

The maximum acceptable amount of data loss, measured in time, that an organisation can tolerate following a disruptive event.

Recovery Time Objective (RTO)

The maximum acceptable duration within which a service must be restored following a disruptive event, driving the architecture and cost of the corresponding recovery capability.

Reference Architecture

A documented, reusable architectural pattern that addresses a common problem, intended to accelerate and standardise future designs rather than be copied without adaptation.

Regional Hub

A hub deployed within a specific Azure region to provide shared connectivity and security services to workloads in that region, required wherever workloads span multiple regions.

Regulatory Compliance

The state of conforming to laws, regulations and industry standards applicable to an organisation's operations, sustained through continuous evidence rather than periodic manual attestation.

Requirements Traceability

The ability to link a delivered capability back to the original business requirement that justified it, supporting both governance and value realisation reporting.

Reservation Management

A FinOps practice of purchasing committed-use discounts for predictable workloads in exchange for reduced pricing, balanced continuously against changing consumption patterns.

Resilience

The tested ability of an organisation and its systems to continue delivering value, or to recover quickly, when disrupted. Resilience is proven through rehearsal, not assumed from the existence of a backup.

Resource Locks

An Azure governance feature that prevents accidental deletion or modification of critical resources, independent of role-based access permissions.

Retention Policy

A defined rule specifying how long data or backups must be kept and when they must be deleted, balancing compliance, cost, and operational need.

Retire (application strategy)

A migration and rationalisation decision to decommission an application entirely because it no longer delivers sufficient business value to justify its ongoing cost and risk.

Risk Appetite

The amount and type of risk an organisation is willing to accept in pursuit of its objectives, ideally agreed explicitly by leadership rather than inferred after an incident.

Role-Based Access Control (RBAC)

An access control model that grants permissions based on a user's role within an organisation, simplifying administration compared with assigning permissions to individuals directly.

Runbook

A documented set of procedures for carrying out a specific operational task or responding to a specific incident, written so that it can be executed consistently by different team members.

S**Scope Creep**

The uncontrolled expansion of a project's requirements beyond its original agreed boundaries, a common cause of transformation delay and cost overrun.

SD-WAN

Software-Defined Wide Area Networking, an approach that provides a unified, centrally managed overlay across multiple underlying connection types such as internet, MPLS and VPN.

Security Operations Centre (SOC)

The team and technology responsible for continuous monitoring, detection, investigation and response to security threats across an organisation's estate.

Segmentation

The division of a network, identity space or environment into isolated zones to limit the impact of a failure or compromise, a core technique for reducing blast radius.

Separation of Duties

A control principle that divides critical tasks among multiple people or systems so that no single individual can complete a sensitive process alone, reducing the risk of error or fraud.

Service Level Indicator (SLI)

A quantitative measure of a service's observed behaviour, such as availability, latency or error rate, used to determine whether a defined Service Level Objective is being achieved.

Service Level Objective (SLO)

A target value for a service level indicator, such as availability or latency, that a team commits to meet, forming the basis for reliability engineering and operational accountability.

Service Management

The set of organisational capabilities used to plan, deliver, operate and control the IT services offered to an organisation, encompassing incident, problem, and change management.

Seven Rs

A migration strategy framework describing seven approaches available for each workload: Retire, Retain, Rehost, Replatform, Refactor, Rearchitect and Replace. Selecting the right R for each workload, rather than defaulting to one approach for an entire estate, is central to a credible migration strategy.

Shared Responsibility Model

The division of security and operational responsibility between a cloud provider and its customers, which shifts depending on the service model in use, from infrastructure through to fully managed platforms.

Showback Reporting

A FinOps practice of reporting cloud consumption and cost to business units for visibility and behavioural influence, without a formal internal billing transaction as in chargeback.

Single Sign-On (SSO)

An authentication capability that allows a user to access multiple applications with one set of credentials, improving both user experience and the consistency of identity governance.

Site Reliability Engineering (SRE)

A discipline that applies software engineering practices to operations problems, using error budgets, service level

objectives and automation to balance reliability with the pace of change.

Skills Gap

The difference between the capabilities an organisation currently has and the capabilities it needs to execute its strategy, addressed through training, hiring or partnership.

Sponsor Alignment

See Executive Alignment.

Sprint

A fixed, short time period, typically two to four weeks, during which a defined set of work is completed and reviewed under an agile delivery approach.

Stakeholder Alignment

The process of building sufficient shared understanding among affected parties that a decision can proceed and be sustained without repeated renegotiation.

Stakeholder Matrix

A tool that maps stakeholders according to their level of influence and interest in a transformation, used to plan appropriately targeted engagement and communication.

Standard Operating Procedure (SOP)

A documented, step-by-step set of instructions for carrying out a routine operational activity consistently.

Steering Committee

A governance body composed of senior stakeholders that reviews progress and makes or endorses key decisions for a transformation programme.

Strategic Scalability

An organisation's capacity to grow — geographically, operationally or through acquisition — without a proportional increase in architectural or governance complexity.

Subscription Vending

An automated process for provisioning new Azure subscriptions pre-configured with an organisation's governance, networking and identity standards, removing manual setup steps and reducing the time required to onboard a new workload team.

Supply-Chain Security

The set of practices used to manage the risk that a compromise of a trusted supplier, software dependency or service provider could bypass an organisation's own internal controls.

Synergy Value

The additional value expected from combining two organisations through a merger or acquisition, which remains a hypothesis until it is demonstrated in realised financial results.

T**Tagging Standards**

A consistent naming and metadata convention applied to cloud resources, enabling cost allocation, ownership tracking and policy enforcement at scale.

Technical Debt

The future cost created when a design, implementation or operating decision favours short-term speed over long-term maintainability. Like financial debt, it includes both a principal, the cost of the shortcut, and interest, the ongoing cost of working around it.

Technology Debt

See Technical Debt.

Testing and Exercising

The practice of regularly rehearsing recovery, incident response and continuity plans under realistic conditions, distinguishing a genuine capability from an untested assumption.

Threat Intelligence

Information about existing or emerging threats, used to enrich detection and inform proactive defensive measures rather than relying solely on internally observed signals.

Total Cost of Ownership (TCO)

The complete cost of owning and operating a system or platform over its lifetime, including infrastructure, licensing, operations and eventual decommissioning, not only the initial purchase or migration cost.

Transformation Roadmap

A sequenced plan that organises a transformation programme into waves or phases, balancing business priority, technical dependency and organisational capacity to absorb change.

Trusted Advisor

A leadership posture in which a technology professional earns the standing to guide business decisions through demonstrated judgement, not only technical expertise — translating architecture into risk, value, and confidence for executive audiences.

Trusted Advisor Principle

A recurring, memorable statement of judgement offered throughout this book to distil a chapter's argument into a single portable idea for use in an executive conversation.

U**Unified Identity Platform**

A single identity system, typically Microsoft Entra ID, that governs authentication and authorisation consistently across on-premises, cloud and software-as-a-service applications.

V**Value Realisation**

The process of confirming that the business benefits promised in a business case have actually been achieved, closing the loop between investment and outcome.

Vendor Lock-in

A condition in which switching away from a given vendor or platform becomes prohibitively costly or complex, mitigated through architectural choices and a documented exit strategy.

Virtual Network (VNet)

An isolated network environment within Azure that provides the foundation for private communication between resources, on-premises networks and the internet.

Virtual WAN

A Microsoft-managed networking service that simplifies global branch connectivity, VPN and ExpressRoute integration through centrally managed regional hubs, reducing the operational burden of a customer-built hub.

VPN Gateway

A service that establishes encrypted, site-to-site or point-to-site connectivity between an on-premises network and Azure, typically used for smaller sites or as resilient backup connectivity.

W**Waterfall Methodology**

A sequential project delivery approach in which each phase is completed before the next begins, contrasted in this book with more iterative, wave-based transformation approaches.

Well-Architected Framework

See Azure Well-Architected Framework.

Whiteboarding

The practice of working through architectural problems collaboratively and visually with stakeholders, valued for making disagreement productive and assumptions visible before they are committed to a design.

Workload

A distinct application or capability, together with its resources and dependencies, treated as a unit of planning for migration, governance, and operational accountability.

Workload Segmentation

The practice of isolating workloads from one another according to business, risk or lifecycle boundaries, rather than by geography or administrative convenience alone.

Z**Zero Trust**

A security model that replaces network-location-based trust with continuous, explicit verification of identity, device health and context for every access request, resting

on the principles of verify explicitly, use least-privilege access, and assume breach.

Zero Trust Maturity Model

A staged framework describing an organisation's progression from basic multi-factor authentication through to a fully integrated, continuously risk-evaluated Zero Trust architecture.

Zero-Day Vulnerability

A software vulnerability that is exploited before the vendor has released a fix, requiring layered defences that do not depend solely on timely patching.