EFSP Auxiliary ESL Curriculum

General IT English

Instructor guide for high-level ESL learners working in IT operations, service management, infrastructure, cloud, security, and support

Audience: instructors, coaches, technical English trainers, IT learning partners, and team leads

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.

Purpose and Teaching Position

This EFSP curriculum is for high-level ESL learners working in general IT: service desk specialists, system administrators, network technicians, endpoint engineers, cloud operations staff, security analysts, technical support leads, IT managers, and IT-adjacent project or business partners.

The course is not a beginner computer class. It assumes learners know the work but need more precise English for live troubleshooting, escalations, risk discussions, documentation, post-incident reviews, vendor conversations, and cross-functional meetings.

Core language challenge

General IT English is full of compressed phrases: P1 bridge, DNS propagation, least privilege, conditional access, rollback plan, open a vendor severity case, noisy alert, RTO miss, firewall exception, and error-budget burn. Learners need to understand the words, but more importantly they need the workplace moves around the words: clarify, narrow scope, ask for evidence, protect users, state risk, and recommend a next step.

Course objectives

- Use general IT terminology accurately in tickets, incident calls, change reviews, access discussions, vendor meetings, and executive updates.
- Triage ambiguous technical problems by asking about scope, impact, timeline, evidence, dependencies, and recent changes.
- Explain infrastructure, identity, networking, endpoint, cloud, security, and operations issues in concise professional English.
- Push back on risky shortcuts using business impact, operational evidence, security principles, and customer-facing consequences.
- Participate in realistic IT dialogues: outage bridges, service desk escalations, access reviews, patch windows, cloud cost reviews, and post-incident reviews.
- Write clear workplace outputs: ticket updates, change summaries, risk statements, incident notes, root-cause language, and action items.

General IT Communication Principles

Translate symptoms into evidence

Users naturally describe pain, not architecture. 'The internet is down' may mean a browser issue, Wi-Fi issue, DNS issue, proxy issue, SaaS outage, identity failure, expired certificate, or local device problem. Strong IT English respects the user experience while converting the report into testable evidence.

Separate restoration from investigation

- During an incident, say what is affected, what is being mitigated, who owns the next action, and when the next update will arrive.
- After restoration, discuss root cause, contributing factors, detection gaps, process gaps, and durable corrective actions.
- Do not use final root-cause language while the team is still working from hypotheses.
- Use exact uncertainty: 'we have not seen evidence of data loss' is stronger and safer than 'there is no data loss' when logs are incomplete.

Use decision-grade risk language

Weak sentence	Decision-grade IT sentence
It is risky.	The risk is broad network exposure from an unrestricted source range; mitigation would require a narrower rule, monitoring, and an expiration date.
The patch can wait.	The patch can wait only if we apply compensating controls, document risk acceptance, and schedule production within the agreed window.
The cloud bill is too high.	Compute in non-production increased 42 percent, and untagged resources prevent owner accountability; we can stop idle instances today and enforce tags this sprint.
The user needs access.	The user needs read-only access to customer reports until Friday, approved by the data owner and removed automatically after the review.

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.
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.

Term	Working meaning
CVE	A public identifier for a known cybersecurity vulnerability.
SIEM	Security information and event management: collects and analyzes security-relevant events.
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.

Instructor Module Plans

Module 1. IT Service Language, Tickets, and Triage (90 minutes)

General IT work often starts with incomplete reports: 'VPN is broken,' 'the app is slow,' or 'users cannot log in.' Strong IT English turns vague pain into scope, impact, evidence, priority, and next action.

Learning objectives

- Distinguish incident, service request, problem, change, task, and known error.
- Ask triage questions about impact, urgency, affected users, timeline, and recent changes.
- Write ticket updates that are useful to both technical teams and business stakeholders.

Core concepts

- Severity vs priority: severity describes technical or business impact; priority also includes urgency, customer importance, deadlines, and risk.
- SLA vs SLO: an SLA is usually a formal commitment; an SLO is an internal reliability target used to guide operations.
- Escalation: moving work to a higher skill group, manager, vendor, or incident process because risk, time, or authority requires it.

Activities

1. Ticket surgery: learners rewrite vague tickets with observed behavior, expected behavior, scope, evidence, and next owner.
2. Triage interview: learners question a frustrated user without sounding robotic or dismissive.
3. Priority debate: learners assign severity and priority to five incidents, then defend their reasoning.

Learner outputs

- Ticket update template.
- Triage question bank.
- Severity/priority explanation script.

> **Facilitator note**
>
> When learners say a system is down, slow, broken, unsafe, or fixed, ask for scope, evidence, timestamp, business impact, owner, and confidence level. The goal is not more English; it is more operational usefulness.

Module 2. Networks, Connectivity, and Root-Cause Hypotheses (90 minutes)

Network conversations require careful hypothesis language. DNS, DHCP, VPN, routing, firewall rules, certificates, proxies, and load balancers can create similar user symptoms.

Learning objectives

- Explain common network components and failure modes in workplace English.
- Separate user-side, device-side, network-side, and application-side evidence.
- Use cautious root-cause language before proof is available.

Core concepts

- DNS resolution, IP addressing, DHCP lease, subnet, gateway, VPN tunnel, VLAN, firewall rule, proxy, TLS certificate, and load balancer.
- Packet path thinking: client, local network, VPN, firewall, DNS, load balancer, application server, database, and external dependency.
- Symptom does not equal root cause. 'Cannot reach the app' may be identity, DNS, network, server, certificate, or browser cache.

Activities

1. Path map: learners draw the connection path for a remote user accessing an internal HR system.
2. Hypothesis ladder: learners rank possible causes from most likely to least likely using evidence.
3. Network-status update: learners explain a connectivity issue without overclaiming root cause.

Learner outputs

- Connectivity triage map.

- Network hypothesis language list.

Facilitator note

When learners say a system is down, slow, broken, unsafe, or fixed, ask for scope, evidence, timestamp, business impact, owner, and confidence level. The goal is not more English; it is more operational usefulness.

Module 3. Identity, Access, and Permissions (90 minutes)

Access requests are rarely just technical. They involve identity proof, authorization, least privilege, auditability, urgency, and sometimes uncomfortable pushback to senior people.

Learning objectives

- Distinguish authentication, authorization, SSO, MFA, RBAC, groups, roles, and service accounts.
- Explain least privilege and conditional access without sounding obstructive.
- Handle urgent access requests with controls, time limits, approvals, and audit trails.

Core concepts

- Authentication verifies identity; authorization determines what that identity can access.
- Joiner/mover/leaver process: access changes when people join, change roles, or leave.
- Privilege creep: users accumulate access over time unless roles are reviewed and removed.

Activities

1. Access review: learners identify excessive permissions and propose removals in diplomatic language.
2. Urgent exception role-play: a director wants admin access immediately before a deadline.
3. IAM explainer: learners explain MFA fatigue, conditional access, and service accounts to non-specialists.

Learner outputs

- Access approval question set.
- Least-privilege pushback script.

Facilitator note

When learners say a system is down, slow, broken, unsafe, or fixed, ask for scope, evidence, timestamp, business impact, owner, and confidence level. The goal is not more English; it is more operational usefulness.

Module 4. Cloud, Infrastructure, and Cost-Aware Operations (90 minutes)

Cloud IT conversations combine architecture, operations, cost, security, and ownership. Learners need to discuss tradeoffs without treating cloud as unlimited or invisible.

Learning objectives

- Use terms such as region, availability zone, VPC, subnet, VM, storage, snapshot, autoscaling, IaC, tagging, and shared responsibility.
- Explain reliability, performance, security, sustainability, and cost tradeoffs.
- Discuss unexpected cloud spend with evidence and practical mitigation options.

Core concepts

- Shared responsibility: cloud providers and customers each own different parts of security and operations.
- Infrastructure as code: infrastructure defined and changed through versioned configuration rather than only manual clicks.
- Cost drivers: compute size, idle resources, storage retention, data transfer, logs, backups, and over-provisioning.

Activities

1. Architecture walkthrough: learners explain a small cloud workload to a finance manager.
2. Cost spike meeting: learners identify possible causes and propose immediate and structural fixes.
3. Risk tradeoff: learners compare manual changes, IaC, rollback plans, and approval gates.

Learner outputs

- Cloud architecture explanation.
- Cost-spike summary email.

Facilitator note

When learners say a system is down, slow, broken, unsafe, or fixed, ask for scope, evidence, timestamp, business impact, owner, and confidence level. The goal is not more English; it is more operational usefulness.

Module 5. Endpoints, Servers, Patching, and Configuration Management (90 minutes)

Endpoint and server operations require clear language about assets, baselines, patches, compatibility, exceptions, maintenance windows, rollback, and user disruption.

Learning objectives

- Discuss patching and configuration risk with technical and business audiences.
- Explain asset inventory, MDM, EDR, encryption, baseline configuration, and policy compliance.
- Negotiate maintenance windows and exception requests.

Core concepts

- Patch management: identifying, testing, deploying, and verifying updates for vulnerabilities, bugs, and stability.
- Configuration drift: systems gradually differ from the approved baseline.
- Rollback plan: a prepared way to return to the previous working state if a change fails.

Activities

1. Patch window negotiation: learners balance security risk, downtime, and business deadlines.
2. Exception review: learners decide whether a legacy system can remain unpatched and under what controls.
3. Baseline explanation: learners explain why configuration standards matter to a skeptical team.

Learner outputs

- Patch communication template.
- Exception risk statement.

Facilitator note

When learners say a system is down, slow, broken, unsafe, or fixed, ask for scope, evidence, timestamp, business impact, owner, and confidence level. The goal is not more English; it is more operational usefulness.

Module 6. Security Operations, Risk, and Incident Response (90 minutes)

Security conversations require precision and restraint. Vulnerability, exploit, alert, event, incident, risk, compromise, and breach are not interchangeable words.

Learning objectives

- Use security operations vocabulary accurately in alerts, tickets, escalations, and briefings.
- Explain risk using likelihood, impact, exposure, compensating controls, and evidence.

- Participate in incident response without creating panic or hiding uncertainty.

Core concepts

- Event vs alert vs incident: not every log event is an alert, and not every alert is a confirmed incident.
- Vulnerability vs exploit: a weakness is not the same as active use of that weakness by an attacker.
- Zero Trust principles often emphasize explicit verification, least privilege, and assuming compromise is possible.

Activities

1. Alert triage: learners decide what evidence would move an alert to an incident.
2. Phishing response: learners guide a user, preserve evidence, and escalate if needed.
3. Risk statement rewrite: learners convert dramatic security language into decision-grade language.

Learner outputs

- Security escalation script.
- Risk language checklist.

Facilitator note

When learners say a system is down, slow, broken, unsafe, or fixed, ask for scope, evidence, timestamp, business impact, owner, and confidence level. The goal is not more English; it is more operational usefulness.

Module 7. Change, Release, Problem, and Post-Incident Communication (90 minutes)

Mature IT teams separate fixing the current outage from understanding recurring causes. Learners need language for change records, CAB review, maintenance windows, rollback, problem management, root cause, and action items.

Learning objectives

- Discuss normal, standard, emergency, and high-risk changes.
- Explain root cause, contributing factors, detection gaps, and corrective actions without blame.
- Write action items that have owners, due dates, and verification criteria.

Core concepts

- Change enablement reduces risk by making intent, impact, testing, implementation, rollback, and communications visible.
- Problem management looks for underlying causes and recurring patterns, not only immediate restoration.
- Post-incident reviews should improve systems, monitoring, process, and communication rather than punish individuals.

Activities

1. CAB simulation: learners present a risky firewall change and answer objections.
2. Postmortem rewrite: learners remove blame and add evidence, contributing factors, and follow-up actions.
3. Emergency change debrief: learners explain why process was shortened and how risk was controlled.

Learner outputs

- Change review script.
- Post-incident action-item table.

Facilitator note

When learners say a system is down, slow, broken, unsafe, or fixed, ask for scope, evidence, timestamp, business impact, owner, and confidence level. The goal is not more English; it is more operational usefulness.

Module 8. Platform, DevOps, Observability, and Kubernetes Conversations (90 minutes)

Even general IT staff increasingly discuss CI/CD, containers, Kubernetes, logs, metrics, traces, SLOs, and automation. Learners need enough language to participate without pretending to be specialists.

Learning objectives

- Explain containers, images, registries, pods, deployments, services, ingress, and rollout behavior.
- Use observability terms: logs, metrics, traces, dashboards, alerts, latency, throughput, saturation, and error budget.
- Connect platform symptoms to business impact and incident decisions.

Core concepts

- Containers package an application and dependencies; Kubernetes orchestrates containers across a cluster using resources such as Pods, Deployments, Services, and Ingress.
- Observability helps teams understand what is happening from system outputs: logs, metrics, traces, and events.
- Automation reduces repeat work but also requires review, version control, rollback, and monitoring.

Activities

1. Kubernetes incident: learners explain crashing pods, failed readiness checks, and rollback options.
2. Dashboard readout: learners turn metrics into a spoken incident update.
3. Automation review: learners identify where a script or pipeline needs approval, logging, or safeguards.

Learner outputs

- Platform incident update.
- Observability phrase bank.

> **Facilitator note**
>
> When learners say a system is down, slow, broken, unsafe, or fixed, ask for scope, evidence, timestamp, business impact, owner, and confidence level. The goal is not more English; it is more operational usefulness.

Assessment and Coaching

Pre-course diagnostic

- Learner explains their current IT role in 90 seconds, including users supported, systems owned, common incidents, and escalation paths.
- Learner defines twelve common IT terms and uses six in realistic workplace sentences.
- Learner handles a short role-play: a business stakeholder asks whether an outage is fixed and whether data was lost.

Performance rubric

Skill	Developing	Proficient	Strong
Terminology	Recognizes terms but uses them loosely.	Uses common terms accurately in context.	Defines terms, notices misuse, and adjusts for audience.
Triage	Collects symptoms but misses scope or impact.	Asks about impact, timeline, evidence, and recent changes.	Builds hypotheses and assigns next owners clearly.
Risk language	Uses vague risk words or alarmist language.	Names likelihood, impact, exposure, and mitigation.	Frames risk as a decision with controls and owner accountability.
Incident communication	Gives long technical explanations during pressure.	Reports impact, mitigation, owner, and next update.	Controls bridge language and separates facts from hypotheses.

Skill	Developing	Proficient	Strong
Documentation	Writes updates that are hard to act on.	Writes clear ticket and change notes.	Writes concise operational records usable for review and audit.

Capstone simulation

Learners lead a 25-minute incident and recovery scenario. A SaaS login problem affects a regional sales team, the vendor status page is ambiguous, some users report MFA loops, and a senior stakeholder asks for a workaround that may weaken security. The learner must triage scope, communicate impact, propose mitigations, push back on unsafe shortcuts, and write a final incident summary.

Source orientation for instructors

- 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.