EFSP Auxiliary ESL Curriculum

General IT English

Participant workbook: service language, infrastructure discussion, security risk, incident updates, and IT workplace practice

Audience: advanced ESL learners working in IT operations, support, infrastructure, cloud, security, or adjacent 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 This Workbook

This workbook helps you sound precise and credible in general IT conversations. The goal is not to use more jargon. The goal is to use the right term, ask better questions, explain risk calmly, and write updates that help people act.

Your starting point

- Which conversations are hardest for you: user calls, incident bridges, access reviews, change meetings, security escalations, vendor calls, or executive updates?
- Which IT terms do you understand when reading but avoid when speaking?
- When someone pressures you for a risky shortcut, do you become too indirect, too blunt, or too technical?
- What is one recent ticket or incident you wish you had explained more clearly?

IT Stack Language

Layer	Useful verbs	Example sentence
User/device	report, reproduce, capture, reset, verify	The user can reproduce the issue only on the managed laptop.
Network	resolve, route, block, allow, tunnel, inspect	DNS resolves to the old address for some remote users.
Identity	authenticate, authorize, grant, revoke, audit	Authentication succeeded, but authorization failed because the user lacks the role.
Server/cloud	provision, scale, patch, snapshot, restore	The instance scaled up, but the storage volume is near saturation.
Application	deploy, roll back, validate, monitor, log	The application is healthy, but the load balancer health check is failing.
Security	detect, contain, investigate, remediate, report	We contained the account compromise and are reviewing sign-in logs.

Practice Pages

Module 1. IT Service Language, Tickets, and Triage

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.

What you should be able to do

- 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.

Practice task

Situation

A user reports, 'Everything is down.' Rewrite the ticket with scope, impact, evidence, affected business process, and next owner.

Clarification questions

Evidence and impact

Final professional response

Module 2. Networks, Connectivity, and Root-Cause Hypotheses

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

What you should be able to do

- 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.

Practice task

Situation

A remote user can connect to VPN but cannot reach one internal app. Write five triage questions and three likely hypotheses.

Clarification questions

Evidence and impact

Final professional response

Module 3. Identity, Access, and Permissions

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

What you should be able to do

- 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.

Practice task

Situation

A senior employee wants broad access to a financial database for one afternoon. Write a least-privilege response that still helps them finish the work.

Clarification questions

Evidence and impact

Final professional response

Module 4. Cloud, Infrastructure, and Cost-Aware Operations

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

What you should be able to do

- 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.

Practice task

Situation

Cloud spend increases sharply after a new analytics environment launches. Prepare a short update with evidence, immediate actions, and longer-term controls.

Clarification questions

Evidence and impact

Final professional response

Module 5. Endpoints, Servers, Patching, and Configuration Management

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

What you should be able to do

- 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.

Practice task

Situation

Security wants an urgent patch, but the business owner rejects downtime. Write a compromise plan with risk language and decision points.

Clarification questions

Evidence and impact

Final professional response

Module 6. Security Operations, Risk, and Incident Response

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

What you should be able to do

- 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.

Practice task

Situation

A phishing victim reports quickly. Write your first five sentences to the user and your first technical update to security.

Clarification questions

Evidence and impact

Final professional response

Module 7. Change, Release, Problem, and Post-Incident Communication

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.

What you should be able to do

- 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.

Practice task

Situation

A firewall change is requested with vague source and destination information. Write clarification questions and a risk statement.

Clarification questions

Evidence and impact

Final professional response

Module 8. Platform, DevOps, Observability, and Kubernetes Conversations

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.

What you should be able to do

- 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.

Practice task

Situation

A restore test meets the RTO but misses the RPO. Explain the problem to a non-technical business owner and recommend next steps.

Clarification questions

Evidence and impact

Final professional response

Phrase Bank

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.

Personal Action Plan

Situation	Term or phrase I will practice	Evidence I used it well