EFSP Auxiliary ESL Curriculum

Cybersecurity English Participant Workbook

Practice pages for realistic field-specific meetings, pushback, documentation, and role-play preparation

Audience: security analysts, SOC staff, incident responders, security engineers, GRC specialists, identity teams, vulnerability managers, and security leaders

Focus: A cybersecurity English curriculum for incident response, vulnerability triage, identity, threat modeling, risk communication, compliance, executive briefings, and security pushback.

Designed for advanced ESL learners who already use professional English and need industry-specific terminology, realistic meetings, role-play pressure, careful pushback, and polished workplace outputs.

Teaching stance: this is language and workplace-communication training, not legal, medical, financial, safety, or regulatory advice. Instructors should connect every scenario to the learner's current company policies, local rules, and approved procedures.

How to Use This Workbook

For each module, define the terms, identify the decision pressure, write a careful response, and practice the conversation aloud. Strong answers are specific, calm, evidence-aware, and tied to owner and next step.

Module 1. Security Triage and Alert Investigation

Situation

The SOC receives repeated alerts from a privileged account.

Stakeholder pressure: Close them as false positives because the user is senior.

Constraint: Privilege, behavior, context, and evidence need review.

Terms to use

- SIEM
- alert
- false positive
- privileged account

Evidence, owner, or policy boundary

Pushback sentence

Draft the alert triage note

Module 2. Incident Response and Containment

Situation

A ransomware note appears on a shared server.

Stakeholder pressure: Tell everyone the company is breached.

Constraint: Scope, containment, evidence preservation, communications, and legal review matter.

Terms to use

- incident
- containment
- ransomware
- forensics

Evidence, owner, or policy boundary

Pushback sentence

Draft the incident bridge update

Module 3. Vulnerability Management

Situation

A critical CVE affects an internet-facing system.

Stakeholder pressure: Patch every system immediately.

Constraint: Exploitability, exposure, asset criticality, compensating controls, and downtime must be balanced.

Terms to use

- CVE
- CVSS
- exploitability

- compensating control

Evidence, owner, or policy boundary

Pushback sentence

Draft the vulnerability prioritization memo

Module 4. Identity, Access, and Least Privilege

Situation

A contractor asks for admin rights to troubleshoot faster.

Stakeholder pressure: Grant temporary admin access.

Constraint: Least privilege, approval, logging, and time-bound access are required.

Terms to use

- IAM
- least privilege
- MFA
- RBAC

Evidence, owner, or policy boundary

Pushback sentence

Draft the access request response

Module 5. Threat Modeling and Secure Design

Situation

A product team wants to skip threat modeling to meet a launch date.

Stakeholder pressure: Do a quick review after launch.

Constraint: Abuse cases, data flows, trust boundaries, and mitigations need design-time attention.

Terms to use

- threat model
- attack surface
- trust boundary
- abuse case

Evidence, owner, or policy boundary

Pushback sentence

Draft the threat model findings

Module 6. Governance, Risk, and Compliance

Situation

Audit finds incomplete access reviews.

Stakeholder pressure: Say the control is mostly working.

Constraint: Control design, evidence, ownership, remediation, and risk acceptance need clarity.

Terms to use

- control
- audit evidence
- risk acceptance
- remediation

Evidence, owner, or policy boundary

Pushback sentence

Draft the GRC remediation plan

Module 7. Security Awareness and Phishing

Situation

An executive clicks a phishing simulation link.

Stakeholder pressure: Send a public warning.

Constraint: Behavior, training, reporting culture, and technical controls all matter.

Terms to use

- phishing
- social engineering

- reporting culture
- security awareness

Evidence, owner, or policy boundary

Pushback sentence

Draft the awareness coaching script

Module 8. Executive Risk Briefings

Situation

The board asks whether the organization is safe from attacks.

Stakeholder pressure: Give a yes-or-no answer.

Constraint: Residual risk, threat landscape, controls, investment, and response readiness require nuance.

Terms to use

- residual risk
- threat actor
- maturity
- investment ask

Evidence, owner, or policy boundary

Pushback sentence

Draft the board cyber-risk update

Capstone Simulation

Lead a cross-functional meeting in cybersecurity. Choose four modules from this workbook, connect the risks, and prepare a five-minute update with decision, evidence, constraint, owner, and next step.