ECLIT TECHNOLOGY GLOSSARY

150 terms, in plain English.

What the terms used in managed IT, cloud, disaster recovery and security operations actually mean.

This document is the downloadable form of eclit.com/en/sozluk.

TERMS	LANGUAGE	UPDATED
150	**English**	**2026-10-10**

Why this glossary exists

The person buying IT infrastructure is often not the person who runs it. When a proposal says “RPO 15 minutes”, knowing what that means is the precondition for comparing proposals at all.

The definitions are kept short and aim to answer the question the reader actually arrives with. On the site each term links through to the relevant service page and, where one exists, to a deeper article: **eclit.com/en/sozluk**

A

Active Directory
Microsoft's directory service. It defines and authorizes network resources — user accounts, computers, printers and groups — from one place, and is where sign-on, group policy and access control are centralized in most enterprise environments.

Network security
Protecting data and systems on a network against unauthorized access, attack and malicious software. Firewalling, segmentation, monitoring and access control are the core tools under this heading.

Agility
The ability to adapt quickly to changing business needs. On the IT side that means standing up a new environment in hours rather than weeks, and being able to reverse a decision once it is made.

Active database
The production database serving real-time read and write traffic. What separates it from a standby or archive copy is that it carries the live workload.

Antivirus
Security software that detects, blocks and removes malicious code. Modern products go beyond signature matching to behavioral analysis.

AP controller
The device or software that manages wireless access points centrally — channel selection, power levels, client roaming and configuration distribution all run from one place.

API
Application programming interface — the defined contract through which two pieces of software talk to each other. Most integrations are built on APIs today, which is why API security has become a discipline of its own.

Fault management
The process of detecting, classifying, resolving and recording a fault. A mature practice measures itself by root causes found and recurrences prevented rather than by tickets closed.

Autoscaling
Automatically adding and removing resources in response to demand. Configured well, it adds capacity at peak and lowers cost off-peak; configured with the wrong thresholds, it does neither.

B

B2B (business to business)
Commerce between businesses. What separates it from consumer sales is that the buying decision belongs to a committee rather than a person, and the cycle is long.

Backend
The part of an application the user never sees: server logic, database and integrations. The interface is the front end; the layer feeding it is the backend.

Backup-as-a-Service (BaaS)
Backup delivered as a service. Rather than building and running the infrastructure, you define retention and recovery targets and the provider operates it. The clause to insist on is reporting of restore tests.

SAP Basis management
Managing the technical layer of SAP systems: installation, system copy, transport routes, performance tuning, patching and user administration. It owns the infrastructure side of SAP, not the functional side.

Big data
Datasets too large, too fast-moving or too varied to process with conventional tools. The definition is less about size than about existing methods no longer being enough.

Information processing cycle
The sequence of collecting data, processing and storing it, and turning it into meaningful output. Each step carries its own security and retention requirements.

Bug
A defect that makes software behave differently from what was expected. Catching one before release is far cheaper than catching it after, which is the argument for test automation.

Cloud infrastructure
The compute, storage, network and virtualization layer that carries cloud services. The user sees virtual resources; underneath sit physical servers, arrays and switches.

Cloud computing
Compute, storage and application resources delivered over the internet, on demand and paid for by consumption. In Türkiye, the cloud decision also involves data residency.

Cloud storage
Storing data in a service reached over the internet. It brings cost and scale advantages; the question to ask when deciding is which country and which facility the data sits in.

Cloud server
A server running on virtualized resources and managed remotely, with no hardware to buy. Being able to create and destroy it in minutes is what separates it from a physical server.

C - Ç

Cache
Holding frequently accessed data temporarily in a faster layer. Used well, it delivers one of the largest performance gains available; used with the wrong invalidation rule, it produces some of the hardest bugs to find.

CDN
Content delivery network. It serves static content from the server geographically closest to the user, which lowers latency and reduces both load and attack surface on the origin server.

Multi-cloud
Using more than one cloud provider together. It reduces dependence on a single vendor but raises operational complexity and makes cost tracking harder; without a clear reason it does not pay off.

Cookies
Small pieces of data websites store in the browser. Uses range from session management to tracking, and because they can carry personal data they may require notice and consent under data protection law.

CPU
Central processing unit — the component that executes instructions. In virtualized environments the ratio between physical and virtual cores directly determines performance.

D

Data lake
A pool where structured and unstructured data is stored raw, with no schema imposed up front. The flexibility is the advantage; ungoverned, it turns into a data swamp where nobody knows what is stored.

Data migration
Moving data from one system or storage platform to another. The risk lies less in the transfer than in the cutover window and in verifying integrity once it is done.

Deep learning
The branch of machine learning that uses multi-layer neural networks to learn patterns from large datasets. It is the method behind the leap in vision, speech and language processing, and training it demands serious GPU capacity.

DevOps
A way of working that removes the wall between development and operations. It rests on automation, small frequent releases, shared ownership and measurement. It is an operating model, not a tool.

Digital transformation
Rebuilding business processes around technology. Digitizing an existing process is not transformation; transformation is the process itself changing because the technology made a different one possible.

Disaster recovery
Bringing systems and data back after a major outage, data loss or disaster. Having a plan is not enough; what counts in an audit and in a real event is a recovery time measured in an exercise.

Disaster recovery as a service (DRaaS)
Disaster recovery delivered as a service. Instead of building and running a secondary site, you get replication and failover capability from the provider. Judge it by the recovery time achieved in an exercise rather than by the monthly fee.

Domain name
The human-readable form of a web address. Its expiration date, DNS records and ownership belong in the corporate asset inventory, because a domain allowed to lapse can mean a lost brand.

Hardware
The physical components of a computing system: servers, storage, network devices, end-user devices. Managing their lifecycle (warranty, firmware, refresh and disposal) is part of security too.

E

Email management
Operating corporate mail: account lifecycle, mail flow security, quotas, archiving and retention. Getting SPF, DKIM and DMARC right is the most basic step in stopping mail spoofed in your name.

Edge computing
Processing close to where data is produced rather than in a central data center. It is chosen where latency is critical and moving raw data to the center is expensive.

Integration
Connecting different systems at the data and process level. Design tends to cover the happy path and skip error handling and retry policy.

Elasticity

A system's ability to adapt to changing demand and requirements. It differs from scalability in that it covers contraction and change of direction as well as growth.

F

Disaster recovery site
The secondary facility that takes over workloads when the primary data center becomes unusable. Its value depends on the measured time it takes to fail over to it, more than on distance or hardware.

Physical server
A server running directly on hardware, not virtualized. It is still preferred in certain high-performance and licensing scenarios, though any capacity change then requires a hardware purchase.

Flexi cloud
A cloud consumption model where resources flex up and down with need, built on variable consumption rather than a fixed capacity commitment.

G

Firewall
A system that inspects network traffic against defined rules and blocks unauthorized access. The most common problem in the field is a rule set that accumulates until nobody dares touch it.

H

Hypervisor
The layer that lets several virtual machines run on one physical server. VMware ESXi, KVM and Hyper-V are the common examples; today the choice is less a strategic decision than a commodity one.

Hosted Exchange
Microsoft Exchange delivered as a hosted service. Instead of running in-house, the mail infrastructure runs on the provider's side.

Hosting
Running a website or application, or storing data, on a provider's infrastructure. When comparing offers, look past price to guaranteed resources, redundancy and the support model.

HTTPS
Web traffic encrypted with TLS. It prevents data from being read or altered in transit, and is now expected as the default rather than the exception.

Hybrid cloud
A model combining on-premises infrastructure with cloud. In Türkiye the most common rationale is keeping regulated data local while the rest runs in the cloud.

I - İ

IDE
Integrated development environment — code editing, debugging and build tooling brought together in one interface.

Requirements analysis
Measuring what is actually needed before a project starts. Skipping it does not produce the wrong solution so much as the right solution applied to the wrong problem.

Infrastructure-as-a-Service (IaaS)
Infrastructure (servers, storage, network) delivered as a service. The operating system and everything above it stays the customer's responsibility, and where that boundary sits belongs in the contract.

Internet
The global network connecting devices and networks over shared protocols.

Internet gateway
The point that governs traffic between a network and the internet — where address translation, routing and usually security inspection are applied.

Internet of Things (IoT)
Sensors and devices that produce data and are managed over a network. The real security difficulty is that most of them cannot be patched and stay in service for years.

Business continuity
Keeping critical business processes running through a disruption or crisis. Broader in scope than disaster recovery: it covers people, suppliers and process as well as technology.

ISO 20000
The international standard for IT service management. It defines a management system for how services are designed, delivered and improved.

ISO 27001
The information security management system standard. It mandates no particular product or configuration; it requires you to assess risk, select controls and evidence that you applied them. The certificate runs three years, with an annual surveillance audit.

IT (information technology)

The technologies used to collect, process, store and transmit information.

ITIL
The widely used good-practice framework for IT service management, defining incident, problem, change and release processes. It is guidance rather than a standard.

J

JavaScript
The programming language that makes web pages interactive. It runs in the browser and, through Node.js, on the server as well.

K

Capacity planning
Measuring current resource use and projecting future need. Decisions made because a disk filled up always cost more than decisions made on schedule.

Mixed workload
Applications with different workload profiles sharing the same infrastructure. This is where the noisy neighbor problem comes from: an I/O-heavy workload degrading a latency-sensitive one beside it.

Colocation
Housing your own server and network hardware in rented rack space at a data center. The hardware is yours; space, power, cooling and physical security come from the facility.

Container
A lightweight unit of isolation that packages an application with its dependencies and shares the host kernel. Unlike a virtual machine, it carries no operating system of its own.

Kubernetes
The open-source platform that deploys, scales and manages containerized applications. Its operational weight matches its power; without the capability to run it, it creates more problems than it solves.

L

Linux
The open-source, Unix-like kernel and the distributions built around it. It is the dominant server platform, and the choice of distribution matters for support lifetime and patch policy.

LLM (large language model)
An AI model that can understand and generate language, trained on very large text corpora. In enterprise use the question is less the model's capability than which data goes where, and what that means for compliance.

Load balancer
The component distributing incoming traffic across several servers. It does more than spread load: health checks take a failing node out of rotation, which raises availability.

Logging
Recording system and application events. An audit asks about three things: coverage, the integrity of the record, and how quickly it can be produced on request.

LUN
A logical unit presented to a server by a storage system. It abstracts the physical disks; the server sees it as a single volume.

M

Machine learning
Methods that predict and classify by learning from data rather than being explicitly programmed. Model quality depends almost entirely on data quality.

Cost advantage
A solution delivering the same outcome at a lower total cost than the alternative. Comparisons based only on license or hardware costs are usually misleading.

Monitoring
Continuous observation of systems, networks and applications. Collecting and monitoring are not the same thing: a metric nobody looks at will pass an audit and prevent nothing.

MSP (managed service provider)
A provider that takes on the operation of IT infrastructure under contract. Before comparing prices, ask what the SLA measures, who is on call at night, how you access records, and what happens when you want to leave.

N

NAT
Network address translation — mapping private network addresses to a public address on the way out to the internet.

Object storage
A storage model that keeps data as objects, each with its ID and metadata, in a flat namespace

instead of a folder hierarchy. Access is over HTTP through an API, most often the Amazon S3 API. It holds backups, archives and large volumes of unstructured data.

Network
Devices connected so they can exchange data. Network design is as much about security as about performance: segmentation is the most effective way to limit how far an incident spreads.

Network virtualization
Abstracting physical network resources in software and presenting them as logical networks. This is what makes micro-segmentation and per-workload policy possible.

Node.js
The runtime that executes JavaScript server-side. Its event-driven architecture lets it handle large numbers of concurrent connections efficiently.

O - Ö

Scalability
A system's ability to absorb increasing load. Vertical scaling grows the same machine; horizontal scaling adds machines. The architecture decides up front which of the two is available to you.

Operations
Everything that keeps systems running day to day: monitoring, incident response, patching, backup and change management.

Operational burden
The ongoing cost to the team of keeping a system running. When choosing a technology this belongs in the calculation alongside the license fee.

Optimization
Reworking a system or process to deliver the same result with fewer resources. Optimizing without measuring usually means speeding up the wrong thing.

P

PaaS (Platform-as-a-Service)
A platform for building and running applications, delivered as a service. Infrastructure management stays with the provider; in exchange, platform lock-in rises.

Private cloud
A cloud model where resources are allocated to a single organization. Under Turkish banking regulation it is one of the two models available to banks; the other is a community cloud serving banks only.

Proxy server
A server that mediates between client and destination, used for access control, caching and traffic logging.

Public cloud
A cloud model where resources are shared across customers and delivered over the internet. For regulated workloads in Türkiye its use can be restricted.

R

Replication
Continuously copying data from a source to one or more targets. It is not enough for a replica to be up; you need to measure how far behind it is.

Reseller hosting
A model that lets purchased hosting resources be resold to others.

Router
The device that forwards packets between networks, using its routing table to decide which path each packet takes.

S - Ş

SaaS (Software-as-a-Service)
Software used over the internet with nothing to install. The point most often missed on the data protection side is that most SaaS tools are hosted abroad, which makes using them a cross-border data transfer.

Virtual server
A server with its own operating system running on physical hardware through a hypervisor. It shares resources but runs isolated.

Virtualization
Abstracting physical resources in software and presenting them as several logical ones. It is the basis of server consolidation, and platform choice becomes a live question again whenever a licensing model changes.

SD-WAN
Software-defined management of the wide area network. It uses multiple links together and steers traffic by application priority, which lowers cost and adds flexibility for branch connectivity.

Service desk
The single point of contact for user requests and incident tickets. An issue that keeps coming back

points to an unresolved root cause rather than a support problem.

Cybersecurity
Protecting information systems, networks and data against attack. In Türkiye, organizations covered by Law No. 7545 are already required to provide logs, report vulnerabilities and report incidents without delay.

Penetration testing
Controlled testing of a system's weaknesses using a real attacker's methods. It differs from vulnerability scanning in showing whether what was found is actually exploitable.

Snapshot
A record of a system or volume at a point in time. It is not a substitute for backup: it lives on the same storage, and if that storage is lost the snapshot goes with it.

SSL / TLS
The protocol that encrypts communication over the internet. Although the name SSL persists, what is actually in use today is TLS. Certificate expiry is among the most common causes of outages.

Continuous monitoring
Uninterrupted observation of systems with automatic alerting on threshold breaches. For an alert to be meaningful it has to be tied to impact rather than to a symptom.

Switch
The network device that forwards frames between devices on the same network. Managed models add VLANs, port security and traffic prioritization.

T

Technology
The methods, tools and systems used to get work done.

Time to first byte (TTFB)
The time between a request being sent and the first byte arriving. It is the most direct indicator of server-side latency and it affects the speed metrics that search engines evaluate.

Tokenisation
Replacing sensitive data with a token that carries no meaning of its own. Widely used to protect card data; unlike with encryption, the real value never sits in the system at all.

U - Ü

Upload
Transferring data from a device to a remote system.

Uptime
The proportion of time a system stays available. A percentage alone in a contract is not enough: ask what counts as up, and whether planned maintenance is excluded.

Application management
Managing an application across its whole lifecycle, from deployment to retirement: versions, configuration, performance, access and support.

V

VDS
Virtual dedicated server — running on shared physical hardware but with resources allocated to a single customer.

Data
Raw, unprocessed information. The moment it contains personal data, storing, processing and transferring it require a legal basis.

Data warehouse
A structured store where data from different sources is gathered for analysis. Unlike in a data lake, the schema is applied on load.

Data storage
Holding data persistently. Tiering by access frequency is how performance and cost get managed together rather than traded off.

Data privacy
Protecting personal and sensitive data against unauthorized access and disclosure. Under Turkish data protection law, transfer abroad requires its own legal basis.

Data center
A facility housing server, storage and network hardware with power, cooling and physical security. Dense GPU racks need their power and cooling calculated separately.

Database
A system where data is stored in structured form and can be queried. Relational and non-relational families are designed for different problems; the choice follows the workload.

Database operations services
Database installation, monitoring, backup, tuning and version management delivered as a service. The output to require in the contract is the restore test report.

Efficiency
Producing a given output with as few resources as possible.

Virtual machine (VM)
A software-created equivalent of a physical computer, running its own operating system. Unlike a container, it carries a full OS.

Virtual private cloud (VPC)
A logically isolated network space inside a public cloud. Because the isolation is logical, it may not count as a private cloud for regulated workloads.

Virtualization
Abstracting physical resources and presenting them as logical ones.

VPN
Technology that establishes an encrypted private connection over a public network. It is common for remote access, and audits ask who used it and when.

VPS
Virtual private server — a partition of a physical server with its own operating system and allocated resources.

Y

Simplification
Removing unnecessary steps from a process. It belongs before automation: automating a broken process makes it fast and broken.

Artificial intelligence (AI)
Systems performing tasks normally considered to require human intelligence. In enterprise use the decision turns less on model capability than on where data is processed and what that means for compliance.

Software
The programs and instructions that tell hardware what to do.

Backup
Keeping a separate copy of data against loss or corruption. A backup that ran proves nothing on its own; what counts is a restore that has been tested and documented.

Managed antivirus
Endpoint protection deployment, updates, policy management and incident follow-up delivered as a service.

Managed cloud
Monitoring, management, security and cost tracking of cloud infrastructure taken on by a provider. Using cloud and operating cloud are different jobs.

Managed storage
Operation of storage infrastructure as a service, including capacity planning, performance monitoring, snapshot policy and growth management.

Managed services
Handing the operation of IT infrastructure and systems to a provider under contract. What transfers is the operation; accountability to the regulator stays with the organization.

Managed operating systems
Installation, hardening, patching and version lifecycle of operating systems run as a service.

Managed virtualization
Deployment, resource planning and day-to-day operation of virtual machines and the hypervisor cluster, delivered as a service.

Managed system infrastructure
End-to-end service covering deployment, monitoring, maintenance and incident response across server, storage and network infrastructure.

Managed server
Server configuration, monitoring, patching and security taken on by a provider.

Managed terminal services
Deployment, session management and performance monitoring of remote desktop and terminal server environments, run as a service.

Managed applications
Running the infrastructure side of business applications: environment management, performance, resilience and maintenance window coordination.

Managed web server
Web server configuration, certificate management, security and performance tuning delivered as a service.

Load testing
Measuring how a system behaves under expected and above-expected traffic, so the capacity decision rests on measurement rather than estimate.

Z

Zero trust
A security model in which being inside the network confers no trust. Every access request is re-verified

against identity, device posture and context. The principle is "never trust, always verify."

W

Web
The interlinked documents and applications reached over the internet.

Web 3.0
A vision of the web built on decentralized protocols and user ownership.

Web application firewall (WAF)
A security layer protecting web applications against application-layer attacks. The critical step at deployment is running rules in monitoring mode first to clear false positives; enforcing them immediately can stop production.

X

XaaS (anything-as-a-service)
The umbrella term for delivering any IT capability as a subscription service.

XML
A tag-based format for structuring data in transport and storage, still widespread in enterprise integration.

Q

Queue
A structure where work accumulates to be processed in order. It buffers integrations between systems, and if nobody monitors queue depth, a backlog can grow silently.

R

RPO (recovery point objective)
The maximum acceptable data loss in an outage, measured in time. It sets replication frequency, and it is calculated from business cost rather than from what the technology can do.

RTO (recovery time objective)
How quickly a system must be back after an outage. In most organizations the RTO on paper and the RTO measured in an exercise are different numbers; the measured one is the real one.

S - Ş

SLA (service level agreement)
The contract annex defining the service level a provider commits to. "99.9%" says nothing on its own: ask what counts as up, whether planned maintenance is excluded, and what happens if it is breached.

K

KVKK (Turkish data protection law)
Türkiye's personal data protection law. It ties processing to a legal basis and sets conditions for transfers abroad. For organizations using cloud, the point missed most often is where backups are held.

B

BDDK (Turkish banking regulator)
Türkiye's Banking Regulation and Supervision Agency. For banks, buying cloud services counts as outsourcing, and only a private cloud or a community cloud serving banks alone may be used.

M

MTTR (mean time to repair)
The average time from the start of an incident to its resolution. Not to be confused with response time: opening a ticket is a response, not a resolution.

D

DDoS
A distributed denial-of-service attack, which makes a target unreachable with traffic from many sources. The defense has to be configured before the attack, not during it.

F

Ransomware
Malware that encrypts data and demands payment. What determines recovery is whether the backup was stored where an attacker could not delete it.

I - İ

IaC (infrastructure as code)
Defining and building infrastructure in code rather than by hand. It removes drift between environments and makes a change reviewable before it is applied.