EFSP Auxiliary ESL Curriculum

General IT Jargon Field Guide

Quick reference for high-level ESL learners who need precise IT vocabulary and workplace meeting language

Audience: advanced ESL learners in IT operations, service desk, infrastructure, cloud, endpoint, security, and platform roles

Focus: high-level professional English for general IT teams, including service management, networks, identity, cloud, endpoints, security operations, change control, observability, and realistic workplace dialogue.

Designed for advanced ESL learners who already work in IT or IT-adjacent roles and need field-specific fluency rather than basic technical vocabulary.

Teaching stance: general IT is not one job. Learners need enough shared language to move across help desk, infrastructure, security, cloud, platform, vendor, and business conversations without losing precision or credibility.

How to Use Jargon Well

- Use the term only when it locates the issue more precisely.
- Pair jargon with evidence: log, metric, timestamp, screenshot, ticket, trace, affected user count, or business process.
- Define the term when speaking to non-technical stakeholders.
- Avoid vague IT blame. Name the layer, the owner, the business impact, and the next diagnostic step.

Nomenclature and Jargon

Teach these terms as working vocabulary. Learners should be able to define the term, use it in a realistic sentence, ask one clarification question about it, and explain the business consequence.

Service management

Term	Working meaning
Incident	An unplanned interruption or reduction in service quality that needs restoration.
Service request	A standard user request, such as access, equipment, information, or a routine change.
Problem	An underlying cause or recurring pattern behind one or more incidents.
Change	A planned modification to a service, system, configuration, process, or environment.
SLA	A formal service-level agreement, often with customer or contractual consequences.
SLO	A service-level objective used internally to set reliability targets and guide operations.
MTTR	Mean time to restore or repair; a common measure of operational recovery speed.
Runbook	A documented procedure for responding to known operational situations.

Networking and connectivity

Term	Working meaning
DNS	The system that resolves names such as app.example.com to network addresses.
DHCP	A service that assigns IP addresses and network configuration to clients.
VPN	A protected tunnel that allows remote users or sites to access private resources.
VLAN	A logical network segment used to separate traffic inside a physical network.
Subnet	A range of IP addresses inside a larger network.
Gateway	The route a device uses to reach networks outside its local segment.
Firewall	A control that allows, blocks, or inspects network traffic based on rules.
Load balancer	A component that distributes traffic across multiple backends.

Identity and access

Term	Working meaning
IAM	Identity and access management: systems and policies controlling who can access what.
Authentication	Verifying who a user, service, or device is.

Term	Working meaning
Authorization	Determining what the verified identity is allowed to do.
SSO	Single sign-on: one identity session used across multiple applications.
MFA	Multifactor authentication: two or more proof factors for identity verification.
RBAC	Role-based access control: permissions assigned by role rather than one by one.
Least privilege	Giving only the access required for the job, for only as long as needed.
Service account	A non-human identity used by applications, jobs, or integrations.

Cloud and infrastructure

Term	Working meaning
VM	Virtual machine: a software-defined server running on shared physical infrastructure.
Container	A packaged application unit with dependencies and runtime isolation.
IaC	Infrastructure as code: infrastructure managed through versioned configuration files.
Region	A cloud provider geographic area containing multiple data-center locations.
Availability zone	A separated location inside a region, used for resilience planning.
Autoscaling	Automatically adding or removing capacity based on demand or policy.
Snapshot	A point-in-time copy of a disk, volume, database, or system state.
Tagging	Applying metadata labels to resources for ownership, cost, automation, or policy.

Endpoint and server operations

Term	Working meaning
Asset inventory	A current list of hardware, software, owners, versions, and risk-relevant details.
MDM	Mobile device management for enforcing policies on laptops, phones, and tablets.
EDR	Endpoint detection and response tooling for monitoring and responding to endpoint threats.
Baseline	An approved standard configuration for a system or device type.
Configuration drift	When systems gradually differ from the approved baseline.
Patch	A software update that fixes a bug, vulnerability, or compatibility issue.
Maintenance window	An approved time period for work that may affect users or services.
Rollback	A planned return to the previous working state after a failed change.

Security operations

Term	Working meaning
Vulnerability	A weakness that could be accidentally triggered or intentionally exploited.
Exploit	A method or action that takes advantage of a vulnerability.
CVE	A public identifier for a known cybersecurity vulnerability.
SIEM	Security information and event management: collects and analyzes security-relevant events.

Term	Working meaning
IDS/IPS	Intrusion detection/prevention systems that detect or block suspicious network activity.
Phishing	A social-engineering attempt to trick a user into revealing information or taking action.
Zero Trust	A security approach that avoids implicit trust and emphasizes verification and least privilege.
Audit log	A record of relevant system, user, or administrative actions.

Observability and reliability

Term	Working meaning
Log	A record of events or messages from an application, system, or device.
Metric	A numerical measurement tracked over time, such as latency or error rate.
Trace	A view of a request path across services and dependencies.
Alert	A notification triggered when a condition may require human attention.
Latency	How long a request takes to complete.
Throughput	How much work a system handles over a period of time.
Saturation	How close a resource is to its limit, such as CPU, memory, disk, or connection pool.
Error budget	The acceptable amount of unreliability implied by an SLO over a period of time.

Backup, recovery, and continuity

Term	Working meaning
Backup	A copy of data or system state kept for recovery after deletion, corruption, or failure.
Restore	The process of recovering data or service from a backup or snapshot.
Replication	Maintaining copies of data or systems in another location or environment.
Retention	How long backups, logs, or records are kept before deletion.
RPO	Recovery point objective: the maximum acceptable data loss measured in time.
RTO	Recovery time objective: the maximum acceptable restoration time.
DR	Disaster recovery: plans and systems for recovering after major disruption.
Failover	Moving traffic or service to a standby system when the primary fails.

Common Meeting Moves

Triage and scope

- Can we separate user impact from component health?
- How many users, which locations, and which business process are affected?
- What changed recently: deployment, configuration, certificate, DNS, firewall, identity policy, or vendor status?
- Do we have logs, timestamps, screenshots, error messages, and a reproducible path?

Cautious root-cause language

- Current evidence points to DNS, but we have not confirmed root cause yet.
- This appears to be a configuration issue rather than a platform outage.
- We have restored service; the contributing factors are still under review.
- I would avoid saying 'breach' until security confirms unauthorized access or data exposure.

Pushback and risk

- I understand the urgency, but broad admin access is not the right control.
- The shortcut reduces delivery risk today but increases security and audit risk.
- Can we approve a time-limited exception with monitoring and an expiration date?
- Before we make this change, we need a rollback plan and a communication owner.

Incident bridge language

- The immediate goal is service restoration; root-cause analysis comes after stabilization.
- The mitigation is in progress, and the next checkpoint is in 15 minutes.
- We need one owner for customer communication and one owner for technical recovery.
- Please post only confirmed facts in the incident channel; hypotheses should be labeled as hypotheses.

Security and identity

- Authentication succeeded, but authorization failed because the user lacks the required role.
- Least privilege protects the user, the system, and the audit trail.
- We should revoke sessions, reset credentials, and review sign-in logs before closing the incident.
- A vulnerability is confirmed, but we do not yet have evidence of exploitation.

Business-facing explanations

- RTO is how long recovery takes; RPO is how much data loss the business can tolerate.
- The application is healthy, but users cannot reach it because name resolution is inconsistent.
- The cost increase is mostly idle compute and longer log retention, not user growth.
- The change is technically simple, but the blast radius is large if it fails.

Fast Contrast Pairs

Do not confuse	Working contrast
Incident vs problem	An incident restores service; problem management investigates underlying cause or recurrence.
Severity vs priority	Severity describes impact; priority combines impact, urgency, deadline, and business context.
Authentication vs authorization	Authentication verifies identity; authorization determines allowed actions.
Vulnerability vs exploit	A vulnerability is a weakness; an exploit is a way to use that weakness.
Alert vs incident	An alert signals possible attention; an incident is confirmed service, security, or business impact requiring response.
RTO vs RPO	RTO is acceptable recovery time; RPO is acceptable data loss measured in time.
Rollback vs roll forward	Rollback returns to the previous known state; roll forward fixes by moving to a newer corrected state.

Do not confuse	Working contrast
Logs vs metrics vs traces	Logs are event records; metrics are measurements; traces follow a request across systems.

Source Orientation

- NIST Computer Security Resource Center Glossary and Cybersecurity Framework terminology.
- AWS Well-Architected Framework pillars: operational excellence, security, reliability, performance efficiency, cost optimization, and sustainability.
- Microsoft Learn Zero Trust and Microsoft Entra identity/access management guidance.
- Kubernetes documentation for Pods, Deployments, Services, Ingress, and container orchestration concepts.
- Google Site Reliability Engineering book chapters on SLOs, error budgets, incident response, and reliability tradeoffs.
- PeopleCert ITIL 4 practice areas for incident management, change enablement, service request management, and problem management.